



Citrix Workspace-App für Mac

Contents

| | |
|--|------------|
| Info zu diesem Release | 3 |
| Features in Technical Previews | 94 |
| Native Unterstützung für Mac mit Apple Silicon (M1- und M2-Serie) | 113 |
| Systemanforderungen und Kompatibilität | 116 |
| Installieren, Deinstallieren und Aktualisieren | 122 |
| Aktualisieren | 125 |
| Konfigurieren | 135 |
| Mobilgeräteverwaltung | 208 |
| Authentifizieren | 215 |
| Sichere Kommunikation | 219 |

Info zu diesem Release

December 18, 2023

Erfahren Sie mehr über neue Features, Verbesserungen sowie behobene und bekannte Probleme in der Citrix Workspace-App für Mac.

Im Abschnitt [Features in Technical Previews](#) finden Sie eine aktualisierte Liste der Features in Technical Previews. Erkunden Sie die Technical Preview-Features und teilen Sie uns Ihr Feedback mit dem Podio-Formular mit.

Hinweis:

Der automatische Updatedienst wird ab Version 2304 unterstützt. Wenn Sie Version 2301 (oder früher) der Citrix Workspace-App für Mac verwenden, können Sie den automatischen Updatedienst nicht zur Installation der neuesten Versionen verwenden. Stattdessen müssen Sie manuell die Citrix Workspace-App für Mac Version 2304 oder höher installieren, indem Sie die DMG-Datei herunterladen, die auf der Seite [Downloads](#) verfügbar ist. Weitere Informationen finden Sie unter [Manuelle Installation](#).

Native Unterstützung für Mac mit Apple Silicon (M1 und M2 Series) Universal Architecture

Mit dem Release des Universal Architecture-Builds bietet die Citrix Workspace-App jetzt native Unterstützung für Macs mit Apple Silicon (M1- und M2-Serie). Der Universal Architecture-Build kann auf jedem Mac-Gerät ausgeführt werden, unabhängig von der Prozessorarchitektur.

Wenn Sie den x86_64 Intel-basierten Architekturbuild der Citrix Workspace-App für Macs mit Apple Silicon verwenden, müssen Sie die Rosetta-Emulation zum Ausführen der App verwenden.

Sie finden die neueste Version von Universal Architecture-Build und x86_64 Intel-basiertem Architekturbuild unter [Downloads](#).

Hinweis:

Citrix unterstützt weiterhin Intel-basierte Macs und Macs mit Apple Silicon (M1- und M2-Serie). Der x86_64 Intel-basierte Architekturbuild für Intel-basierte Macs wird jedoch in Kürze als veraltet eingestuft. Citrix unterstützt weiterhin den Universal Architecture Build für Intel-basierte Macs und für Macs mit Apple Silicon (M1- und M2-Serie). Die Ankündigung wird im Abschnitt [Einstellung von Features und Plattformen](#) erfolgen.

Wenn Sie die Citrix Workspace-App auf einem Mac mit Apple Silicon (M1 und M2 Series) verwenden, müssen Sie das HDX RealTime Optimization Pack (RTOP) aktualisieren. Durch dieses Upgrade wird sichergestellt, dass Audio-/Videokonferenzen und Enterprise VoIP-Unternehmenstelefonie über Mi-

Microsoft Skype for Business optimiert werden. Sie können HDX RealTime Media Engine 2.9.500 für Mac von der Citrix Website unter [Downloads](#) herunterladen und installieren.

Wenn Sie Plug-Ins von Drittanbietern oder virtuelle Kanäle verwenden, müssen diese mit Apple Silicon-Macs kompatibel sein. Wenn die Plug-Ins intern entwickelt wurden, müssen Sie sie neu erstellen, bevor Sie den Universal Architecture Build installieren.

Weitere Informationen, etwa zur Deinstallation des Universal Architecture Build oder zur Verwendung des Custom Virtual Channel SDK (VCSDK), finden Sie unter [Native Unterstützung für Apple Silicon](#).

Was ist neu in 2309

Unterstützung für macOS 14 Sonoma

Die Citrix Workspace-App für Mac wird unter macOS 14 Sonoma unterstützt.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 115.1.1.103, der auf Chromium Version 115 basiert. Weitere Informationen finden Sie in der [Dokumentation zu Citrix Enterprise Browser](#).

Citrix veröffentlicht ab jetzt unabhängige Upgrades für Citrix Enterprise Browser. Ab der Citrix Workspace-App 2309 für Mac können Sie Citrix Enterprise Browser unabhängig auf eine kompatible Version aktualisieren, sobald Upgrades unter [Downloads](#) verfügbar sind. Die Aktualisierung kann manuell oder über den automatischen Updatedienst erfolgen. Unabhängige Upgrades von Citrix Enterprise Browser werden stets nur für die jeweils neueste Version der Citrix Workspace-App für Mac unterstützt.

Technical Preview

- Unterstützung für Citrix Secure Private Access für On-Premises-Stores

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme in 2309

- In optimiertem Microsoft Teams hören Sie den Klingelton möglicherweise zufällig, wenn Sie einen Anruf vor dem Klingeln annehmen. [HDX-55799]
- Die **USB**-Einstellungen zum automatischen Verbinden von Geräten, die im Fenster **Einstellungen** auf der Registerkarte **Geräte** verfügbar sind, funktionieren in der Citrix Workspace-App 2308 für Mac möglicherweise nicht wie erwartet. [RFMAC-14658]

- Wenn Sie auf Geräten mit macOS Sonoma ein Bild im JPEG/PNG-Format vom Mac in die virtuelle Sitzung kopieren, ist das kopierte Bild in der virtuellen Sitzung möglicherweise beschädigt. [HDX-55307]

Bekannte Probleme in 2309

- In diesem Release wurden keine neuen Probleme festgestellt.

Frühere Releases

In diesem Abschnitt werden Features in früheren Releases zusammen mit behobenen und bekannten Problemen aufgeführt. Releases erreichen 18 Monate nach Veröffentlichung das Ende des Lebenszyklus (EOL). Einzelheiten zu den Lebenszyklusdaten für die unterstützten Versionen finden Sie unter [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

2308

Was ist neu

Citrix Workspace-App für Mac unter macOS Sonoma Beta

Die Citrix Workspace-App 2308 für Mac wurde unter macOS Sonoma Public Beta 7 Version 23A5337a getestet. Verwenden Sie dieses Setup in einer Testumgebung und geben Sie uns [Feedback](#).

Verbesserte Grafikleistung

Ab Version 2308 bieten Seamless-App-Sitzungen eine bessere Grafikleistung. Dieses Feature optimiert auch die CPU-Auslastung.

Verbesserte Kontrolle von Netzwerküberlastungen

Ab Version 2308 wurde das von Citrix entwickelte Transportprotokoll EDT (Enlightened Data Transport) verbessert, um Netzwerküberlastungen effizient zu kontrollieren. Dieses Feature verbessert den Datendurchsatz und reduziert die Latenz.

Erhöhung der Anzahl der unterstützten virtuellen Kanäle

Bisher unterstützte die Citrix Workspace-App für Mac bis zu 32 virtuelle Kanäle. Ab Version 2308 können Sie bis zu 64 virtuelle Kanäle in einer Sitzung nutzen.

App Protection

Unterstützung der Erkennung von Richtlinienmanipulationen

Das Feature zur Erkennung von Richtlinienmanipulationen verhindert den Benutzerzugriff auf eine virtuelle App- oder Desktopsitzung, wenn die Richtlinien zu Screenshotschutz und Keyloggingschutz in App Protection manipuliert wurden. Wenn eine Richtlinienmanipulation festgestellt wurde, wird die virtuelle App- oder Desktopsitzung beendet. Weitere Informationen zur Erkennung von Richtlinienmanipulationen finden Sie unter [Erkennung von Richtlinienmanipulationen](#).

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 115.1.1.103, der auf Chromium Version 115 basiert. Weitere Informationen finden Sie in der [Dokumentation zu Citrix Enterprise Browser](#).

Technical Preview

- Option “Hoher DPI-Wert” verbessert
- Storebasierte Konfiguration des Dateizugriffs
- Unterstützung für Aktivitätsmanager in Cloudstores
- Unterstützung der Bildschirmfreigabe bei aktiviertem App Protection
- Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit On-Premises-Stores

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Beim Zugriff auf einen virtuellen Desktop über die Citrix Workspace-App für Mac kann die Größe des Mauszeigers auf dem virtuellen Desktop schwanken. [CVADHELP-23158]
- Die Symbole aktiver Apps werden möglicherweise nicht im Aktivitätsmanager angezeigt. [WSUI-8011]
- Die Citrix Workspace-App verbraucht möglicherweise nach einigen Minuten viel Anwendungsspeicher. [CVADHELP-23528]

Bekannte Probleme

- Nach dem Upgrade der Citrix Workspace-App für Mac auf Version 2308 reagiert das Einstellungsfenster möglicherweise nicht mehr auf Benutzeraktionen. Erzwingen Sie das Beenden der Citrix Workspace-App als Workaround und starten Sie sie neu. Weitere Informationen zum erzwungenen Beenden einer App auf einem Mac finden Sie im [zugehörigen Apple-Supportartikel](#). [RF-MAC-14596]

2307

Was ist neu

Native Unterstützung für Macs mit M2-Chip

Ab Version 2307 bietet die Citrix Workspace-App für macOS native Unterstützung für die M2-Serie von Apple Silicon (zusätzlich zur bereits unterstützten M1-Serie). Weitere Informationen finden Sie unter [Native Unterstützung für Apple Silicon](#).

Citrix Workspace-App für Mac unter macOS Sonoma Beta

Die Citrix Workspace-App 2307 für Mac wurde unter macOS Sonoma Public Beta 1 Version 23A5286i getestet. Verwenden Sie dieses Setup in einer Testumgebung und geben Sie uns [Feedback](#).

Achtung:

Verwenden Sie die Citrix Workspace-App für Mac unter macOS Sonoma Beta-Versionen nicht in Produktionsumgebungen.

Einstellung der Unterstützung von macOS-Version Catalina

Wie in Version 2304 angekündigt, ist die macOS-Version Catalina (10.15) veraltet und wird ab Release 2307 eingestellt. Weitere Informationen finden Sie unter [Einstellung von Features und Plattformen](#).

Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit Cloudstores

Ab Version 2307 können Benutzer sich ohne Kennwort per FIDO2 authentifizieren, wenn sie eine Verbindung zum Cloudstore herstellen. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Desktops, die FIDO2 unterstützen, authentifizieren. Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code und Touch ID. Dieses Feature wird unter macOS 12 und späteren Versionen unterstützt. Weitere Informationen finden Sie unter [FIDO2-Authentifizierung beim Verbinden mit einem Cloudstore](#).

Unterstützung für die Authentifizierung mit FIDO2 in HDX-Sitzungen

Ab Version 2307 können Benutzer sich innerhalb von HDX-Sitzungen ohne Kennwort per FIDO2 authentifizieren. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Websites, die FIDO2 unterstützen, authentifizieren. Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code. Dieses Feature wird unter macOS 12 und späteren Versionen unterstützt. Weitere Informationen finden Sie unter [FIDO2-Authentifizierung in HDX-Sitzungen](#).

Hinweis:

Dieses Release unterstützt nur einen Passkey auf Geräten mit FIDO2-Unterstützung. Besitzt ein Gerät mehrere Passkeys, wird der erste Passkey zur Authentifizierung der HDX-Sitzung verwendet.

Versionssteuerung für automatische Updates

Administratoren können jetzt angeben, auf welche Version der Citrix Workspace-App Geräte in der Organisation automatisch aktualisiert werden.

Hierfür legen sie den Versionsbereich im Global App Configuration Service mit den Eigenschaften für `maximumAllowedVersion` und `minimumAllowedVersion` fest.

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

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12                  Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        "category": "AutoUpdate",
19        "userOverride": false,
20        "assignedTo": [
21          "AllUsersNoAuthentication"
22        ],
23        "settings": [
24          {
25
26            "name": "Auto update plugins settings",
27            "value": [
28              {
29
```



```
30         "pluginName": "Citrix Workspace",
31         "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
32         "pluginSettings": {
33
34             "deploymentMode": "Update",
35             "upgradeToLatest": false,
36             "minimumAllowedVersion": "23.07.0.63",
37             "maximumAllowedVersion": "23.07.0.63",
38             "delayGroup": "Medium",
39             "detectRule": ""
40         }
41     }
42 }
43 ]
44 }
45 }
46
47 ]
48 }
49
50 ]
51 }
52
53 }
54
55 }
56
57
58 <!--NeedCopy-->
```

Wenn der Bereich festgelegt ist, wird die Citrix Workspace-App auf dem Benutzergerät automatisch auf die höchste verfügbare Version aktualisiert, die im genannten Bereich liegt.

Wenn Sie die Citrix Workspace-App automatisch auf eine bestimmte Version aktualisieren möchten, geben Sie im Global App Configuration Service in den Eigenschaften “maximumAllowedVersion” und “minimumAllowedVersion” zweimal dieselbe Version ein. Weitere Informationen finden Sie unter [Versionssteuerung für automatische Updates](#).

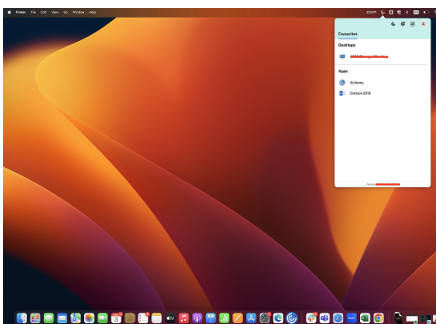
Hinweis:

- Um die Versionssteuerung für automatische Updates zu aktivieren, setzen Sie die Einstellung “upgradeToLatest” im Global App Configuration Service auf “false”. Wenn die Einstellung “upgradeToLatest” auf “true” gesetzt ist, werden “maximumAllowedVersion” und “minimumAllowedVersion” ignoriert.

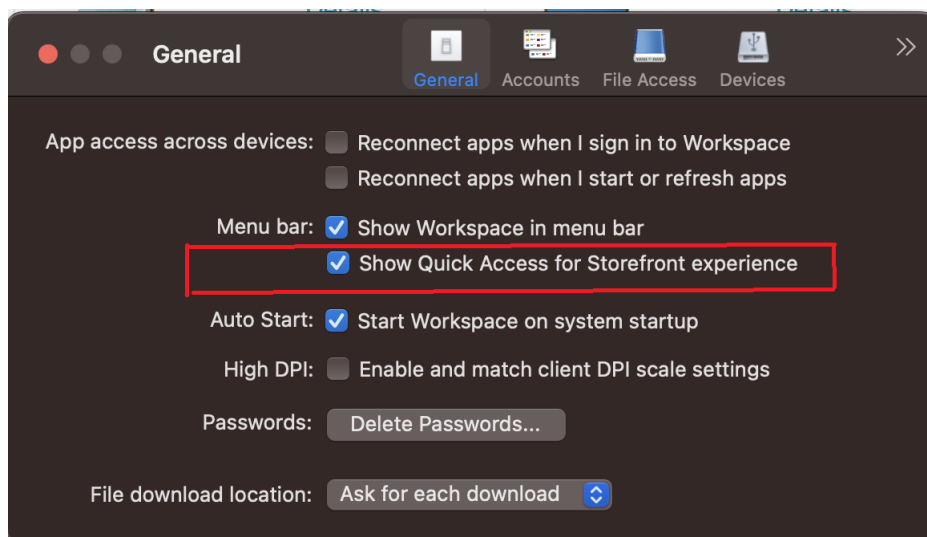
- Ändern Sie nicht die PluginID. Die PluginID ist der Citrix Workspace-App zugeordnet.
- Wenn die Version nicht im Global App Configuration Service konfiguriert ist, wird die Citrix Workspace-App standardmäßig auf die neueste verfügbare Version aktualisiert.
- Sie können nur die Versionsbereiche verwenden, die für ein Upgrade der Citrix Workspace-App festgelegt sind. Ein Downgrade wird nicht unterstützt.
- Dieses Feature wird ab Release 2307 unterstützt.

Schnellzugriffsmenü für StoreFront

Ab Version 2307 können Sie über das Schnellzugriffsfeature für On-Premises-Stores schnell und einfach zu Ihren bevorzugten Apps und Desktops gelangen. Um den Schnellzugriff zu aktivieren, klicken Sie in der Symbolleiste mit der rechten Maustaste auf **Citrix Workspace**, gehen Sie zu **Einstellungen > Allgemein** und wählen Sie dann **Schnellzugriff für Storefront-Erlebnis anzeigen**. Mit diesem Feature können Sie Ihre Lieblingsdaten direkt über die Mac-Menüleiste anzeigen.



Sie können den Schnellzugriff über die **Einstellungen** aktivieren.



Administratoren können den Schnellzugriff über die Mobilgeräteverwaltung (MDM) oder Global App Configuration Service (GACS) aktivieren und deaktivieren. Weitere Informationen finden Sie unter [Schnellzugriffsmenü für StoreFront](#).

Schnellzugriff mit MDM aktivieren/deaktivieren

Um den Schnellzugriff über MDM zu aktivieren, müssen Administratoren die folgenden Einstellungen verwenden:

```
<key>ShowQuickAccessForStoreFront</key>  
<false/>
```

Schnellzugriff mit GACS aktivieren/deaktivieren

Um den Schnellzugriff über GACS zu aktivieren, müssen Administratoren die folgenden Einstellungen verwenden:

```
enableQuickAccessForStoreFront
```

Storebasierte Konfiguration des Zugriffs auf Mikrofon und Webcam

Ab Version 2307 ist der storebasierte Zugriff auf Mikrofon und Webcam als Bestandteil der clientselektiven Vertrauensfunktion enthalten. Mit dieser Verbesserung können Sie den Zugriff auf Mikrofon und Webcam pro Store gewähren.

Um den Zugriff auf Mikrofon und Webcam für einen Store zu aktivieren, müssen Sie **Einstellungen > Mikrofon und Webcam** wählen. Wählen Sie auf der Registerkarte **Mikrofon und Webcam** den Store und die Zugriffsart, die für den Store erforderlich ist.

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.

Zum Anzeigen des benötigten Formulars wählen Sie **Hilfe > Feedback senden**. Sie können Details wie die angegebenen Beispiele eingeben.

Send feedback

Provide a descriptive title*

Tell us more*

Include details such as:

- What you expected to happen
- What actually happened
- Steps to recreate the issue

Logs

Basic logs are attached. We recommend you click 'Record my issue' to capture detailed logs.

For more information, see [Log collection](#)

Record my issue WorkspaceLogs_2023_07_18-14_23_43.zip

Attachments

Screenshots or screen recordings of the problem.

Choose files (Max 4 files)

Your feedback will be used to improve Citrix Workspace app. If you don't use the Mail app on your Mac, please send feedback to **cwa-mac-feedback@cloud.com** with files added manually.

Send **Cancel**

Sie können bestehende Protokolldateien anhängen oder neue Protokolldateien generieren. Um Protokolldateien zu generieren, klicken Sie auf **Mein Problem aufzeichnen > Aufzeichnung starten** und reproduzieren Sie dann das Problem. Nachdem das Problem reproduziert wurde, klicken Sie auf **Aufzeichnung beenden**. Die Protokolldatei wird automatisch gespeichert und ersetzt bestehende Protokolle.

Hinweis:

Citrix erfasst keine personenbezogenen Informationen (PII) aus den Protokollen.

Sie können Screenshots oder Bildschirmaufzeichnungen zur weiteren Erläuterung des Problems anhängen. Klicken Sie auf **Dateien auswählen** und fügen Sie die Anhänge hinzu (Screenshots, Bildschirmaufzeichnungen o. Ä.). Sie können maximal vier Dateien anhängen.

Wenn Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Senden**, damit in Ihrer

E-Mail-App automatisch eine E-Mail mit den von Ihnen hinzugefügten Informationen erstellt wird. Klicken Sie dort auf die Schaltfläche **Senden**, um das Feedback an Citrix zu senden. Weitere Informationen finden Sie unter [Feedback zur Citrix Workspace-App senden](#).

Hinweis:

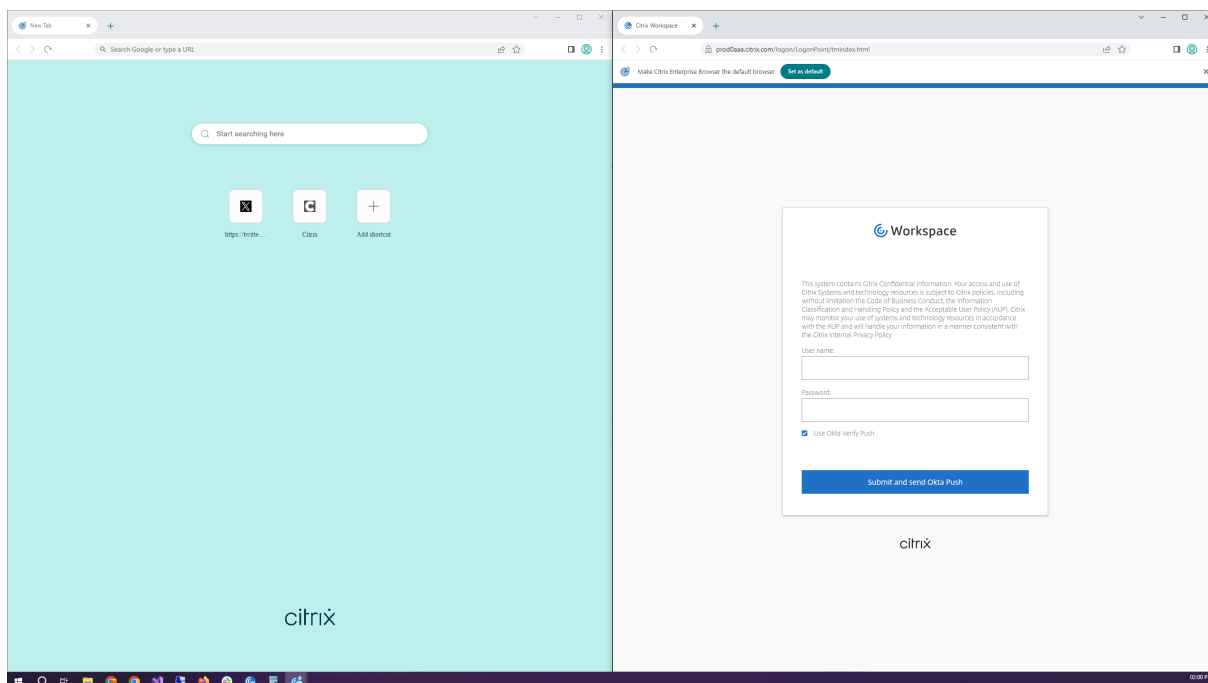
Wenn Sie nicht die Standard-E-Mail-App verwenden, senden Sie Feedback von Ihrem E-Mail-Client an cwa-mac-feedback@cloud.com. Fügen Sie Problemdetails, Protokolldateien, Screenshots oder Bildschirmaufzeichnungen manuell hinzu.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 113.1.1.34, der auf Chromium Version 113 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Unterstützung für geteilte Ansicht

Citrix Enterprise Browser unterstützt unter macOS die geteilte Ansicht für bequemes Multitasking. Mit der geteilten Ansicht können Sie den Citrix Enterprise Browser und ein weiteres Fenster nebeneinander verwenden, ohne diese manuell verschieben und ihre Größe ändern zu müssen. Weitere Informationen finden Sie im [Support-Artikel von Apple](#).



Verknüpfung für Citrix Enterprise Browser

Ab Version 2307 der Citrix Workspace-App für Mac kann ein Administrator das Vorhandensein der Citrix Enterprise Browser-Verknüpfung auf dem Launchpad konfigurieren und steuern.

Hinweis:

Dieses Feature ist standardmäßig nicht konfiguriert.

Konfiguration

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

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)
- Datei web.config.

Hinweis:

- 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 das Feature für Workspace-Stores zu deaktivieren, müssen Administratoren eine der folgenden Einstellungen vornehmen:
 - Attribut `CEBShortcutEnabled` in MDM oder der Datei web.config auf "false" festlegen.
 - Eigenschaft "Citrix Enterprise Browser-Verknüpfung aktivieren" in GACS deaktivieren.

Mobilgeräteverwaltung (MDM)

Administratoren können die Einstellung **true** für **CEBShortcutEnabled** auf das Gerät des Benutzers übertragen.

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

Hinweis:

Diese Art der Konfiguration gilt für Workspace und StoreFront.

Global App Configuration Service (GACS)

Gehen Sie zu **Workspacekonfiguration > App-Konfiguration > Citrix Enterprise Browser** und aktivieren Sie die Eigenschaft **Citrix Enterprise Browser-Verknüpfung aktivieren**.

List Of Allowed Extensions 0 Configured, 0 Unsaved

You can add a list of extensions that the end users can install within the Citrix Enterprise Browser. The end user can't install other extensions apart from the allowed list. [Learn More](#).

Add Managed Bookmarks 0 Configured, 0 Unsaved

You can add a list of bookmarks to the Citrix Enterprise Browser. The end user can't modify these bookmarks.

Delete Browsing Data On Exit 0 Configured, 0 Unsaved

You can configure what type of data the Citrix Enterprise Browser can delete when the end user exits the browser. Note: Deleting the browsing data can affect usability. [Learn More](#)

Enable Citrix Enterprise Browser Shortcut 0 Configured, 2 Unsaved

Creates a Citrix Enterprise Browser shortcut on the Start menu in Windows and Launchpad in macOS. If a user marks Enterprise Browser as favorite, a shortcut is created irrespective of the configuration.

| | | | | |
|-------------------------------------|---------|----------|-------------------------------------|---------|
| <input checked="" type="checkbox"/> | Mac | Enabled | <input checked="" type="checkbox"/> | Unsaved |
| <input checked="" type="checkbox"/> | Windows | Disabled | <input type="checkbox"/> | Unsaved |

Warning: You have saved drafts that are not yet published in Production. You may continue editing or publish now to apply changes to Workspace for your end users. [Review 2 unsaved setting\(s\)](#) [Discard](#) [Publish Drafts](#)

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

Hinweis:

Diese Art der Konfiguration gilt für Workspace und StoreFront.

Datei web.config

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

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

Hinweis:

Diese Art der Konfiguration 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`.

- Suchen Sie das Benutzerkonto-Element in der Datei (Store ist der Kontoname Ihrer Bereitstellung).

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

- Vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

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

Dies ist ein Beispiel für die Datei `web.config`:

```
1 <account>
2     <clear />
3     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
4         description="" published="true" updaterType="Citrix"
5         remoteAccessType="None">
6         <annotatedServices>
7             <clear />
8             <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
9                 <metadata>
10                    <plugins>
11                        <clear />
12                    </plugins>
13                    <trustSettings>
14                        <clear />
15                    </trustSettings>
16                    <properties>
17                        <property name="CEBShortcutEnabled" value="True" />
18                    </properties>
19                </metadata>
20            </annotatedServiceRecord>
21        </annotatedServices>
22        <metadata>
23            <plugins>
24                <clear />
25            </plugins>
26            <trustSettings>
27                <clear />
28            </trustSettings>
29            <properties>
```



```
29         <clear />
30     </properties>
31 </metadata>
32 </account>
33
34 <!--NeedCopy-->
```

Mit web.config konfigurieren

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

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

3. Vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

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

Technical Preview

- Tastenkombination für Symbolleiste auf dem virtuellen Desktop

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Beim Starten einer veröffentlichten App über den Browser wird die App nicht direkt gestartet, sondern eine ICA-Datei heruntergeladen. Der Benutzer muss die heruntergeladene ICA-Datei möglicherweise manuell öffnen, um die App zu starten. [CVADHELP-20835]
- Versuche, eine Sitzung zu starten, schlagen möglicherweise fehl, wenn das StoreFront-Schlüsselwort auf "KEYWORDS:LogoffOnClose=true PromptMessage="Möchten Sie sich abmelden?" festgelegt ist. [CVADHELP-23170]
- Möglicherweise können Sie das erforderliche Gateway nicht aus der Liste der verfügbaren Optionen auswählen, wenn Sie die Citrix Workspace-App für Mac verwenden. [CVADHELP-22777]

Bekannte Probleme

In diesem Release wurden keine neuen Probleme festgestellt.

2306

Was ist neu

Rückverfolgbarkeit von Protokollen und Benutzeraktivität

Wenn ein Benutzer ein Problem meldet, können Administratoren ab Version 2306 die Protokolldateien durchsuchen, um grundlegende Informationen (macOS-Version, Version der Citrix Workspace-App, Details zum vorherigen Upgrade, Anzahl der hinzugefügten Stores usw.) einzusehen. Administratoren können jetzt die folgenden Aktivitäten in der Citrix Workspace-App für Mac einsehen:

- App-Start sowie macOS-Version, der Anzahl der Stores und andere Metadaten.
- Hinzufügungen und Löschungen von Stores und zum Hinzufügen eines Kontos erforderliche Metadaten.
- Uhrzeit und Status des Sitzungsstarts.
- Aktivierung und Status von automatischen Updates.
- Systemereignisse (Verschieben der App in den Hintergrund, Ruhemodus oder Beenden).

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 112.1.1.23, der auf Chromium Version 112 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Behobene Probleme

- Nach dem Upgrade der Citrix Workspace-App für Mac auf Version 2305 reagieren bestimmte virtuelle Apps von Drittanbietern mit Popup-Dialogfeldern zur Eingabe von Benutzernamen und Kennwort nach dem Öffnen möglicherweise nicht mehr. [CVADHELP-23032]

Bekannte Probleme

In diesem Release wurden keine neuen Probleme festgestellt.

2305

Was ist neu

Unterstützung für horizontales Scrollen

Bisher unterstützte die Citrix Workspace-App für Mac nur vertikales Scrollen auf einem Trackpad. Ab Version 2305 wird auch horizontales Scrollen unterstützt. Weitere Informationen finden Sie unter [Unterstützung für horizontales Scrollen](#).

Verbesserte Unterstützung der Audioechounterdrückung

Die Citrix Workspace-App unterstützt jetzt die Echounterdrückung in adaptivem Audio und Legacyaudiocodern. Dieses Feature wurde für Anwendungsfälle von Echtzeitaudio entwickelt und verbessert die Benutzererfahrung. Citrix empfiehlt, adaptives Audio zu verwenden. Weitere Informationen finden Sie unter [Verbesserte Unterstützung der Audioechounterdrückung](#)

Verbesserte Grafikleistung [Technical Preview]

Ab Version 2305 bieten Seamlessitzungen eine bessere Grafikleistung. Das Feature reduziert auch die CPU-Auslastung.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Unterstützung für die zertifikatbasierte Authentifizierung

Ab Version 2305 können Workspace-Administratoren Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei der Citrix Workspace-App authentifizieren.

Die folgenden Methoden können verwendet werden, um die Authentifizierung mit bedingtem Zugriff zu aktivieren:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Die von der Citrix Workspace-App gelesenen Flagwerte haben folgende Vorrangreihenfolge:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Weitere Informationen finden Sie unter [Unterstützung für die zertifikatbasierte Authentifizierung](#).

Kanalunterstützung für Global App Configuration Service

Der Global App Configuration Service für Citrix Workspace ermöglicht Citrix-Administratoren, Workspace-Dienst-URLs und Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen. Mit dem Global App Configuration Service können Administratoren jetzt Einstellungen testen, bevor sie für alle Benutzer bereitgestellt werden. Mit diesem Feature können mögliche Probleme behoben werden, bevor App-Konfigurationen global für alle Benutzer angewendet werden. Weitere Informationen finden Sie unter [Kanalunterstützung für Global App Configuration Service](#).

Verbesserung der automatischen Updates

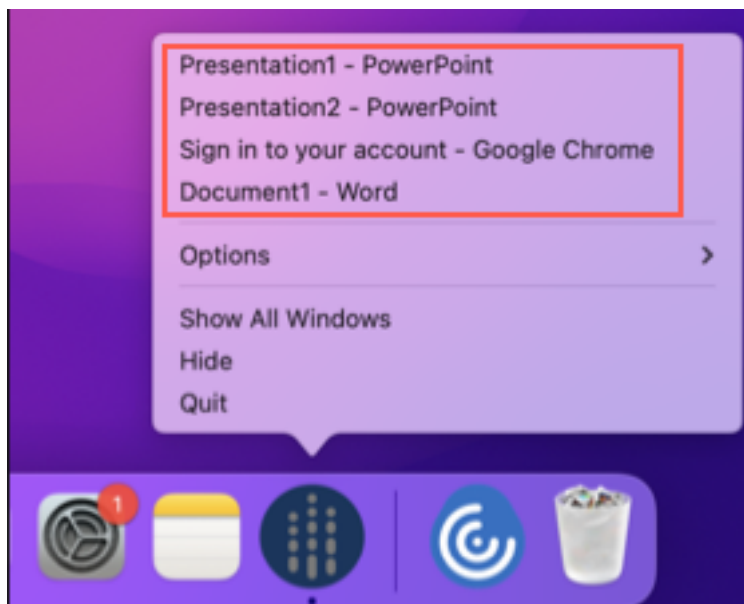
Mit dem Feature "Automatische Updates" wird die Citrix Workspace-App automatisch auf die neueste Version aktualisiert, ohne dass ein Benutzereingriff erforderlich ist.

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.

Weitere Informationen finden Sie unter [Verbesserung der automatischen Updates](#).

Anzeige geöffneter Apps im Dock mit nativen App-Symbolen

Bisher hat das Klicken auf virtuelle Apps in der Citrix Workspace-App den **Citrix Viewer** ausgelöst, in dem die Apps verfügbar waren. Wenn Sie viele Apps öffnen, werden die Apps oder Instanzen im **Citrix Viewer** geöffnet. Zum Anzeigen der geöffneten Apps klicken Sie mit der rechten Maustaste auf das **Citrix Viewer**-Symbol.



Ab Version 2305 werden virtuelle Apps, die Sie öffnen, im Dock (rechts unten im Bildschirm) mit den entsprechenden Symbolen angezeigt und sind leicht identifizierbar. Sie können dann über das Dock

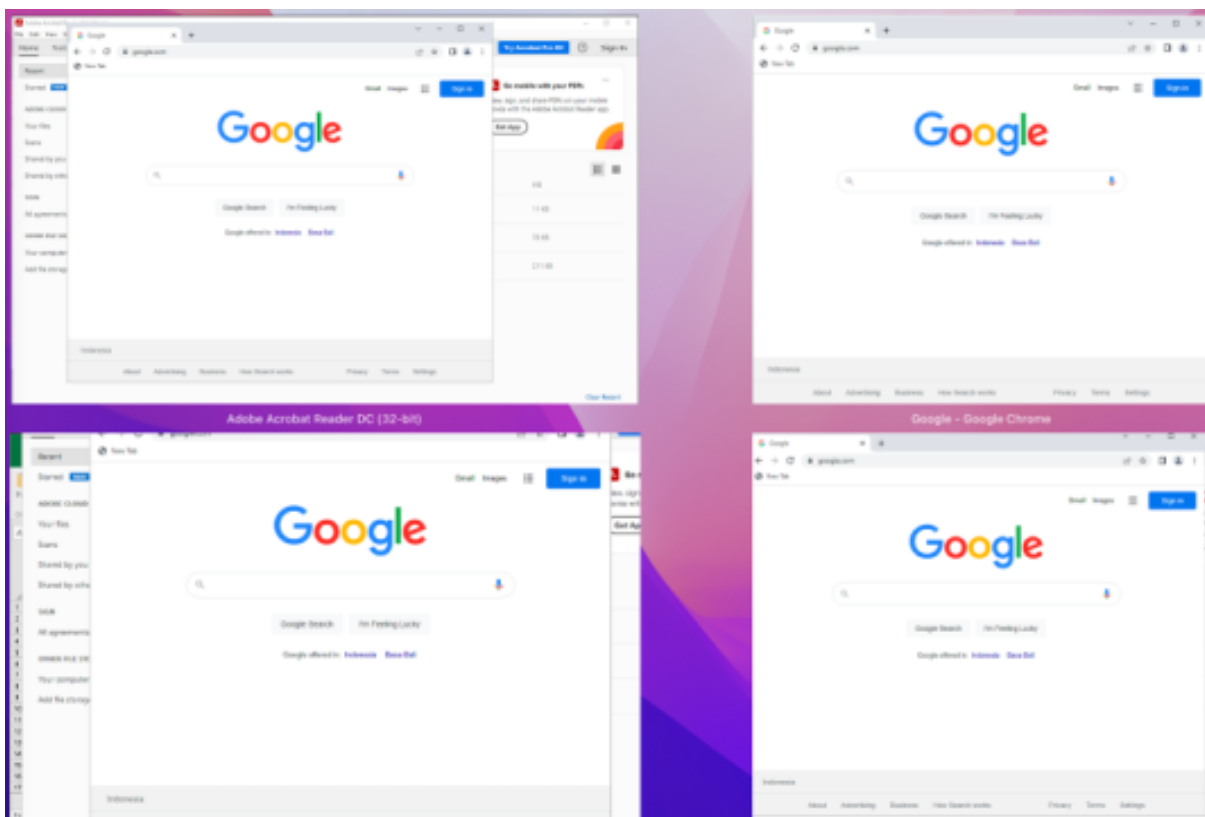
auf die virtuelle App zugreifen. Wenn Sie mehrere Instanzen einer App öffnen, werden diese im Dock nicht dupliziert, sondern in einer Instanz im Dock angeordnet.



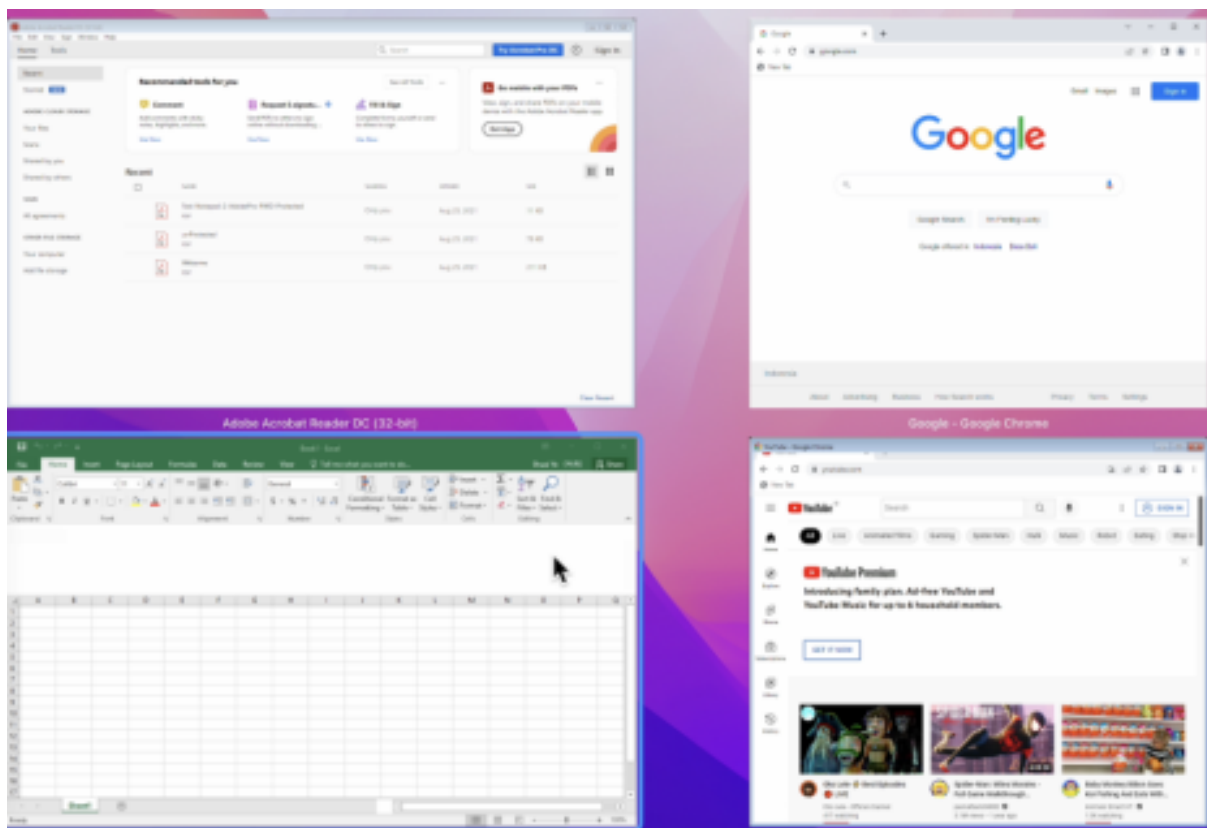
Weitere Informationen finden Sie unter [Anzeige geöffneter Apps im Dock mit nativen App-Symbolen](#).

Verbessertes Mission Control- und App Expose-Erlebnis

Bisher führte die Verwendung des Features **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung zu einer großen Zahl überlappender Fenster.



Wenn Sie ab Version 2305 das Feature **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung verwenden und viele Fenster öffnen, überlappen sich die Fenster nicht und stehen übersichtlich zur Verfügung.



Weitere Informationen finden Sie unter [Verbessertes Mission Control- und App Expose-Erlebnis](#).

Verbesserter Energiesparmodus für optimierte Microsoft Teams-Anrufe

Bisher ging die Citrix Workspace-App oder der optimierte Microsoft Teams-Bildschirm gelegentlich in den Energiesparmodus über, wenn in einer Besprechung mit optimiertem Microsoft Teams keine Maus- oder Tastaturinteraktion stattfand.

Ab Version 2305 gehen die Citrix Workspace-App oder der optimierte Microsoft Teams-Bildschirm nicht in den Energiesparmodus über, wenn in einer Besprechung mit optimiertem Microsoft Teams keine Maus- oder Tastaturinteraktion auftritt.

Weitere Informationen finden Sie unter [Verbesserter Energiesparmodus für optimierte Microsoft Teams-Anrufe](#).

Unterstützung für Integrationskamera

Mit der Integrationskamera (Continuity Camera) können Sie Ihr iPhone jetzt als Webcam verwenden. Platzieren Sie Ihr iPhone dabei so, dass die Kamera für das Mac-Gerät verfügbar ist. Sie müssen **Web-**

cam > Automatic Camera Selection auswählen, damit das iPhone auf dem Mac-Gerät automatisch als externe Kamera angezeigt wird. Sie können manuell zu jeder anderen Kamera wechseln, indem Sie beispielsweise **Webcam > FaceTime HD Camera** auswählen. Die Integrationskamera funktioniert kabelgebunden oder drahtlos und liefert ein qualitativ hochwertiges Bild. Weitere Informationen finden Sie unter [Unterstützung für Integrationskamera](#).

Erhöhung der Anzahl der unterstützten virtuellen Kanäle [Technical Preview]

In früheren Versionen des Clients wurden bis zu 32 virtuelle Kanäle in einer Sitzung unterstützt. Ab Version 2305 können Sie bis zu 64 virtuelle Kanäle in einer Sitzung nutzen.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Storebasierte Konfiguration der Zugriffsebenen für Mikrofon und Webcam [Technical Preview]

Ab Version 2305 ist der storebasierte Zugriff auf Mikrofon und Webcam als Bestandteil der clientselktiven Vertrauensfunktion enthalten. Mit dieser Verbesserung können Sie die Einstellungen für jeden Store einzeln festlegen. Sie können auf einen Store klicken, um den erforderlichen Mikrofon- oder Kamerazugriff zu aktivieren. Die ausgewählte Einstellung für den Mikrofon- oder Kamerazugriff wird pro Store angewendet.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit Cloudstores [Technical Preview]

Ab Version 2305 können Benutzer sich mit kennwortlosen FIDO2-Sicherheitsschlüsseln authentifizieren, wenn sie sich mit der Citrix Workspace-App für Mac verbinden. Benutzer können sich

mit den FIDO2-Sicherheitsschlüsseln bei den Cloudstores anmelden. Die Sicherheitsschlüssel unterstützen verschiedene Arten von Sicherheitseingaben wie Sicherheits-PIN, Biometrie, Magnetstreifenkarte, Smartcard und Public-Key-Zertifikat. Dieses Feature wird unter macOS 12 und späteren Versionen unterstützt. Weitere Informationen zu FIDO2 finden Sie unter [FIDO2-Authentifizierung](#).

Die Citrix Workspace-App verwendet den Standardbrowser des Benutzers für die FIDO2-Authentifizierung (Webauthn). Administratoren können den Browsertyp für die Authentifizierung bei der Citrix Workspace-App konfigurieren. Die konfigurierte Einstellung kann mit MDM (Mobilgeräteverwaltung), GACS (Global App Configuration Service) oder per Befehlszeilenschnittstelle übertragen werden. Das FIDO2-Feature wird nicht für On-Premises-Stores unterstützt. Weitere Informationen zu den Webbrowsereinstellungen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

Mit den folgenden Einstellungen können Sie den Browsertyp auswählen, der für die Authentifizierung eines Endbenutzers in der Citrix Workspace-App verwendet wird:

Embedded: Ermöglicht die Authentifizierung innerhalb der Citrix Workspace-App. Die Citrix Workspace-App speichert die Sitzungsdaten oder Cookies für den Single Sign-On (z. B. SaaS-Apps), wenn das [erweiterte Single Sign-On-Feature](#) aktiviert ist. Diese Authentifizierungsmethode unterstützt keine kennwortlosen Authentifizierungen wie FIDO2.

EmbeddedWithPrivateSession: Diese Einstellung ähnelt der Einstellung **Embedded**. Single Sign-On wird nicht unterstützt, da keine Sitzungsdaten oder Cookies in der Citrix Workspace-App vorhanden sind.

System: Hiermit können Sie den Standardbrowser des Benutzers für die Authentifizierung verwenden (z. B. Safari oder Chrome). Die Authentifizierung erfolgt außerhalb der Citrix Workspace-App. Verwenden Sie diese Einstellung, um die kennwortlose Authentifizierung zu unterstützen. Diese Einstellung versucht, die bestehende Benutzersitzung vom Browser des Benutzers zu verwenden.

SystemWithPrivateSession: Diese Einstellung entspricht der **Systemeinstellung**. Die Citrix Workspace-App verwendet eine private Sitzung im Browser für die Authentifizierung. Der Browser speichert keine Authentifizierungscookies oder -daten. Single Sign-On wird in dieser Option nicht unterstützt.

Authentifizierung mit MDM aktivieren

Um die Authentifizierung per Mobilgeräteverwaltung (MDM) zu aktivieren, müssen Administratoren folgende Einstellungen verwenden:

```
<key>WebBrowserForAuthentication</key>  
<string>System</string>
```

Authentifizierung mit GACS aktivieren

Um die Authentifizierung per GACS zu aktivieren, müssen Administratoren folgende Einstellungen verwenden:

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Productivity Apps",
11    "description": "Provides access to MS Office and other basic apps",
12    "useForAppConfig": true,
13    "appSettings": {
14
15      "macos": [
16        {
17
18          "assignedTo": [
19            "AllUsersNoAuthentication"
20          ],
21          "category": "authentication",
22          "settings": [
23            {
24
25              "name": "web browser for authentication",
26              "value": "SystemWithPrivateSession"
27            }
28          ],
29          "userOverride": false
30        }
31      ]
32    }
33  }
34 }
35
36 }
37
38 }
39
40
41 <!--NeedCopy-->
```

Authentifizierung per Befehlszeilenschnittstelle aktivieren

Um die Authentifizierung per Befehlszeilenschnittstelle zu aktivieren, müssen Administratoren den folgenden Befehl ausführen:

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication System
```

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserungen des Tastatureingabemodus

Die Citrix Workspace-App für Mac bietet Optionen zum Konfigurieren des Tastatureingabemodus.

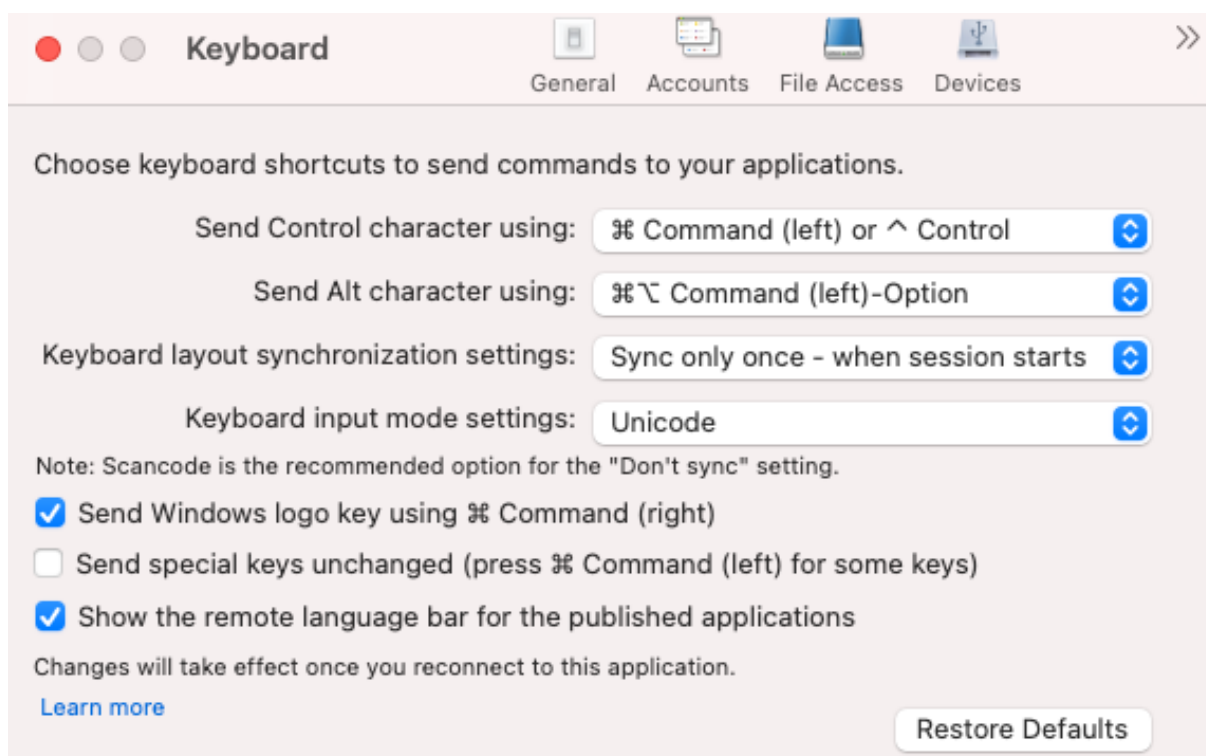
Gehen Sie wie folgt vor, um den Tastatureingabemodus über die GUI zu konfigurieren:

1. Klicken Sie über das Citrix Workspace-App-Symbol in der Menüleiste auf das Kontosymbol oben rechts und gehen Sie zu **Einstellungen > Tastatur**.

Die Einstellungen für den Tastatureingabemodus werden angezeigt.

2. Wählen Sie eine der folgenden Optionen:
 - **Scancode:** Sendet die Tastenposition von der clientseitigen Tastatur an den VDA, welcher das entsprechende Zeichen generiert. Wendet serverseitiges Tastaturlayout an
 - **Unicode:** Sendet die Taste von der clientseitigen Tastatur an den VDA, welcher das gleiche Zeichen auf dem VDA generiert. Wendet clientseitiges Tastaturlayout an.

Diese Erweiterung ist standardmäßig aktiviert.



Angenommen, Sie verwenden das Tastaturlayout USA international und der VDA das russische Tastaturlayout. Wenn Sie **Scancode** auswählen und die Taste neben der **Feststelltaste** drücken, wird der Scancode "1E" an den VDA gesendet. Der VDA verwendet dann "1E", um das Zeichen "ϕ" anzuzeigen. Wenn Sie **Unicode** wählen und die Taste neben **Feststelltaste** drücken, wird das Zeichen "a" an den VDA gesendet. Obwohl der VDA das russische Tastaturlayout verwendet, erscheint das Zeichen "a" auf dem Bildschirm.

Citrix empfiehlt den folgenden Tastatureingabemodus für die verschiedenen Tastaturlayoutsynchronisierungsoptionen:

- Scancodemodus für die Option **Nicht synchronisieren**.
- Modus "Unicode" für **Dynamische Synchronisierung zulassen** und **Nur einmal beim Sitzungsstart synchronisieren**

Hinweis:

Änderungen an der Tastaturkonfiguration werden wirksam, sobald Sie die Verbindung zur Anwendung wieder herstellen.

Sie können die Konfiguration des Tastatureingabemodus in der Citrix Workspace-App ändern. Um eine optimale Leistung zu erzielen, sollten Sie die von Citrix empfohlenen Modi die für verschiedene Szenarien, physische Tastaturen und Clientgeräte verwenden.

Weitere Informationen zu Konfigurationsdetails und Einschränkungen finden Sie unter [Verbesserungen des Tastatureingabemodus](#).

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 112.1.1.23, der auf Chromium Version 112 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

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.

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. Weitere Einstellungen finden Sie unter [Global App Configuration Service](#).

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

Verwaltung des Citrix Enterprise Browser mit GACS

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

Der GACS ermöglicht Administratoren die einfache Konfiguration von Citrix Workspace und die Verwaltung der Einstellungen für die Citrix Workspace-App. Mit diesem Feature können Administratoren per GACS verschiedene 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 im [Global App Configuration Service](#) sind in der folgenden Kategorie:

```
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

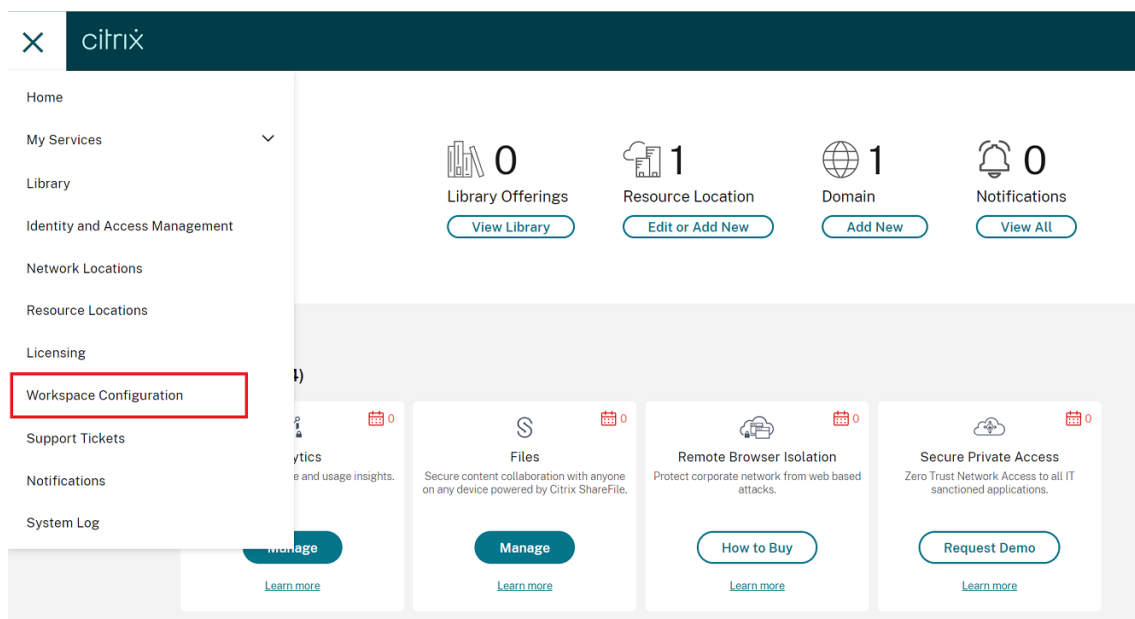
Führen Sie folgende Schritte aus, um den Citrix Enterprise Browser über die Verwaltungsoberfläche des GACS zu konfigurieren:

1. Melden Sie sich mit Ihren Anmeldeinformationen bei citrix.cloud.com 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](#).

Technical Preview

- Client-App-Verwaltung

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Mit dieser Verbesserung können die Standortdaten gesammelt und an Microsoft Teams gesendet werden, um den dynamischen Notruf zu unterstützen. [CVADHELP-21117]
- Wenn Sie in einer Benutzersitzung, die über die Citrix Workspace-App für Mac geöffnet wird, mit dem Touchpad auf einem MacBook scrollen, ist das Scrollerlebnis möglicherweise nicht reibungslos. [CVADHELP-21427]
- Wenn Sie die Citrix Workspace-App für Mac verwenden, werden externe Benutzer möglicherweise gelegentlich von den Sitzungen getrennt. [CVADHELP-22191]
- Das Hinzufügen einer Store-URL, die einen Abfrageparameter enthält, kann in der Citrix Workspace-App für Mac fehlschlagen, und es wird folgende Fehlermeldung angezeigt:

Dieser Store ist nicht vorhanden. Wiederholen Sie den Versuch oder wenden Sie sich an den Support.

[CVADHELP-22445]

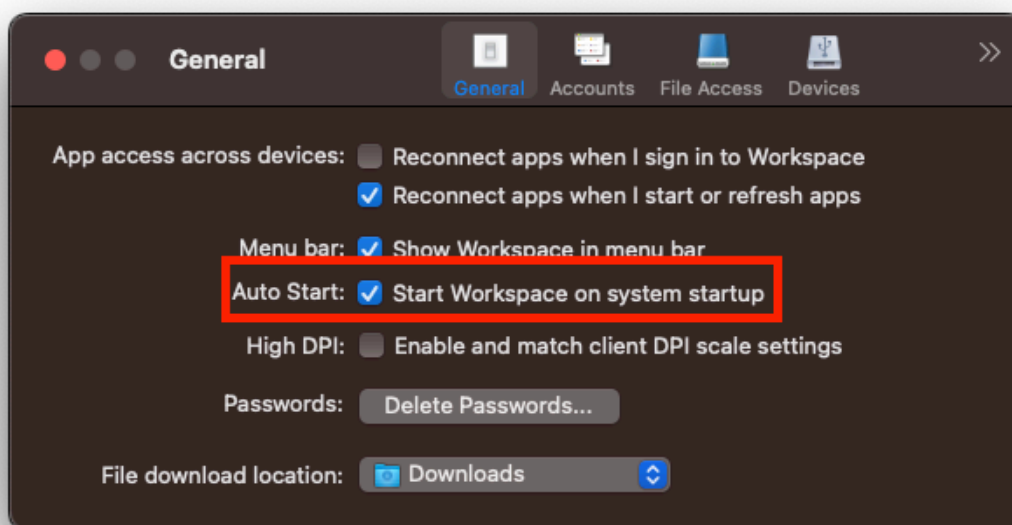
- Wenn Sie in einem On-Premises-Store versuchen, die Citrix Workspace-App über die **Menüleiste** zu öffnen, kann eine Endloswarteschleife auftreten. [CVADHELP-22688]

2304

Was ist neu

Verbesserter automatischer Start

Bisher wurde die Citrix Workspace-App für Mac automatisch gestartet, wenn ein Computer eingeschaltet wurde. Ab Version 2304 können Sie den automatischen Start der Citrix Workspace-App für Mac deaktivieren oder aktivieren, indem Sie zu **Einstellungen > Allgemein > Workspace beim Systemstart starten** gehen. Die Autostart-Einstellung ist standardmäßig aktiviert.



Weitere Informationen finden Sie unter [Verbesserter automatischer Start](#).

Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen

Ab Version 2304 ist die Simulcast-Unterstützung standardmäßig für optimierte Microsoft Teams-Videokonferenzen aktiviert. Dadurch werden die Qualität und das Erlebnis bei Videokonferenzen an

verschiedenen Endpunkten verbessert. Dies wird erreicht, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank dieser verbesserten Benutzererfahrung kann jeder Benutzer abhängig von der Endpunktfähigkeit, den Netzwerkbedingungen usw. mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.) senden. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann, sodass alle Benutzer das optimale Videoerlebnis erhalten.

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.

Weitere Informationen finden Sie unter

[Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen.](#)

Unterstützung für die zertifikatbasierte Authentifizierung [Technical Preview]

Ab Version 2304 können Workspace-Administratoren Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei der Citrix Workspace-App authentifizieren.

Die folgenden Methoden können verwendet werden, um die Authentifizierung mit bedingtem Zugriff zu aktivieren:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Die von der Citrix Workspace-App gelesenen Flagwerte haben folgende Vorrangreihenfolge:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Weitere Informationen finden Sie unter [Unterstützung für die zertifikatbasierte Authentifizierung.](#)

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Anmeldeaufforderung für Verbundidentitätsanbieter erzwingen

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

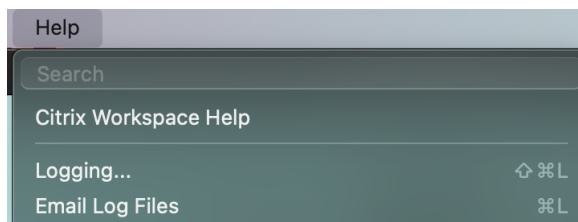
Die Verwendung der Richtlinie “Authentifizierungstoken speichern” ist zum Erzwingen der Anmeldeaufforderung nicht mehr nötig. Weitere Informationen finden Sie unter [Anmeldeaufforderung für Verbundidentitätsanbieter erzwingen](#).

Unterstützung für nicht englische IME-Tastaturlayouts

Die Unterstützung für nicht englische IME-Tastaturlayouts funktioniert ohne Unterbrechung weiter, wenn die Carbon-APIs zusammen mit den Cocoa-APIs auslaufen. Weitere Informationen finden Sie unter [Unterstützung für nicht englische IME-Tastaturlayouts](#).

Protokollsammlung

Protokollsammlung vereinfacht das Sammeln von Protokollen für die Citrix Workspace-App. Die Protokolle helfen Citrix bei der Fehlerbehebung und erleichtern bei komplizierten Problemen den Support. Benutzer können jetzt über das Menü **Hilfe** schnell Protokolle sammeln, indem sie zu **Hilfe** gehen und die Option **Protokollierung...** oder **Protokolldateien per E-Mail senden** auswählen. Dieses Feature verbessert die Benutzererfahrung während des Protokollerfassungsprozesses.



- **Protokollierung...:** Wenn Sie auf diese Option klicken, gelangen Sie zu **Einstellungen > Erweitert > Protokollierung**.
- **Protokolldateien per E-Mail senden:** Wenn Sie auf diese Option klicken, können Sie die neuesten Protokolle sammeln.

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

Unterstützung für die Synchronisation von mehr Tastaturlayouts

Ab Version 2304 unterstützt die Citrix Workspace-App für Mac die Synchronisierung des Tastaturlayouts für die folgenden Layouts oder Eingabemethoden-Editoren (IME):

- Englisch ABC
- Englisch ABC - Indien
- Chinesisch, traditionell: Zhuyin - traditionell

- Chinesisch, traditionell: Sucheng - Traditionell
- Google Japanese IME
- Sougou Chinese IME

Weitere Informationen finden Sie unter [Unterstützung für die Synchronisation von mehr Tastaturlayouts](#).

Verbesserung für Microsoft Teams

Schnittstelle für bevorzugtes Netzwerk konfigurieren

Sie können jetzt eine bevorzugte Netzwerkschnittstelle für den Medienverkehr konfigurieren. Führen Sie den folgenden Befehl in einem Terminal aus:

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Wählen Sie einen der folgenden Werte aus:

- 1: Ethernet
- 2: Wi-Fi
- 3: Cellular
- 4: VPN
- 5: Loopback
- 6: Any

Standardmäßig und wenn kein Wert festgelegt ist, wählt die WebRTC Media Engine die beste verfügbare Route aus.

Weitere Informationen finden Sie unter [Schnittstelle für bevorzugtes Netzwerk konfigurieren](#).

Videoauflösungen einschränken

Wenn Benutzer Clientendpunkte mit niedrigerer Leistung verwenden, können Administratoren die Auflösung eingehender oder ausgehender Videos reduzieren, um die Videocodierung und -decodierung auf diesen Endpunkten zu verbessern. Ab Version 2304 der Citrix Workspace-App für Mac können Sie diese Auflösungen über die Clientkonfigurationsoptionen einschränken.

Weitere Informationen finden Sie unter [Videoauflösungen einschränken](#).

Unterstützung für horizontales Scrollen [Technical Preview]

Bisher unterstützte die Citrix Workspace-App für Mac nur vertikales Scrollen auf einem Trackpad. Ab Version 2304 wird auch horizontales Scrollen unterstützt.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserungen des Tastatureingabemodus

Die Citrix Workspace-App für Mac bietet Optionen zum Konfigurieren des Tastatureingabemodus.

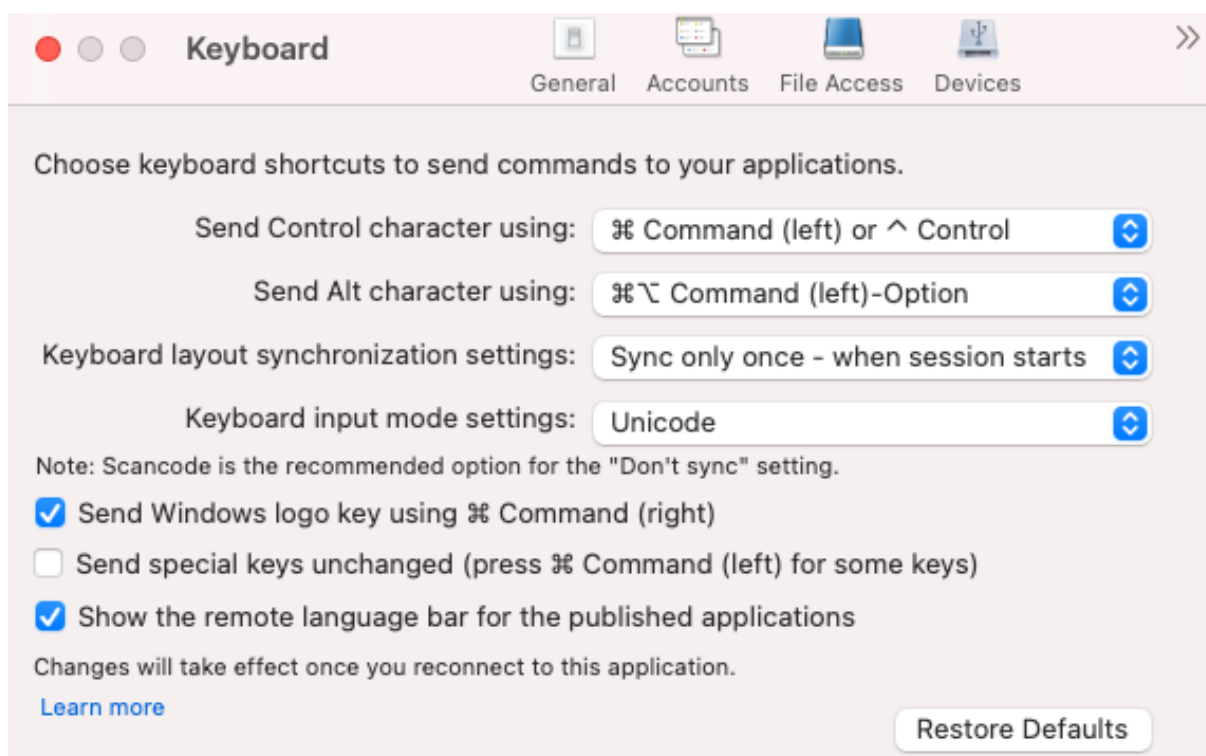
Gehen Sie wie folgt vor, um den Tastatureingabemodus über die GUI zu konfigurieren:

1. Klicken Sie über das Citrix Workspace-App-Symbol in der Menüleiste auf das Kontosymbol oben rechts und gehen Sie zu **Einstellungen > Tastatur**.

Die Einstellungen für den Tastatureingabemodus werden angezeigt.

2. Wählen Sie eine der folgenden Optionen:
 - **Scancode:** Sendet die Tastenposition von der clientseitigen Tastatur an den VDA, welcher das entsprechende Zeichen generiert. Wendet serverseitiges Tastaturlayout an
 - **Unicode:** Sendet die Taste von der clientseitigen Tastatur an den VDA, welcher das gleiche Zeichen auf dem VDA generiert. Wendet clientseitiges Tastaturlayout an.

Diese Erweiterung ist standardmäßig aktiviert.



Angenommen, Sie verwenden das Tastaturlayout USA international und der VDA das russische Tastaturlayout. Wenn Sie **Scancode** auswählen und die Taste neben der **Feststelltaste** drücken, wird der Scancode "1E" an den VDA gesendet. Der VDA verwendet dann "1E", um das Zeichen "ϕ" anzuzeigen. Wenn Sie **Unicode** wählen und die Taste neben **Feststelltaste** drücken, wird das Zeichen "a" an den VDA gesendet. Obwohl der VDA das russische Tastaturlayout verwendet, erscheint das Zeichen "a" auf dem Bildschirm.

Citrix empfiehlt den folgenden Tastatureingabemodus für die verschiedenen Tastaturlayoutsynchronisierungsoptionen:

- Scancodemodus für die Option **Nicht synchronisieren**.
- Modus "Unicode" für **Dynamische Synchronisierung zulassen** und **Nur einmal beim Sitzungsstart synchronisieren**

Hinweis:

Änderungen an der Tastaturkonfiguration werden wirksam, sobald Sie die Verbindung zur Anwendung wieder herstellen.

Sie können die Konfiguration des Tastatureingabemodus in der Citrix Workspace-App ändern. Um eine optimale Leistung zu erzielen, sollten Sie die von Citrix empfohlenen Modi die für verschiedene Szenarien, physische Tastaturen und Clientgeräte verwenden.

Weitere Informationen zu Konfigurationsdetails und Einschränkungen finden Sie unter [Verbesserungen des Tastatureingabemodus](#).

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 109.1.1.31, der auf Chromium Version 109 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Technical Preview

- Schnellscan
- Verbessertes Start von virtuellen Apps und Desktops
- Unterstützung für mehrere Audiogeräte

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Wenn Sie zwei XML-Dateien auf einem lokalen Mac-Client erstellen, öffnet der VDA möglicherweise die falsche XML-Datei. Beispielsweise öffnet der VDA die Datei Snapshot.xml anstelle der Datei SnapshotPopup.xml. [HDX-45326]
- Wenn Sie die aktiven Audiogeräte in den Toneinstellungen auf dem Endpunkt ändern, erhält Microsoft Teams möglicherweise keine Benachrichtigung über die Änderung. Aus diesem Grund kann Microsoft Teams die Änderungen nicht berücksichtigen. [HDX-47080]
- Citrix Viewer wird möglicherweise gelegentlich beendet, wenn Sie eine VDA-Sitzung schließen. [HDX-45668, HDX-47138]
- Die mit Citrix ADC konfigurierte Responder-Richtlinie funktioniert möglicherweise nicht mit der Citrix Workspace-App für Mac. Das Problem tritt auf, wenn die konfigurierte Richtlinie überprüft, ob der Benutzeragent **CWAWEBVIEW**, **Citrix Receiver** oder **Citrix Workspace** als Teilzeichenfolge gesendet hat, was nicht übereinstimmt. Benutzer werden daher möglicherweise zu einer anderen Citrix Gateway-URL umgeleitet. [CVADHELP-20519]
- Wenn Sie eine Verbindung zum Citrix Gateway Store herstellen und versuchen, sich bei der Citrix Workspace-App für Mac anzumelden, bleibt die Anmeldung möglicherweise hängen oder es wird für einige Zeit das Wartesymbol angezeigt. [CVADHELP-21323]
- Die Citrix Workspace-App für Mac kann eine Sitzung möglicherweise nicht starten, wenn die **Dateitypzuordnung** für eine App unter **Anwendungseinstellungen** in Citrix Studio festgelegt ist. [CVADHELP-21371]
- In der Citrix Workspace-App für Mac wird möglicherweise automatisch ein Anmeldefenster angezeigt, wenn Sie Ihr System einschalten oder neu starten. [CVADHELP-21484]

- Die Citrix Workspace-App für Mac wird möglicherweise unerwartet beendet, wenn die UWP-Apps (Universelle Windows-Plattform) innerhalb des VDI versuchen, sich mit der FIDO2-Authentifizierung zu authentifizieren. [CVADHELP-21576]
- Das Öffnen von Webressourcen kann fehlschlagen und es wird folgende Fehlermeldung angezeigt:

Wechseln Sie zu einem anderen Store mit den erforderlichen Berechtigungen. Wenn das Problem weiterhin besteht, wenden Sie sich mit den Fehlerdetails an Ihren Administrator.

[CVADHELP-21787]

- Die Citrix Workspace-App für Mac verwendet evtl. fälschlicherweise den Benutzeragent **CitrixReceiver** anstelle von **Citrix Workspace** als Teilzeichenfolge. Die Autorisierungsrichtlinien werden infolgedessen nicht befolgt. [CVADHELP-21969]
- Wenn Sie das Notchdisplay-Feature verwenden, kann es vorkommen, dass Textteile abgeschnitten werden. [CVADHELP-22134]
- Wenn Sie Citrix Enterprise Browser statt von einer neuen Registerkarte vom Dock aus öffnen, wird angezeigt, dass die Seite geladen wird. Geben Sie als Workaround die URL in die Adressleiste ein oder öffnen Sie eine weitere Registerkarte, um fortzufahren. [CTXBR-4706]
- Wenn Sie den Citrix Secure Private Access-aktivierten Store verwenden, wird beim Starten des veröffentlichten Inhalts möglicherweise dauerhaft ein Wartesymbol angezeigt. Das Problem tritt auf, wenn Citrix Enterprise Browser nicht auf dem Benutzergerät ausgeführt wird. Daher können Sie die veröffentlichten Inhalte nicht ansehen. [CTXBR-4813]

2301.1

Was ist neu

Im Release 2301.1 wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme

- Möglicherweise treten Probleme auf, wenn Sie einen Store hinzufügen oder authentifizieren oder eine Ressource (Apps oder Desktops) mit der nativen Citrix Workspace-App starten. [CVADHELP-22372]
- Das eingehende Video und die Bildschirmfreigabe funktionieren möglicherweise nicht bei für Microsoft Teams optimierten Videoanrufen. [HDX-50059]

Bekannte Probleme in Release 2301.1

- Sie können kein Update auf Version 2301.1 der Citrix Workspace-App für Mac mit dem automatischen Updatedienst durchführen. Als Workaround müssen Sie Version 2301.1 der Citrix Workspace-App für Mac manuell installieren, indem Sie die DMG-Datei herunterladen, die auf der Seite [Downloads](#) verfügbar ist.

2301

Was ist neu

Hintergrundunschärfe und Hintergrundersatz für Citrix Optimized Microsoft Teams

Citrix Optimized Microsoft Teams in der Citrix Workspace-App für Mac unterstützt jetzt Hintergrundunschärfe und das Ersetzen des Hintergrunds. Sie können das Feature verwenden, indem Sie in einer Besprechung oder einem Anruf **Mehr > Hintergrundeffekte anwenden** wählen.

Versionssteuerung für automatische Updates [Technical Preview]

Administratoren können jetzt angeben, auf welche Version der Citrix Workspace-App Geräte in der Organisation automatisch aktualisiert werden.

Hierfür legen sie den Versionsbereich im Global App Configuration Service mit den Eigenschaften "maximumAllowedVersion" und "minimumAllowedVersion" fest.

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

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12      Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        "category": "AutoUpdate",
```

```
19     "userOverride": false,
20     "assignedTo": [
21         "AllUsersNoAuthentication"
22     ],
23     "settings": [
24         {
25
26             "name": "Auto update plugins settings",
27             "value": [
28                 {
29
30                     "pluginName": "Citrix Workspace",
31                     "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
32                     "pluginSettings": {
33
34                         "deploymentMode": "Update",
35                         "upgradeToLatest": false,
36                         "minimumAllowedVersion": "23.04.0.36",
37                         "maximumAllowedVersion": "23.04.0.36",
38                         "delayGroup": "Medium",
39                         "detectRule": ""
40                     }
41                 }
42             ]
43         }
44     ]
45 }
46
47 ]
48 }
49
50 ]
51 }
52
53 }
54
55 }
56
57
58 <!--NeedCopy-->
```

Wenn der Bereich festgelegt ist, wird die Citrix Workspace-App auf dem Benutzergerät automatisch auf die höchste verfügbare Version aktualisiert, die im genannten Bereich liegt.

Wenn Sie die Citrix Workspace-App automatisch auf eine bestimmte Version aktualisieren möchten,

geben Sie im Global App Configuration Service in den Eigenschaften `maximumAllowedVersion` und `minimumAllowedVersion` zweimal dieselbe Version ein.

Hinweis:

- Um die Versionssteuerung für automatische Updates zu aktivieren, muss die Einstellung `upgradeToLatest` im Global App Configuration Service auf “false” gesetzt sein. Wenn die Einstellung “`upgradeToLatest`” auf “true” gesetzt ist, werden `maximumAllowedVersion` und `minimumAllowedVersion` ignoriert.
- Ändern Sie nicht die `PluginID`. Die `PluginID` ist der Citrix Workspace-App zugeordnet.
- Wenn die Version nicht im Global App Configuration Service konfiguriert ist, wird die Citrix Workspace-App standardmäßig auf die neueste verfügbare Version aktualisiert.
- Sie können nur die Versionsbereiche verwenden, die für ein Upgrade der Citrix Workspace-App festgelegt sind. Ein Downgrade wird nicht unterstützt.
- Dieses Feature wird ab Release 2301 unterstützt.

Sie können Feedback zu dieser Technical Preview mit diesem [Podio-Formular](#) geben.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserte automatische Updates [Technical Preview]

Mit dem Feature “Automatische Updates” wird die Citrix Workspace-App automatisch auf die neueste Version aktualisiert. Die Citrix Workspace-App sucht regelmäßig nach neuen Updates und lädt die neueste verfügbare Version der App herunter. Automatische Updates sind standardmäßig aktiviert, sofern sie nicht vom Administrator deaktiviert wurden.

Die Installation beginnt, wenn die Citrix Workspace-App oder die Sitzungen inaktiv sind.

Hinweis:

Während der Installation kann nicht auf die Citrix Workspace-App zugegriffen werden.

Beim Start der Citrix Workspace-App wird eine Benachrichtigung mit dem Status der Installation angezeigt.

Sie können das Feature “Automatische Updates” deaktivieren, indem Sie unter **Einstellungen > Erweitert > Updates** die Option **Workspace-App automatisch auf dem aktuellen Stand halten** deaktivieren.

tivieren.

Sie können Feedback zu dieser Technical Preview mit diesem [Podio-Formular](#) geben.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserte Unterstützung für Notchdisplays

Ab Version 2301 unterstützt die Citrix Workspace-App für Mac auch Macs mit Notchdisplay. Macs unterstützen ein natives Notchdisplay im Vollbildmodus für Retina-Displays und Multimonitoranzeigen. Der Sitzungsbereich auf dem Notchdisplay ist jetzt noch größer und bietet Kunden mehr Bildschirmfläche. Diese Verbesserung unterstützt auch eine hohe DPI-Skalierung. Die Mausposition wird auf allen externen Monitoren korrekt angezeigt.

Hinweis:

Stellen Sie sicher, dass die Option **Scale to fit below built-in camera** im Citrix Viewer nicht ausgewählt ist. Die Option ist standardmäßig deaktiviert und nur auf Macs mit Notchdisplay verfügbar.

Verbesserung von App Protection

Ab Version 2301 sichert das Feature "App Protection" auch die Citrix Workspace-App. Geschützt werden der Authentifizierungsbildschirm und der Bildschirm, der nach der Anmeldung an der Workspace-App zu sehen ist. Weitere Informationen finden Sie unter [App Protection](#).

Unterstützung für Global App Configuration Service-Kanal [Technical Preview]

Der Global App Configuration Service für Citrix Workspace ermöglicht Citrix-Administratoren, Workspace-Dienst-URLs und Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen. Weitere Informationen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

Administratoren können mit dem Global App Configuration Service jetzt Einstellungen definieren, die nur für bestimmte Benutzergruppen gelten. Dieses Feature stellt sicher, dass manche Funktionen je nach Bedarf nur bestimmten Benutzern zur Verfügung stehen.

Sie können Feedback zu dieser Technical Preview mit diesem [Podio-Formular](#) geben.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserte Unterstützung der Menüleiste

Ab Version 2301 wird die macOS-Option **Automatically hide and show the menu bar in full screen** vollständig durch die Citrix Workspace-App unterstützt. Für Versionen vor macOS 13 müssen Sie unter **System Preferences > Dock & Menu Bar** die Option **Automatically hide and show the menu bar in full screen** deaktivieren. Für macOS 13 und neuere Versionen müssen Sie unter **System Preferences > Desktop & Dock** die Option **Automatically hide and show the menu bar in full screen** deaktivieren. Sie können diese Option entweder aktivieren oder deaktivieren. Diese Verbesserung unterstützt auch eine hohe DPI-Skalierung. Die Mausposition wird auf allen externen Monitoren korrekt angezeigt.

Die folgende Abbildung zeigt ein Fenster mit ausgeblendeter Menüleiste.



Die folgende Abbildung zeigt ein Fenster mit angezeigter Menüleiste.



Citrix Enterprise Browser

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 Arbeitslinks zu öffnen. Sie können einen anderen Browser zum Öffnen nicht arbeitsbezogener Links auswählen.

Ein Arbeitslink ist den Web- oder SaaS-Apps zugeordnet, die der Administrator für den Endbenutzer konfiguriert. 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 jedem vom Endbenutzer gewählten Browser geöffnet.

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

Behobene Probleme

- Das HTTP Live Streaming (HLS)-Protokoll mit AAC-HE-Stream (High Efficiency Advanced Audio Coding) kann Audio im Citrix Enterprise Browser nicht wiedergeben. [CTXBR-3899]
- Wenn Sie im benutzerdefinierten Portal auf einen Hyperlink klicken, wird vor dem Öffnen des Links eine Fehlermeldung angezeigt. Danach wird der Link nicht in Citrix Enterprise Browser, sondern in einem Systembrowser (z. B. Google Chrome) geöffnet. [CTXBR-4051]
- Wenn Sie die Citrix Workspace-App für Mac mit einer benutzerdefinierten Webstore-URL verwenden, werden die Versionen des Betriebssystems und der Citrix Workspace-App möglicherweise nicht in der User-Agent-Zeichenfolge angezeigt. [CVADHELP-21377]
- Dieser Fix kann in einigen Fällen verhindern, dass bestimmte Apps von Drittanbietern wie Epic oder Kronos beim Start einfrieren. [HDX-46140]
- Wenn Sie zum ersten Mal eine Sitzung mit einer ICA-Datei aus der Betaversion der Citrix Workspace-App 2301 für Mac starten, wird die Sitzung möglicherweise unerwartet beendet. [HDX-47361]
- Wenn Sie die benutzerdefinierte Portalwebsite zur Citrix Workspace-App für Mac hinzufügen, wird möglicherweise eine leere Seite angezeigt. [RFMAC-12857]

2211.1

Was ist neu

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

Behobene Probleme

- Möglicherweise treten Probleme auf, wenn Sie einen Store hinzufügen oder authentifizieren oder eine Ressource (Apps oder Desktops) mit der nativen Citrix Workspace-App starten. [CVADHELP-22372]
- Das eingehende Video und die Bildschirmfreigabe funktionieren möglicherweise nicht bei für Microsoft Teams optimierten Videoanrufen. [HDX-50059]

2211

Was ist neu

Workspace-Apps werden beim Öffnen im Dock mit nativen App-Symbolen angezeigt [Technical Preview]

Dieses Feature ist ab Version 2211 standardmäßig deaktiviert.

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Verbessertes Mission Control- und App Expose-Erlebnis [Technical Preview]

Dieses Feature ist ab Version 2211 standardmäßig deaktiviert.

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

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](#).

Behobene Probleme

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

2210

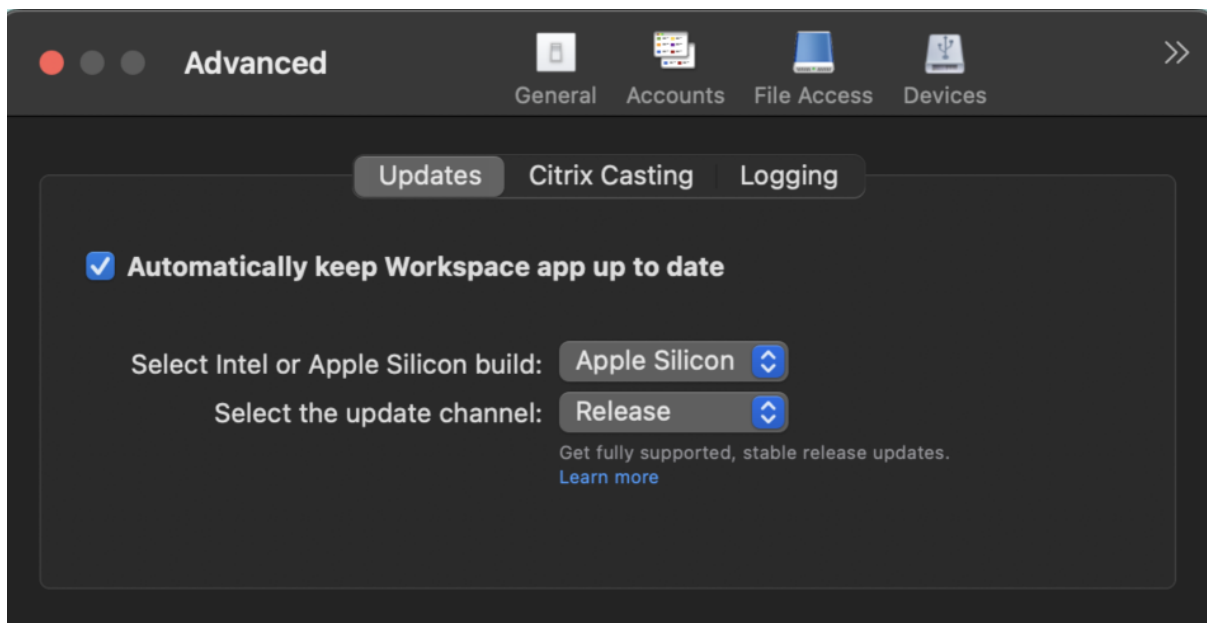
Was ist neu

Unterstützung für macOS 13 Ventura

Die Citrix Workspace-App für Mac wird unter macOS 13 Ventura (13.0) unterstützt.

Verbesserte automatische Updates auf Mac mit Apple Silicon (M1 Series)

Ab dieser Version können Sie beim Download des Universal Architecture-Builds zwischen Apple Silicon- und Intel-Builds zur Unterstützung von Apple Silicon- und Intel-basierten Mac-Maschinen wählen.



Auf Apple Silicon-Maschinen haben Benutzer die Option, Intel-Build automatisch zu aktualisieren, selbst wenn sie den Apple Silicon-Build heruntergeladen haben. Die Option wird auf der Registerkarte **Einstellungen** angeboten.

Erweiterte Konfiguration für automatische Updates

Sie können automatische Updates von Citrix Workspace auf Mac mit Apple Silicon (M1 Series) mit folgenden Methoden konfigurieren:

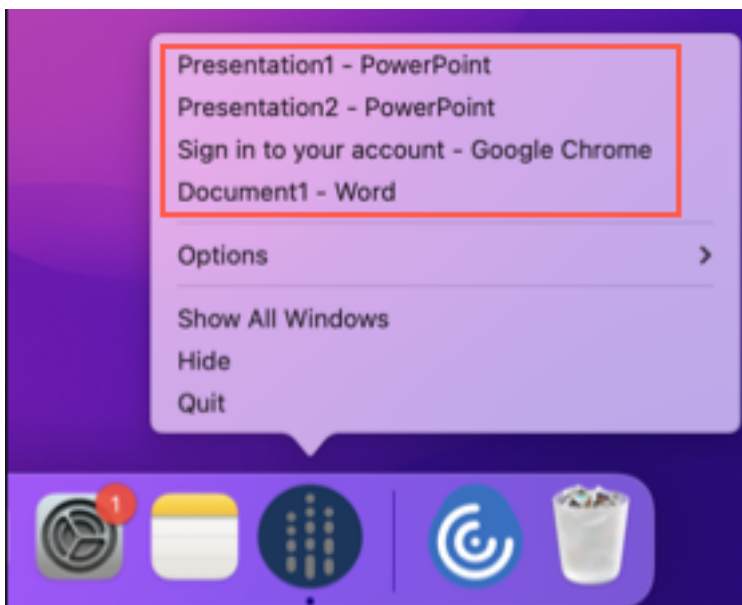
- Grafische Benutzeroberfläche
- Global App Configuration Service (GACS)
- Mobilgeräteverwaltung (MDM)
- StoreFront

Weitere Informationen finden Sie unter [Erweiterte Konfiguration für automatische Updates](#).

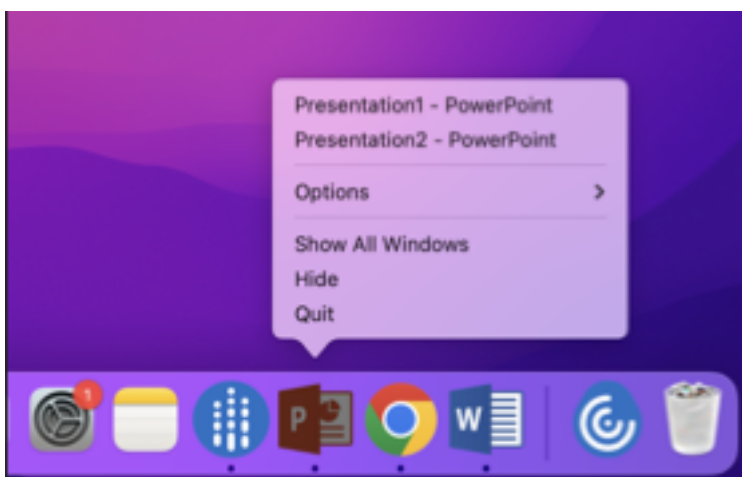
Workspace-Apps werden beim Öffnen im Dock mit nativen App-Symbolen angezeigt [Technical Preview]

Bisher hat das Klicken auf virtuelle Apps in der Citrix Workspace-App den Citrix Viewer ausgelöst, in dem die Apps verfügbar waren. Wenn Sie viele Apps öffnen, werden die Apps oder die Instanzen im

Citrix Viewer geöffnet. Zum Anzeigen der geöffneten Apps klicken Sie mit der rechten Maustaste auf das Citrix Viewer-Symbol.



Ab dieser Version werden virtuelle Apps, die Sie öffnen, im Dock mit den entsprechenden Symbolen angezeigt und sind leicht identifizierbar. Sie können dann über das Dock auf die virtuelle App zugreifen. Wenn Sie mehrere Instanzen einer App öffnen, werden diese im Dock nicht dupliziert, sondern in einer Instanz im Dock angeordnet.



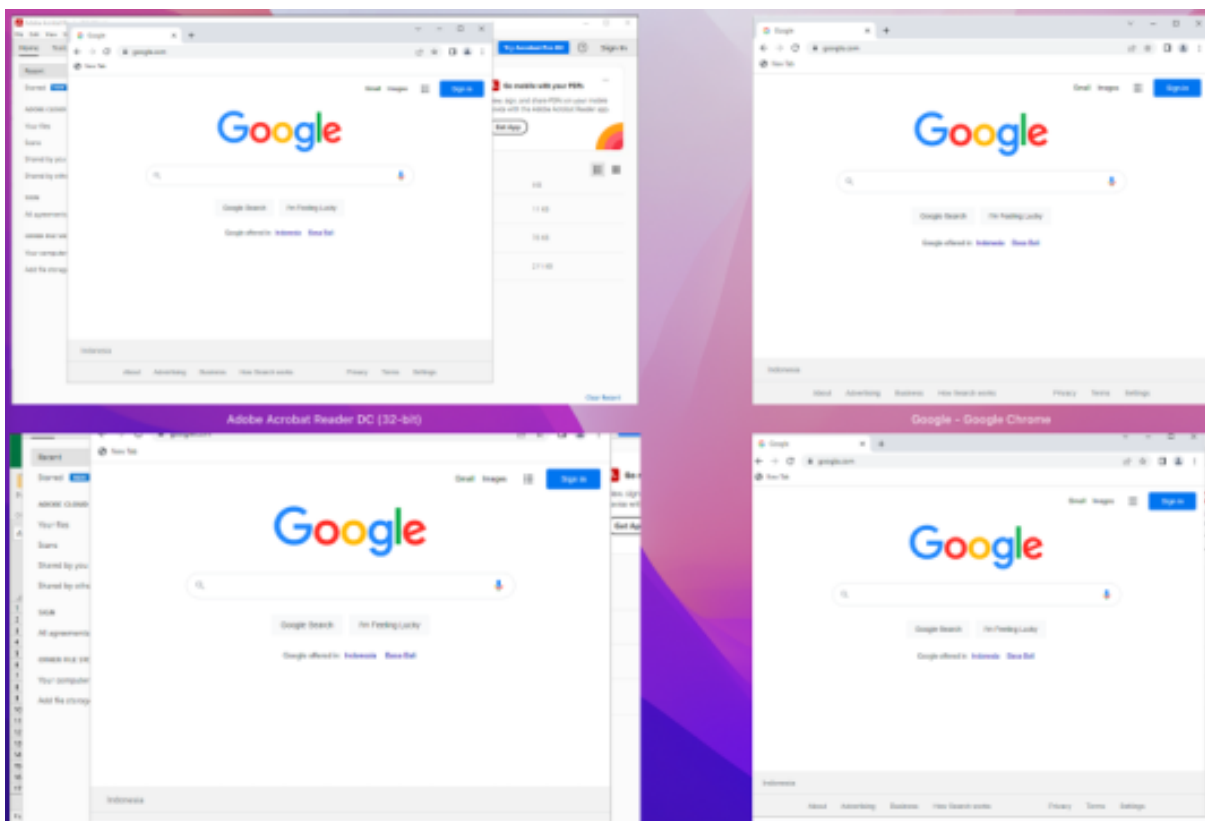
Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in

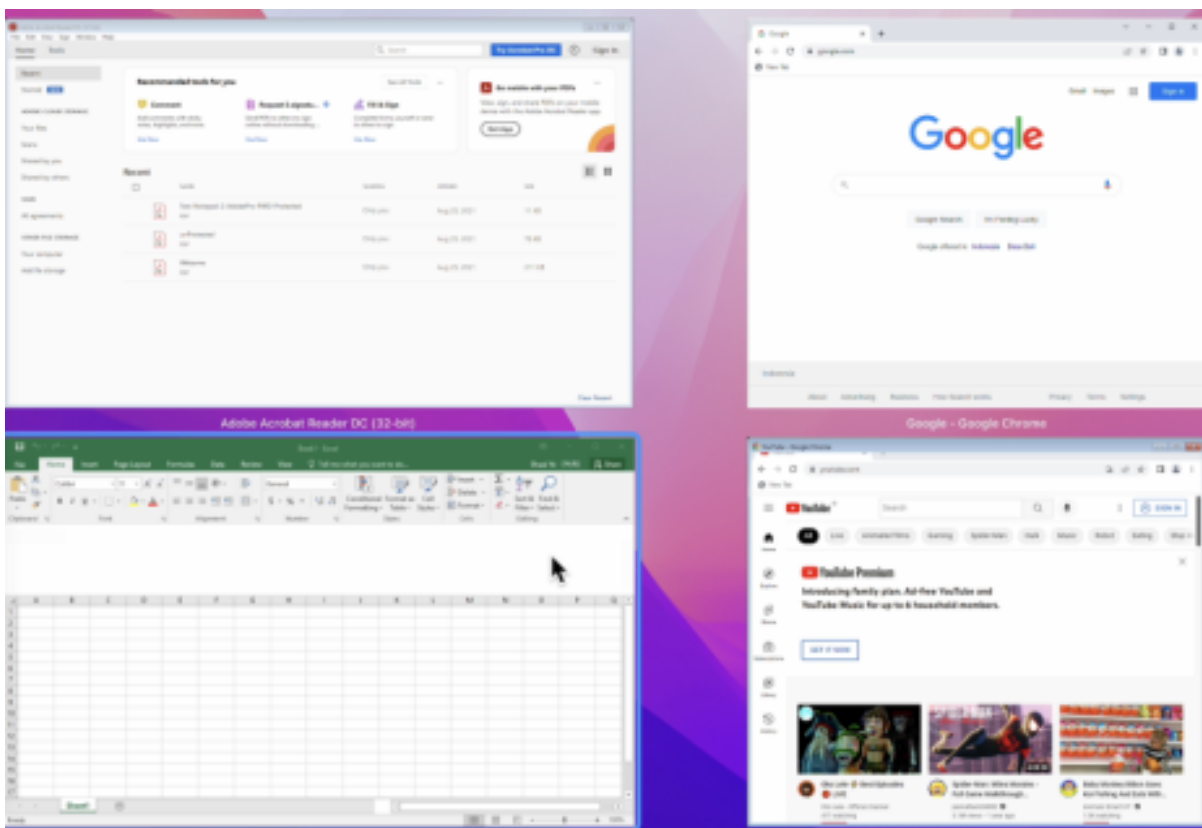
Produktionsumgebungen bereitgestellt werden dürfen.

Verbessertes Mission Control- und App Expose-Erlebnis [Technical Preview]

Bisher führte die Verwendung des Features **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung zu einer großen Zahl überlappender Fenster.



Wenn Sie ab dieser Version das Feature **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung verwenden und viele Fenster öffnen, überlappen sich die Fenster nicht und stehen übersichtlich zur Verfügung.



Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserte Grafikleistung [Technical Preview]

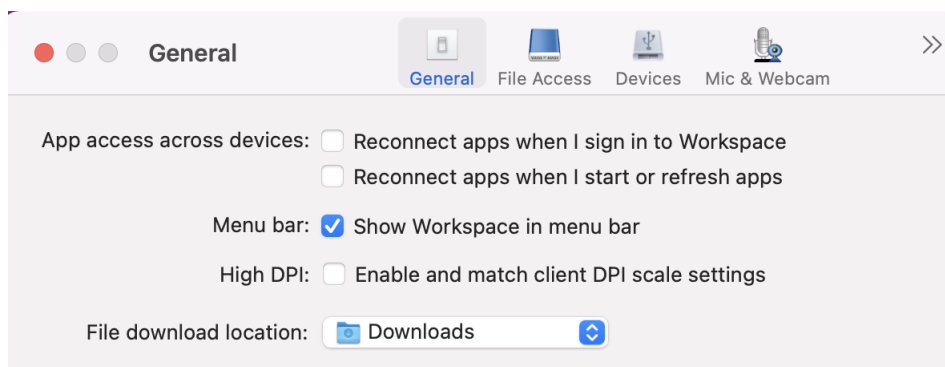
Ab dieser Version ist die Grafikleistung für Desktopsitzungen besser.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Unterstützung für hohe DPI-Werte

Sie können die DPI-Skalierungseinstellungen des Clients jetzt aktivieren und anpassen, indem Sie die Sitzungssymbolleiste starten und zu **Einstellungen > Allgemeines > Hoher DPI-Wert** gehen. Die Option "Hoher DPI-Wert" ist standardmäßig deaktiviert.



Unterstützung für die Konfiguration von Benutzergeräten durch Administratoren per MDM

Administratoren können bei der Bereitstellung der Citrix Workspace-App mit einem beliebigen MDM-Tool (z. B. Citrix Endpoint Management) jetzt die folgenden Einstellungen konfigurieren:

- **StoreURLs:** Konfigurieren Sie Details des Stores, damit er zur Vereinfachung der Anmeldung automatisch hinzugefügt wird, wenn der Benutzer die Citrix Workspace-App öffnet.

Geben Sie zum Hinzufügen eines Stores die Details für die Einstellung **StoreURLs** ein. Beispiel:
<string>https://myorg.com/Org/storename</string>

- **BlockStoreAddition:** Verhindert, dass Benutzer Stores hinzufügen.

Um zu verhindern, dass Benutzer einen Store hinzufügen, legen Sie den Wert der Einstellung **BlockStoreAddition** auf **True** fest.

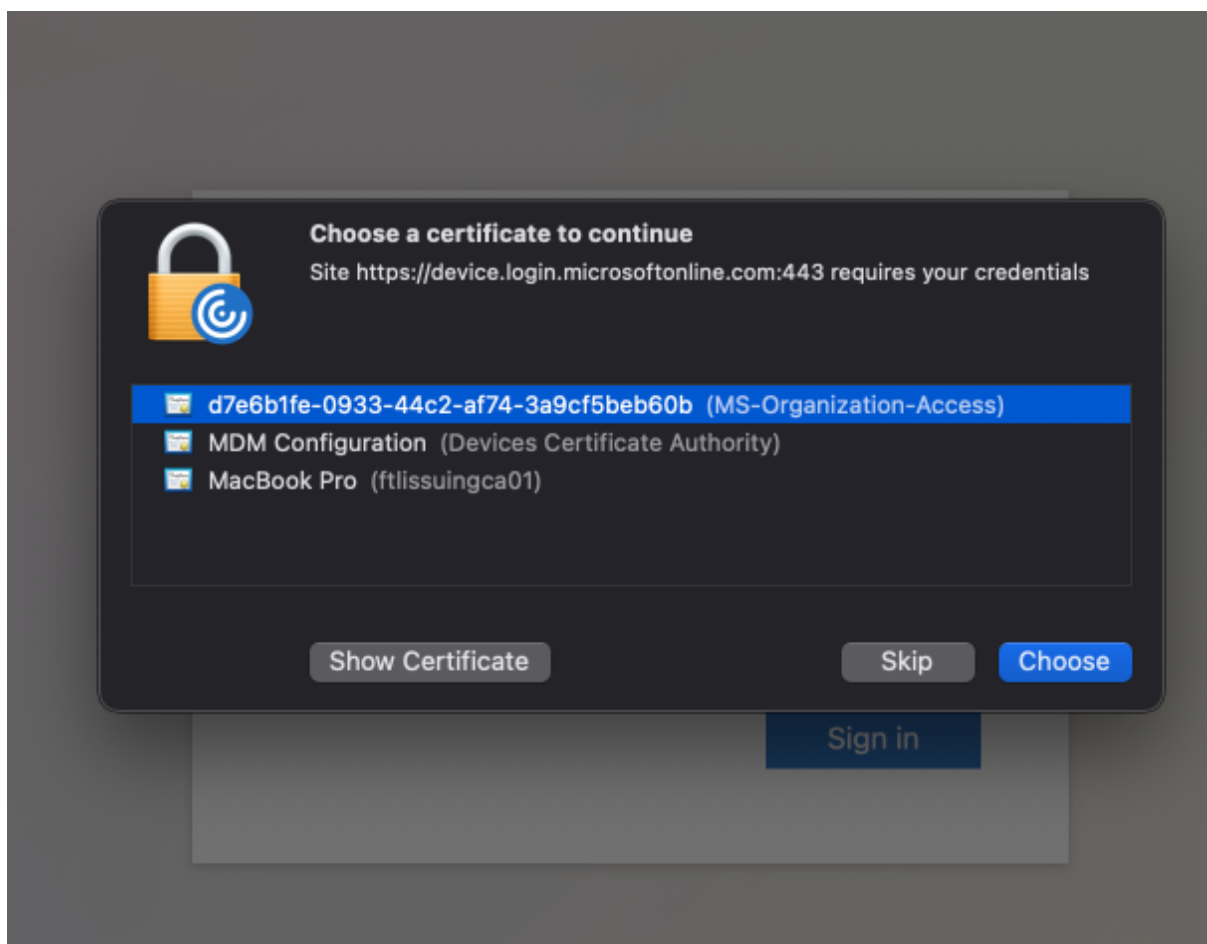
Unterstützung für die zertifikatbasierte Authentifizierung [Technical Preview]

Sie können sich jetzt mit einem Clientzertifikat bei der Citrix Workspace-App (Cloudstores) authentifizieren.

Bisher wurde die zertifikatbasierte Authentifizierung für On-Premises-Umgebungen unterstützt und Cloud-Kunden konnten sich nicht bei der Citrix Workspace-App anmelden. Das Feature ist standardmäßig deaktiviert und Administratoren müssen sich an den Citrix Helpdesk wenden, um dieses Feature zu aktivieren, indem sie dieses Anforderungsformular ausfüllen.

Wenn für Ihre Organisation bedingter Zugriff mit Azure Active Directory konfiguriert wurde, wird der Benutzer bei der Anmeldung aufgefordert, ein Clientzertifikat für die Authentifizierung auszuwählen. Die zertifikatbasierte Authentifizierung bildet eine zusätzliche Sicherheitsebene und gewährleistet, dass das Gerät richtlinientreu ist.

Wenn Sie einen Store hinzufügen und gültige Anmeldeinformationen für diesen Store eingeben, zeigt die Citrix Workspace-App eine Liste gültiger Zertifikate in Ihrem Schlüsselbund für die Clientauthentifizierung an. Umfasst der Schlüsselbund nur ein gültiges Zertifikat, wird es standardmäßig ausgewählt.



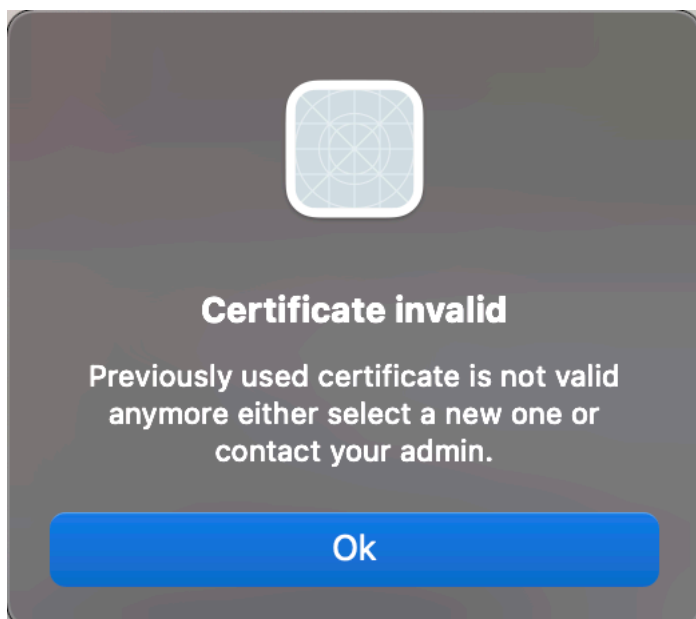
Wenn Sie ein Zertifikat auswählen, überprüft der Identitätsanbieter es und der Workspace-App-Store wird bei erfolgreicher Validierung angezeigt.

Hinweis:

- Wenn im Schlüsselbund keine gültigen Zertifikate vorhanden sind, führt die Citrix Workspace-App die Standardverarbeitung für die Zertifikatauthentifizierungsanforderung vom Server durch.
Die Benutzer können sich dann möglicherweise nicht anmelden.
- Wenn für Ihr Unternehmen ein bedingter Zugriff mit Azure Active Directory konfiguriert ist und keine gültigen Zertifikate im Schlüsselbund gefunden werden, können Sie sich nicht bei der Citrix Workspace-App anmelden.

Wenn ein zuvor ausgewähltes Zertifikat nicht mehr gültig ist, wird eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, ein gültiges Zertifikat auszuwählen oder sich an den Administrator zu

wenden, wenn es keines gibt.



Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

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.
- Zugehörige Produktdokumentation

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 105.1.1.19, der auf Chromium Version 105 basiert. Weitere Informationen zum Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#). Andere Ressourcen (z. B. Videos und Blogposts), die von dieser Produktdokumentation verlinkt werden, verwenden möglicherweise weiterhin die früheren Namen.

Citrix Enterprise Browser zum Arbeitsbrowser machen [Technical Preview]

Sie können Citrix Enterprise Browser jetzt zum Öffnen aller geschäftlichen oder Unternehmenslinks und -Apps konfigurieren, die von Ihrem Administrator in der Citrix Workspace-App konfiguriert wurden. Mit diesem Feature können Sie gezielt nur Arbeitslinks oder Web- und SaaS-Anwendungen in Citrix Enterprise Browser öffnen.

Sie können einen anderen Browser auswählen, um nicht arbeitsbezogene Links oder Anwendungen zu öffnen.

Alle Web- und SaaS-Anwendungen über Citrix Enterprise Browser öffnen

Ab dieser Version werden alle internen Web-Apps und externen SaaS-Apps, die in der Citrix Workspace-App verfügbar sind, in Citrix Enterprise Browser geöffnet.

Unterstützung für Browsererweiterungen [Technical Preview]

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. Weitere Einstellungen finden Sie unter [Global App Configuration Service](#).

Hinweis:

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Informationen zur Konfiguration finden Sie in der Dokumentation zum [Citrix Enterprise Browser](#).

Citrix Enterprise Browser mit dem Global App Configuration Service verwalten [Technical Preview]

Der Administrator kann mit dem Global App Configuration Service für Citrix Workspace 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 Global App Configuration Service 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.

Hinweise:

- Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.
- Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.
- Bei Namen-/Wertpaaren wird zwischen Groß- und Kleinschreibung unterschieden.
- Alle Browsereinstellungen im [Global App Configuration Service](#) sind in der folgenden Kategorie:

```
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](#).

Technical Preview

- Aktualisierte Version von WebRTC für optimiertes Microsoft Teams

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Die Citrix Workspace-App kann den Neustart oder das Herunterfahren eines Mac-Geräts unterbrechen. [RFMAC-12530]
- Die Umschalttaste funktioniert möglicherweise in der Version 2206 der Citrix Workspace-App für Mac nicht wie erwartet. [CVADHELP-20674]

2209

Was ist neu

Beim Schließen der Citrix Workspace-App vom benutzerdefinierten Webstore abmelden

Wenn die Einstellung **signoutCustomWebstoreOnExit** auf **True** festgelegt ist, werden Sie beim Schließen des Fensters der Citrix Workspace-App vom benutzerdefinierten Webstore abgemeldet. Wenn Sie die Citrix Workspace-App wieder öffnen, wird die Webstore-URL erneut geladen. Sie können die Einstellung **signoutCustomWebstoreOnExit** im Global App Configuration Service konfigurieren.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser (früher “Citrix Workspace 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](#).

Behobene Probleme

- Die Citrix Workspace-App für Mac wird möglicherweise automatisch gestartet, wenn Sie die Citrix Workspace-App für Mac neu starten oder die Citrix Workspace-App installieren. [RFMAC-12392]

- Die Bildschirmfreigabe im optimierten Microsoft Teams für bestimmte Apps von Drittanbietern schlägt möglicherweise in der Citrix Workspace-App für Mac fehl. Das Problem tritt auf, wenn die Thinwire-Codec-Richtlinie auf **Für den gesamten Bildschirm** festgelegt ist. Infolgedessen ist die App-Freigabe deaktiviert und im Freigabebereich sind keine Optionen verfügbar. [CVADHELP-20853]

2208.1

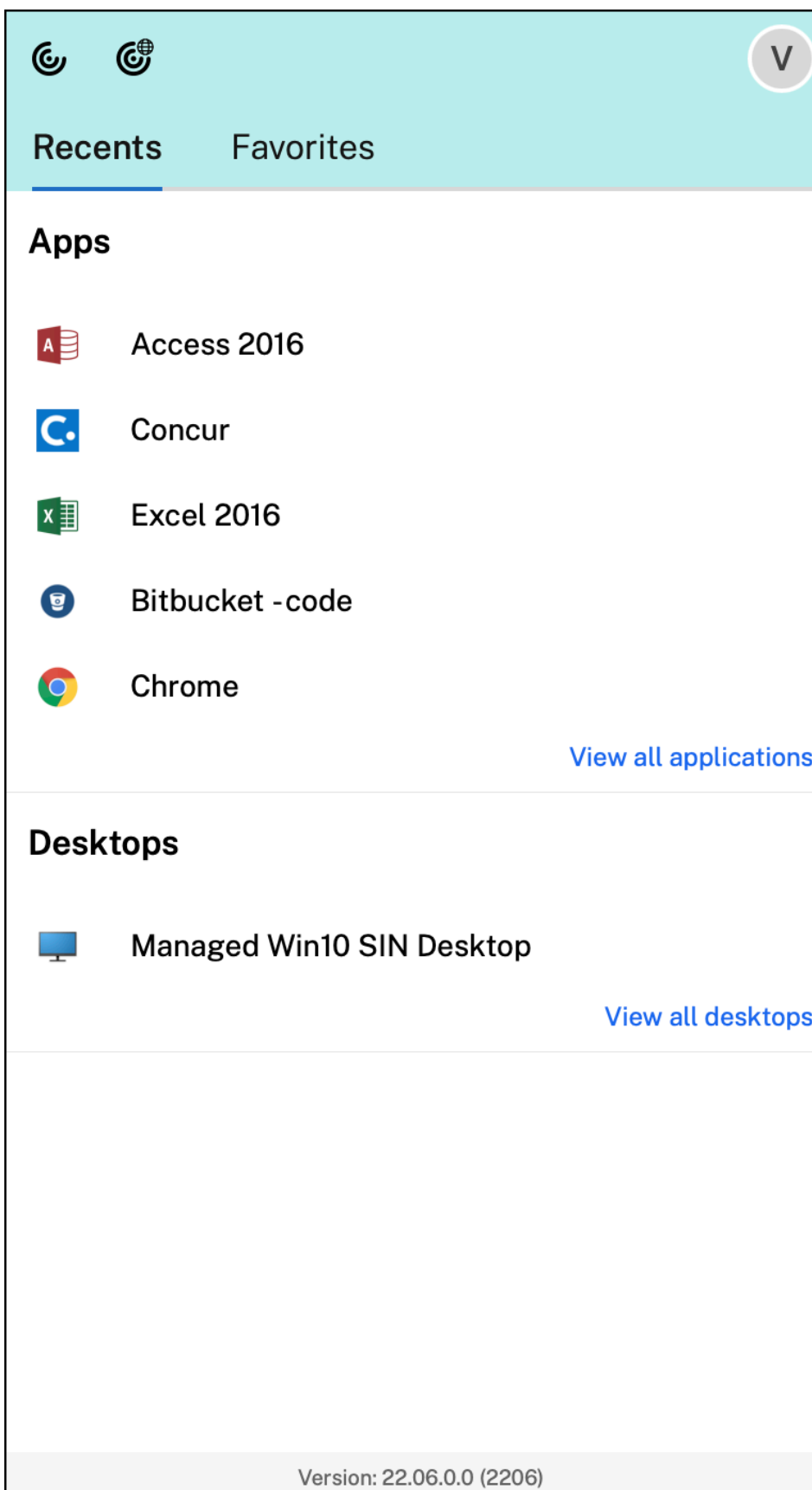
Was ist neu

Schnellzugriff auf Apps, Desktops und Citrix Enterprise Browser über die Menüleiste

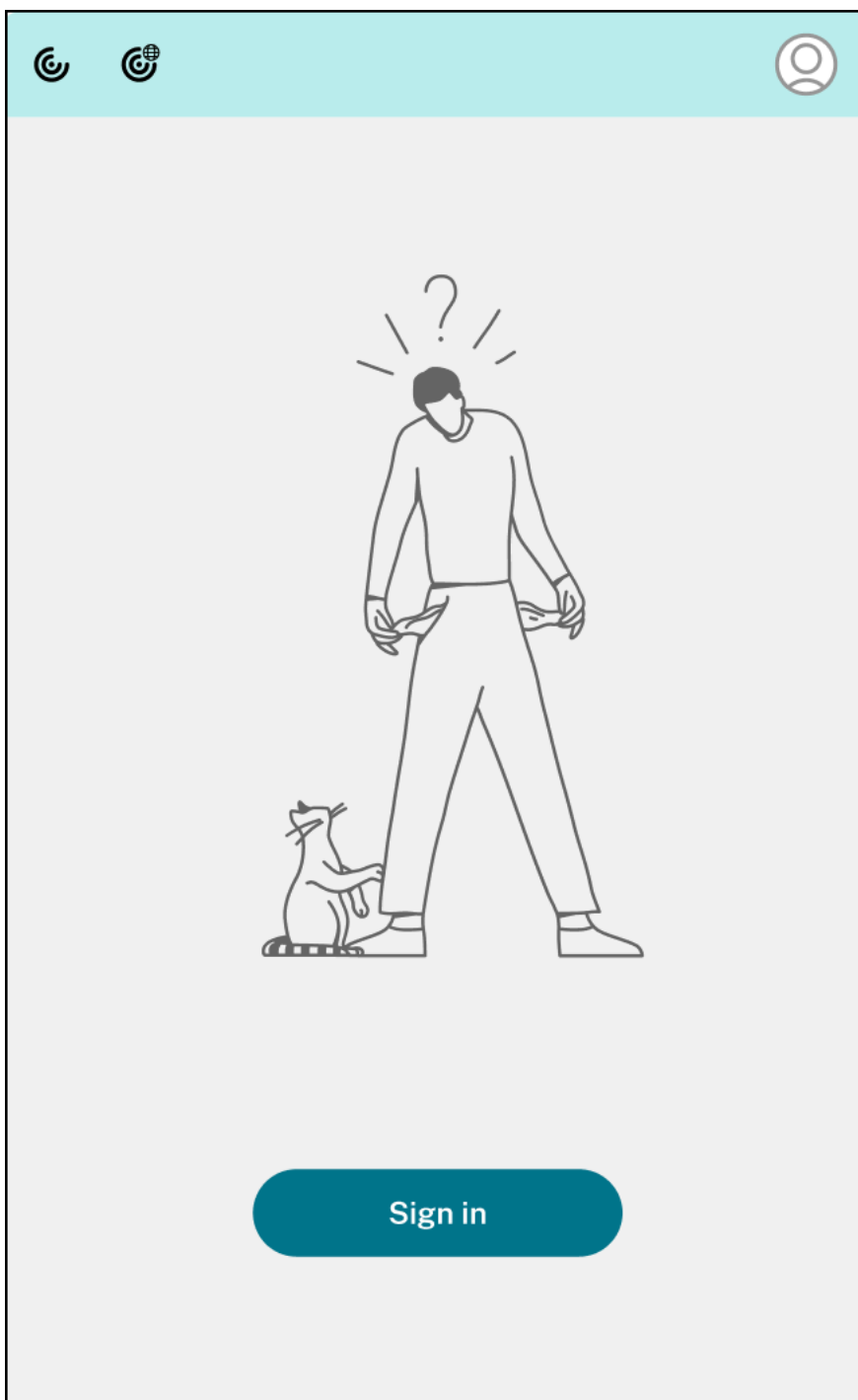
Sie können jetzt bevorzugte oder zuletzt verwendete Apps und Desktops anzeigen oder ein Citrix Enterprise Browser-Fenster öffnen, indem Sie in der Menüleiste auf das Citrix Workspace-Symbol klicken. So erhalten Sie Zugriff auf einige Ihrer Ressourcen, ohne die Citrix Workspace-App öffnen zu müssen.

Hinweis:

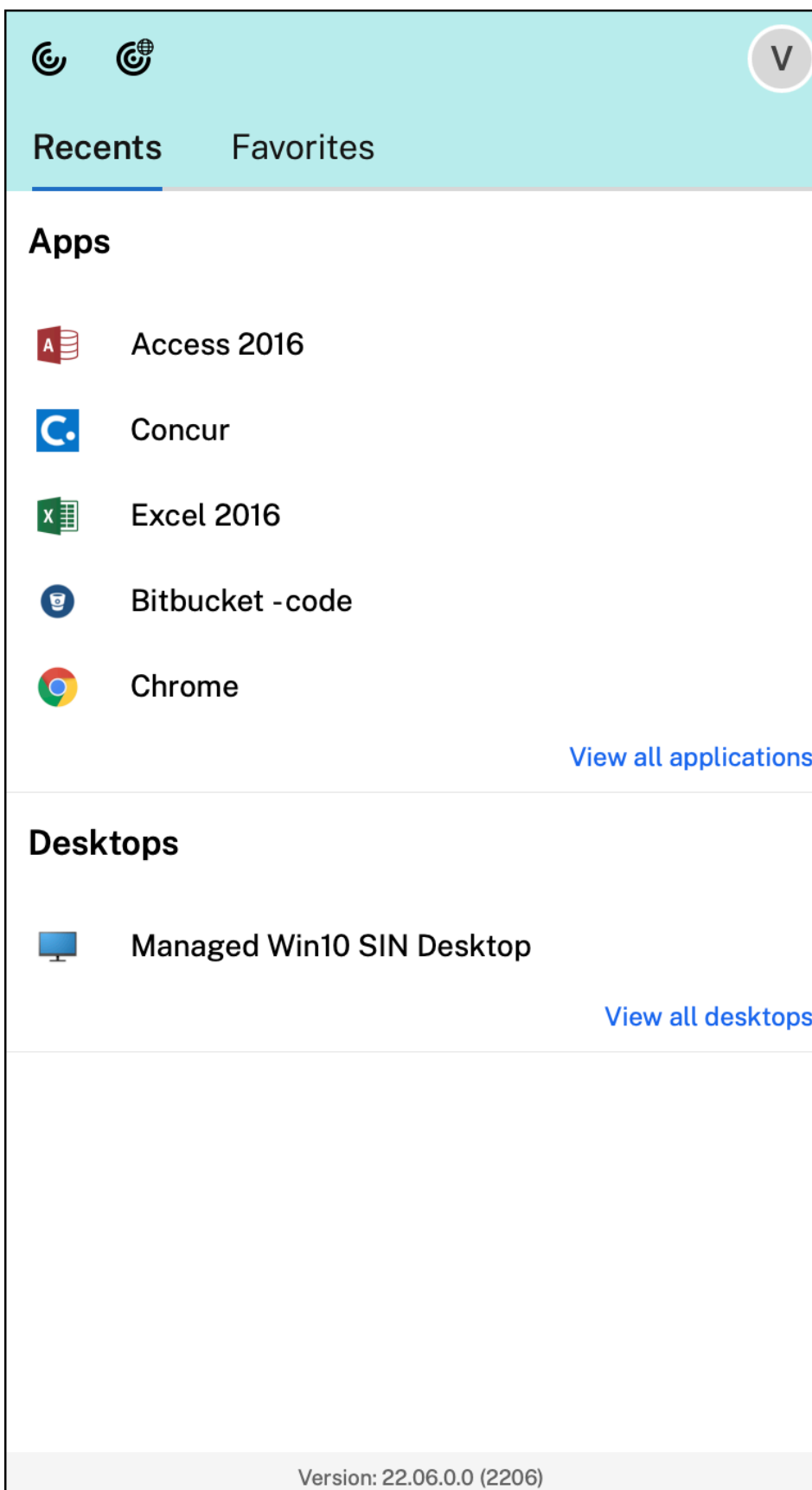
Dieses Feature ist nicht für On-Premises-Bereitstellungen verfügbar.



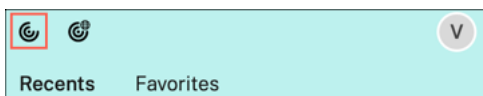
Wenn Sie keine Konten konfiguriert haben, wird eine Anmeldeaufforderung angezeigt.



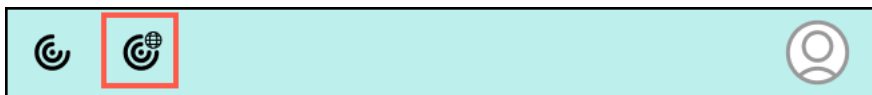
In den Optionen auf den Registerkarten **Zuletzt verwendet** bzw. **Favoriten** werden maximal 5 bevorzugte oder zuletzt verwendete Apps oder Desktops angezeigt. Um die übrigen Apps in der Citrix Workspace-App anzuzeigen, klicken Sie auf **Alle Anwendungen anzeigen**. Um die übrigen Desktops in der Citrix Workspace-App anzuzeigen, klicken Sie auf **Alle Desktops anzeigen**.



Sie können die Citrix Workspace-Benutzeroberfläche öffnen, indem Sie auf das Symbol der Citrix Workspace-App klicken.

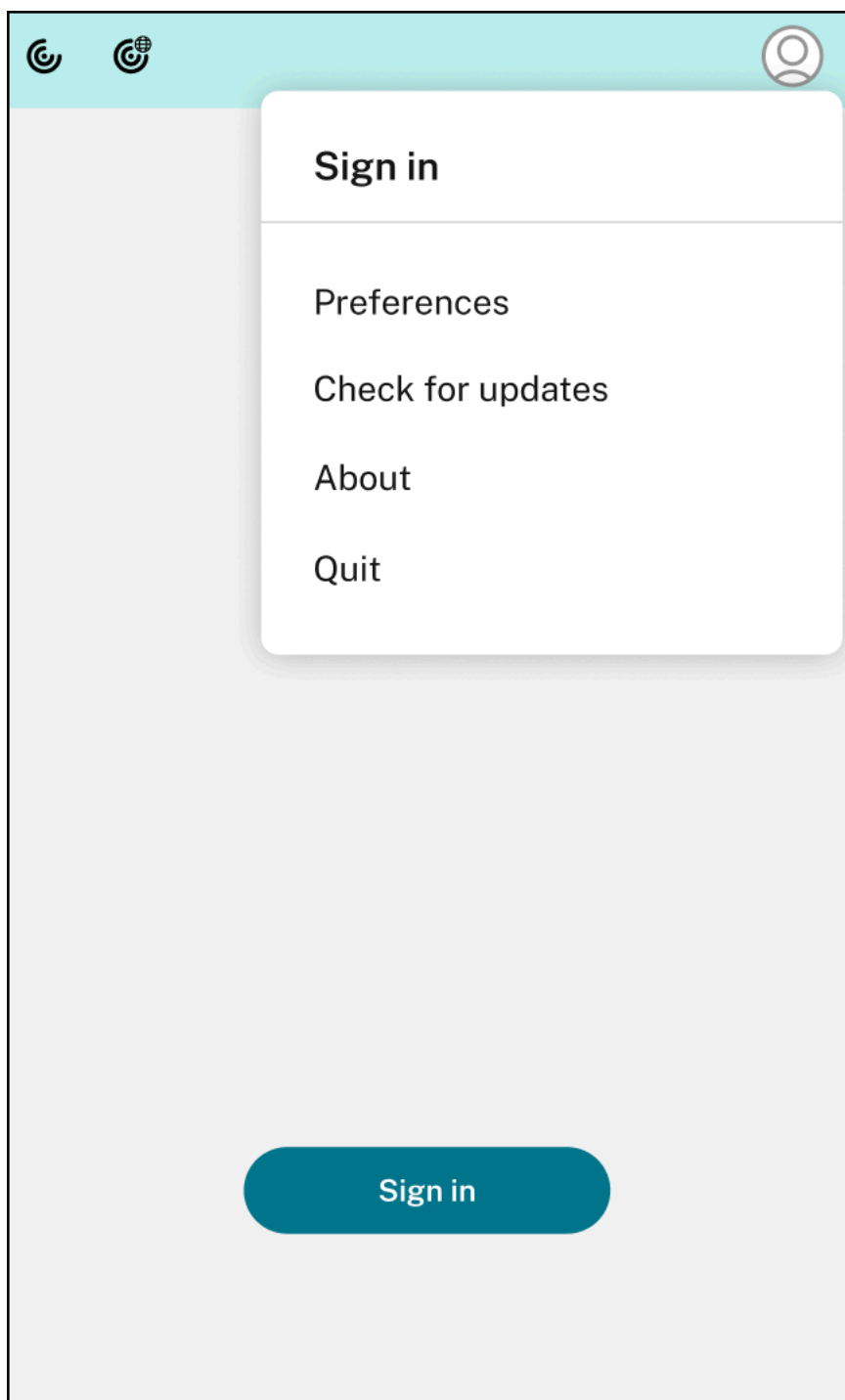


Sie können Citrix Enterprise Browser öffnen, ohne eine Web- oder SaaS-App zu öffnen. Klicken Sie hierfür auf das Citrix Enterprise Browser-Symbol.



Hinweis:

Der Citrix Enterprise Browser ist nicht verfügbar, wenn der konfigurierte Store keine Web- oder SaaS-Apps enthält. Er ist zudem nur dann verfügbar, wenn Ihr Administrator Citrix Secure Private Access konfiguriert hat.



Folgende Optionen werden angezeigt, wenn Sie auf das **Kontosymbol** in der oberen rechten Ecke klicken:

- Einstellungen
- Nach Updates suchen
- Info
- Beenden

Unterstützung für Authentifizierung mit FIDO2 [Technical Preview]

Bei dieser Version können sich Benutzer innerhalb einer HDX-Sitzung mit kennwortlosen FIDO2-Sicherheitsschlüsseln authentifizieren. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Desktops, die FIDO2 unterstützen, authentifizieren. Weitere Informationen zu FIDO2 finden Sie unter [FIDO2-Authentifizierung](#).

Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code und Touch-Funktionen. Sie können die Authentifizierung mit FIDO2-Sicherheitsschlüsseln konfigurieren. Informationen zu den Voraussetzungen und zur Verwendung dieses Features finden Sie unter [Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2](#).

Beim Zugriff auf eine App oder Website, die FIDO2 unterstützt, wird eine Aufforderung zur Eingabe des Sicherheitsschlüssels angezeigt. Wenn Sie Ihren Sicherheitsschlüssel zuvor mit einer PIN registriert haben (4 bis 64 Zeichen), müssen Sie die PIN bei der Anmeldung eingeben.

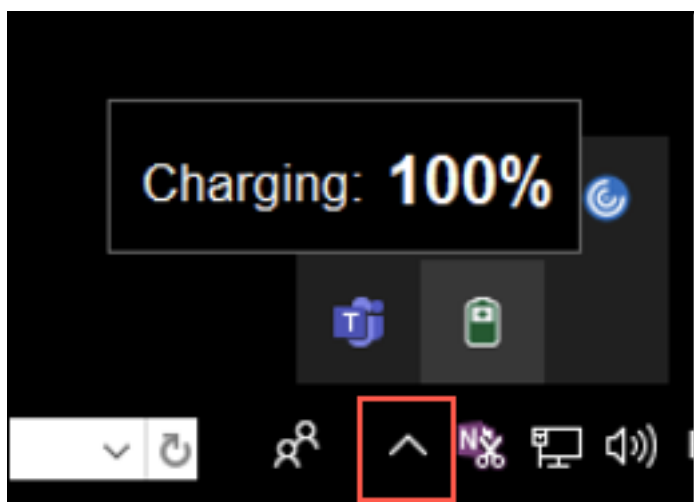
Wenn Sie Ihren Sicherheitsschlüssel zuvor ohne PIN registriert haben, tippen Sie einfach auf den Sicherheitsschlüssel, um sich anzumelden.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Akkustatusanzeige

Der Akkustatus des Geräts wird jetzt im Infobereich einer Citrix Desktop-Sitzung angezeigt. Um den Akkustatus innerhalb der Desktopsitzung anzuzeigen, klicken Sie in der Taskleiste auf den Pfeil zur Anzeige **ausgeblendeter** Symbole.



Hinweis:

Die Akkustatusanzeige wird für Server-VDA's nicht angezeigt.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 103.1.1.14, 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 103.1.1.14 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.

Öffnen aller Web- und SaaS-Ap's über Citrix Enterprise Browser [Technical Preview]

Ab dieser Version werden alle internen Web-Ap's und externen SaaS-Ap's, die in der Citrix Workspace-App verfügbar sind, in Citrix Enterprise Browser geöffnet. Sie können sich mit diesem [Podio-Formular](#) für die Technical Preview registrieren.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Behobene Probleme

- Wenn die Citrix Workspace-Anmeldeaufforderung angezeigt wird, kann das Pop-upfenster nicht durch Klicken auf die Schaltfläche "Abbrechen" geschlossen werden und wird wiederholt angezeigt. [CVADHELP-19919]
- Wenn Sie die direkte Workloadverbindung in Citrix Cloud verwenden, um sich direkt mit VDAs zu verbinden, wird ein schwarzer Bildschirm angezeigt, und Sie werden vom VDA getrennt. Dieses Problem tritt auf, wenn der Netzwerkpositionsdienst (NLS) aktiviert ist. [HDX-40588]
- Wenn Sie eine Multitouch-Geste verwenden, um zwischen Apps im Vollbildmodus zu wechseln, wird das Sitzungsfenster des Citrix Workspace-Desktops kurzzeitig schwarz. Dieses Problem tritt bei Macs mit Notchdisplay auf. [HDX-42314]

2206.1

Was ist neu

Deinstallation der Citrix Workspace-App durch Ziehen des App-Symbols in den Papierkorb

Die Citrix Workspace-App wird jetzt vollständig deinstalliert, wenn Sie das Symbol der App in den Papierkorb verschieben.

Bisher wurde durch Ziehen des Workspace-App-Symbols in den Papierkorb die App entfernt, aber bestimmte Systemdateien auf Ihrem Mac wurden zurückgelassen. Ab dieser Version werden die Citrix Workspace-App und alle zugehörigen Dateien von Ihrem Gerät entfernt, wenn Sie das Symbol in den Papierkorb ziehen.

Mit den folgenden Schritten deinstallieren Sie die Citrix Workspace-App, indem Sie sie in den Papierkorb verschieben:

1. Schließen Sie die Citrix Workspace-App, falls sie ausgeführt wird.
2. Ziehen Sie die Citrix Workspace-App in den Papierkorb.
Alternativ können Sie mit der rechten Maustaste auf die Citrix Workspace-App klicken und **Optionen > In Papierkorb verschieben** auswählen.

3. Geben Sie auf Aufforderung Ihre Systemanmeldeinformationen ein.
4. Schließen Sie alle laufenden Apps (Citrix Workspace) und klicken Sie zur Bestätigung auf **Weiter**. Die Citrix Workspace-App und alle ihre Systemdateien werden von Ihrem Gerät gelöscht.

Unterstützung für Servicekontinuität im Safari-Browser

Die Citrix Workspace-Servicekontinuität von Citrix Workspace wird jetzt für den Safari-Browser unterstützt. Benutzer müssen die Citrix Workspace-App für Mac und die Citrix Workspace-Webextension installieren. Die Servicekontinuität beseitigt (oder minimiert) die Abhängigkeit, dass bestimmte am Verbindungsprozess beteiligte Komponenten verfügbar sein müssen. Es ermöglicht Ihnen, unabhängig vom Clouddienststatus eine Verbindung zu Ihren virtuellen Apps und Desktops herzustellen. Weitere Informationen zur Servicekontinuität finden Sie im Abschnitt [Servicekontinuität](#).

Verbesserte Unterstützung der Audioechounterdrückung [Technical Preview]

Die Citrix Workspace-App unterstützt jetzt die Echounterdrückung in adaptivem Audio und Legacyaudiocodecs. Dieses Feature wurde für Anwendungsfälle von Echtzeitaudio entwickelt und verbessert die Benutzererfahrung.

Citrix empfiehlt, adaptives Audio zu verwenden.

Hinweis:

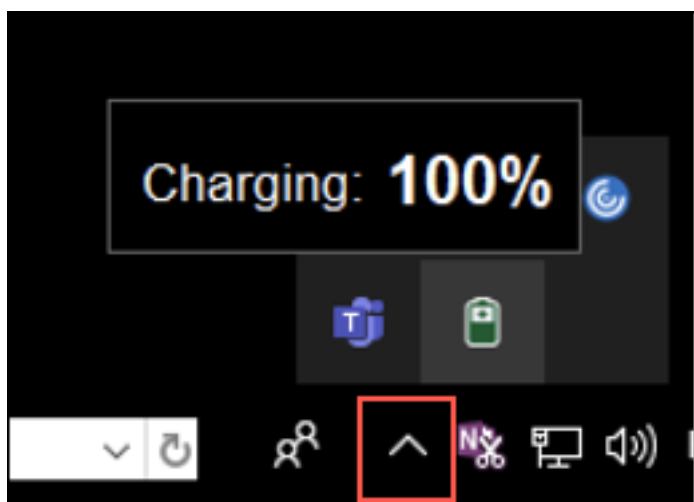
Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Verbesserungen an der Microsoft Teams-Optimierung

In optimiertem Microsoft Teams können Sie die Videofunktion jetzt verwenden, wenn mehr als eine virtuelle Desktop- oder App-Sitzung verwendet wird.

Akkustatusanzeige [Technical Preview]

Der Akkustatus des Geräts wird jetzt im Infobereich einer Citrix Desktop-Sitzung angezeigt.



Hinweis:

Die Akkustatusanzeige wird für Server-VDAs nicht angezeigt.

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 101.1.1.14, der auf Chromium Version 101 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Behobene Probleme

- Bei Macs mit Notchdisplay ist der Mauszeiger falsch ausgerichtet. [CVADHELP-19337]
- Sie werden nicht von der Workspace-App abgemeldet, wenn der Wert für das Inaktivitätstimeout abgelaufen ist. Das Problem tritt zeitweilig auf. [CVADHELP-19812]
- Bei dem Versuch, die Citrix Workspace-App zu deinstallieren, wird möglicherweise eine Fehlermeldung angezeigt. [CVADHELP-19121]
- In optimiertem Microsoft Teams funktioniert die Videofunktion möglicherweise nicht, wenn Sie eine weitere virtuelle Desktop- oder App-Sitzung starten. [HDX-40451]
- Wenn Sie den Bildschirm oder eine App während des Microsoft Teams-Anrufs freigeben, sehen die Teilnehmer möglicherweise visuelle Artefakte. Dieses Problem tritt aufgrund instabiler

Bildfrequenzen auf, wie z. B. falsche Videowiedergabe (eingefrorene oder vorübergehende schwarze Frames). Diese Version enthält verbesserte Bildfrequenzen oder Samplingraten, die dazu beitragen, visuelle Artefakte zu reduzieren. [HDX-38032]

2204

Was ist neu

Global App Configuration Service-Einstellungen für `allowedWebStoreURLs`

Administratoren können jetzt den Global App Configuration Service verwenden, um die Einstellungen von benutzerdefinierten Webstores zu konfigurieren. Administratoren können die benutzerdefinierten Webstores mit der Eigenschaft `allowedWebStoreURLs` konfigurieren. Weitere Informationen zum Global App Configuration Service finden Sie unter [Erste Schritte](#).

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

Administratoren können die Eigenschaft `maximise workspace window` im Global App Configuration Service so konfigurieren, dass die Citrix Workspace-App standardmäßig im maximierten Modus geöffnet werden kann. Weitere Informationen zum Global App Configuration Service finden Sie unter [Erste Schritte](#).

Unterstützung für Monitore mit hohem DPI-Wert [Technical Preview]

Die Citrix Workspace-App für Mac ist jetzt mit Monitoren mit einer DPI-Auflösung von mehr als 4K kompatibel. Bei Desktopsitzungen werden Apps, Text, Bilder und andere grafische Elemente in einer Größe angezeigt, die auf diesen hochauflösenden Monitoren bequem angezeigt werden kann.

Führen Sie den folgenden Befehl im macOS-Terminal aus, um das Feature zu aktivieren:

```
defaults write com.citrix.receiver.nomas EnableHighDPI -bool YES
```

Administratoren können die Richtlinie **Anzeigespeicherlimit** bearbeiten, die die maximale Videopuffergröße in Kilobyte für eine Desktopsitzung festlegt, um sie an die Bildschirmauflösung anzupassen. Der Standardwert für die Richtlinie "Anzeigespeicherlimit" ist 65536 KB. Das reicht für bis zu 2x4K-Monitore (2 x 32400 KB). Administratoren müssen diesen Wert bearbeiten, indem sie zu **Citrix Studio > Richtlinien > Speicherlimit anzeigen** navigieren und einen Wert von 393216 KB angeben, um dieses Feature zu verwenden.

Weitere Informationen zur Richtlinie "Anzeigespeicherlimit" finden Sie unter [Anzeigespeicherlimit](#).

Hinweis:

Dieses Feature funktioniert mit maximal zwei angeschlossenen Monitoren.

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und [Feedback](#) zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Erweiterung der permanenten Clientzugriffslizenz (CAL) für Remotedesktopsitzungen

Ab dieser Version können Sie, wenn Sie CALs in Ihrer Umgebung für den Zugriff auf Remotedesktops ausführen und die Client-ID länger als 15 Zeichen ist, die Remotedesktopsitzung mit einer dauerhaften Lizenz starten.

Um diese Funktion zu aktivieren, müssen Administratoren die Datei **default.ica** wie folgt konfigurieren:

1. Navigieren Sie auf dem StoreFront-Server zu `C:\inetpub\wwwroot\Citrix<StoreName>\App_Data` und öffnen Sie die Datei **default.ica** mit einem beliebigen Editor.
2. Fügen Sie dem Abschnitt **[WFClient]** folgende Zeilen hinzu:

```
isRDSLicensingEnabled=On
```

Standardeinstellungen für Tastatur wiederherstellen

Wenn Sie die Tastatureinstellungen in der Citrix Workspace-App geändert haben, können Sie jetzt die Standardeinstellungen für die Tastatur wiederherstellen. Hierfür öffnen Sie die Citrix Workspace-App, navigieren zu **Einstellungen > Tastatur** und klicken auf **Standardeinstellungen wiederherstellen**. Klicken Sie zur Bestätigung auf **Ja**.

Kompatibilität von App Protection mit HDX-Optimierung für Microsoft Teams

Ab dieser Version wird die vollständige Monitor- oder Desktop-Freigabe deaktiviert, wenn App Protection für die Bereitstellungsgruppe aktiviert ist. Wenn Sie in Microsoft Teams auf **Inhalt freigeben** klicken, wird die Option **Desktop** aus der Bildschirmauswahl entfernt. Nur bei einer VDA-Version ab 2109 können Sie die Option Fenster auswählen, um eine beliebige geöffnete App zu teilen. Wenn Sie mit einem VDA verbunden sind, der älter als 2019 ist, können keine Inhalte ausgewählt werden.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 99.1.1.8, der auf Chromium Version 99 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Festlegen von Citrix Enterprise Browser als Standardbrowser

Sie können jetzt Citrix Enterprise Browser als Standardbrowser festlegen. Nachdem Sie Citrix Enterprise Browser zu Ihrem Standardbrowser gemacht haben, werden alle Links sowie Web- und SaaS-Apps standardmäßig in Citrix Enterprise Browser geöffnet.

Gehen Sie wie folgt vor, um Citrix Enterprise Browser unter macOS zu Ihrem Standardbrowser zu machen:

1. Öffnen Sie Citrix Enterprise Browser, klicken Sie auf die drei Punkte und öffnen Sie das Menü **Einstellungen**.
2. Klicken Sie im linken Bereich auf die Option **Standardbrowser**.
3. Klicken Sie auf der Seite "Standardbrowser" auf **Als Standard festlegen**. Klicken Sie auf **Citrix Workspace Enterprise verwenden**, um Ihre Auswahl zu bestätigen und die Änderungen zu übernehmen.

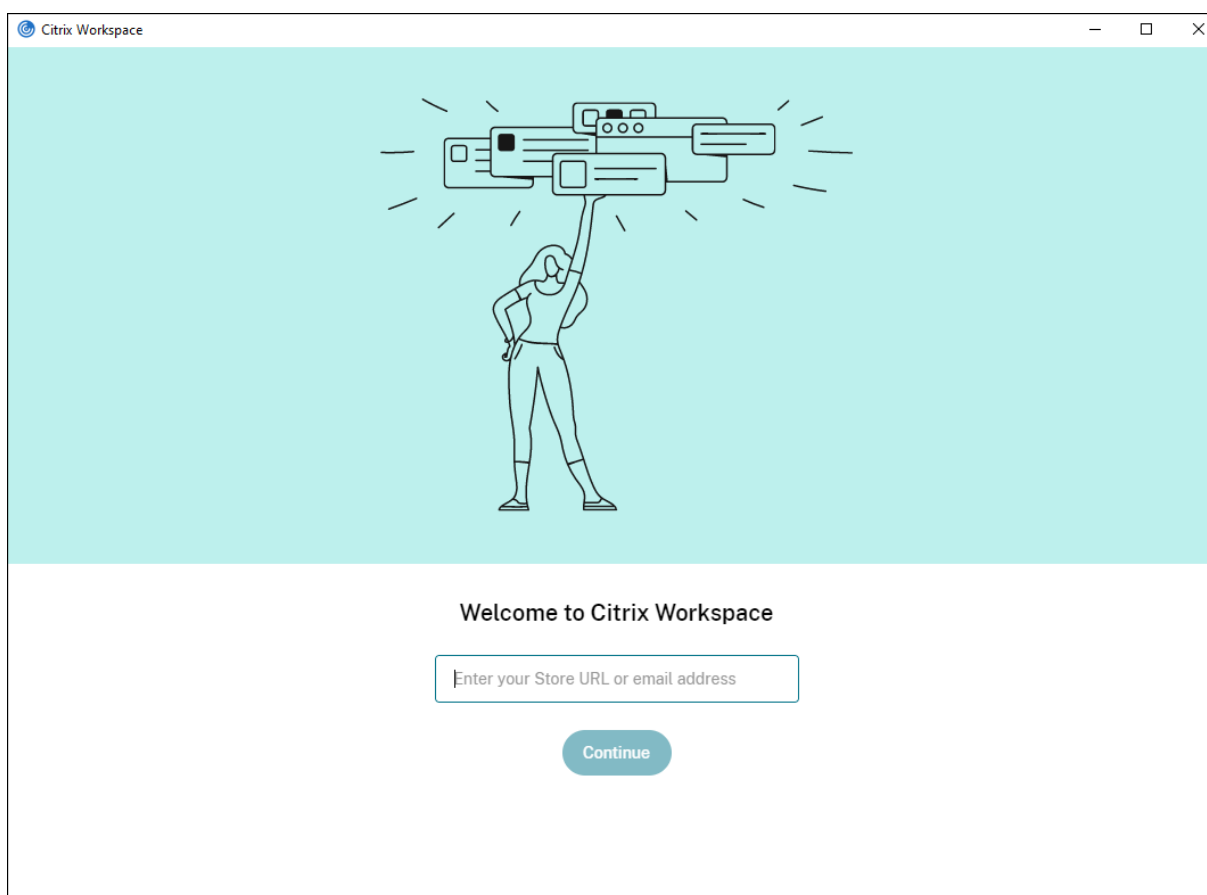
Behobene Probleme

- Bei Macs mit Notchdisplay ist der Mauszeiger falsch ausgerichtet. [CVADHELP-19337]
- Sie werden nicht von der Workspace-App abgemeldet, wenn der Wert für das Inaktivitätstimeout abgelaufen ist. Das Problem tritt zeitweilig auf. [CVADHELP-19812]
- Bei dem Versuch, die Citrix Workspace-App zu deinstallieren, wird möglicherweise eine Fehlermeldung angezeigt. [CVADHELP-19121]
- In optimiertem Microsoft Teams funktioniert die Videofunktion möglicherweise nicht, wenn Sie eine weitere virtuelle Desktop- oder App-Sitzung starten. [HDX-40451]
- Wenn Sie den Bildschirm oder eine App während des Microsoft Teams-Anrufs freigeben, sehen die Teilnehmer möglicherweise visuelle Artefakte. Dieses Problem tritt aufgrund instabiler Bildfrequenzen auf, wie z. B. falsche Videowiedergabe (eingefrorene oder vorübergehende schwarze Frames). Diese Version enthält verbesserte Bildfrequenzen oder Samplingraten, die dazu beitragen, visuelle Artefakte zu reduzieren. [HDX-38032]

2203.1

Was ist neu

Diese Version bietet ein vereinfachtes und intuitives Onboarding-Erlebnis für Erstanwender.



Inaktivitätstimeout für die Citrix Workspace-App

Die Inaktivitätstimeout-Funktion meldet Sie basierend auf einem vom Administrator festgelegten Wert von der Citrix Workspace-App ab. Administratoren können die zulässige Leerlaufzeit angeben, bevor ein Benutzer automatisch von der Citrix Workspace-App abgemeldet wird. Sie werden automatisch abgemeldet, wenn innerhalb des angegebenen Zeitintervalls im Fenster der Citrix Workspace-App keine Aktivität über Maus, Tastatur oder Berührung erfolgt. Das Inaktivitätstimeout hat keine Auswirkungen auf die bereits ausgeführten Citrix Virtual Apps and Desktops- und Citrix DaaS-Sitzungen (früher Citrix Virtual Apps and Desktops Service) oder die Citrix StoreFront-Stores.

Weitere Informationen finden Sie unter [Inaktivitätstimeout für die Citrix Workspace-App](#).

Universelles PDF-Drucken

Sie können jetzt die universelle PDF-Druckfunktion verwenden, wenn Sie von einem Mac aus drucken. Beim automatischen Erstellen von Druckern mit dem universellen Citrix Druckertreiber auf einem Mac brauchen Sie den Treiber für HP Color LaserJet 2800 Series PS nicht mehr zu installieren.

Weitere Informationen zu diesem Feature finden Sie unter [Drucken](#).

Freigeben von Apps mit dem Feature “Inhalt freigeben” in Microsoft Teams

Mit dem Feature für die Bildschirmfreigabe in Microsoft Teams können Sie jetzt einzelne Anwendungen, Fenster oder den gesamten Bildschirm freigeben. Citrix Virtual Delivery Agent 2109 ist eine Voraussetzung für dieses Feature.

Um eine bestimmte Anwendung anzuzeigen, klicken Sie in den Steuerelementen der Besprechung auf **Inhalt freigeben** und wählen Sie die gewünschte Anwendung aus. Wenn ein roter Rand um die von Ihnen ausgewählte App angezeigt wird, können die anderen Besprechungsteilnehmer Ihre App sehen. Wenn Sie die App minimieren, zeigt Microsoft Teams das letzte Bild der freigegebenen App an. Maximieren Sie das Fenster, um die Freigabe fortzusetzen.

Chat und Besprechungen mit mehreren Fenstern für Microsoft Teams

Benutzer können jetzt mehrere Fenster für Chat und Besprechungen in Microsoft Teams verwenden (1.5.00.5967 oder höher), wenn die Optimierung durch HDX in Citrix Virtual Apps and Desktops und Citrix DaaS erfolgt. Benutzer können ihre Konversationen oder Besprechungen auf verschiedene Arten ausklappen. Einzelheiten zum Ausklappen von Fenstern finden Sie unter [Microsoft Teams Pop-Out Windows for Chats and Meetings](#) auf der Microsoft Office 365-Website.

Benutzer älterer Versionen der Citrix Workspace-App oder des VDAs sollten bedenken, dass Microsoft den Einzelfenstercode künftig nicht mehr unterstützen wird. Sie haben jedoch mindestens neun Monate Zeit, um auf eine Version von VDA/CWA (2203 oder höher) zu aktualisieren, die mehrere Fenster unterstützt.

Hinweis:

Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Weitere Einzelheiten finden Sie unter [Microsoft 365-Roadmap](#).

Geben oder Übernehmen der Kontrolle in Microsoft Teams

Mit der Schaltfläche **Steuerung übergeben** können Sie anderen Besprechungsteilnehmern die Steuerung Ihres freigegebenen Bildschirms übergeben. Die anderen Teilnehmer können per Tastatur, Maus und Zwischenablageeingaben eine Auswahl treffen und den freigegebenen Bildschirm modifizieren. Sie können den freigegebenen Bildschirm jetzt beide steuern, und Sie können die Kontrolle jederzeit zurückfordern.

In Sitzungen mit Bildschirmfreigabe kann jeder Teilnehmer mit der Schaltfläche **Steuerung anfordern** die Kontrolle anfordern. Der Benutzer, der den Bildschirm freigibt, kann die Anforderung genehmigen oder ablehnen. Wenn Sie die Steuerung übernehmen, können Sie Tastatur- und Mauseingaben auf dem freigegebenen Bildschirm steuern und die Freigabe der Steuerung beenden.

Hinweis:

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

Migration von StoreFront zu Workspace

Wenn Ihre Organisation von On-Premises-StoreFront zu Workspace wechselt, müssen Benutzer die neue Workspace-URL der Citrix Workspace-App manuell hinzufügen. Dieses Feature ermöglicht es Administratoren, Benutzer nahtlos von einem StoreFront-Store zu einem Workspace-Store unter minimaler Benutzerinteraktion zu migrieren.

Weitere Informationen zu diesem Feature finden Sie unter [URL-Migration von StoreFront zu Workspace](#).

Global App Configuration Service

Der neue Global App Configuration Service für Citrix Workspace ermöglicht Citrix-Administratoren, Workspace-Dienst-URLs und Citrix Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen.

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

Vollbildmodus auf mehreren Monitoren

Sie können jetzt auf zwei oder mehr Monitoren gleichzeitig in den Vollbildmodus wechseln. Führen Sie die folgenden Schritte aus, um diese Funktion zu verwenden:

1. Öffnen Sie den Citrix Viewer.
2. Um den Vollbildmodus auf den anderen angeschlossenen Monitoren zu verwenden, ziehen Sie das Fenster von Ihrem primären Monitor, sodass es sich auf die angeschlossenen Monitore ausdehnt. Wählen Sie in der Menüleiste die Option **Ansicht > Zu Vollbild wechseln**. Das Fenster wechselt auf diesen Monitoren in den Vollbildmodus.

Hinweis:

Wenn Sie zuvor die Option **Alle Displays in Vollbild verwenden** ausgewählt haben, heben Sie die Auswahl auf, da diese Auswahl auf allen angeschlossenen Monitoren den Vollbildmodus festlegt.

Citrix empfiehlt die Verwendung von maximal 3 Monitoren, einschließlich des primären Monitors.

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 98.1.2.17, der auf Chromium Version 98 basiert. Informationen zu Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter [Neue Features](#) in der Dokumentation zu Citrix Enterprise Browser.

Technical Preview

- Unterstützung für besseres Single Sign-On (SSO) bei Web- und SaaS-Apps
- Unterstützung des Transport Layer Security (TLS)-Protokolls Version 1.3 auf Linux VDAs

Eine Liste aller Features in Technical Previews finden Sie auf der Seite [Features in Technical Previews](#).

Behobene Probleme

- Während aktiver Sitzungen wird das Wasserzeichen der Citrix Workspace-App transparent und zeigt Inhalte aus Fenstern im Hintergrund an. Das Problem tritt nur im Seamlessmodus auf. [CVADHELP-19153]
- Wenn Sie eine Sitzung von einem VDA (2112 oder höher) über Citrix ADC starten, kann es zu einer Sitzungsunterbrechung kommen; die Sitzungszuverlässigkeit startet, stellt aber nicht die Verbindung wieder her. [CVADHELP-19687]
- Das Dialogfeld zum Erhalt großer Dateien aus dem Mimecast-Plug-In wird in Outlook nicht angezeigt. [HDX-37137]
- Wenn der Wert für Path MTU Discovery (PMTUD) nicht 1500 (Standard) beträgt, können Benutzer in einer Azure-Cloudumgebung kein Fallback auf TCP ausführen. [HDX-37215]
- Es kann zu einer hohen CPU-Auslastung an einem Endpunkt kommen, wenn die Webcam in einem optimierten Microsoft Teams-Videoanruf eingeschaltet wird. [HDX-37168]
- In der Citrix Workspace-App können gelegentlich Fehler auftreten, wenn Sie einen Microsoft Teams-Anruf beantworten oder tätigen. Die folgende Fehlermeldung wird angezeigt: "Call can not be established." [HDX-38819]
- Citrix Workspace-App-Sitzungen werden möglicherweise nicht gestartet, wenn Citrix AppFlow in Citrix ADC konfiguriert ist. [HDX-39496]
- Wenn die automatische Aktualisierung deaktiviert ist und Sie zu **Einstellungen > Erweitert** navigieren, stürzt die Citrix Workspace-App ab. [RFMAC-10978]

2201

Was ist neu

Migration von StoreFront zu Workspace [Technical Preview]

Wenn Ihre Organisation von On-Premises-StoreFront zu Workspace wechselt, müssen Benutzer die neue Workspace-URL der Citrix Workspace-App manuell hinzufügen. Dieses Feature ermöglicht es Administratoren, Benutzer nahtlos von einem StoreFront-Store zu einem Workspace-Store unter minimaler Benutzerinteraktion zu migrieren.

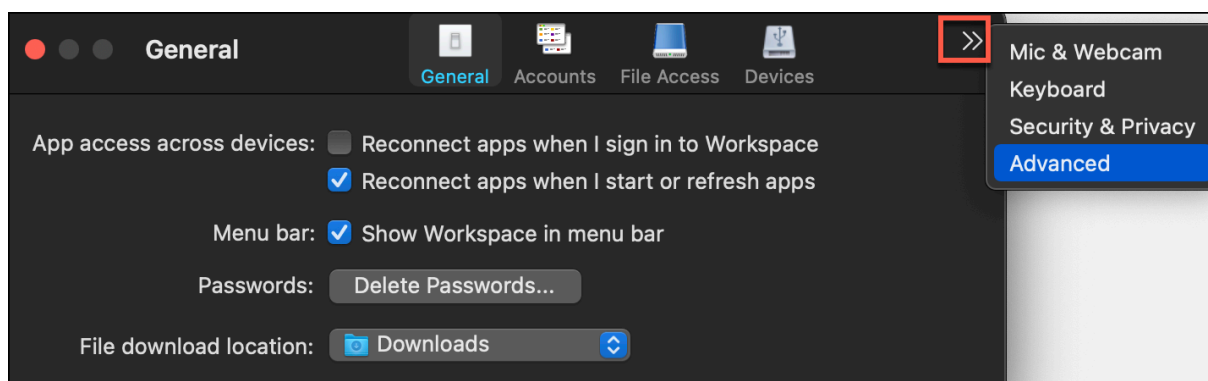
Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch [Feedback](#) zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

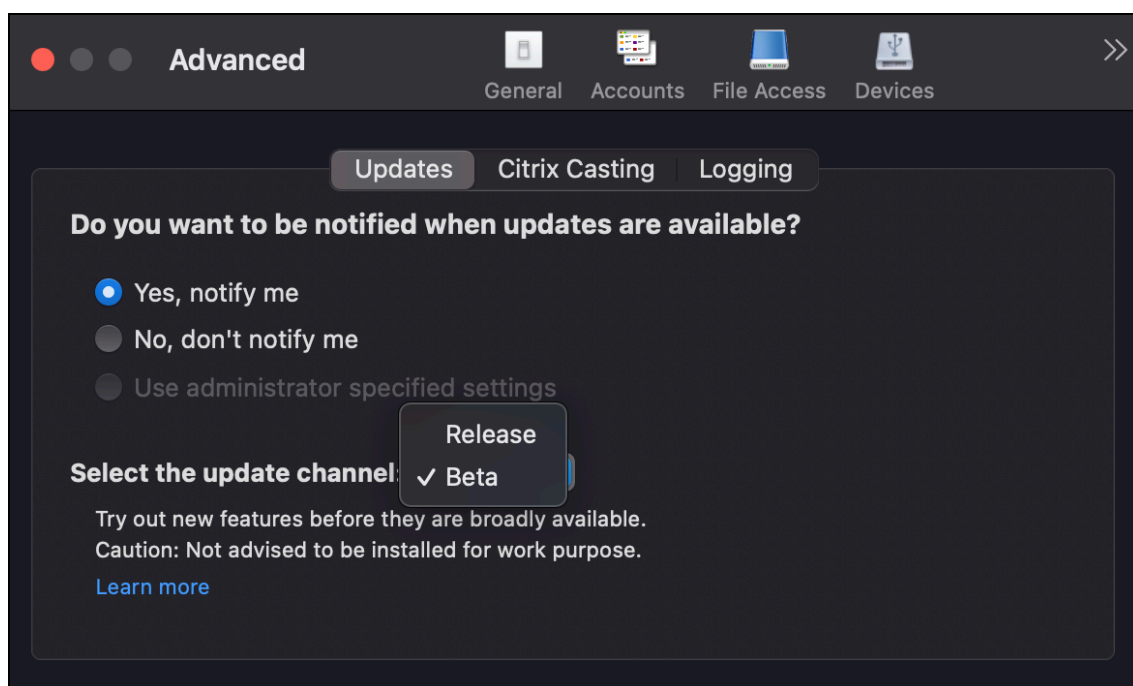
Beta-Programm für Citrix Workspace-App

Ab dieser Version können Sie vorhandene Installationen von Citrix Workspace-Apps automatisch auf die neuesten Beta Builds aktualisieren und diese testen. Beta Builds sind Early Access-Versionen, die vor der allgemeinen Verfügbarkeit eines vollständig unterstützten stabilen Releaseupdates veröffentlicht werden. Sie erhalten eine Updatebenachrichtigung, wenn die Citrix Workspace-App für automatische Updates konfiguriert ist.

Um auf die Beta-Builds zuzugreifen, öffnen Sie die Citrix Workspace-App, klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und klicken Sie dann auf **Einstellungen** > **Erweitert**. Um auf Beta Builds zu aktualisieren, wählen Sie den **Beta-Kanal** in der Dropdownliste aus.



- **Beta:** Early Access Release zum einfachen Testen und Melden von Problemen vor der allgemeinen Verfügbarkeit.
- **Release:** Vollständig unterstütztes stabiles Releaseupdate.



Weitere Informationen zur Verwendung dieser Funktion finden Sie unter [Aktualisierung](#).

Vollbildmodus auf mehreren Monitoren [Technical Preview]

Sie können jetzt auf zwei oder mehr Monitoren gleichzeitig in den Vollbildmodus wechseln. Führen Sie die folgenden Schritte aus, um diese Funktion zu verwenden:

1. Öffnen Sie den Citrix Viewer.
2. Um den Vollbildmodus auf den anderen angeschlossenen Monitoren zu verwenden, ziehen Sie das Fenster von Ihrem primären Monitor, sodass es sich auf die angeschlossenen Monitore ausdehnt. Wählen Sie in der Menüleiste die Option **Ansicht > Zu Vollbild wechseln**. Das Fenster wechselt auf diesen Monitoren in den Vollbildmodus.

Hinweis:

Wenn Sie zuvor die Option **Alle Displays in Vollbild verwenden** ausgewählt haben, heben Sie die Auswahl auf, da diese Auswahl auf allen angeschlossenen Monitoren den Vollbildmodus festlegt.

Citrix empfiehlt die Verwendung von maximal 3 Monitoren, einschließlich des primären Monitors.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch [Feedback](#) zur

Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Behobene Probleme

- Beim Auswählen des Kandidatentexts aus dem Kompositionsfenster des Eingabemethoden-Editors mit den Pfeilen nach links oder rechts auf der Tastatur bewegt sich der Eingabecursor nicht entsprechend. Dieses Problem tritt auf, wenn Sie einen Desktop starten und das Kontrollkästchen **Lokales Tastaturlayout statt des Remoteserver-Tastaturlayouts verwenden** im Fenster **Einstellungen > Tastatur** der Citrix Workspace-App aktiviert ist. Dieses Problem tritt nur in chinesischer und japanischer Sprache auf. [HDX-34956]
- Der Mauszeiger verschwindet zeitweise in Workspace-App-Sitzungen und Sie können nichts anklicken. [HDX-36820]
- Die Desktopsitzung wird unerwartet geschlossen, wenn Sie in einem Excel-Arbeitsblatt eine Zelle in einer PivotTable ziehen. [HDX-37178]
- Wenn Richtlinien für verlustfreien Codec oder Vollbild-H.264-Codec angewendet werden, treten nach der Aktualisierung auf Version 2112 manchmal Probleme mit Grafiken in Ihrer Desktopsitzung auf. [HDX-37272]
- Nach dem Upgrade der Citrix Workspace-App von Version 2010 auf Version 2112 können Sie keine Verbindung zu Desktops oder Apps herstellen. [RFMAC-10811]

2112

Was ist neu

Unterstützung für benutzerdefinierte Webstores

Sie können jetzt über die Citrix Workspace-App für Mac auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Zuvor konnten Sie nur über den Browser auf die benutzerdefinierten Stores zugreifen.

Die Citrix Workspace-App für Mac lädt die benutzerdefinierten Webstores ähnlich wie ein Browser und erweitert die Funktionen des App-Schutzes auf benutzerdefinierte Webstores. Durch den Zugriff auf das benutzerdefinierte Portal über die native Citrix Workspace-App werden Benutzern umfassende Funktionen und eine gute Benutzererfahrung für dieses Feature geboten. Weitere Informationen zum Global App Configuration Service finden Sie unter [Erste Schritte](#).

Weitere Informationen zum Konfigurieren eines benutzerdefinierten Webstores finden Sie unter [Benutzerdefinierter Webstore](#).

Anfordern der Steuerung in Microsoft Teams

Ab dieser Version können Sie bei einem Microsoft Teams-Anruf die Steuerung anfordern, wenn ein Teilnehmer den Bildschirm freigibt. Wenn Sie die Steuerung übernommen haben, können Sie auf dem freigegebenen Bildschirm auswählen, bearbeiten und andere Änderungen vornehmen.

Zum Übernehmen der Steuerung bei Freigabe eines Bildschirms klicken Sie oben im Microsoft Teams-Bildschirm auf **Steuerung anfordern**. Der Teilnehmer des Meetings, der den Bildschirm freigibt, kann die Anforderung akzeptieren oder ablehnen. Wenn Sie fertig sind, klicken Sie auf **Steuerung freigeben**.

Einschränkung:

Bei Peer-zu-Peer-Anrufen zwischen einem optimierten Benutzer und einem Benutzer mit dem nativen Microsoft Teams-Desktopclient, der auf dem Endpunkt ausgeführt wird, ist die Option **Steuerung anfordern** nicht verfügbar. Als Workaround können Benutzer einer Besprechung beitreten, um die Option **Steuerung anfordern** zu erhalten.

Dynamisches e911

Ab dieser Version unterstützt die Citrix Workspace-App den dynamischen Notruf. Wenn Sie Microsoft-Anrufpläne, Operator Connect und Direct Routing verwenden, haben Sie folgende Möglichkeiten:

- Konfigurieren und Übermitteln von Notrufen
- Benachrichtigen von Sicherheitspersonal

Die Benachrichtigung erfolgt basierend auf dem aktuellen Standort der Citrix Workspace-App auf dem Endpunkt anstelle des Microsoft Teams-Clients, der auf dem VDA ausgeführt wird. Das US-Gesetz (Ray Baum's Law) schreibt vor, dass der Standort des Notrufanrufers an die entsprechende Einsatzleitstelle (PSAP) übertragen wird. Ab Citrix Workspace-App 2112.1 für Windows erfüllt die Microsoft Teams-Optimierung mit HDX die Bestimmungen von Ray Baum's Law. Weitere Informationen zu diesem Feature finden Sie unter [Unterstützung für dynamisches e911](#) im Abschnitt **Microsoft-Telefonsystem**.

PDF Universal Printing (Technical Preview)

Das Feature PDF Universal Printing ist mit Citrix Virtual Apps and Desktops 2112 verfügbar. Das Feature ist in der Standardeinstellung deaktiviert. Um das Feature nutzen zu können, müssen Sie sich mit diesem [Webformular](#) registrieren. Sobald wir Ihre Informationen erhalten haben, wird das Feature für Sie aktiviert. Sie erhalten außerdem Anweisungen zur Verwendung des Features und zu den Druckrichtlinien, die aktiviert sein müssen.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur

eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Servicekontinuität

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Benutzer können so ihre virtuellen Apps und Desktops unabhängig vom Integritätsstatus der Cloud-Dienste starten. Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen.

Die Citrix Workspace-App und die Workspace Web-Erweiterung verwenden gemeinsam Workspace-Verbindungsleases, um bei Ausfällen den Zugriff auf Apps und Desktops über einen Browser zu ermöglichen. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Citrix Enterprise Browser

Dieses Release von Citrix Enterprise Browser basiert auf Chromium Version 95. Informationen zu Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter [Was ist neu](#) in der Dokumentation zu Citrix Enterprise Browser.

Behobene Probleme

- Der Fehler “Verbindung zum Server nicht möglich” wird angezeigt, wenn das Transportprotokoll von Enlightened Data Transport (EDT) zu TCP wechselt. [CVADHELP-18310]
- Wenn eine geschützte Progressive Web App (PWA) unter macOS geöffnet wird, werden die **App-Schutzrichtlinien** nicht erzwungen. [RFMAC-10128]

2111

Was ist neu

- Ab dieser Version können Benutzer die Citrix Workspace-App für Mac nicht manuell auf eine Version zurücksetzen, die niedriger ist als die auf ihren Systemen installierte Version. Wenn auf einem Mac-Gerät beispielsweise die Citrix Workspace-App Version 2109 installiert ist, können Sie die App nicht manuell auf Version 2108 oder niedriger zurücksetzen.

- Starten Sie die Remotedesktopsitzung mit einer dauerhaften Lizenz, wenn Sie Clientzugriffslizenzen (CAL) für den Zugriff auf Remotedesktops ausführen. Sie können die Remotedesktopsitzung starten, wenn die Client-ID länger als 15 Zeichen ist.
- Um das Citrix Virtual Channel SDK auf einen Mac zu laden, auf dem die Citrix Workspace-App 2111 ausgeführt wird, müssen Sie Ihre benutzerdefinierten virtuellen Kanäle neu kompilieren. Einzelheiten finden Sie unter [Update Custom Virtual Channels on Citrix Workspace app for Mac](#).

Unterstützung für benutzerdefinierte Webstores [Technical Preview]

Ab dieser Version können Sie über die Citrix Workspace-App für macOS auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Administratoren müssen den benutzerdefinierten Webstore der Liste der zulässigen URLs im Global App Configuration Service hinzufügen, um dieses Feature verwenden zu können. Nach dem Hinzufügen der URLs können Sie die URL des benutzerdefinierten Webstores unter “Konto hinzufügen” in der Citrix Workspace-App angeben. Der benutzerdefinierte Webstore wird im nativen Citrix Workspace-App-Fenster für macOS geöffnet.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch [Feedback](#) zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

[Citrix Enterprise Browser](#): Informationen zu neuen Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter **Neue Features** in der Dokumentation zu Citrix Enterprise Browser.

Behobene Probleme

- Auf Geräten mit macOS wird Advanced Audio Coding (AAC) nicht unterstützt. [CTXBR-1844]
- Wenn Sie die Citrix Workspace-App mit der Datei `.cr` konfigurieren und sich dann mit Ihren Anmeldeinformationen anmelden, wird die Homepage verzögert angezeigt. [RFMAC-9990]
- Öffnen Sie eine geschützte SaaS-App, öffnen Sie eine neue Registerkarte und trennen Sie die neue Registerkarte, indem Sie sie aus der Registerkartenleiste in ein neues Fenster ziehen. Ordnen Sie nun zwei Fenster nebeneinander an und öffnen Sie eine neue Registerkarte im zweiten Fenster, um einen Screenshot zu erstellen. Sie können auch die Screenshots für die geschützte SaaS-App erfassen. [RFMAC-10060]
- Wenn Sie von einem Store zum anderen wechseln, werden Sie möglicherweise vom ersten Store abgemeldet. [RFMAC-10137]

- Wenn Sie bei der Anmeldung an der Citrix Workspace-App falsche Anmeldeinformationen eingeben, wird die Fehlermeldung “Falsche Anmeldeinformationen” nicht angezeigt. Es wird erneut eine Authentifizierungsaufforderung angezeigt. Manchmal wird **Domäne\Benutzer** in der Authentifizierungsaufforderung anstelle von **Benutzername** angezeigt. [RFMAC-10210]
- Anrufe schlagen fehl, wenn ein optimierter Microsoft Teams P2P-Anruf von der Citrix Workspace-App für Mac 2109 zur Citrix Workspace-App für Windows 2109 getätigt wird. [HDX-35223]

2109.1

Was ist neu

macOS Monterey-Unterstützung

Die Citrix Workspace-App für Mac wird auf macOS Monterey (12.0.1) unterstützt.

Behobene Probleme

- Wenn Sie eine geschützte App, eine nicht geschützte SaaS-App und eine geschützte Desktopsitzung geöffnet haben, wird der Browser unerwartet beendet. Dieses Problem tritt auf, wenn Sie vom Fenster der geschützten Desktopsitzung zu der nicht geschützten SaaS-App wechseln. [CTXBR-2087]
- Wenn vom Administrator externe Erweiterungen in Google Chrome installiert wurden, stürzt Citrix Enterprise Browser beim Öffnen ab. [CTXBR-2135]

2109

Was ist neu

Hinweis:

Bei aktivierter Servicekontinuität werden beim Upgrade auf Version 2109 die Verbindungslease-dateien aktualisiert. Alle vorhandenen Leases werden gelöscht und neue Leases werden im Rahmen von Funktionsverbesserungen abgerufen.

Citrix Workspace-App für Mac auf macOS Monterey Beta

Die Citrix Workspace-App 2109 für Mac wurde auf macOS Monterey Beta 7 getestet. Verwenden Sie dieses Setup in einer Testumgebung und geben Sie uns Feedback.

Achtung:

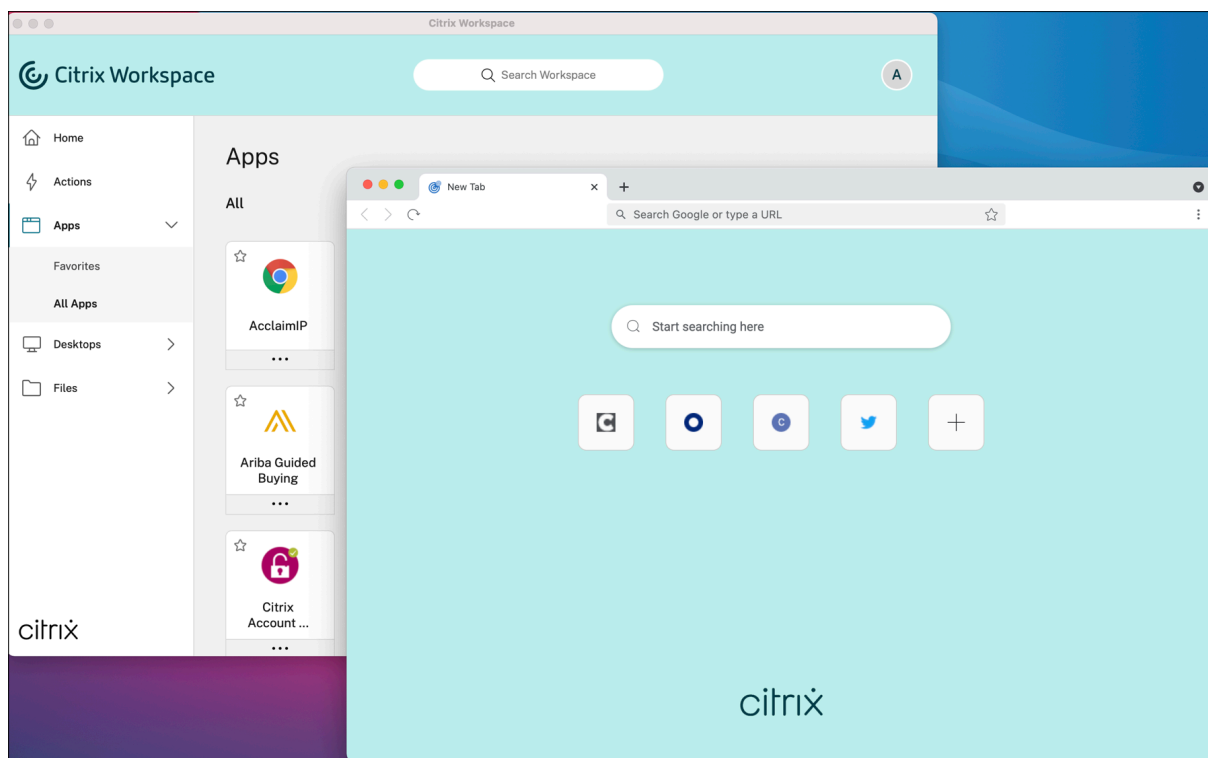
Verwenden Sie die Citrix Workspace-App für Mac unter macOS Monterey Beta-Versionen nicht in Produktionsumgebungen.

Automatische Storesuche per E-Mail-Adresse

Sie können jetzt Ihre E-Mail-Adresse in der Citrix Workspace-App für Mac eingeben, um automatisch den zugehörigen Store zu ermitteln. Wenn einer Domäne mehrere Stores zugeordnet sind, wird standardmäßig der erste vom Global App Configuration Service zurückgegebene Store als bevorzugter Store hinzugefügt. Benutzer können bei Bedarf stets zu einem anderen Store wechseln.

Citrix Enterprise Browser

Citrix Enterprise Browser ist ein systemeigener Browser, der auf der Clientmaschine ausgeführt wird. Damit können Benutzer Web- oder SaaS-Apps in der Citrix Workspace-App sicher öffnen. Der Browser gewährleistet eine konsistente Benutzeroberfläche beim Zugriff auf verschiedene Web- oder SaaS-Apps. Gleichzeitig verbessern Sie Ihre Produktivität und erzielen eine gute Leistung bei der Wiedergabe der Apps.



Der neue Citrix Enterprise Browser ermöglicht eine verbesserte Benutzererfahrung im Stil eines systemeigenen Browsers und bietet folgende Features:

- Zugriff ohne VPN auf interne Webseiten
- Unterstützung für Mikrofon und Webcam

- Browsing mit Registerkarten
- Mehrfensteransichten
- Bearbeitbare Omnibox
- Lesezeichen
- Verknüpfungen auf der neuen Registerkarte
- Anpassbare Einstellungen
- Analytics

Administratoren können Secure Private Access- oder App Protection-Richtlinien wie Keyloggingschutz, Screenshotschutz, Download, Drucken, Zwischenablagebeschränkungen und Wasserzeichen in unterschiedlichen Kombinationen pro URL aktivieren.

Weitere Informationen finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Verbesserung der Endpunktanalyse (EPA)

Ab dieser Version unterstützt die Citrix Workspace-App für macOS die Endpunktanalyse (EPA). Die Endpunktanalyse scannt das Gerät auf Endpunktsicherheitsanforderungen, die auf dem Citrix Gateway konfiguriert sind. Wenn der Scan erfolgreich abgeschlossen wurde, erhält ein Benutzer Zugriff.

Hinweis:

Dieses Feature funktioniert nur, wenn Sie die Multifaktorauthentifizierung (nFactor) in der Umgebung konfiguriert haben.

Weitere Informationen zum EPA-Scan finden Sie unter [Advanced Endpoint Analysis scans](#).

Adaptives Audio

Bei adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht konfigurieren. Adaptives Audio optimiert die Einstellungen für Ihre Umgebung und ersetzt Legacy-Audiokomprimierungsformate für eine hervorragende Benutzererfahrung. Weitere Informationen finden Sie unter [Adaptives Audio](#).

Unterstützung für H.264 Advanced Video Coding (MPEG-4 AVC) mit Microsoft Teams

Dieses Release unterstützt die hardwarebeschleunigte H.264-Videocodierung/-decodierung. Dies verringert die CPU-Auslastung und verbessert die Qualität von Videokonferenzen. Die Multimediaengine von Citrix HDX-optimiertem Microsoft Teams (HdxRtcEngine.exe) verwendet jetzt Apples Video Toolbox Framework zur Codierung und Decodierung. Dieses Framework komprimiert und dekomprimiert Video schneller und in Echtzeit. Darüber hinaus wird das Auslagern von Codierung und Decodierung an die GPU optimiert. Die hardwarebeschleunigte Videodecodierung und -codierung ist standardmäßig aktiviert, wenn ein Gerät sie unterstützt. Durch diese Verbesserung wird die CPU-Auslastung bei Multimedianeutzung reduziert, wenn Microsoft Teams mit HDX optimiert ist.

Behobene Probleme

- Nach der Anmeldung bei der Citrix Workspace-App für Mac werden Sie nach einigen Stunden zur Authentifizierung aufgefordert. [RFMAC-10032]
- Wenn Sie einen Store in der Citrix Workspace-App hinzufügen, die Authentifizierungsdomäne in der Serverkonsole ändern, die App einige Minuten lang inaktiv lassen und dann eine beliebige App- oder Desktopsitzung öffnen, stürzt die Citrix Workspace-App möglicherweise ab. [RFMAC-10133]
- Wenn bereits eine virtuelle App oder ein virtueller Desktop ausgeführt wird und Sie eine weitere virtuelle App oder einen virtuellen Desktop starten, wird Citrix Viewer angezeigt, aber die virtuelle App wird nicht geöffnet. Dieses Problem tritt auf Geräten mit macOS 11.6 auf. [RFMAC-10134]

2108.1

Was ist neu

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

Behobene Probleme

Wenn bereits eine virtuelle App oder ein virtueller Desktop ausgeführt wird und Sie eine weitere virtuelle App oder einen virtuellen Desktop starten, wird Citrix Viewer angezeigt, aber die virtuelle App wird nicht geöffnet. Dieses Problem tritt auf Geräten mit macOS 11.6 auf. [RFMAC-10134]

2108

Was ist neu

Die Citrix Workspace-App für Mac unterstützt nun MTU-Discovery (Maximum Transmission Unit = maximale Übertragungseinheit) für Enlightened Data Transport (EDT). Das Feature erhöht die Zuverlässigkeit und Kompatibilität des EDT-Protokolls und bietet eine verbesserte Benutzererfahrung.

Hinweis:

MTU-Discovery für EDT wird unter macOS Big Sur und höher unterstützt.

Behobene Probleme

- Es kommt zu einer Videoverzögerung bei Konferenzgesprächen in Microsoft Teams. [HDX-32603]

- Auf Mac-Clients, auf denen macOS Big Sur ausgeführt wird, kann ein interner HTTP 404- oder HTTP/1.1-Serverfehler auftreten. Das Problem tritt auf, wenn versucht wird, die Verbindung zu Sitzungen wiederherzustellen. [RFMAC-9448]

2107

Was ist neu

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

Behobene Probleme

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

2106

Was ist neu

Unterstützung für benutzerdefinierte URLs für 301-Weiterleitungen

Sie können URLs für HTTP 301-Weiterleitungen von StoreFront oder Citrix Gateway an Citrix Workspace hinzufügen.

Bei der Migration von StoreFront zu Citrix Workspace können Sie die StoreFront-URL per HTTP 301-Weiterleitung an eine Citrix Workspace-URL weiterleiten. Beim Hinzufügen einer alten StoreFront-URL erfolgt dann automatisch eine Weiterleitung an Citrix Workspace.

Beispiel einer Weiterleitung:

Die StoreFront-URL `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` kann an die Citrix Workspace-URL `https://<Citrix Workspace url>/Citrix/Roaming/Accounts` umgeleitet werden.

Hinweis:

- Die Citrix Workspace-App für Mac unterstützt nicht das Mehrfrequenzwahlverfahren (Dual Tone Multi Frequency, DTMF) für Microsoft Teams aufgrund ausstehender Änderungen von Microsoft.
- Ab dieser Version stimmen die Versionsnummer des Citrix Viewers und die Versionsnummer der Citrix Workspace-App möglicherweise nicht überein. Diese Änderung hat keinen Einfluss auf Ihre Benutzererfahrung.

Servicekontinuität

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Benutzer können so ihre virtuellen Apps und Desktops unabhängig vom Integritätsstatus der Cloud-Dienste starten.

Weitere Informationen finden Sie unter [Servicekontinuität](#) in der Dokumentation zu Citrix Workspace.

Verbesserungen bei Microsoft Teams

Wenn der **Desktop Viewer** im Vollbildmodus ausgeführt wird, können Benutzer aus den Bildschirmen, die der **Desktop Viewer** abdeckt, einen auswählen und freigeben. Im Fenstermodus können Benutzer das Fenster des **Desktop Viewers** freigeben. Im Seamlessmodus können Benutzer einen Bildschirm unter den mit dem Endpunktgerät verbundenen Bildschirmen auswählen.

Wenn der Desktop Viewer den Fenstermodus ändert (maximieren, wiederherstellen oder minimieren), wird die Bildschirmfreigabe beendet.

Wenn der Benutzer den Bildschirm freigeben möchte, werden Vorschauen für alle verfügbaren Bildschirme im Bereich der Bildschirmfreigabe angezeigt, sodass es intuitiv ist, den richtigen Bildschirm aus den Vorschauen auszuwählen.

Behobene Probleme

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

2104

Was ist neu

Die Citrix Workspace-App für Mac unterstützt die manuelle Anmeldung von Benutzern bei Netzwerkfreigaben, es sei denn, Ihre Organisation aktiviert Single Sign-On. Um auf freigegebene Netzwerkspeicherorte zuzugreifen, öffnen Sie die Citrix Workspace-App, navigieren Sie zu **Dateien > Netzwerkfreigaben** und geben Sie Ihre Anmeldeinformationen ein. Weitere Informationen zum Einrichten von Netzwerkfreigaben finden Sie unter [Create and manage storage zone connectors](#).

Behobene Probleme

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

2102

Was ist neu

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

Behobene Probleme

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

2101

Was ist neu

Unterstützung für Apple M1-Chip

Die Citrix Workspace-App für Mac unterstützt jetzt Apple M1-Chips mit Rosetta 2 unter macOS Big Sur (11.0 und höher). Daher müssen alle virtuellen Kanäle von Drittanbietern Rosetta 2 verwenden. Andernfalls funktionieren diese virtuellen Kanäle möglicherweise nicht in der Citrix Workspace-App für Mac unter macOS Big Sur (11.0 und höher). Weitere Informationen über Rosetta finden Sie in diesem [Apple-Supportartikel](#).

Unterstützung der Microsoft Teams-Optimierung für nahtlose App-Sitzungen

Die Citrix Workspace-App für Mac unterstützt jetzt die Microsoft Teams-Optimierung für nahtlose App-Sitzungen. Daher können Sie Microsoft Teams als Anwendung aus der Citrix Workspace-App starten. Weitere Informationen finden Sie in den folgenden Artikeln:

- [Optimierung für Microsoft Teams](#)
- [Microsoft Teams-Umleitung](#)

Unterstützung für Mehrfrequenzwahlverfahren (Dual Tone Multi Frequency, DTMF) mit Microsoft Teams

Die Citrix Workspace-App für Mac unterstützt das Mehrfrequenzwahlverfahren (DTMF) mit Telefonesystemen (z. B. PSTN) und Telefonkonferenzen in Microsoft Teams. Dieses Feature ist standardmäßig aktiviert.

Behobene Probleme

- Versuche, eine Microsoft Teams-Besprechung mit der OWA (Outlook Web-App) zu öffnen, schlagen möglicherweise fehl, wodurch alle zugehörigen Fenster unerwartet geschlossen werden. [CTXBR-1175]
- Wenn Sie einen Videoanruf starten, reagiert Microsoft Teams möglicherweise nicht mehr und zeigt den Fehler `Citrix HDX not connected` an. [RFMAC-6727]
- Unter macOS Big Sur (11.0.1) kann das Anschließen von USB-Geräten fehlschlagen, wodurch die Sitzung unerwartet beendet wird. [RFMAC-7079]
- Auf einem veröffentlichten Desktop wird für Dateien, die auf Ihrem lokalen Mac gespeichert sind, als Dateierstellungsdatum möglicherweise 30. November 1979 statt des aktuellen Datums angezeigt. [CVADHELP-16309]
- Manchmal wird der Anmeldebildschirm in veröffentlichten Apps möglicherweise nicht richtig angezeigt, was zu einer reduzierten Fenstergröße und einer roten Hintergrundfarbe führt. [CVADHELP-16027]
- Audioanrufe werden möglicherweise auf Ihrer Seite getrennt, wenn Sie Audiogeräte trennen und anschließen. [RFMAC-7371]
- Versuche, Text aus Office 365-Apps zu kopieren, sind u. U. auch dann erfolgreich, wenn die Richtlinie für die Einschränkung der Zwischenablage aktiviert ist. [CTXBR-1166]
- Versuche, Microsoft Teams zu starten, schlagen möglicherweise aufgrund von Problemen mit der HDX RealTime Connector Engine fehl und die folgende Fehlermeldung wird angezeigt.

`Sorry, we couldn't connect you`

[CVADHELP-16432]

2012

Was ist neu

Apple M1-Chip - Preview

Die Citrix Workspace-App für Mac unterstützt jetzt Apple-Geräte mit M1-Chip auf Previewbasis.

Optimierung der Bildschirmfreigabe in Microsoft Teams

Die Citrix Workspace-App für Mac unterstützt jetzt die Optimierung der Bildschirmfreigabe in Microsoft Teams. Weitere Informationen:

- [Optimierung für Microsoft Teams](#)
- [Microsoft Teams-Umleitung](#)

Leistungsverbesserungen

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

Behobene Probleme

- Wenn Sie die Citrix Workspace-App für Mac 2008 oder höher verwenden, schlagen Versuche, mehrere Instanzen einer veröffentlichten Anwendung zu starten, möglicherweise fehl. [CVADHELP-16019]
- Versuche, die generische USB-Umleitung zu starten, schlagen möglicherweise fehl, wenn Sie eine USB-Dockingstation verwenden. [RFMAC-6687]
- Beim Öffnen eines Fensters mit STRG+O in veröffentlichten Desktops werden u. U. zwei Fenster geöffnet. [CVADHELP-15747]
- Das Starten von Citrix Files von der Citrix Workspace-App für Mac aus schlägt möglicherweise aufgrund von Problemen mit Single Sign-On fehl. [RFMAC-4477]
- Wenn Sie die Citrix Workspace-App für Mac unter macOS Big Sur Beta verwenden, werden Audioanrufe möglicherweise getrennt. Das Problem tritt auf, wenn Sie Audiogeräte trennen und verschiedene Audiogeräte während eines Audioanrufs anschließen. [RFMAC-6112]
- Die HDX RealTime Connector-Engine wird möglicherweise unerwartet beendet, wenn Sie die Kamera in Microsoft Teams ein- und ausschalten. [RFMAC-6293]

Bekannte Probleme

Bekannte Probleme in 2308

- Nach dem Upgrade der Citrix Workspace-App für Mac auf Version 2308 reagiert das Einstellungs-fenster möglicherweise nicht mehr auf Benutzeraktionen. Erzwingen Sie das Beenden der Citrix Workspace-App als Workaround und starten Sie sie neu. Weitere Informationen zum erzwungenen Beenden einer App auf einem Mac finden Sie im [zugehörigen Apple-Supportartikel](#). [RFMAC-14596]

Bekannte Probleme in Release 2307

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2306

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2305

- Nach dem Upgrade der Citrix Workspace-App für Mac auf Version 2305 reagieren bestimmte virtuelle Apps von Drittanbietern mit Popup-Dialogfeldern zur Eingabe von Benutzernamen und Kennwort nach dem Öffnen möglicherweise nicht mehr. [CVADHELP-23032]

Bekannte Probleme in Release 2304

- Für Benutzer mit mehreren Konten wird der Ladebildschirm der Citrix Workspace-App möglicherweise lange Zeit angezeigt. Beenden Sie als Workaround die Citrix Workspace-App beenden und starten Sie sie neu. [RFMAC-13432]

Bekannte Probleme in Release 2301.1

- Sie können kein Update auf Version 2301.1 der Citrix Workspace-App für Mac mit dem automatischen Updatedienst durchführen. Als Workaround müssen Sie Version 2301.1 der Citrix Workspace-App für Mac manuell installieren, indem Sie die DMG-Datei herunterladen, die auf der Seite [Downloads](#) verfügbar ist.

Bekannte Probleme in Release 2301

- Auf macOS Ventura-Geräten können Progressive Web Apps (PWA) nicht geöffnet werden. Die folgende Fehlermeldung wird angezeigt:

App Name is damaged and can't be opened. You should move it to the Bin.

Klicken Sie mit der rechten Maustaste auf die App und wählen Sie "Öffnen", um das Problem zu umgehen. Wenn Sie die Tastatur verwenden, drücken Sie die Ctrl-Taste und klicken Sie auf die App. Wählen Sie dann "Öffnen". [CTXBR-3885]

- Wenn Benutzer sich am Citrix Workspace mit zugeordnetem Global App Configuration Service anmelden, wird möglicherweise dauerhaft ein Wartesymbol angezeigt. StoreFront und benutzerdefinierte Webstores sind von diesem Problem nicht betroffen. [RFMAC-13086]

Bekanntes Problem in 2211.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2211

- Wenn Sie die Citrix Workspace-App für Mac 2209 und höher verwenden, wird die Anmeldeseite für Benutzer möglicherweise nicht angezeigt, wenn Sie das benutzerdefinierte Webportal ver-

wenden. Als Workaround beenden Sie die Citrix Workspace-App mit der Option **Beenden** über das Citrix Workspace-Symbol in der Menüleiste. [CVADHELP-21377]

Bekannte Probleme in Release 2210

- Unter macOS 13 Ventura kann es zu Problemen bei der Seamless-App-Interaktion kommen, wenn Sie im **Stage Manager**-Feature in der Einstellung **Stage Manager** die Option **All at Once default** in **One at a Time** ändern. [HDX-44567]
- Versuche, eine Desktopsitzung im Offlinemodus zu starten, schlagen möglicherweise fehl. Um das Problem zu umgehen, ändern Sie die Größe des Sitzungsfensters. [HDX-45081]
- Wenn Sie die Anzeige einer Sitzung auf einem MacBook in den Vollbildmodus ändern, wird der Cursorfokus möglicherweise leicht oberhalb der tatsächlichen Cursorposition angezeigt. Gehen Sie als Workaround zu **System Preferences > Dock & Menu Bar** und aktivieren Sie die Option **Automatically hide and show the menu bar in full screen**. [HDX-45585]
- Ab Version 2210 kann die Verwendung der Features “Mission Control” oder “App Expose” in einer App-Sitzung dazu führen, dass die Citrix Workspace-App unerwartet geschlossen wird. [HDX-46130]
- Beim Starten bestimmter Drittanbieter-Apps, wie Epic oder Kronos, wird das Anmeldefenster der Apps möglicherweise von einem anderen Fenster verdeckt. Infolgedessen friert die gesamte Sitzung ein. Führen Sie als Workaround eine der folgenden Aktionen aus:
 - Ziehen Sie das Fenster, das das Anmeldefenster blockiert, zur Seite.
 - Navigieren Sie mit dem Feature “Mission Control” zum Anmeldefenster.
 - Verwenden Sie die Tastenkombination **Befehl+~** zum Wechseln zwischen Fenstern.

[HDX-46140]

Bekannte Probleme in Release 2209

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2208.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2206.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2204

- Wenn der Datenverkehr über NGS getunnelt wird, kann die Citrix Workspace-App möglicherweise keine Dateien hoch- oder herunterladen, die größer als 64 MB sind. [CTXBR-3354]

Bekannte Probleme in Release 2203.1

- Bei minimiertem Browserfenster können Sie in der Jira-App nicht auf die Schaltfläche **Erstellen** klicken. [CTXBR-1976]
- Websocket-Verbindungen werden nicht durch Citrix Secure Private Access getunnelt. [CTXBR-2439]
- Nach dem Upgrade der Citrix Workspace-App auf Version 2203 wird ein Fragezeichensymbol auf dem Symbol von Citrix Enterprise Browser angezeigt. Dieses Problem tritt auf, wenn Citrix Enterprise Browser vor dem Upgrade an das Dock angeheftet wurde. [CTXBR-2864]
- Wenn Sie in Citrix Enterprise Browser in den Einstellungen unter **Erweitert** auf die Option **Einstellungen zurücksetzen** klicken, werden die Protokolleinstellungen nicht auf die Standardeinstellungen zurückgesetzt. Klicken Sie als Workaround auf der Seite **Protokolle** auf die Option **Auf Standardprotokolleinstellungen zurücksetzen**. [CTXBR-2929]
- Nach dem Upgrade von Citrix Enterprise Browser von Version 2201 auf Version 2203 können Sie keine neuen Kennwörter speichern, und bereits gespeicherte Kennwörter gehen verloren. [CTXBR-3063]
- Der Vollbildmodus ist auf Macs mit Einkerbung (Notch) nicht verfügbar. [CVADHELP-19337]
- Wenn Sie eine Desktop- oder App-Sitzung im Browser starten, wird das Sitzungsfenster im Hintergrund hinter dem Browserfenster geöffnet. [RFMAC-11362]

Bekannte Probleme in Release 2201

- Der Clientname wird im Citrix Brokerdienst und in Citrix Director mit zufälligen Zeichen angezeigt, wenn Sie die Citrix Workspace-App im Offlinemodus (Intranetmodus) verwenden. [RFMAC-10842]

Bekannte Probleme in Release 2112

- In der Citrix Workspace-App können gelegentlich Fehler auftreten, wenn Sie einen Microsoft Teams-Anruf beantworten oder tätigen. Die folgende Fehlermeldung wird angezeigt: "Call could not be established." [HDX-38819]

Bekannte Probleme in Release 2111

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2109.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2109

- Wenn Sie die Citrix Workspace-App mit der Datei `.cr` konfigurieren und sich dann mit Ihren Anmeldeinformationen anmelden, wird die Homepage verzögert angezeigt. [RFMAC-9990]
- Wenn eine geschützte Progressive Web App (PWA) unter macOS geöffnet wird, werden die *App-Schutzrichtlinien* nicht erzwungen. [RFMAC-10128]
- Wenn Sie Stores in der Citrix Workspace-App hinzufügen, die Einstellung **Aktueller Zeitraum für die erneute Authentifizierung** in **Neuauthentifizierungszeitraum für die Workspace-App** ändern und nach einigen Minuten vom On-Premises-Store zum Cloudstore wechseln, werden Sie vom Cloudstore abgemeldet und müssen sich erneut authentifizieren. Wenn Sie sich in der Citrix Workspace-App anmelden, wird das Wartezeichen dauerhaft angezeigt und Sie können sich nicht anmelden. [RFMAC-10140]

Bekannte Probleme in Release 2108.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2108

- Wenn Sie eine abonnierte SaaS-App starten, nachdem die Authentifizierungsdomäne in der Serverkonsole geändert wurde, wird die Sitzung nicht gestartet und die folgende Fehlermeldung angezeigt:

“Die Authentifizierungsdomäne hat sich geändert. Warten Sie etwas und melden Sie sich dann erneut an.”

[RFMAC-9616]

Bekannte Probleme in Release 2107

- Wenn Sie die Authentifizierungsdomäne in der Serverkonsole ändern und sich mit Ihren Anmeldeinformationen anmelden, wird die folgende Fehlermeldung angezeigt:

Verbindung mit dem Server ist nicht möglich

Sie können auf den Store zugreifen, sobald Sie auf “OK” geklickt haben.

[RFMAC-9494]

Bekannte Probleme in Release 2106

- Wenn Sie Ihren Bildschirm freigeben, wird ein schwarzes Fenster angezeigt. [HDX-30083]

Bekannte Probleme in Release 2104

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2102

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2101

- Versuche, von der Citrix Workspace-App für Mac aus auf Dateien in Netzwerkfreigaben zuzugreifen, schlagen möglicherweise fehl, auch wenn die Option aktiviert ist. [RFMAC-7272]
- Unter macOS Big Sur schlagen Versuche, die SAML Single Sign-On-App in der Citrix Workspace-App für Mac zu starten, möglicherweise fehl und die folgende Fehlermeldung wird angezeigt.

Page could not load. Please **try** again later or contact your administrator **for** assistance. Incident ID:-202

[RFMAC-7282]

Bekannte Probleme in Release 2012

- Wenn Sie einen Videoanruf starten, reagiert Microsoft Teams möglicherweise nicht mehr und zeigt den Fehler `Citrix HDX not connected` an. Starten Sie als Workaround Microsoft Teams oder den VDA neu. [RFMAC-6727]
- Videoanrufe über Microsoft Skype for Business werden unter macOS Big Sur (11.0.1) nicht unterstützt.
- Unter macOS Big Sur (11.0.1) kann das Anschließen von USB-Geräten fehlschlagen, wodurch die Sitzung unerwartet beendet wird. Schließen Sie als Workaround das USB-Gerät erneut an. [RFMAC-7079]

Hinweise zu Drittanbietern

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

[Citrix Workspace-App für Mac – Hinweise zu Drittanbietern](#)

Features in Technical Previews

December 18, 2023

Kunden haben die Möglichkeit, Technical Previews in ihren Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu nutzen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Features in Technical Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor.

Unterstützung für Citrix Secure Private Access für On-Premises-Stores

Dieses Feature ist ab Release 2309 als Technical Preview verfügbar.

Ab Version 2309 unterstützt die Citrix Workspace-App für Mac Citrix Secure Private Access für On-Premises-Bereitstellungen. Weitere Informationen finden Sie unter [Secure Private Access for on-premises - Preview](#).

Hinweis:

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.

Option “Hoher DPI-Wert” verbessert

Dieses Feature ist ab Release 2308 als Technical Preview verfügbar.

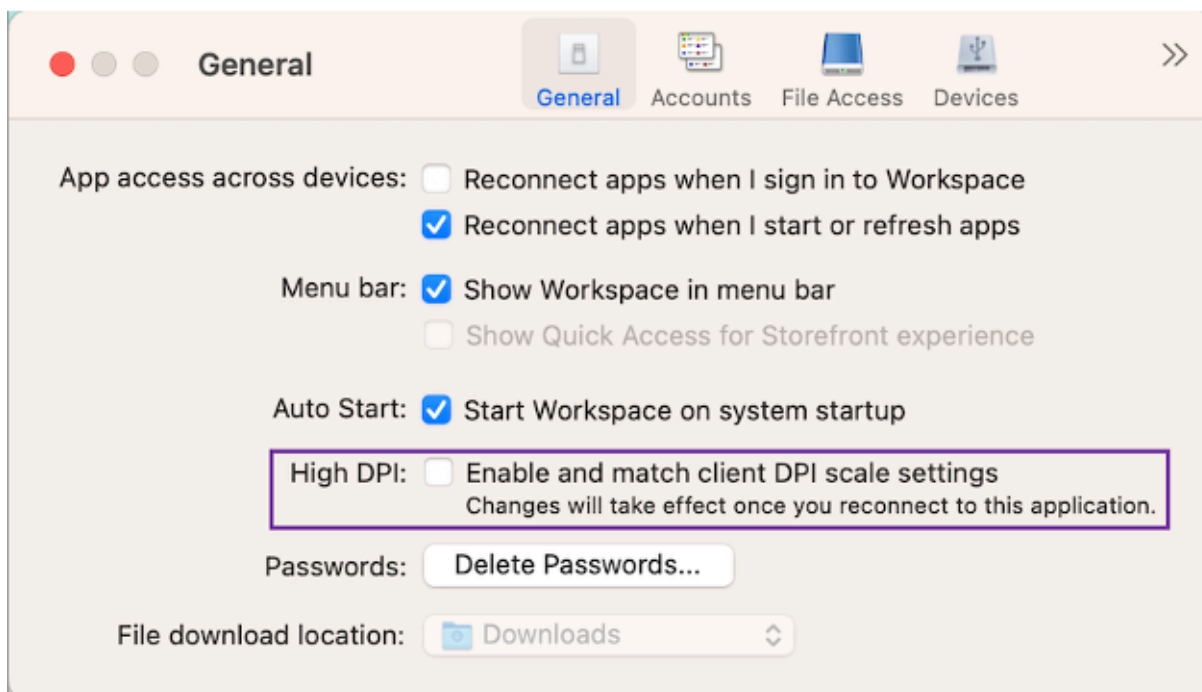
Bisher unterstützte die Citrix Workspace-App die Option **Hoher DPI-Wert** nur für virtuelle Desktopsitzungen.

Ab Version 2308 kann die Option **Hoher DPI-Wert** auch für Seamless-App-Sitzungen aktiviert werden. Außerdem können Sie die Option “Hoher DPI-Wert” jetzt auf drei 4K-Monitoren aktivieren. Diese Features sind standardmäßig deaktiviert.

Um die Option **Hoher DPI-Wert** zu aktivieren, müssen Sie **Einstellungen > Allgemein** auswählen. Wählen Sie auf der Registerkarte **Allgemein** die Option **DPI-Skalierungseinstellungen des Clients aktivieren und übernehmen**. Starten Sie die Anwendungen neu, damit die Änderungen wirksam werden.

Hinweis:

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.



Unterstützung für Aktivitätsmanager in Cloudstores

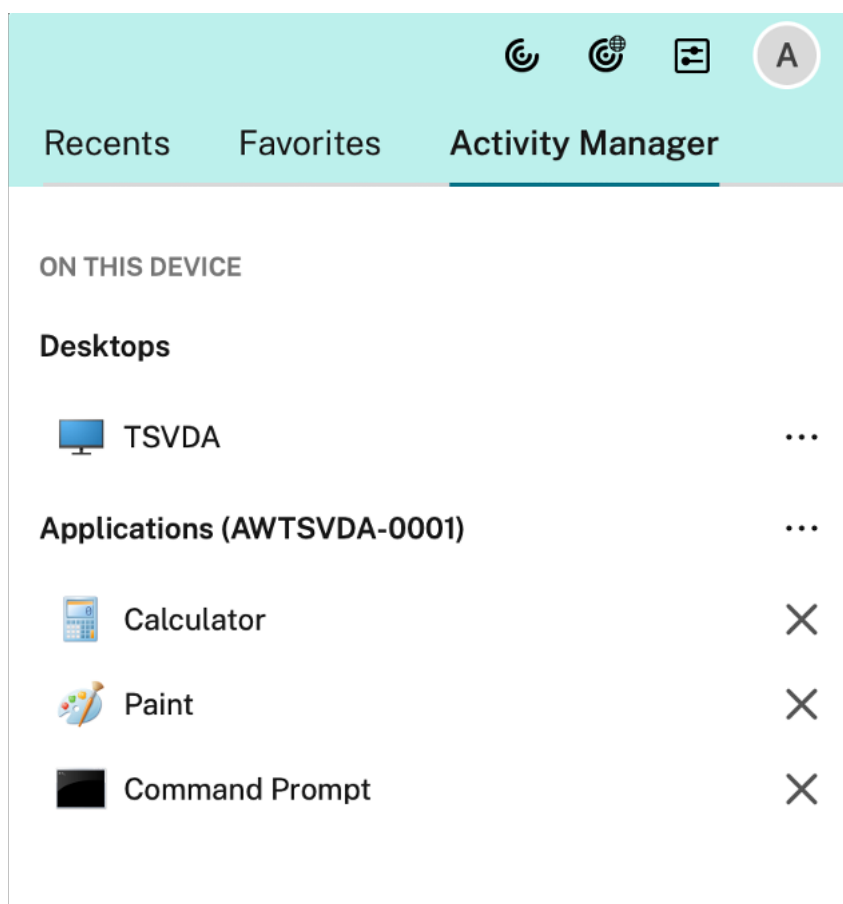
Dieses Feature ist ab Release 2308 als Technical Preview verfügbar.

Die Citrix Workspace-App für Mac unterstützt das Feature “Aktivitätsmanager”. Mit diesem Feature können Endbenutzer alle aktiven App- und Desktopsitzungen auf einen Blick anzeigen und damit interagieren. Sie können die aktiven Sitzungen direkt im Aktivitätsmanager trennen oder beenden.

Um aktive Sitzungen im **Aktivitätsmanager** anzuzeigen, wählen Sie in der Menüleiste das Symbol der Citrix Workspace-App und klicken dann auf **Aktivitätsmanager**. Um die Verbindung zu aktiven Desktopsitzungen zu trennen, wählen Sie das entsprechende Dreipunktmenü (...) und klicken dann auf **Trennen**. Klicken Sie auf die Schaltfläche “X”, um die aktive App-Sitzung zu beenden. Weitere Informationen finden Sie unter [Aktivitätsmanager](#).

Hinweise

- Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Um dieses Feature in Ihrer Umgebung zu aktivieren, füllen Sie das [Podio-Formular](#) aus.
- Sie können Feedback zu diesem Feature mit dem [Podio-Formular](#) geben.



Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit On-Premises-Stores

Dieses Feature ist ab Release 2308 als Technical Preview verfügbar.

Bisher wurde die FIDO2-basierte kennwortlose Authentifizierung für die Verbindung zu Cloudstores unterstützt. Weitere Informationen finden Sie unter [FIDO2-Authentifizierung beim Verbinden mit einem Cloudstore](#).

Ab dieser Version können Benutzer mithilfe der FIDO2-Authentifizierung auch eine Verbindung zu On-Premises-Stores herstellen. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Desktops, die FIDO2 unterstützen, authentifizieren. Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code und Touch ID. Dieses Feature wird unter macOS 12 und späteren Versionen unterstützt.

Mit den folgenden Einstellungen können Sie den Browsertyp auswählen, der für die Authentifizierung eines Endbenutzers in der Citrix Workspace-App verwendet wird:

| Einstellungen | Beschreibung |
|-----------------------------------|---|
| System | Hiermit können Sie den Standardbrowser des Benutzers für die Authentifizierung verwenden (z. B. Safari oder Chrome). Die Authentifizierung erfolgt außerhalb der Citrix Workspace-App. Verwenden Sie diese Einstellung, um die kennwortlose Authentifizierung zu unterstützen. Diese Einstellung versucht, die bestehende Benutzersitzung vom Browser des Benutzers zu verwenden. |
| SystemWithPrivateSession | Diese Einstellung ähnelt der Einstellung System . Die Citrix Workspace-App verwendet eine private Sitzung im Browser für die Authentifizierung. Der Browser speichert keine Authentifizierungscookies oder -daten. Single Sign-On wird in dieser Option nicht unterstützt. |
| Eingebettet | Ermöglicht die Authentifizierung innerhalb der Citrix Workspace-App. Die Citrix Workspace-App speichert die Sitzungsdaten oder Cookies für den Single Sign-On (z. B. SaaS-Apps), wenn das erweiterte Single Sign-On-Feature aktiviert ist. Diese Authentifizierungsmethode unterstützt keine kennwortlosen Authentifizierungen wie FIDO2. |
| EmbeddedWithPrivateSession | Diese Einstellung ähnelt der Einstellung Embedded . Single Sign-On wird nicht unterstützt, da keine Sitzungsdaten oder Cookies in der Citrix Workspace-App vorhanden sind. |

Um die konfigurierten Einstellungen zu übertragen, führen Sie die folgenden Befehle über die Mobilgeräteverwaltung (MDM), Global App Configuration Service (GACS) oder die Befehlszeilenschnittstelle aus:

- **FIDO2 mit MDM aktivieren:** Um die Authentifizierung per Mobilgeräteverwaltung (MDM) zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
<key>WebBrowserForAuthentication</key><string>System</string>
```

- **FIDO2 mit GACS aktivieren:** Um die Authentifizierung per GACS zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Web browser for Authenticating into Citrix Workspace",
11    "description": "Allows admin to select the type of browser used
12      for authenticating an end user into Citrix Workspace app",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        "assignedTo": [
19          "AllUsersNoAuthentication"
20        ],
21        "category": "authentication",
22        "settings": [
23
24          {
25            "name": "web browser for authentication",
26            "value": "SystemWithPrivateSession"
27          }
28
29        ],
30        "userOverride": false
31      }
32
33    ]
34  }
35
36 }
37
38 }
39
40
41 <!--NeedCopy-->
```

- **FIDO2 über die Befehlszeilenschnittstelle aktivieren:** Um die Authentifizierung per Befehlszeilenschnittstelle zu aktivieren, müssen Administratoren den folgenden Befehl ausführen:

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication  
System
```

Hinweise

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.

Storebasierte Konfiguration des Dateizugriffs

Dieses Feature ist ab Release 2308 als Technical Preview verfügbar.

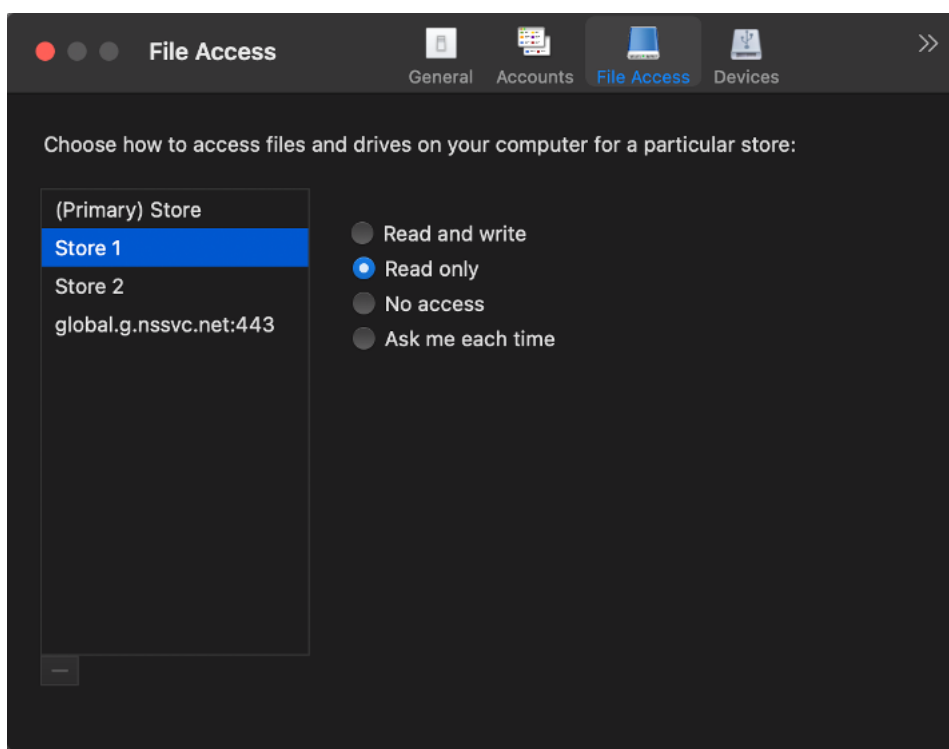
Ab Release 2308 ist der storebasierte Dateizugriff als Bestandteil der clientselektiven Vertrauensfunktion enthalten. Mit dieser Verbesserung können Sie den Zugriff auf Dateien pro Store gewähren.

Um den Dateizugriff für einen Store zu aktivieren, müssen Sie **Einstellungen > Dateizugriff** wählen. Wählen Sie auf der Registerkarte **Dateizugriff** den Store und den Zugriffstyp, der für den Store erforderlich ist. Sie können eine der folgenden Zugriffsarten für Dateien und Laufwerke auf Ihrem Computer wählen:

- **Lesen und Schreiben:** Ermöglicht Lese- und Schreibzugriff auf Dateien und Laufwerke für den ausgewählten Store.
- **Lesezugriff:** Ermöglicht einen schreibgeschützten Zugriff auf Dateien und Laufwerke für den ausgewählten Store.
- **Kein Zugriff:** Beschränkt den Zugriff auf Dateien und Laufwerke für den ausgewählten Store.
- **Jedes Mal fragen:** Erlaubnis wird jedes Mal angefordert, wenn der Lese- oder Schreibzugriff auf Dateien und Laufwerke für den ausgewählten Store erforderlich ist.

Hinweise

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.



Unterstützung der Bildschirmfreigabe bei aktiviertem App Protection

Dieses Feature ist ab Release 2308 als Technical Preview verfügbar.

Ab Release 2308 können Sie auch dann Inhalte über Microsoft Teams mit HDX-Optimierung teilen, wenn App Protection aktiviert ist. Mit diesem Feature können Sie Bildschirme in der virtuellen Desktopsitzung optimal teilen.

Hinweise

- Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.
- Sie können Feedback zu diesem Feature mit dem [Podio-Formular](#) geben.

Tastenkombination für Symbolleiste auf dem virtuellen Desktop

Dieses Feature ist ab Release 2307 als Technical Preview verfügbar.

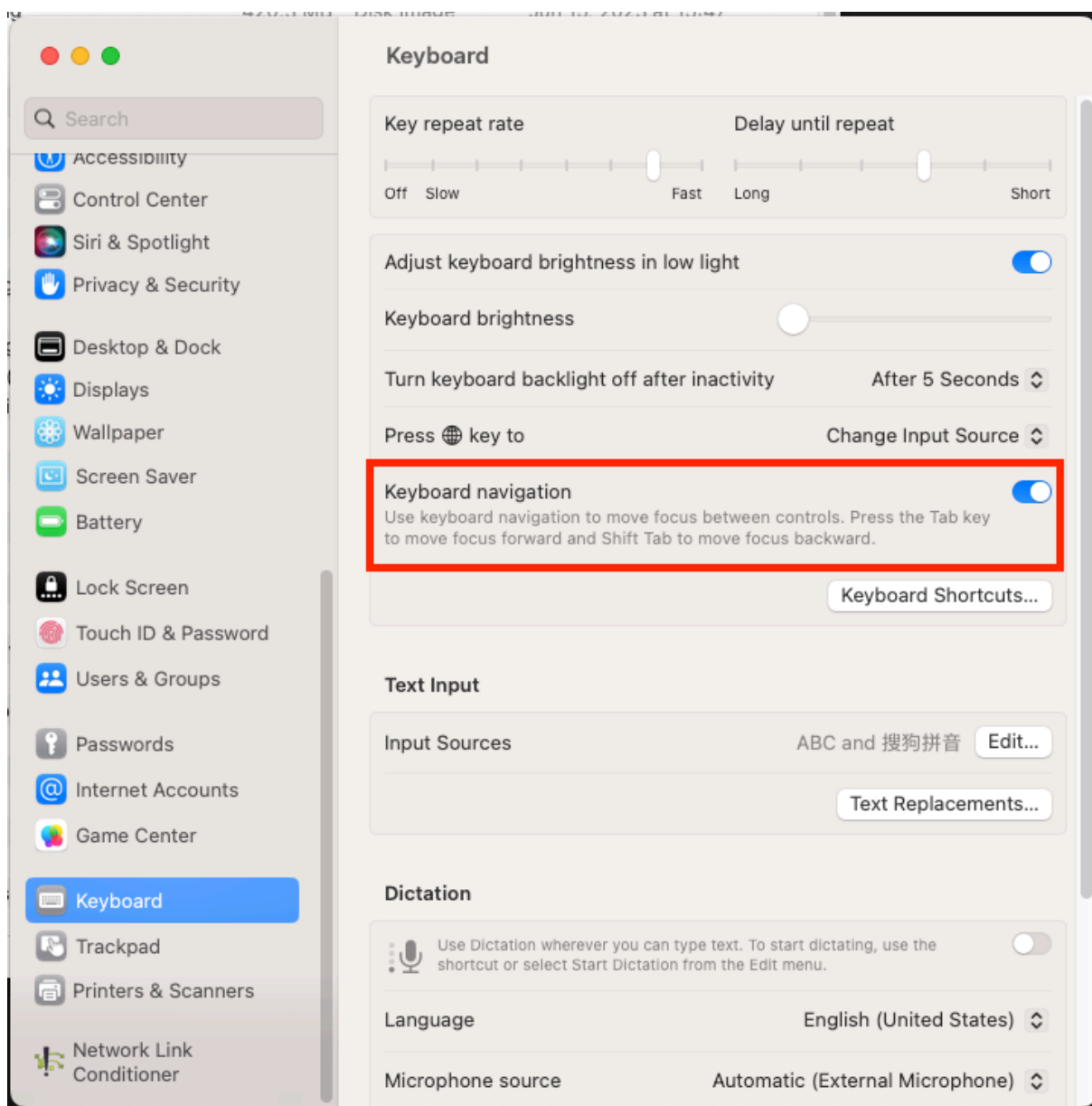
Ab Release 2307 können Sie für über Tastenkombinationen auf die Symbolleiste der virtuellen Desktopinfrastruktur (VDI) zugreifen. Klicken Sie hierfür im **CITRIX VIEWER** in der Menüleiste auf **ANSICHT** und wählen Sie **Tastenkombination für Symbolleiste verwenden**. Standardmäßig ist die Option **Tastenkombination für Symbolleiste verwenden** aktiviert.



Sie können folgende Tastenkombinationen verwenden, um über die Tastatur auf die VDI-Symbolleiste zuzugreifen:

- **Umschalt + Befehl + T**: Aktivieren der VDI-Symbolleiste.
- **Tab**: Navigieren durch die VDI-Symbolleiste im Uhrzeigersinn.
- **Umschalt + Tab**: Navigieren durch die VDI-Symbolleiste entgegen dem Uhrzeigersinn.
- **Leertaste**: Auswahl einer Option auf der VDI-Symbolleiste.
- **Esc**: Schließen eines Modals im Fokus.

Das Fenster für die Symbolleisten und CWA-Einstellungen unterstützt jetzt die **Tastatursteuerung**, die den Wechsel zwischen den UI-Elementen erleichtert und das fokussierte Element hervorhebt.



Hinweise

- Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.
- Sie können Feedback zu diesem Feature mit dem [Podio-Formular](#) geben.

Client App Management

Dieses Feature ist ab Release 2305 als Technical Preview verfügbar.

Die Citrix Workspace-App 2305 für Mac bietet jetzt Client-App-Verwaltungsfunktionen, mit der die Citrix Workspace-App als einzige Client-App auf dem Endpunkt erforderlich ist, um Agents wie das EPA-Plug-In zu installieren und zu verwalten.

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

Hinweis:

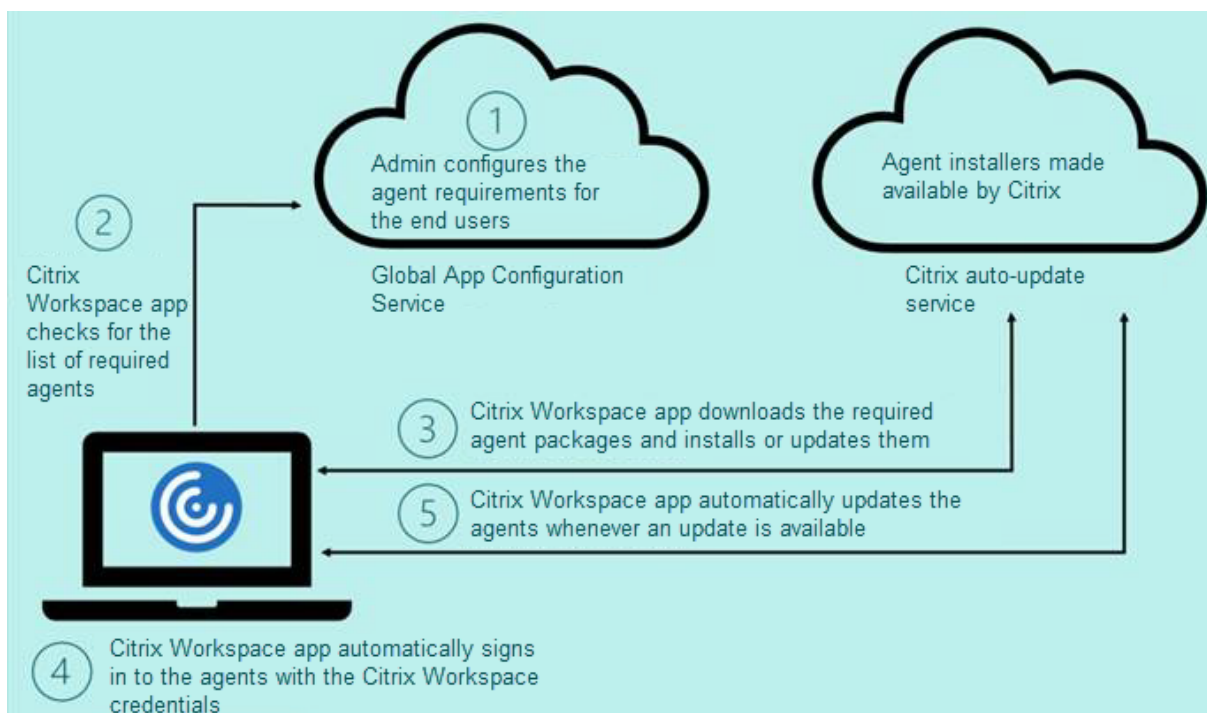
- Dieses Feature ist nur in Workspace-Sitzungen (Cloud) verfügbar.
- Der Global App Configuration Service ist eine Voraussetzung für dieses Feature.

Client App Management umfasst die folgenden Schritte:

- Administratoren müssen die auf den Endbenutzergeräten erforderlichen Agents im Global App Configuration Service angeben. In dieser Technical Preview können Administratoren einen 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.

Im folgenden Diagramm ist der Workflow dargestellt:



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

```

1  {
2
3    "serviceURL": {
4
5      "url": "https://serviceURL:443"
6    }
7  ,
8    "settings": {
9
10     "name": "Client App management",
11     "description": "Client App management",
12     "useForAppConfig": true,
13     "appSettings": {
14
15       "macos": [
16         {
17
18           "category": "AutoUpdate",
19           "userOverride": false,
20           "assignedTo": [
21             "AllUsersNoAuthentication"
22           ],
23           "settings": [

```

```
24         {
25
26             "name": "Auto update plugins settings",
27             "value": [
28                 {
29
30                     "pluginName": "Citrix Endpoint
31     Analysis",
32                     "pluginId": "7303CB73-42EE-42BB-
33     A908-9E6575912106",
34                     "pluginSettings": {
35                         "deploymentMode": "
36     InstallAndUpdate",
37                         "upgradeToLatest": true,
38                         "minimumAllowedVersion": "1.0",
39                         "maximumAllowedVersion": "24.0"
40
41                     ,
42                     "delayGroup": "Medium",
43                     "stream": "",
44                     "isFTU": true,
45                     "isBlocking": true,
46                     "detectRule": ""
47                 }
48             ]
49         }
50     ]
51 }
52
53 ]
54 }
55
56 }
57
58 }
59
60
61 <!--NeedCopy-->
```

In der folgenden Tabelle werden die Einstellungen, Werte und Beschreibung für Client App Manage-

ment aufgeführt.

| Schemaeinstellung | Wert | Beschreibung |
|-----------------------|-------------------------|--|
| isBlocking | “True” oder “False” | Wenn der Parameter “isBlocking” auf “true” gesetzt ist, wird das Plug-In als obligatorisch betrachtet. 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). |
| deploymentMode | InstallAndUpdate/Update | |
| maximumAllowedVersion | | Maximal zulässige Version des Plug-Ins. |
| minimumAllowedVersion | | Minimal zulässige Version des Plug-Ins. |
| upgradeToLatest | “True” oder “False” | |

Ab Release 2301 können Administratoren automatische Updates von EPA-Clients für macOS über die Citrix Workspace-App sowie Single Sign-On bei Citrix Secure Access verwalten, sofern Sie bereits bei der Citrix Workspace-App angemeldet sind.

Automatische Updates von Endpoint Analysis (EPA)

Sie können jetzt automatische Updates von [EPA-Clients für macOS](#) über die Citrix Workspace-App verwalten. Administratoren müssen die auf den Endbenutzergeräten benötigten Agents im Global App Configuration Service festlegen. Wenn der Agent bereits installiert ist und eine neue Version des Agents verfügbar ist, wird dieses Update von der Citrix Workspace-App installiert. Die Citrix Workspace-App stellt sicher, dass die Agents automatisch aktualisiert werden, sobald zukünftig ein neues Update verfügbar ist.

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

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Client App management",
11    "description": "Client App management",
12    "useForAppConfig": true,
13    "appSettings": {
14
15      "macos": [
16        {
17
18          "category": "AutoUpdate",
19          "userOverride": false,
20          "assignedTo": [
21            "AllUsersNoAuthentication"
22          ],
23          "settings": [
24            {
25
26              "name": "Auto update plugins settings",
27              "value": [
28                {
29
30                  "pluginName": "Citrix Endpoint
31                    Analysis",
32                  "pluginId": "7303CB73-42EE-42BB-
33                    A908-9E6575912106",
34                  "pluginSettings": {
35
36                    "deploymentMode": "
37                      InstallAndUpdate",
38                    "upgradeToLatest": true,
39                    "minimumAllowedVersion": "1.0",
40                    "maximumAllowedVersion": "7.0",
41                    "delayGroup": "Medium",
42                    "stream": "",
43                    "isFTU": false,
```

```
41         "isBlocking": false,  
42         "detectRule": ""  
43     }  
44  
45     }  
46  
47     ]  
48 }  
49  
50 ]  
51 }  
52  
53 ]  
54 }  
55  
56 }  
57  
58 }  
59  
60  
61 <!--NeedCopy-->
```

Nachfolgend sind die Bedeutungen der Eigenschaften und ihre möglichen Werte für den Schlüssel “deploymentMode” aufgeführt:

- “InstallAndUpdate”: Das Plug-In kann neu installiert und durch eine neue Version aktualisiert werden.
- “Update”: Nur Updates sind zulässig, keine Neuinstallation.
- “None”: Für das Plug-In ist keine Aktion erforderlich.

Single Sign-On bei Citrix Secure Access mit der Citrix Workspace-App

Sie können Single Sign-On bei Citrix Secure Access verwenden, wenn Sie bereits an der Citrix Workspace-App angemeldet sind. Sie müssen sich dann nicht durch Eingabe der Anmeldeinformationen authentifizieren, wenn Sie sich an der Citrix Workspace-App anmelden und Citrix Secure Access öffnen. Die Authentifizierung erfolgt automatisch. Dieses Feature ermöglicht Single Sign-On für verschiedene Citrix-Anwendungen und verbessert damit das Benutzererlebnis. Dieses Feature ist nur für Kunden in Cloudstores verfügbar. Neben der neuesten Version der Citrix Workspace-App benötigen Sie eine kompatible Version von Citrix Secure Access (22.12.2 und spätere Versionen).

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Hinweise

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.

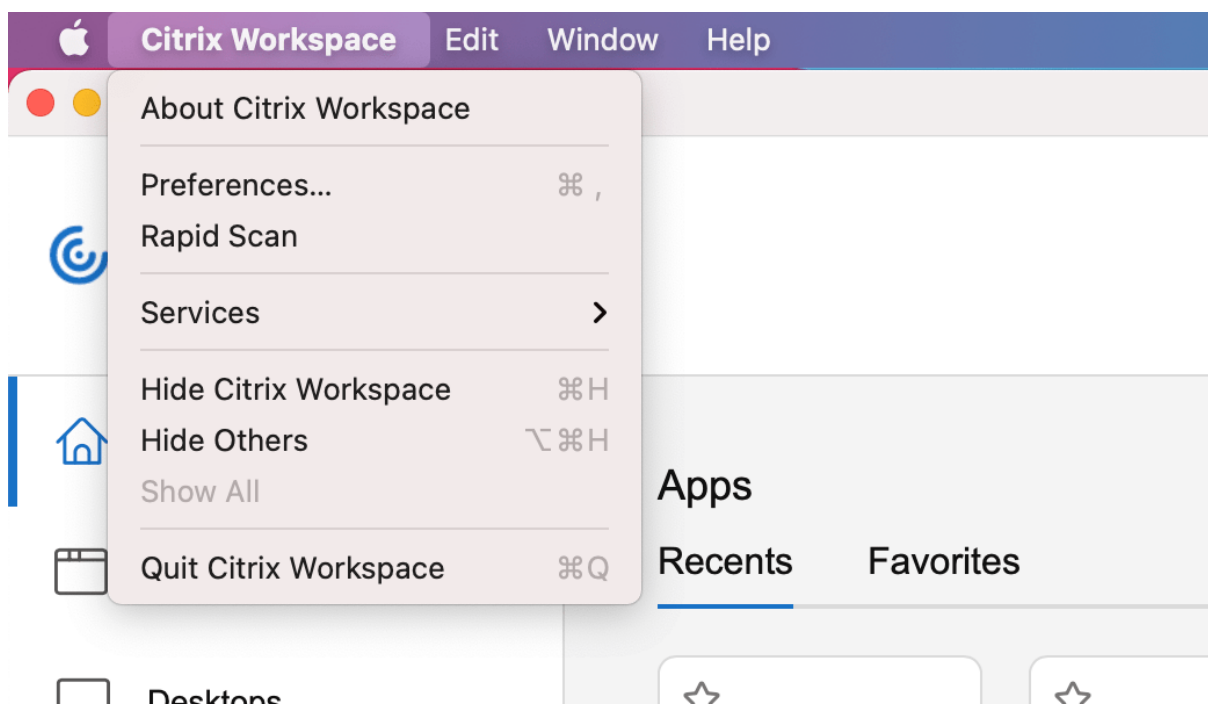
Schnellscan

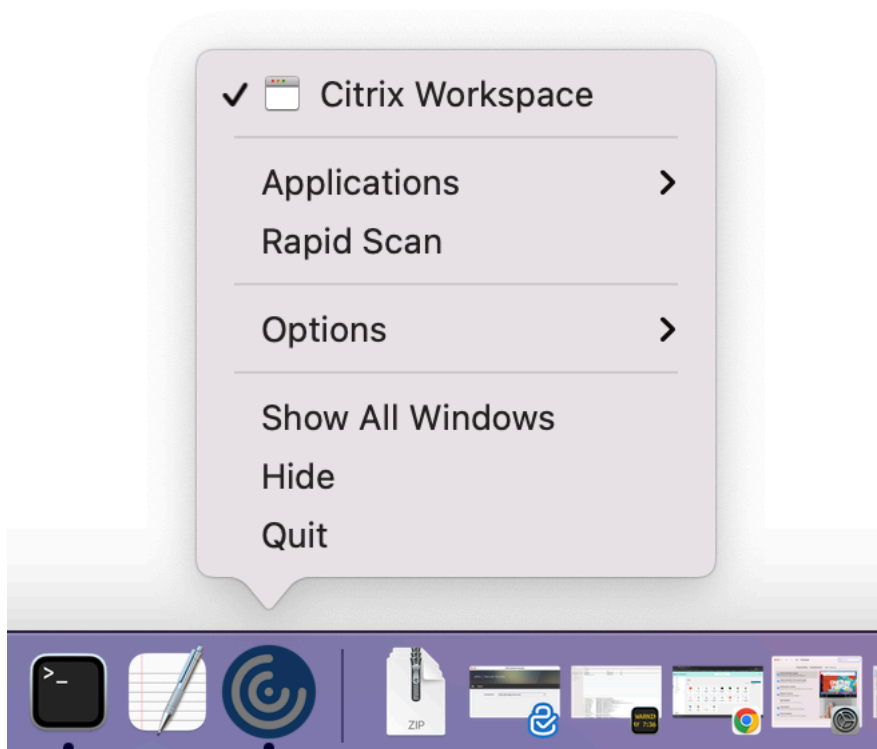
Dieses Feature ist ab Release 2304 als Technical Preview verfügbar.

Wenn Sie auf mehreren Geräten in der Citrix Workspace-App angemeldet sind, können Sie per Schnellscan mehrere Dokumente mit einem iOS-Gerät scannen und die gescannten Dokumente dann auf ein Mac-Gerät übertragen.

Führen Sie folgende Schritte aus, um Dokumente mit dem Schnellscan-Feature zu scannen:

1. Klicken Sie auf dem Mac-Gerät mit der rechten Maustaste auf das Symbol der Citrix Workspace-App in der Desktopsitzung und klicken Sie dann auf **Schnellscan**, um einen QR-Code anzuzeigen.
2. Klicken Sie auf Ihrem iOS-Gerät auf **Einstellungen > Schnellscan**.
3. Scannen Sie den auf dem Mac-Gerät angezeigten QR-Code, um Mac-Gerät und iOS-Gerät miteinander zu verbinden.
4. Scannen Sie ein beliebiges Dokument und senden Sie es an Ihr Mac-Gerät.
5. In der Desktopsitzung auf dem Mac-Gerät können Sie die gescannten Dokumente im Finder aufrufen.





Voraussetzungen

- Die Clientlaufwerkzuordnung (CDM) muss für den Store aktiviert sein.
- Sie müssen auf dem iOS- und Mac-Gerät mit demselben Konto in der Citrix Workspace-App angemeldet sein.
- Sie müssen mit demselben WLAN verbunden sein.
- Die erforderliche Mindestversion der Citrix Workspace-App für Mac ist 2304.
- Dieses Feature wird von der Citrix Workspace-App für iOS ab Version 23.3.5 unterstützt.
- Der Schnellscan erfordert Lese- und Schreibzugriff auf Ihrem Gerät. Führen Sie folgende Schritte aus, um den Zugriff zu aktivieren:
 1. Klicken Sie in Ihrem Profil auf **Anwendungseinstellungen > Storeeinstellungen**.
 2. Klicken Sie auf Ihren aktuellen Store.
 3. Klicken Sie auf **Gerätespeicher** und wählen Sie **Lese- und Schreibzugriff**.

Hinweise

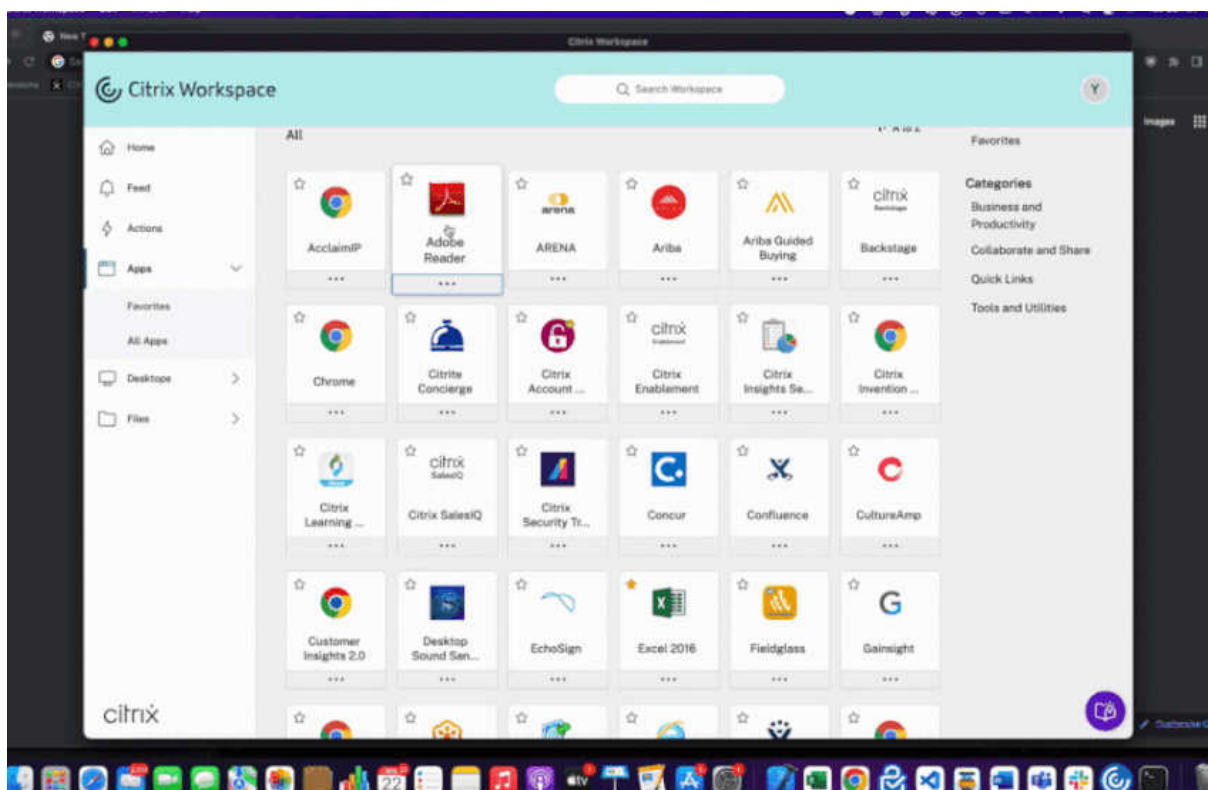
- Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-](#)

- [Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.
- Sie können Feedback zu diesem Feature mit dem [Podio-Formular](#) geben.

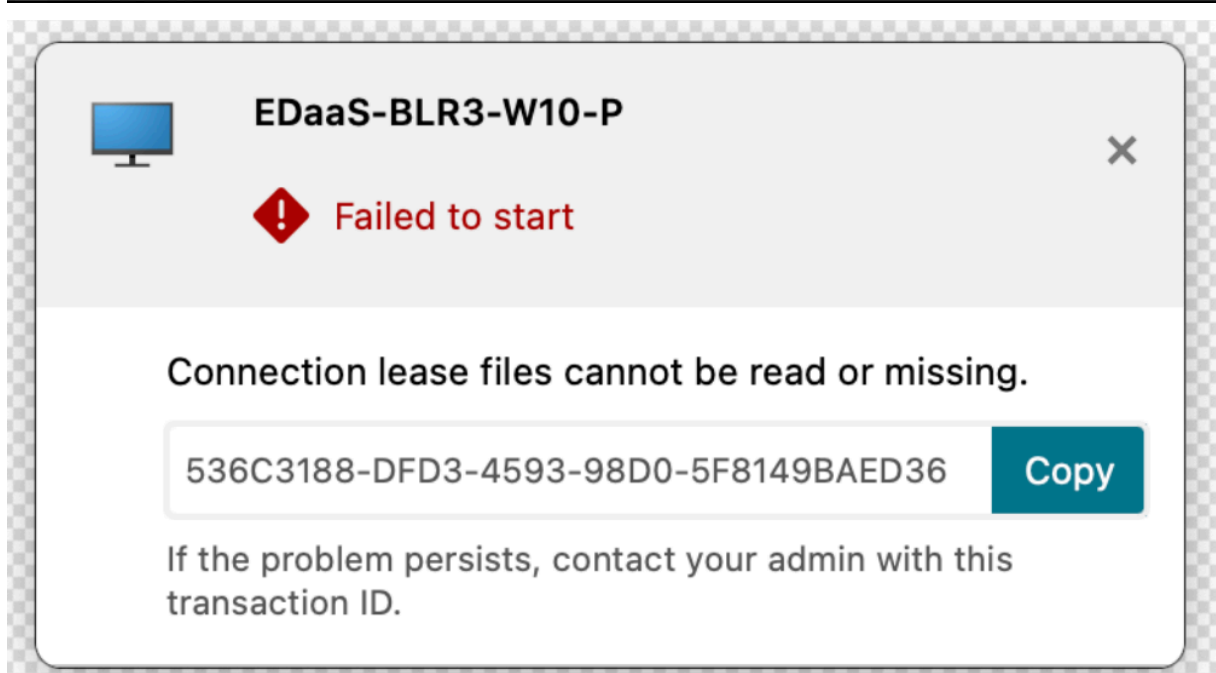
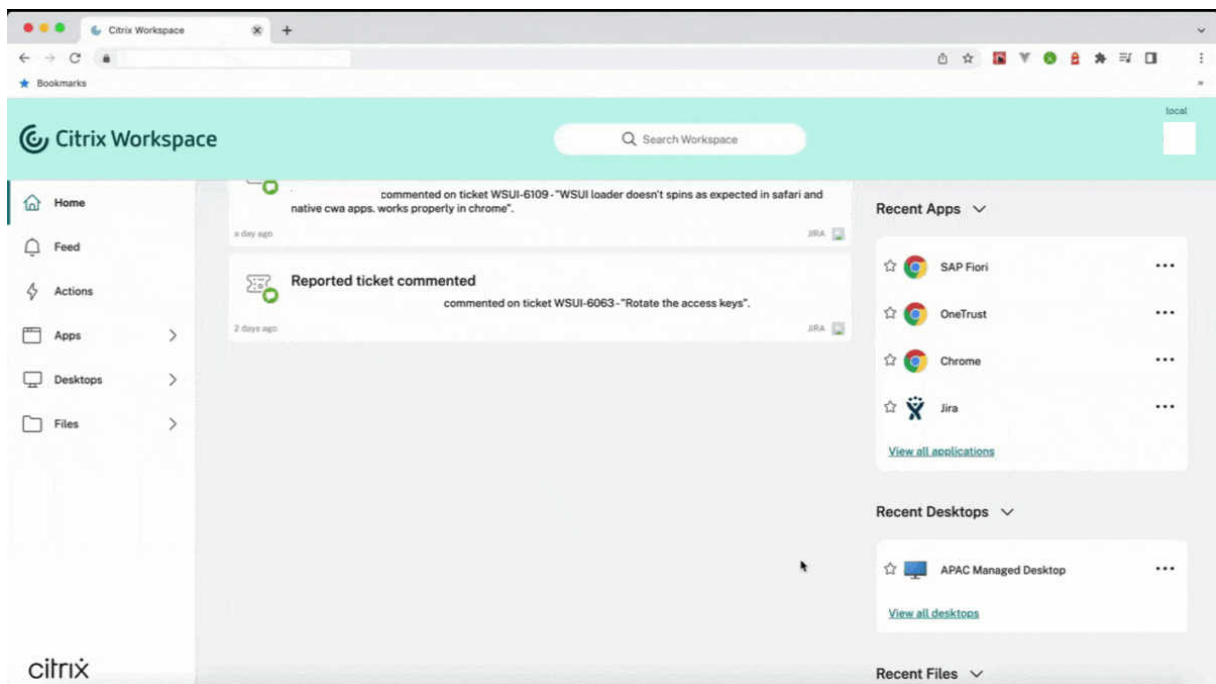
Verbesserter Start von virtuellen Apps und Desktops

Dieses Feature ist ab Release 2304 als Technical Preview verfügbar.

Das Öffnen von Citrix-Ressourcen wurde intuitiver, benutzerfreundlicher und informativer gestaltet. Ab Release 2304 wird der verbesserte Start virtueller Apps und Desktops für benutzerdefinierte Webstores und Hybridstart unterstützt. Weitere Informationen zum Start virtueller Apps und Desktops finden Sie unter [Verbessertes Startverhalten virtueller Apps und Desktops [Technical Preview]] (/en-us/citrix-workspace-app-for-mac/configure.html#improved-virtual-apps-and-desktops-launch-experience-technical-preview).



Die Benachrichtigung über den Startfortschritt wird jetzt in der unteren rechten Bildschirmcke angezeigt. Es erscheint eine Fortschrittsanzeige der Ressourcen, die gerade geöffnet werden. Wenn Sie die Benachrichtigung verwerfen, können Sie sie nicht erneut aufrufen. Nach dem Sitzungsstart ist die Benachrichtigung noch einige Sekunden zu sehen. Wenn die Sitzung nicht gestartet werden kann, enthält die Benachrichtigung eine Fehlermeldung.



Hinweis:

- Dieses Feature ist für Workspace (Cloud)- und StoreFront-Sitzungen verfügbar.
- Sie können Feedback zu dieser Technical Preview mit diesem [Podio-Formular](#) geben.

Unterstützung für mehrere Audiogeräte

Dieses Feature ist ab Release 2304 als Technical Preview verfügbar.

Ab Version 2304 zeigt die Citrix Workspace-App alle in einer Sitzung verfügbaren lokalen Audiogeräte mit Namen an. Darüber hinaus wird Plug and Play unterstützt.

Dieses Feature ist eine Preview und nur auf Anfrage verfügbar. Füllen Sie das [Podio-Formular](#) aus, um das Feature in Ihrer Umgebung zu aktivieren.

Hinweise

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.

Aktualisierte Version von WebRTC für optimiertes Microsoft Teams

Dieses Feature ist ab Release 2210 als Technical Preview verfügbar.

Die Version von WebRTC, die für optimiertes Microsoft Teams verwendet wird, wurde auf Version M98 aktualisiert.

Hinweise

Mit dem [Podio-Formular](#) können Sie Feedback zu diesem Feature geben.

Unterstützung für besseres Single Sign-On (SSO) bei Web- und SaaS-Apps

Dieses Feature ist ab Release 2203.1 als Technical Preview verfügbar.

Diese Funktion vereinfacht die Konfiguration von SSO für interne Web-Apps und SaaS-Apps bei Verwendung von externen Identitätsanbietern (IdP). Die verbesserte SSO-Erfahrung reduziert den gesamten Prozess auf einige Befehle. Es entfällt die Voraussetzung, Citrix Secure Private Access in der IdP-Kette konfigurieren zu müssen, um SSO einzurichten. Zudem ist die Benutzererfahrung verbessert, sofern die Authentifizierung bei der Citrix Workspace-App und bei der Web- oder SaaS-App, die von der Citrix Workspace-App gestartet wird, über denselben IdP erfolgt.

Hinweise

Sie können sich mit diesem [Podio-Formular](#) für die Technical Preview registrieren.

Unterstützung des Transport Layer Security (TLS)-Protokolls Version 1.3 auf Linux VDAs

Dieses Feature ist ab Release 2203.1 als Technical Preview verfügbar.

Wenn Sie TLS-Version 1.3 ausführen, können Sie jetzt eine Verbindung zu virtuellen Desktops und Apps herstellen, die auf dem Linux-Betriebssystem gehostet werden.

Hinweis:

- Sie können keine Verbindung zu virtuellen Windows-Desktops und -Apps herstellen, wenn Sie TLS-Version 1.3 ausführen.
- Sie können Feedback zu diesem Feature mit dem [Podio-Formular](#) geben.

Native Unterstützung für Mac mit Apple Silicon (M1- und M2-Serie)

December 1, 2023

Native Unterstützung für Mac mit Apple Silicon (M1- und M2-Serie) – Universal Architecture

Mit dem Release des Universal Architecture-Builds bietet die Citrix Workspace-App jetzt native Unterstützung für Macs mit Apple Silicon (M1- und M2-Serie). Der Universal Architecture-Build kann auf jedem Mac-Gerät ausgeführt werden, unabhängig von der Prozessorarchitektur.

Wenn Sie den x86_64 Intel-basierten Architekturbuild der Citrix Workspace-App für Macs mit Apple Silicon (M1- und M2-Serie) verwenden, müssen Sie die Rosetta-Emulation zum Ausführen der App verwenden.

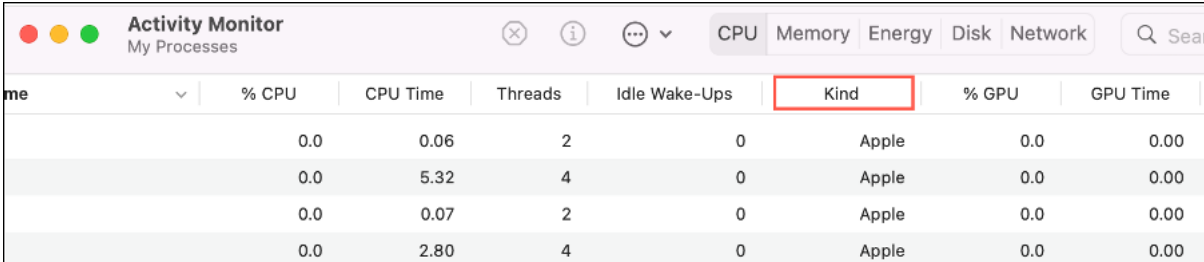
Sie finden die neueste Version von Universal Architecture-Build und x86_64 Intel-basiertem Architekturbuild unter [Downloads](#).

Hinweis:

Die Unterstützung für den x86_64 Intel-basierten Architekturbuild der Citrix Workspace-App wird in Kürze eingestellt. Citrix unterstützt weiterhin den Universal Architecture-Build für Intel-basierte Macs und Macs mit Apple Silicon (M1- und M2-Serie). Die Ankündigung wird im Abschnitt [Einstellung von Features und Plattformen](#) erfolgen.

Wenn Sie die Citrix Workspace-App auf einem Mac mit Apple Silicon (M1- und M2-Serie) verwenden, müssen Sie das HDX RealTime Optimization Pack (RTOP) aktualisieren. Als Upgrade können Sie HDX RealTime Media Engine 2.9.500 für Mac installieren, erhältlich auf der Citrix Website unter [Downloads](#).

Um festzustellen, ob die Citrix Workspace-App nativ unter Apple Silicon ausgeführt wird, öffnen Sie die **Aktivitätsanzeige** auf dem Mac. Die Spalte **Art** auf der Registerkarte **CPU** zeigt an, ob die Workspace-App auf einem Apple Silicon- oder Intel-Prozessor ausgeführt wird.



The screenshot shows the Activity Monitor window with the 'CPU' tab selected. The 'Kind' column is highlighted with a red box. The table below represents the data visible in the screenshot.

| Name | % CPU | CPU Time | Threads | Idle Wake-Ups | Kind | % GPU | GPU Time |
|------|-------|----------|---------|---------------|-------|-------|----------|
| | 0.0 | 0.06 | 2 | 0 | Apple | 0.0 | 0.00 |
| | 0.0 | 5.32 | 4 | 0 | Apple | 0.0 | 0.00 |
| | 0.0 | 0.07 | 2 | 0 | Apple | 0.0 | 0.00 |
| | 0.0 | 2.80 | 4 | 0 | Apple | 0.0 | 0.00 |

Migration zwischen verschiedenen Builds der Citrix Workspace-App

Sie können die Citrix Workspace-App vom x86_64 Intel-basierten Architekturbuild zum Universal Architecture-Build migrieren (und umgekehrt).

Zur Migration zwischen Builds laden Sie die neueste Build-Version unter [Downloads](#) herunter und führen eine manuelle Installation durch. Weitere Informationen finden Sie unter [Manuelle Installation](#).

Hinweis:

Die Deinstallation der App ist für die Migration zwischen Builds nicht erforderlich.

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (VCSDK) 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.

Laden benutzerdefinierter virtueller Kanäle auf Macs mit Apple Silicon (M1- und M2-Serie)

Als Endbenutzer können Sie das Custom Virtual Channel SDK (VCSDK) auf einen Mac mit M1- bzw. M2-Chipsatz laden. In der universellen Architektur müssen Sie das VCSDK laden, indem Sie Ihre benutzerdefinierten virtuellen Kanäle mit dem neuesten VCSDK auf dem Gerät mit M1- bzw. M2-Chip neu kompilieren. Sie können den Universal Architecture Build aus dem Bereich **Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture** unter [Downloads](#) herunterladen.

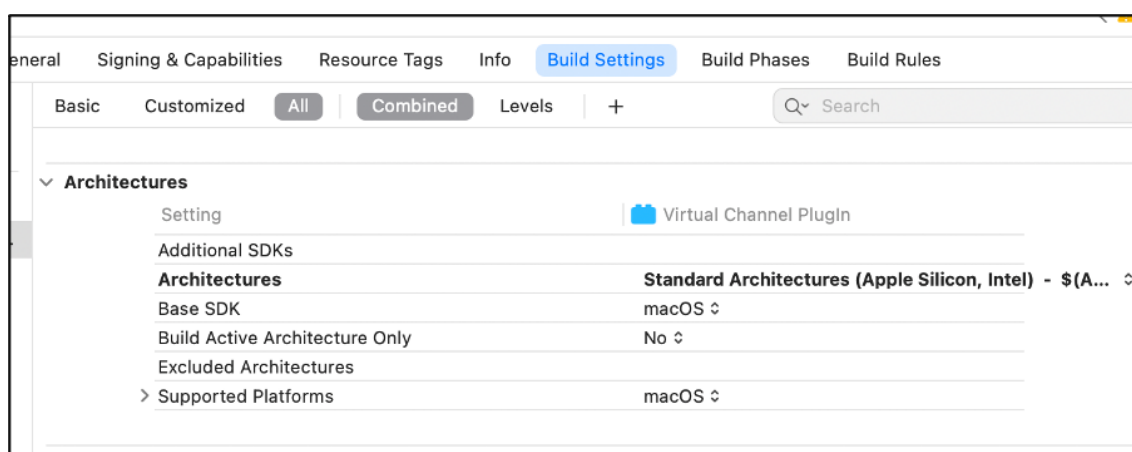
Gehen Sie wie folgt vor, um das VCSDK zu laden:

1. Laden Sie das Virtual Channel SDK 2204 für macOS von [Downloads](#) herunter.
2. Öffnen Sie Ihr Projekt für den benutzerdefinierten virtuellen Kanal in Xcode.
3. Ändern Sie Ihren Code.
4. Kompilieren Sie den benutzerdefinierten virtuellen Kanal, um das Paket für virtuelle Kanäle zu generieren.

Testen Sie Ihr Virtual Channel Software Development Kit (VCSDK)

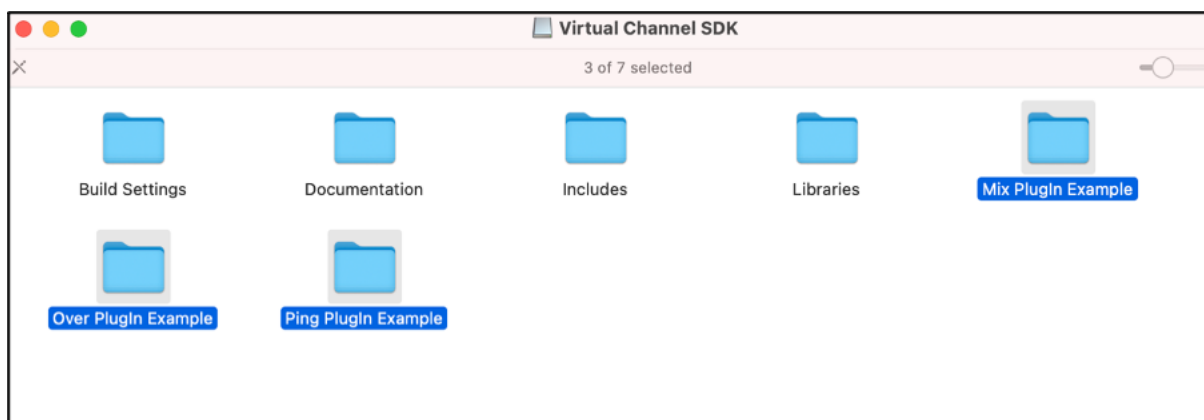
Wenn Sie das Citrix Virtual Channel Software Development Kit (VCSDK) verwenden, müssen Sie einige Anpassungen vornehmen, damit Ihre benutzerdefinierten virtuellen Kanäle ordnungsgemäß ausgeführt werden. Gehen Sie wie folgt vor, um Ihre VCSDKs zu testen:

1. Stellen Sie sicher, dass alle verknüpften Bibliotheken Ihrer benutzerdefinierten virtuellen Kanäle für Universal Binaries kompiliert sind.
2. Ändern Sie die Projektdatei, um Universal Binaries zu unterstützen:
 - Öffnen Sie **Project > Build Settings**.
 - Legen Sie **Architectures** auf **Standard Architectures** fest.



Muster für das VCSDK finden Sie in *VCSDK.dmg*. Diese Muster unterstützen die universelle macOS-Binärdatei von Apple, die nativ auf Apple Silicon- und auf Intel-basierten Macs ausgeführt wird. Sie

enthalten ausführbaren Code für beide Architekturen. Sie können diese Muster als Referenz verwenden.



Systemanforderungen und Kompatibilität

December 1, 2023

Unterstützte Betriebssysteme

Die Citrix Workspace-App für Mac unterstützt folgende Betriebssysteme:

- macOS Sonoma 14
- macOS Ventura 13.5.2
- macOS Monterey 12
- macOS Big Sur 11

Zu jedem Zeitpunkt unterstützt Citrix nur das neueste und die beiden vorherigen macOS-Betriebssysteme (N, N-1 und N-2).

Kompatible Citrix Produkte

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.

Kompatible Browser

Die Citrix Workspace-App für Mac ist mit den folgenden Browsern kompatibel:

- Google Chrome

- Microsoft Edge
- Safari

Hardwareanforderungen

- 1 GB freier Datenträgerspeicher
- Eine funktionierende Netzwerk- oder Internetverbindung für die Verbindung mit Servern

Verbindungen, Zertifikate und Authentifizierung

Verbindungen

Die Citrix Workspace-App für Mac unterstützt folgende Verbindungen mit Citrix Virtual Apps and Desktops und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service):

- HTTPS
- ICA-über-TLS
- ICA-über-DTLS

Die Citrix Workspace-App für Mac unterstützt folgende Konfigurationen:

| Für LAN-Verbindungen | Für sichere Remote- oder lokale Verbindungen |
|--|--|
| StoreFront mit StoreFront Services oder Citrix Receiver für Web-Site | Citrix Gateway 12.x-13.x, einschließlich VPX |

Zertifikate

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, müssen Sie das Stammzertifikat für die Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installieren. Anschließend können Sie mit der Citrix Workspace-App für Mac erfolgreich auf Citrix-Ressourcen zugreifen.

Hinweis:

Wenn das Zertifikat des Remotegateways beim Herstellen der Verbindung nicht verifiziert werden kann, wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt, da das Stammzertifikat nicht im lokalen Schlüsselspeicher vorhanden ist. Wenn ein Benutzer versucht, einen Store hinzuzufügen, schlägt der Vorgang fehl. Im Webbrowser kann der Benutzer sich möglicherweise beim Store authentifizieren, Verbindungen zu Sitzungen schlagen jedoch fehl.

Importieren von Stammzertifikaten für Geräte

Rufen Sie das Stammzertifikat des Zertifikatausstellers ab und senden Sie es an ein Konto, das auf dem Gerät konfiguriert ist. Wenn Sie auf den Anhang klicken, werden Sie zum Importieren des Stammzertifikats aufgefordert.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App für Mac unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate mit Citrix Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat zugeordnet werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu [Citrix Gateway](#). Weitere Informationen zum Installieren, Verknüpfen und Aktualisieren von Zertifikaten finden Sie unter [How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway](#).

Validierungsrichtlinie für Serverzertifikate

Die Citrix Workspace-App für Mac hat eine strenge Validierungsrichtlinie für Serverzertifikate.

Wichtig

Bestätigen Sie vor der Installation dieser Version der Citrix Workspace-App für Mac, dass die Server- oder Gateway-Zertifikate wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:

- Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
- Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
- Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
- Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet die Citrix Workspace-App für Mac **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Die Citrix Workspace-App für Mac prüft dann, ob die Zertifikate vertrauenswürdig sind. Wenn keines der Zertifikate vertrauenswürdig ist, schlägt die Verbindung fehl.

Diese Richtlinie ist strenger als die Zertifikatrichtlinie in Webbrowsern. Viele Webbrowser enthalten eine große Anzahl Stammzertifikate, denen sie vertrauen.

Der Server bzw. das Gateway muss mit den richtigen Zertifikaten konfiguriert sein. Sind nicht die richtigen Zertifikate vorhanden, schlägt die Verbindung mit der Citrix Workspace-App für Mac u. U. fehl.

Angenommen, ein Gateway ist mit gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen. Dabei wird genau ermittelt, welches Stammzertifikat die Citrix Workspace-App für Mac verwendet.

Die Citrix Workspace-App für Mac überprüft, ob alle Zertifikate gültig sind. Die Citrix Workspace-App für Mac überprüft ebenfalls, ob dem "Stammzertifikat" bereits vertraut wird. Wenn die Citrix Workspace-App für Mac dem "Stammzertifikat" nicht vertraut, schlägt die Verbindung fehl.

Wichtig

Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet. Beispielsweise gibt es derzeit zwei Zertifikate ("DigiCert/GTE CyberTrust Global Root" und "DigiCert Baltimore Root/Baltimore CyberTrust Root"), mit denen die gleichen Serverzertifikate validiert werden können. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar ("DigiCert Baltimore Root/Baltimore CyberTrust Root"). Wenn Sie "GTE CyberTrust Global Root" auf dem Gateway konfigurieren, schlagen die Citrix Workspace-App für Mac-Verbindungen auf diesen Benutzergeräten fehl. Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist. Stammzertifikate laufen wie alle Zertifikate irgendwann ab.

Hinweis:

Einige Server und Gateways senden nie das Stammzertifikat, selbst wenn es konfiguriert ist. Eine strengere Validierung ist dann nicht möglich.

Angenommen, ein Gateway ist mit diesen gültigen Zertifikaten konfiguriert. Wir empfehlen die folgende Konfiguration ohne das Stammzertifikat:

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

Die Citrix Workspace-App für Mac verwendet dann die beiden Zertifikate. Dann sucht die App nach einem Stammzertifikat auf dem Benutzergerät. Wird ein vertrauenswürdiges Zertifikat gefunden, das korrekt validiert wird, z. B. "Beispielstammzertifikat", ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt das von der Citrix Workspace-App für Mac benötigte Zwischenzertifikat zur Verfügung, ermöglicht der Citrix Workspace-App für Mac aber auch die Wahl eines gültigen, vertrauenswürdigsten Stammzertifikats.

Nehmen wir nun an, ein Gateway ist mit den folgenden Zertifikaten konfiguriert:

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

- “Falsches Stammzertifikat”

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Die Citrix Workspace-App für Mac ignoriert das falsche Stammzertifikat jedoch nicht und die Verbindung schlägt fehl.

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall ist das Gateway normalerweise wie folgt mit allen Zwischenzertifikaten konfiguriert, jedoch nicht mit dem Stammzertifikat:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat 1”
- “Beispielzwischenzertifikat 2”

Wichtig

Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat, das für Situationen gedacht ist, in denen es mehr als ein Stammzertifikat gibt. Ein früher ausgestelltes Stammzertifikat wird gleichzeitig mit einem später ausgestellten Stammzertifikat verwendet. In diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden. Beispielsweise hat das früher ausgestellte Stammzertifikat “Class 3 Public Primary Certification Authority” das entsprechende übergreifende Zwischenzertifikat “Verisign Class 3 Public Primary Certification Authority - G5”. Ein entsprechendes später ausgestelltes Stammzertifikat “Verisign Class 3 Public Primary Certification Authority - G5” ist ebenfalls verfügbar und es ersetzt “Class 3 Public Primary Certification Authority”. Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.

Hinweis

Das übergreifende Zwischenzertifikat und das Stammzertifikat haben denselben Antragstellernamen (Ausgestellt für), das übergreifende Zwischenzertifikat hat jedoch einen anderen Ausstellernamen (Ausgestellt von). Dieser Unterschied im Namen unterscheidet das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat (wie Beispielzwischenzertifikat 2).

Normalerweise empfiehlt sich die folgende Konfiguration ohne das Stammzertifikat und das übergreifende Zwischenzertifikat:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

Konfigurieren Sie das Gateway nicht für die Verwendung des übergreifenden Zwischenzertifikats, weil es sonst das früher ausgestellte Stammzertifikat auswählt:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Übergreifendes Beispielzwischenzertifikat” [nicht empfohlen]

Es wird nicht empfohlen, das Gateway nur mit dem Serverzertifikat zu konfigurieren:

- “Beispielserverzertifikat”

In diesem Fall schlägt die Verbindung fehl, wenn die Citrix Workspace-App für Mac nicht alle Zwischenzertifikate finden kann.

Authentifizierung

Für Verbindungen mit StoreFront unterstützt die Citrix Workspace-App für Mac die folgenden Authentifizierungsmethoden:

| | Workspace für Web über Browser | StoreFront Services-Site (nativ) | Citrix Gateway bei Workspace für Web (Browser) | Citrix Gateway bei StoreFront Services-Site (nativ) |
|---|--------------------------------|----------------------------------|--|---|
| Anonym | Ja | Ja | | |
| Domäne | Ja | Ja | Ja* | Ja* |
| Domänen-Passthrough | | | | |
| Sicherheitstoken | | | Ja* | Ja* |
| Zweistufige Authentifizierung (Domäne mit Sicherheitstoken) | | | Ja* | Ja* |
| SMS | | | Ja* | Ja* |
| Smartcard | Ja | Ja | Ja* | Ja |
| Benutzerzertifikat | | | Ja | Ja (Citrix Gateway Plug-In) |

* Nur für Bereitstellungen verfügbar, die Citrix Gateway mit oder ohne installiertem zugeordneten Plug-In auf dem Gerät enthalten.

Installieren, Deinstallieren und Aktualisieren

November 21, 2023

Citrix Workspace-App für Mac enthält ein Installationspaket und unterstützt Remotezugriff über Citrix Gateway und Secure Web Gateway.

Sie können die Citrix Workspace-App für Mac auf folgende Weise installieren:

- Über die Citrix Website
- Automatisch aus Workspace für Web
- Mit einem ESD-Tool (Electronic Software Distribution)

Standardmäßig ist die Citrix Workspace-App im Verzeichnis **Anwendungen** installiert. Die Installationspfade sind wie folgt:

- Vollständige Installation – `"/Applications/Citrix\ Workspace.app/"`
- Ausführbare Datei der Citrix Workspace-App für Mac – `"/Applications/Citrix\ Workspace.app/Contents/MacOS/Citrix\ Workspace"`

Manuelle Installation

Von einem Benutzer von Citrix.com

Erstbenutzer können die Citrix Workspace-App für Mac von Citrix.com oder der eigenen Downloadsite herunterladen. Sie können dann ein Konto durch Eingabe einer E-Mail-Adresse anstelle einer Server-URL einrichten. Die Citrix Workspace-App für Mac ermittelt das Citrix Gateway oder den StoreFront-Server, der der E-Mail-Adresse zugeordnet ist. Anschließend wird der Benutzer aufgefordert, sich anzumelden und die Installation fortzusetzen. Dieses Feature wird als e-mail-basierte Kontenermittlung bezeichnet.

Hinweis:

Ein Erstbenutzer ist ein Benutzer, auf dessen Gerät die Citrix Workspace-App für Mac nicht installiert ist.

Die e-mail-basierte Kontenermittlung wird für einen Erstbenutzer nicht angewendet, wenn der Download von einem anderen Speicherort als Citrix.com erfolgte (z. B. von einer Citrix Receiver für Website).

Wenn die Citrix Workspace-App für Mac für Ihre Site konfiguriert werden muss, verwenden Sie eine andere Bereitstellungsmethode.

Mit einem ESD-Tool (Electronic Software Distribution)

Ein Erstbenutzer der Citrix Workspace-App für Mac muss eine Server-URL für das Einrichten des Kontos eingeben.

Von der Citrix Downloads-Seite

Sie können die Citrix Workspace-App für Mac von einer Netzwerkfreigabe oder direkt auf dem Benutzergerät installieren. Sie können die App installieren, wenn Sie die Datei von der Citrix-Website unter [Downloads](#) herunterladen.

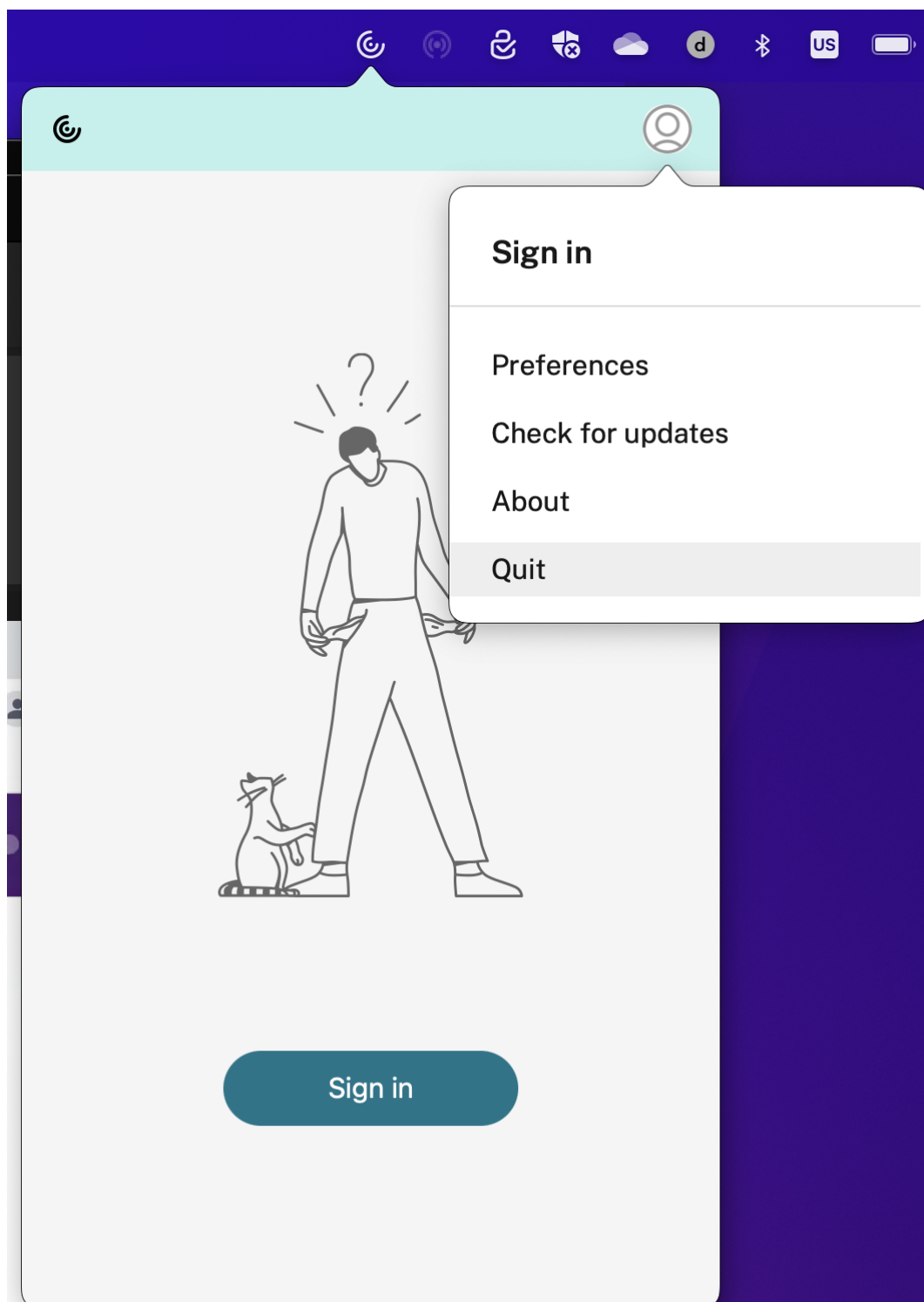
Installieren der Citrix Workspace-App für Mac:

1. Laden Sie die DMG-Datei für die gewünschte Version der Citrix Workspace-App für Mac von der Citrix-Website herunter.
2. Öffnen Sie die heruntergeladene Datei.
3. Klicken Sie auf der Eröffnungsseite auf **Weiter**.
4. Klicken Sie auf der Seite **Lizenzierung** auf **Weiter**.
5. Klicken Sie auf **Akzeptieren**, um die Bedingungen der Lizenzvereinbarung zu akzeptieren.
6. Klicken Sie auf der Seite **Installationstyp** auf **Installieren**.
7. Wählen Sie auf der Seite **Konto hinzufügen** die Option **Konto hinzufügen** aus und klicken Sie dann auf **Weiter**.
8. Geben Sie den Benutzernamen und das Kennwort eines Administrators für das lokale Gerät ein.

Deinstallieren

Sie können jetzt einfach das Symbol der Citrix Workspace-App in den Papierkorb tun, um die Citrix Workspace-App für Mac vollständig zu deinstallieren. Gehen Sie wie folgt vor, um die Citrix Workspace-App zu deinstallieren:

1. Schließen Sie die Citrix Workspace-App, falls sie ausgeführt wird.
Gehen Sie wie folgt vor, um die Citrix Workspace-App zu schließen:
 - a) Navigieren Sie zum Schnellzugriffsmenü.
 - b) Klicken Sie oben rechts auf das Symbol für Ihr **Konto**.



c) Klicken Sie in der Optionsliste auf **Beenden**.

Hinweis:

Wenn Sie die Citrix Workspace-App nicht wie zuvor beschrieben schließen, wird nach dem

Ausführen des nächsten Schritts möglicherweise die folgende Fehlermeldung angezeigt:

The item "Citrix Workspace" can't be moved to the Trash because it's open.

2. Ziehen Sie die Citrix Workspace-App aus dem Ordner **Anwendungen** in den Papierkorb. Alternativ können Sie mit der rechten Maustaste auf die Citrix Workspace-App klicken und **Optionen > In Papierkorb verschieben** auswählen.
3. Geben Sie auf Aufforderung Ihre Systemanmeldeinformationen ein.
4. Schließen Sie alle laufenden Apps (Citrix Workspace) und klicken Sie zur Bestätigung auf **Weiter**. Die Citrix Workspace-App und alle ihre Systemdateien werden von Ihrem Gerät gelöscht.

Sie können die Citrix Workspace-App für Mac auch manuell deinstallieren, indem Sie die DMG-Datei öffnen. Wählen Sie **Citrix Workspace-App deinstallieren** und folgen Sie den Anweisungen auf dem Bildschirm. Die DMG-Datei ist die Datei, die bei der erstmaligen Installation der Citrix Workspace-App für Mac von Citrix heruntergeladen wird. Wenn sich die Datei nicht mehr auf Ihrem Computer befindet, laden Sie die Datei erneut von [Citrix Downloads](#) herunter, um die Anwendung zu deinstallieren.

Upgrade

Die Citrix Workspace-App für Mac sendet Ihnen Benachrichtigungen, wenn ein Update für eine vorhandene Version oder ein Upgrade auf eine neuere Version verfügbar ist. Weitere Informationen zu automatischen Updates finden Sie unter [Automatische Aktualisierung](#).

Sie können die Citrix Workspace-App für Mac von allen Citrix Workspace-App für Mac-Vorversionen aus aktualisieren. Weitere Informationen zum manuellen Aktualisieren der App finden Sie unter [Manuelle Aktualisierung](#).

Wenn Sie ein Upgrade auf eine neuere Version der Citrix Workspace-App für Mac durchführen, wird die vorherige Version automatisch deinstalliert. Sie müssen Ihre Maschine nicht neu starten.

Aktualisieren

December 1, 2023

Manuelle Aktualisierung

Um die Citrix Workspace-App für Mac manuell zu aktualisieren, laden Sie die neueste Version der App von der Seite [Citrix Downloads](#) herunter und installieren Sie sie.

Automatisches Update

Wenn eine neue Version der Citrix Workspace-App veröffentlicht wird, sendet Citrix das Update an das System, auf dem die Citrix Workspace-App installiert ist. Sie werden über das verfügbare Update informiert.

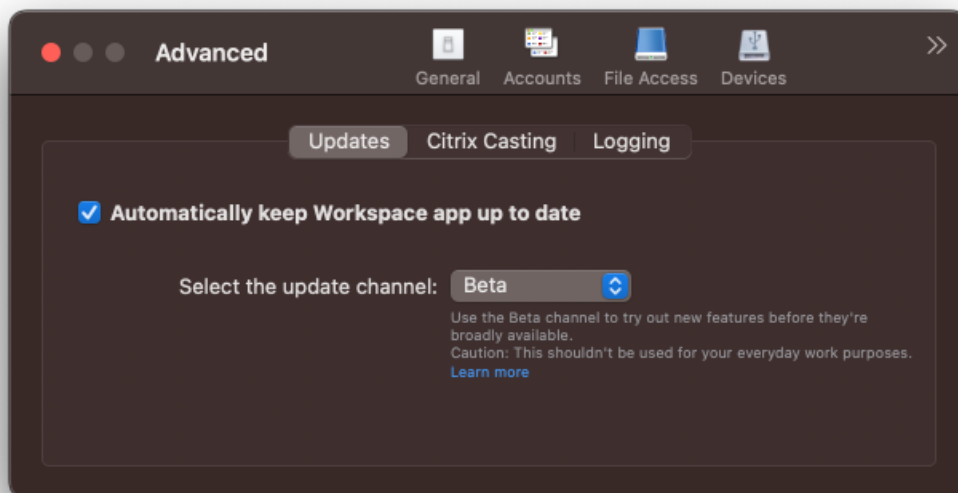
Hinweis:

- 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 Citrix Workspace-App-Versionen vor 2301.1 nicht verfügbar. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX491310](#).
- Ihr System muss über eine Internetverbindung verfügen, um Updates zu erhalten.
- Workspace für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
- Citrix HDX RTME für macOS ist in Citrix Workspace-Updates enthalten. Sie werden über das verfügbare HDX RTME-Update in der Citrix Workspace-App informiert.
- Ab Version 2111 haben die Updateprotokolle für Citrix Workspace neue Pfade. Die Workspace-Updateprotokolle sind unter `/Library/Logs/Citrix Workspace Updater`. Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Installieren des Beta-Programms für die Citrix Workspace-App

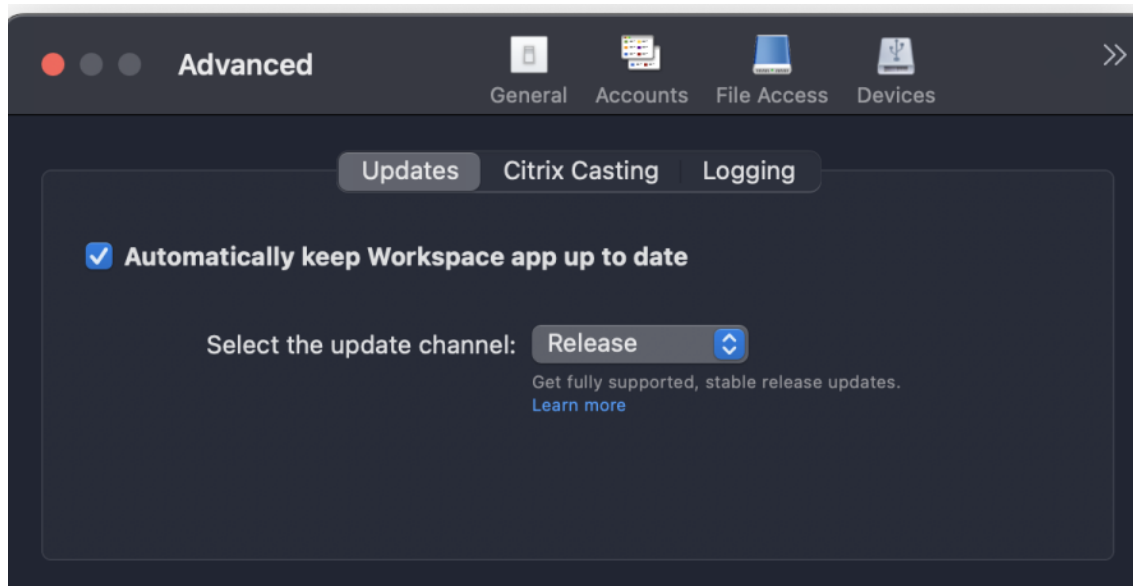
Sie erhalten eine Updatebenachrichtigung, wenn die Citrix Workspace-App für automatische Updates konfiguriert ist. Führen Sie die folgenden Schritte aus, um den Beta-Build auf Ihrem System zu installieren:

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie in der Dropdownliste **Beta** aus, wenn der Beta-Build verfügbar ist.



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

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie in der Dropdownliste **Updatekanal auswählen** die Option **Release**.



Hinweis:

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.

Versionssteuerung für automatische Updates

Administratoren können jetzt angeben, auf welche Version der Citrix Workspace-App Geräte in der Organisation automatisch aktualisiert werden.

Hierfür legen sie den Versionsbereich im Global App Configuration Service mit den Eigenschaften für “maximumAllowedVersion” und “minimumAllowedVersion” fest.

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

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Version Control for Citrix Workspace",
11    "description": "Provides admin ability to Version Control for
12      Citrix Workspace",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        {
19
20          "category": "AutoUpdate",
21          "userOverride": false,
22          "assignedTo": [
23            "AllUsersNoAuthentication"
24          ],
25          "settings": [
26
27            {
28
29              "name": "Auto update plugins settings",
30              "value": [
```



```
30         "pluginName": "Citrix Workspace",
31         "pluginId": "D99C3E77-FBF5-4B97-8EDA-4E381A1E0826",
32         "pluginSettings": {
33
34             "deploymentMode": "Update",
35             "upgradeToLatest": false,
36             "minimumAllowedVersion": "23.07.0.63",
37             "maximumAllowedVersion": "23.07.0.63",
38             "delayGroup": "Medium",
39             "detectRule": ""
40         }
41     }
42 }
43 ]
44 }
45 }
46
47 ]
48 }
49
50 ]
51 }
52
53 }
54
55 }
56
57
58 <!--NeedCopy-->
```

Wenn der Bereich festgelegt ist, wird die Citrix Workspace-App auf dem Benutzergerät automatisch auf die höchste verfügbare Version aktualisiert, die im genannten Bereich liegt.

Wenn Sie die Citrix Workspace-App automatisch auf eine bestimmte Version aktualisieren möchten, geben Sie im Global App Configuration Service in den Eigenschaften “maximumAllowedVersion” und “minimumAllowedVersion” zweimal dieselbe Version ein.

Hinweis:

- Um die Versionssteuerung für automatische Updates zu aktivieren, setzen Sie die Einstellung **upgradeToLatest** im Global App Configuration Service auf “false”. Wenn die Einstellung **upgradeToLatest** auf “true” gesetzt ist, werden “maximumAllowedVersion” und “minimumAllowedVersion” ignoriert.
- Ändern Sie nicht die PluginID. Die PluginID ist der Citrix Workspace-App zugeordnet.

- Wenn die Version nicht im Global App Configuration Service konfiguriert ist, wird die Citrix Workspace-App standardmäßig auf die neueste verfügbare Version aktualisiert.
- Sie können nur die Versionsbereiche verwenden, die für ein Upgrade der Citrix Workspace-App festgelegt sind. Ein Downgrade wird nicht unterstützt.
- Dieses Feature wird ab Release 2307 unterstützt.

Erweiterte Konfiguration für automatische Updates (Citrix Workspace-Updates)

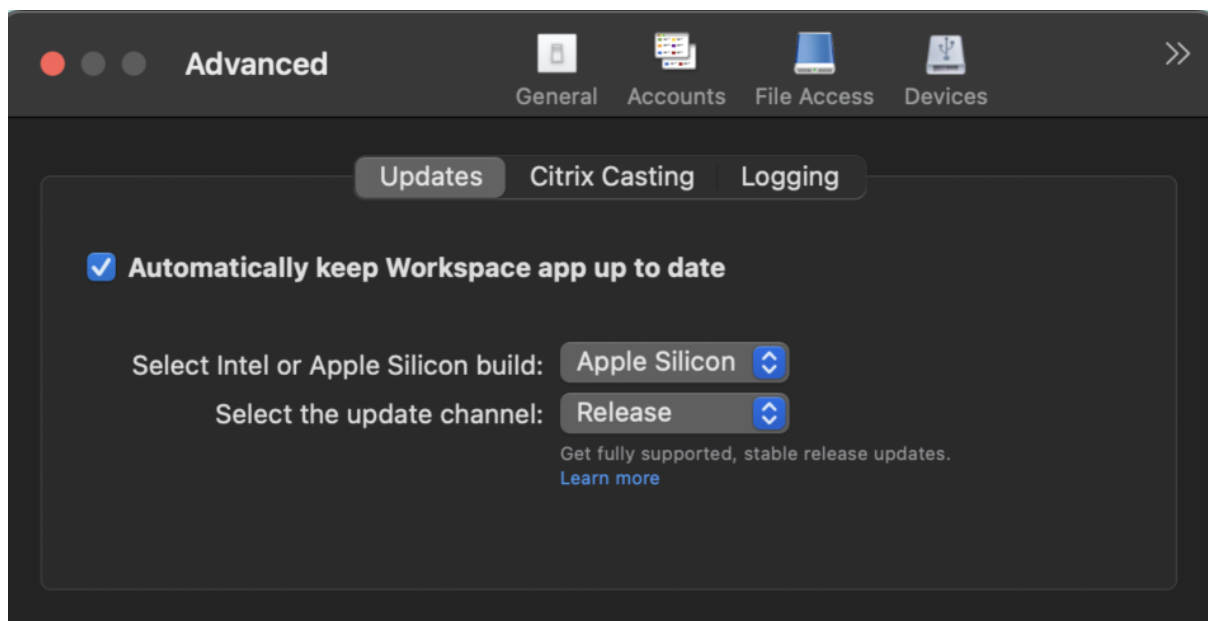
Sie können Citrix Workspace-Updates mit den folgenden Methoden konfigurieren:

- Grafische Benutzeroberfläche (GUI)
- Global App Configuration Service (GACS)
- Mobilgeräteverwaltung (MDM)
- StoreFront

Konfigurieren automatischer Citrix Workspace-Updates über die grafische Benutzeroberfläche

Benutzer können 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. Um das Update über die GUI zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie das Hilfssymbol der Citrix Workspace-App auf Ihrem Mac aus.
2. Wählen Sie in der Dropdownliste **Einstellungen > Erweitert > Updates**.
3. Wählen Sie den Build, für den Sie automatische Updates installieren möchten. Dies kann der Apple Silicon-Build oder Intel-Build sein (nur anwendbar für Benutzer auf Macs mit Apple Silicon (M1-Serie)).



Konfigurieren automatischer 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 (Store ist der Kontoname Ihrer Bereitstellung).

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
10        <annotatedServices>
11
12            <clear />
13
14            <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
15
16                <metadata>
17
18                    <plugins>
19
20                        <clear />
21
22                    </plugins>
23
24                    <trustSettings>
25
26                        <clear />
```

```
27         </trustSettings>
28
29         <properties>
30
31             <property name="Auto-Update-Check" value="Disabled"
32                 />
33
34             <property name="Auto-Update-DeferUpdate-Count" value
35                 ="1" />
36
37             <property name="Auto-Update-Rollout-Priority" value=
38                 "fast" />
39
40             <property name="Auto-Update-Architecture" value="
41                 Universal" or "Intel" />
42
43         </properties>
44
45     </metadata>
46
47 </annotatedServiceRecord>
48
49 </annotatedServices>
50
51 <metadata>
52
53     <plugins>
54
55         <clear />
56
57     </plugins>
58
59     <trustSettings>
60
61         <clear />
62
63     </trustSettings>
64
65     <properties>
66
67         <clear />
68
69     </properties>
70
71 </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: Eine Prüfung auf Updates wird nicht durchgeführt.
- **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 kann automatische Updates beliebig oft verschieben.
- 0: Dem Benutzer wird die Option “Später erinnern” nicht angezeigt.
- Zahl: Dem Benutzer wird die Option “Später erinnern” so oft angezeigt, wie durch die Zahl festgelegt wurde.

Konfigurieren automatischer Citrix Workspace-Updates mit GACS

Mit GACS können Administratoren die automatischen Updates für Apple Silicon- oder Intel-Builds mit den folgenden Einstellungen konfigurieren:

“name”:“autoUpdateArchitecture”

“value”:“Universal” oder “Intel”

Konfigurieren automatischer Citrix Workspace-Updates mit MDM

Mit MDM können Administratoren die automatischen Updates für Apple Silicon- oder Intel-Builds mit den folgenden Einstellungen konfigurieren:

```
<key>AutoUpdateArchitecture</key>
```

```
<string>Universal</string> or <string>Intel</string>
```

```
<key>AutoUpdateState</key>
```

```
<string>Auto</string> or <string>Manual</string> or <string>Disabled</string>
```

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

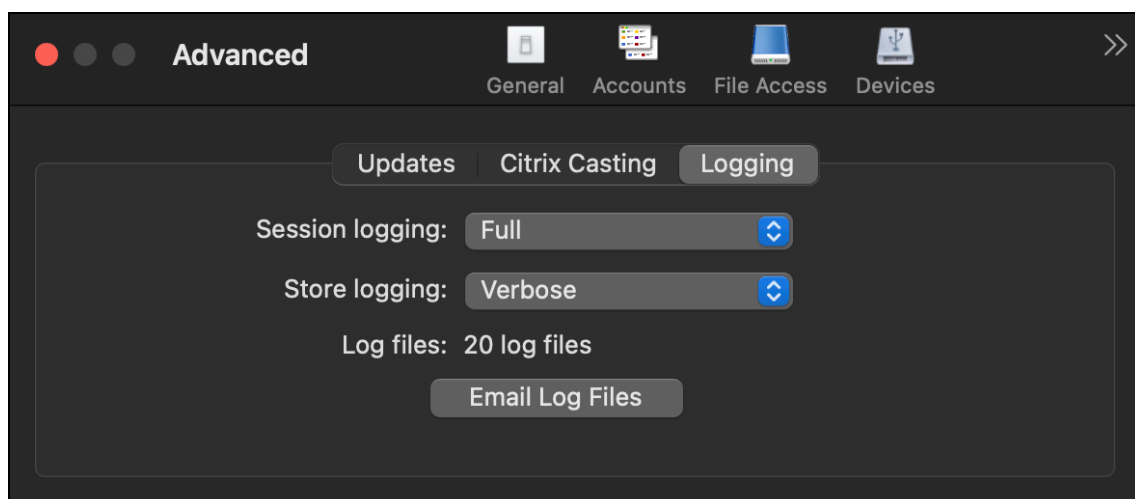
Protokollsammlung

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.

Sie können Protokolle über die GUI sammeln.

Protokolle sammeln:

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie **Protokollierung**.



4. Wählen Sie eine der folgenden Sitzungsprotokollebenen aus:

- **Deaktiviert (Standard):** Es wird ein Minimum an Protokollen zur einfachen Problembearbeitung gesammelt.
- **Verbindungsdiagnose:** Identifiziert Fehler beim Verbinden. Die gesamte Protokollierung ist bis zu dem Zeitpunkt aktiviert, an dem die Sitzung als erfolgreich erkannt wird.
- **Vollständig:** Erfasst alles, einschließlich der Verbindungsdiagnose. Nach der Aktivierung speichert die Citrix Workspace-App bis zu 10 Sitzungsprotokolle. Danach werden sie gelöscht, beginnend mit den ältesten, um bei 10 Protokollen zu bleiben.

Hinweis:

Die Protokollierungsoption **Vollständig** kann sich auf die Leistung auswirken und sollte aufgrund der Datenmenge nur zur Problembearbeitung verwendet werden. Aktivieren Sie die vollständige Protokollierung nicht für den Normalbetrieb. Wenn Sie diese Protokollierungsstufe aktivieren, wird eine Warnung angezeigt, die Sie bestätigen müssen, damit Sie fortfahren können.

5. Wählen Sie eine der folgenden Storeprotokollebenen aus:

- **Deaktiviert (Standard):** Es wird ein Minimum an Protokollen zur einfachen Problembearbeitung gesammelt.
- **Normal:** Es werden nur Storekommunikationsprotokolle gesammelt
- **Ausführlich:** Detaillierte Authentifizierungs- und Storekommunikationsprotokolle werden gesammelt.

6. Klicken Sie auf **Protokolldateien per E-Mail senden**, um Protokolle als ZIP-Datei zu sammeln und freizugeben.

Konfigurieren

December 18, 2023

Nach der Installation der Citrix Workspace-App für Mac-Software sind die folgenden Konfigurationsschritte erforderlich, damit Benutzer auf ihre gehosteten Anwendungen und Desktops zugreifen können.

Benutzer stellen Verbindungen u. a. über das Internet oder von einem Remotestandort her. Konfigurieren Sie für solche Benutzer die Authentifizierung über Citrix Gateway.

Administratortasken und -überlegungen

In diesem Artikel werden Aufgaben und Überlegungen beschrieben, die für Administratoren der Citrix Workspace-App für Mac relevant sind.

Wichtig:

Wenn Sie macOS 10.15 ausführen, stellen Sie sicher, dass Ihr System mit den [Anforderungen für vertrauenswürdige Zertifikate in macOS 10.15](#) von Apple kompatibel ist. Überprüfen Sie dies, bevor Sie das Upgrade auf die Citrix Workspace-App für Mac Version 2106 durchführen.

Featureflags verwalten

Wenn ein Problem mit der Citrix Workspace-App in der Produktion auftritt, können wir ein betroffenes Feature dynamisch in der Citrix Workspace-App deaktivieren, auch nachdem das Feature bereitgestellt wurde. Hierfür verwenden wir Featureflags und den Drittanbieterdienst "LaunchDarkly".

Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen.

Sie können den Datenaustausch und die Kommunikation mit LaunchDarkly wie folgt ermöglichen:

Datenverkehr für folgende URLs zulassen

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- mobile.launchdarkly.com

IP-Adressen in einer Positivliste auflisten

Wenn Sie IP-Adressen in einer Positivliste auflisten müssen, konsultieren Sie die Liste der aktuellen IP-Adressbereiche unter [Liste öffentlicher IP-Adressen von LaunchDarkly](#). Mithilfe 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 [Stausseite von LaunchDarkly](#).

LaunchDarkly-Systemanforderungen

Wenn Sie Split-Tunneling in Citrix ADC für die folgenden Dienste auf **OFF** festgelegt haben, müssen die Apps mit den folgenden Diensten kommunizieren können:

- LaunchDarkly-Dienst.
- APNs-Listenerdienst

Unterstützung für die Konfiguration von Benutzergeräten durch Administratoren per MDM

Administratoren können bei der Bereitstellung der Citrix Workspace-App mit einem beliebigen MDM-Tool (z. B. Citrix Endpoint Management) jetzt die folgenden Einstellungen konfigurieren:

- **StoreURLs:** Konfigurieren Sie Details des Stores, damit er zur Vereinfachung der Anmeldung automatisch hinzugefügt wird, wenn der Benutzer die Citrix Workspace-App öffnet. Geben Sie zum Hinzufügen eines Stores die Details für die Einstellung **StoreURLs** ein. Beispiel:

```
<array>  
<string>https://myorg.com/Org/storename</string>  
</array>
```

Sie können außerdem mehrere Stores wie folgt hinzufügen:

```
<array>  
<string>https://myorg.com/Org/storename1</string>  
<string>https://myorg.com/Org/storename2</string>  
</array>
```

Um die StoreURLs zur Citrix Workspace-App hinzuzufügen, muss der Benutzer die Citrix Workspace-App beenden und neu starten.

- **BlockStoreAddition:** Verhindert, dass Benutzer Stores hinzufügen.

Um zu verhindern, dass Benutzer einen Store hinzufügen, legen Sie den Wert der Einstellung **BlockStoreAddition** auf **True** fest.

Möglichkeit des Deaktivierens des LaunchDarkly-Diensts per MDM-Tool

Ab Version 2210 können Sie den LaunchDarkly-Dienst in der Citrix Workspace-App deaktivieren, unabhängig davon, ob die Benutzer sich innerhalb oder außerhalb der Firewall des Unternehmens befinden. Um den LaunchDarkly-Dienst zu deaktivieren, legen Sie den Wert für die Einstellung **DisableFeatureFlag** auf "True" fest.

Dieser Dienst ist für Administratoren verfügbar, die Mac-Geräte mit dem MDM-Tool verwalten.

Hinweis:

Das Deaktivieren der FeatureFlag-Einstellung erfordert einen Geräte-neustart, damit die Einstellung wirksam wird.

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

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. Weitere Informationen finden Sie in der Dokumentation zu [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 des App-Schutzes in der Citrix Workspace-App für Mac finden Sie im Abschnitt zur Citrix Workspace-App für Mac im Artikel [Konfiguration](#).

Hinweis:

- App Protection wird nur ab Version 2001 der Citrix Workspace-App für Mac unterstützt.

Sentry

Sentry wird zur Erfassung von App-Protokollen verwendet, um Probleme und Abstürze zu analysieren und die Produktqualität zu verbessern. Citrix sammelt oder speichert keine anderen persönlichen Benutzerinformationen und nutzt Sentry nicht für Featureanalysedaten. Weitere Informationen über Sentry finden Sie unter [<https://sentry.io/welcome/>].

FIDO2 für kennwortlose Authentifizierung

Die Citrix Workspace-App für Mac unterstützt die kennwortlose Authentifizierung mit FIDO2-Sicherheitsschlüsseln bei der Verbindung mit einem Cloudstore bzw. innerhalb von HDX-Sitzungen. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Desktops, die FIDO2 unterstützen, authentifizieren. Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code und Touch ID. Dieses Feature wird unter macOS 12 und späteren Versionen unterstützt.

Weitere Informationen zu FIDO2 finden Sie unter [FIDO2-Authentifizierung](#).

Informationen zu den Voraussetzungen und zur Verwendung dieses Features finden Sie unter [Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2](#).

FIDO2-Authentifizierung beim Verbinden mit einem Cloudstore

Die Citrix Workspace-App verwendet den Standardbrowser des Benutzers für die FIDO2-Authentifizierung (Webauthentifizierung), wenn eine Verbindung zum Cloudstore hergestellt wird. Administratoren können den Browsertyp für die Authentifizierung bei der Citrix Workspace-App konfigurieren. Das FIDO2-Feature wird nicht für On-Premises-Stores unterstützt. Weitere Informationen zu den Webbrowsereinstellungen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

Mit den folgenden Einstellungen können Sie den Browsertyp auswählen, der für die Authentifizierung eines Endbenutzers in der Citrix Workspace-App verwendet wird:

| Einstellungen | Beschreibung |
|---------------------------------|---|
| System | Hiermit können Sie den Standardbrowser des Benutzers für die Authentifizierung verwenden (z. B. Safari oder Chrome). Die Authentifizierung erfolgt außerhalb der Citrix Workspace-App. Verwenden Sie diese Einstellung, um die kennwortlose Authentifizierung zu unterstützen. Diese Einstellung versucht, die bestehende Benutzersitzung vom Browser des Benutzers zu verwenden. |
| SystemWithPrivateSession | Diese Einstellung ähnelt der Einstellung System . Die Citrix Workspace-App verwendet eine private Sitzung im Browser für die Authentifizierung. Der Browser speichert keine Authentifizierungscookies oder -daten. Single Sign-On wird in dieser Option nicht unterstützt. |
| Eingebettet | Ermöglicht die Authentifizierung innerhalb der Citrix Workspace-App. Die Citrix Workspace-App speichert die Sitzungsdaten oder Cookies für den Single Sign-On (z. B. SaaS-Apps), wenn das erweiterte Single Sign-On-Feature aktiviert ist. Diese Authentifizierungsmethode unterstützt keine kennwortlosen Authentifizierungen wie FIDO2. |

| Einstellungen | Beschreibung |
|-----------------------------------|---|
| EmbeddedWithPrivateSession | Diese Einstellung ähnelt der Einstellung Embedded . Single Sign-On wird nicht unterstützt, da keine Sitzungsdaten oder Cookies in der Citrix Workspace-App vorhanden sind. |

Um die konfigurierten Einstellungen zu übertragen, führen Sie die folgenden Befehle über die Mobilgeräteverwaltung (MDM), Global App Configuration Service (GACS) oder die Befehlszeilenschnittstelle aus:

- **FIDO2 mit MDM aktivieren:** Um die Authentifizierung per Mobilgeräteverwaltung (MDM) zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
<key>WebBrowserForAuthentication</key><string>System</string>
```

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

- **FIDO2 mit GACS aktivieren:** Um die Authentifizierung per GACS zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://serviceURL:443"
6   }
7 ,
8   "settings": {
9
10    "name": "Web browser for Authenticating into Citrix Workspace",
11    "description": "Allows admin to select the type of browser used
12      for authenticating an end user into Citrix Workspace app",
13    "useForAppConfig": true,
14    "appSettings": {
15
16      "macos": [
17
18        "assignedTo": [
19          "AllUsersNoAuthentication"
20        ],
21        "category": "authentication",
22        "settings": [
```

```
23         {
24
25             "name": "web browser for authentication",
26             "value": "SystemWithPrivateSession"
27         }
28
29     ],
30     "userOverride": false
31 }
32
33 ]
34 }
35
36 }
37
38 }
39
40
41 <!--NeedCopy-->
```

- **FIDO2 über die Befehlszeilenschnittstelle aktivieren:** Um die Authentifizierung per Befehlszeilenschnittstelle zu aktivieren, müssen Administratoren den folgenden Befehl ausführen:

```
defaults write com.citrix.receiver.nomas WebBrowserForAuthentication
System
```

FIDO2-Authentifizierung in HDX-Sitzungen

Sie können FIDO2-Sicherheitsschlüssel für die Authentifizierung innerhalb einer HDX-Sitzung konfigurieren. Dieses Feature unterstützt derzeit Roaming-Authentifikatoren (nur USB) mit PIN-Code.

Beim Zugriff auf eine App oder Website, die FIDO2 unterstützt, wird eine Aufforderung zur Eingabe des Sicherheitsschlüssels angezeigt. Wenn Sie Ihren Sicherheitsschlüssel zuvor mit einer PIN registriert haben (4 bis 64 Zeichen), müssen Sie die PIN bei der Anmeldung eingeben.

Wenn Sie Ihren Sicherheitsschlüssel zuvor ohne PIN registriert haben, tippen Sie einfach auf den Sicherheitsschlüssel, um sich anzumelden.

Dieses Feature ist standardmäßig für die Citrix Workspace-App ab Version 2307 aktiviert. Sie können die FIDO2-Authentifizierung mithilfe von MDM oder der Befehlszeilenschnittstelle wie folgt deaktivieren:

- **FIDO2-Authentifizierung mit MDM deaktivieren:** Um das Feature über MDM zu deaktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
<key>Fido2Enabled</key><false/>
```

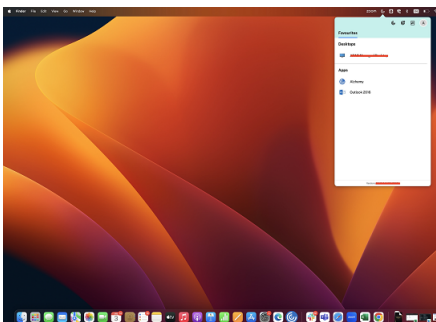
Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

- **FIDO2-Authentifizierung über die Befehlszeilenschnittstelle deaktivieren:** Führen Sie den folgenden Befehl aus, um das Feature zu deaktivieren:

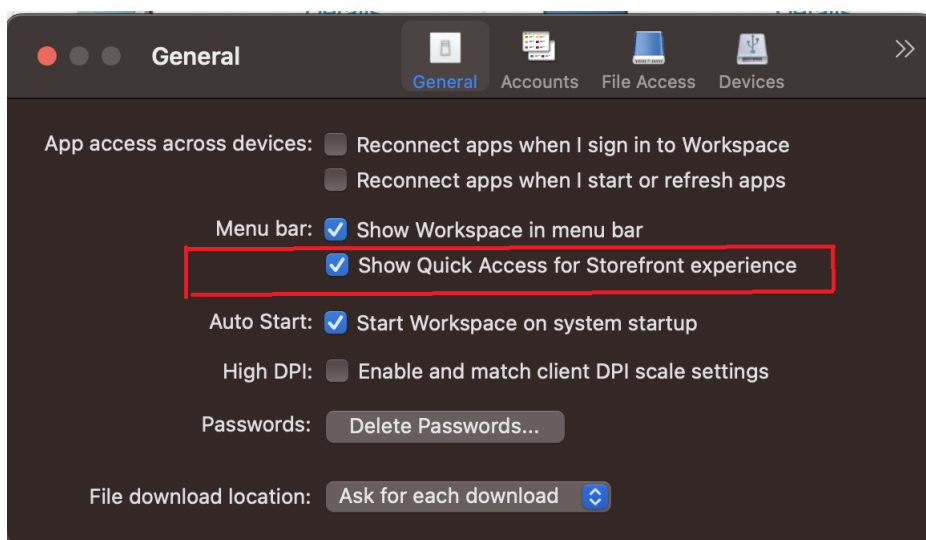
```
defaults write com.citrix.receiver.nomas Fido2Enabled -bool NO
```

Schnellzugriffsmenü für StoreFront

Ab Release 2307 können Sie über das Schnellzugriffsfeature für On-Premises-Stores schnell und einfach zu Ihren bevorzugten Apps und Desktops gehen. Um den Schnellzugriff zu aktivieren, klicken Sie in der Symbolleiste mit der rechten Maustaste auf **Citrix Workspace**, gehen Sie zu **Einstellungen > Allgemein** und wählen Sie dann **Schnellzugriff für Storefront-Erlebnis anzeigen**. Mit diesem Feature können Sie Ihre Lieblingsdaten direkt über die Mac-Menüleiste anzeigen.



Sie können den Schnellzugriff über die **Einstellungen** aktivieren.



Administratoren können den Schnellzugriff über die Mobilgeräteverwaltung (MDM) oder Global App Configuration Service (GACS) aktivieren und deaktivieren.

Schnellzugriff mit MDM aktivieren/deaktivieren

Um den Schnellzugriff über MDM zu aktivieren, müssen Administratoren die folgenden Einstellungen verwenden:

```
<key>ShowQuickAccessForStoreFront</key>  
<false/>
```

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

Schnellzugriff mit GACS aktivieren/deaktivieren

Um den Schnellzugriff über GACS zu aktivieren, müssen Administratoren die folgenden Einstellungen verwenden:

```
enableQuickAccessForStoreFront
```

Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 113.1.1.34, der auf Chromium Version 113 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 Mac kann ein Administrator das Vorhandensein der Citrix Enterprise Browser-Verknüpfung auf dem Launchpad konfigurieren und steuern.

Hinweis:

Dieses Feature ist standardmäßig nicht konfiguriert.

Konfiguration

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

- Mobilgeräteverwaltung (MDM)
- Global Admin Configuration Service (GACS)
- Datei web.config.

Hinweis:

- 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 Cloud-

stores verfügen, wird die Verknüpfung automatisch aktiviert.

- Administratoren können das Feature für Cloudbenutzer deaktivieren, indem sie das Attribut **CEBShortcutEnabled** auf **false** setzen oder die **Eigenschaft zur Aktivierung der Citrix Enterprise Browser-Verknüpfung** deaktivieren.

Mobilgeräteverwaltung (MDM)

Administratoren können die Einstellung für **CEBShortcutEnabled** auf das Gerät des Benutzers übertragen.

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

Hinweis:

Diese Konfigurationsmethode ist in Cloud- und On-Premises-Bereitstellungen anwendbar.

Global Admin Configuration Service (GACS)

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

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

Hinweis:

Diese Konfigurationsmethode ist in Cloud- und On-Premises-Bereitstellungen anwendbar.

Datei web.config

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

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

Hinweis:

Diese Konfigurationsmethode ist in nur in On-Premises-Bereitstellungen anwendbar.

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 Text-Editor. Die Datei ist normalerweise im Verzeichnis C:\inetpub\wwwroot Citrix\Roaming.
2. Suchen Sie das Benutzerkonto-Element in der Datei (Store ist der Kontoname Ihrer Bereitstellung).
Beispiel: `<account id=... name="Store">`
3. Vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

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

Die folgende Konfiguration ist ein Beispiel für die Datei web.config:

```
1 <account>
2     <clear />
3     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
4         description="" published="true" updatertype="Citrix"
5         remoteAccessType="None">
6         <annotatedServices>
7             <clear />
8             <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
9                 <metadata>
10                    <plugins>
11                        <clear />
12                    </plugins>
13                    <trustSettings>
14                        <clear />
15                    </trustSettings>
16                    <properties>
17                        <property name="CEBShortcutEnabled" value="True" />
18                    </properties>
19                </metadata>
20            </annotatedServiceRecord>
21        </annotatedServices>
22        <metadata>
23            <plugins>
24                <clear />
25            </plugins>
```

```
25     <trustSettings>
26         <clear />
27     </trustSettings>
28     <properties>
29         <clear />
30     </properties>
31 </metadata>
32 </account>
33
34 <!--NeedCopy-->
```

Mit web.config konfigurieren

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

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

3. Vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

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

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.

Zum Anzeigen des benötigten Formulars wählen Sie **Hilfe > Feedback senden**. Sie können Details wie die angegebenen Beispiele eingeben.

Send feedback

Provide a descriptive title*

Tell us more*

Include details such as:

- What you expected to happen
- What actually happened
- Steps to recreate the issue

Logs

Basic logs are attached. We recommend you click 'Record my issue' to capture detailed logs.

For more information, see [Log collection](#)

Record my issue WorkspaceLogs_2023_07_18-14_23_43.zip

Attachments

Screenshots or screen recordings of the problem.

Choose files (Max 4 files)

Your feedback will be used to improve Citrix Workspace app. If you don't use the Mail app on your Mac, please send feedback to **cwa-mac-feedback@cloud.com** with files added manually.

Send **Cancel**

Sie können bestehende Protokolldateien anhängen oder neue Protokolldateien generieren. Um Protokolldateien zu generieren, klicken Sie auf **Mein Problem aufzeichnen > Aufzeichnung starten** und reproduzieren Sie dann das Problem. Nachdem das Problem reproduziert wurde, klicken Sie auf **Aufzeichnung beenden**. Die Protokolldatei wird automatisch gespeichert und ersetzt bestehende Protokolle.

Hinweis:

Citrix erfasst keine personenbezogenen Informationen (PII) aus den Protokollen.

Sie können Screenshots oder Bildschirmaufzeichnungen zur weiteren Erläuterung des Problems anhängen. Klicken Sie auf **Dateien auswählen** und fügen Sie die Anhänge hinzu, in denen das Problem beschrieben wird (Screenshots, Bildschirmaufzeichnungen usw.). Sie können maximal vier Dateien anhängen.

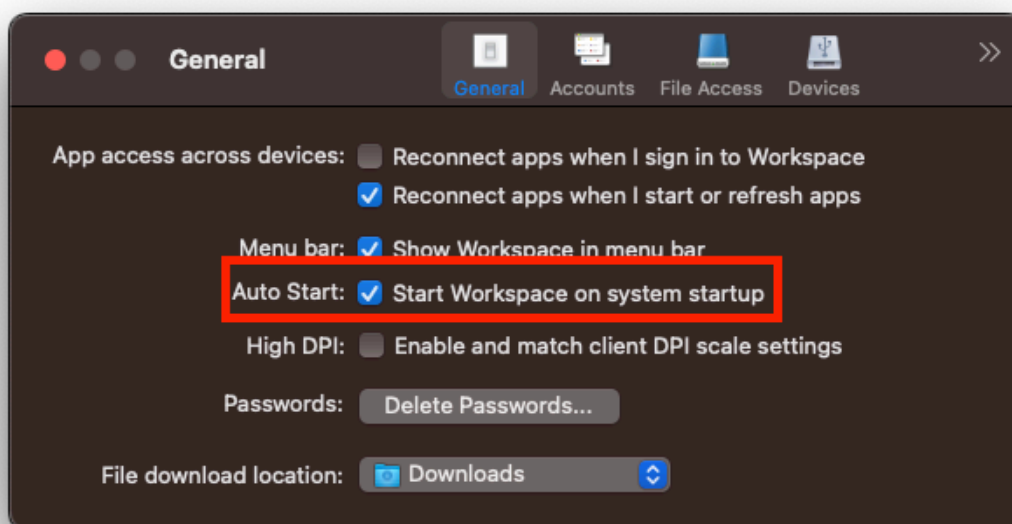
Wenn Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Senden**, damit in Ihrer E-Mail-App automatisch eine E-Mail mit den von Ihnen hinzugefügten Informationen erstellt wird. Klicken Sie dort auf die Schaltfläche **Senden**, um das Feedback an Citrix zu senden. Weitere Informationen finden Sie unter [Feedback zur Citrix Workspace-App senden](#).

Hinweis:

Wenn Sie nicht die Standard-E-Mail-App verwenden, senden Sie Feedback von Ihrem E-Mail-Client an cwa-mac-feedback@cloud.com. Fügen Sie Problemdetails, Protokolldateien, Screenshots oder Bildschirmaufzeichnungen manuell hinzu.

Verbesserter automatischer Start

Bisher wurde die Citrix Workspace-App für Mac automatisch gestartet, wenn ein Computer eingeschaltet wurde. Ab Version 2304 können Sie den automatischen Start der Citrix Workspace-App für Mac deaktivieren oder aktivieren, indem Sie zu **Einstellungen > Allgemein > Workspace beim Systemstart starten** gehen. Die Autostart-Einstellung ist standardmäßig aktiviert.



Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen

Ab Release 2304 ist die Simulcast-Unterstützung standardmäßig für optimierte Microsoft Teams-Videokonferenzen aktiviert. Dadurch werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert. Dies wird erreicht, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank dieser verbesserten Benutzererfahrung kann jeder Benutzer abhängig von der Endpunktfähigkeit, den Netzwerkbedingungen usw. mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.) senden. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann, sodass alle Benutzer das optimale Videoerlebnis erhalten.

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.

Unterstützung für die zertifikatbasierte Authentifizierung

Ab dieser Version können Workspace-Administratoren Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei der Citrix Workspace-App authentifizieren.

Die folgenden Methoden können verwendet werden, um die Authentifizierung mit bedingtem Zugriff zu aktivieren:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Die von der Citrix Workspace-App gelesenen Flagwerte haben folgende Vorrangreihenfolge:

- Mobilgeräteverwaltung (MDM)
- Global App Configuration Service (GACS)

Authentifizierung mit bedingtem Zugriff über MDM aktivieren

Um die Authentifizierung mit bedingtem Zugriff mit Azure AD über MDM zu aktivieren, müssen Administratoren die folgenden Einstellung verwenden:

```
<key>enableAAD</key>  
<true/>
```

Diese Einstellung unterstützt boolesche Werte. Der Wert ist standardmäßig auf "false" gesetzt. Der Standardwert wird berücksichtigt, wenn der Schlüsselwert nicht verfügbar ist.

Informationen zur Verwendung von MDM finden Sie unter [Mobilgeräteverwaltung \(MDM\)](#).

Authentifizierung mit bedingtem Zugriff über GACS aktivieren

Um die Authentifizierung mit bedingtem Zugriff mit Azure AD über GACS zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

```
enable conditional AAD
```

Weitere Informationen finden Sie unter [Supported settings and their values per platform](#) für macOS in der GACS-Dokumentation.

Kanalunterstützung für Global App Configuration Service

Der Global App Configuration Service für Citrix Workspace ermöglicht Citrix-Administratoren, Workspace-Dienst-URLs und Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen. Mit dem Global App Configuration Service können Administratoren jetzt Einstellungen testen, bevor sie für alle Benutzer bereitgestellt werden. Mit diesem Feature können mögliche Probleme behoben werden, bevor App-Konfigurationen global für alle Benutzer angewendet werden.

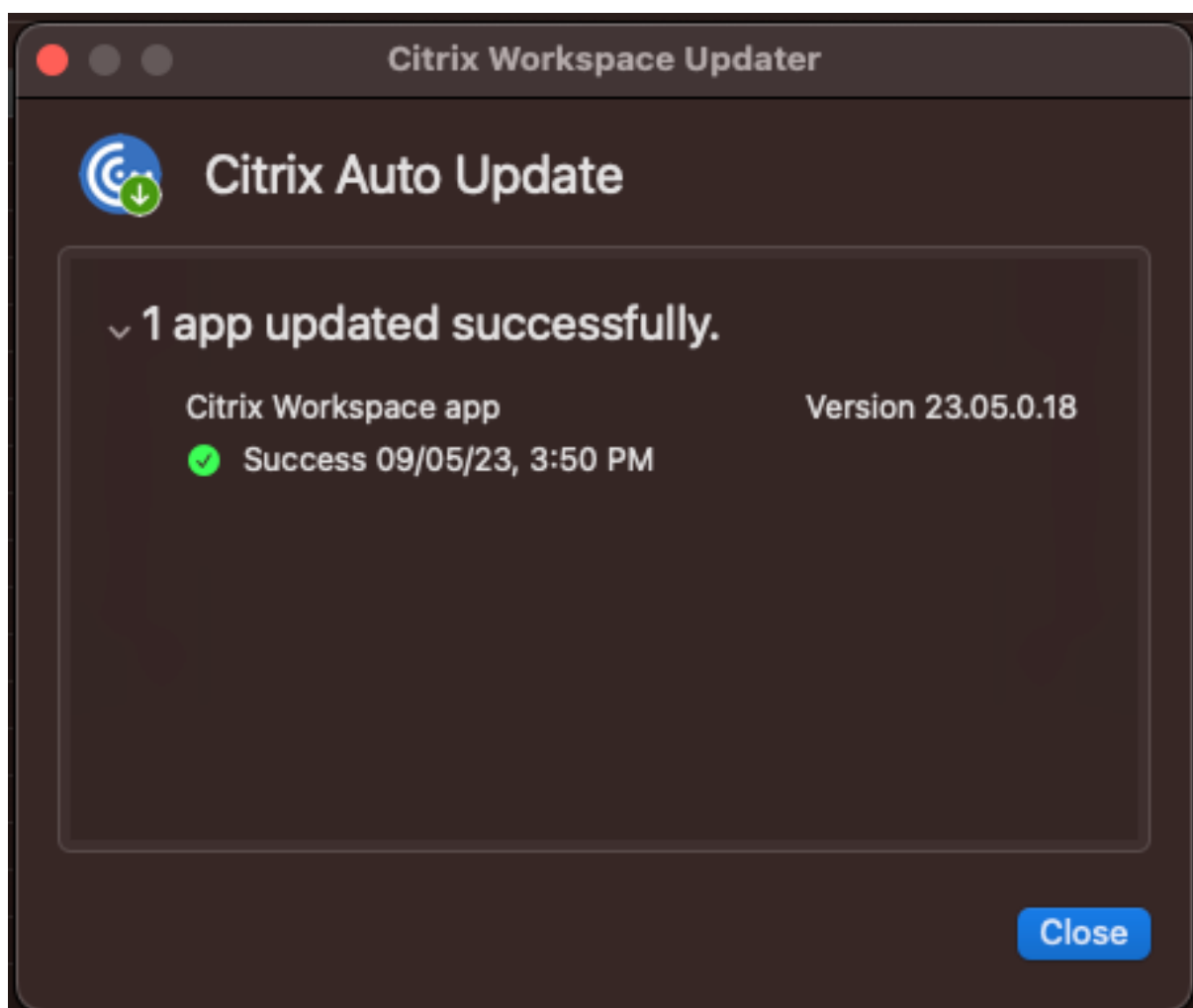
Sie können die Kanalunterstützung erreichen, indem Sie die zu testenden Einstellungen einem Kanal zuordnen und diesen dann in der Payload hinzufügen. Weitere Informationen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

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 keinen passenden Zeitpunkt zur Hintergrundinstallation von Updates findet, kann Citrix Workspace Updater den Benutzer zur Installation auffordern.

Anmeldeaufforderung für Verbundidentitätsanbieter erzwingen

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

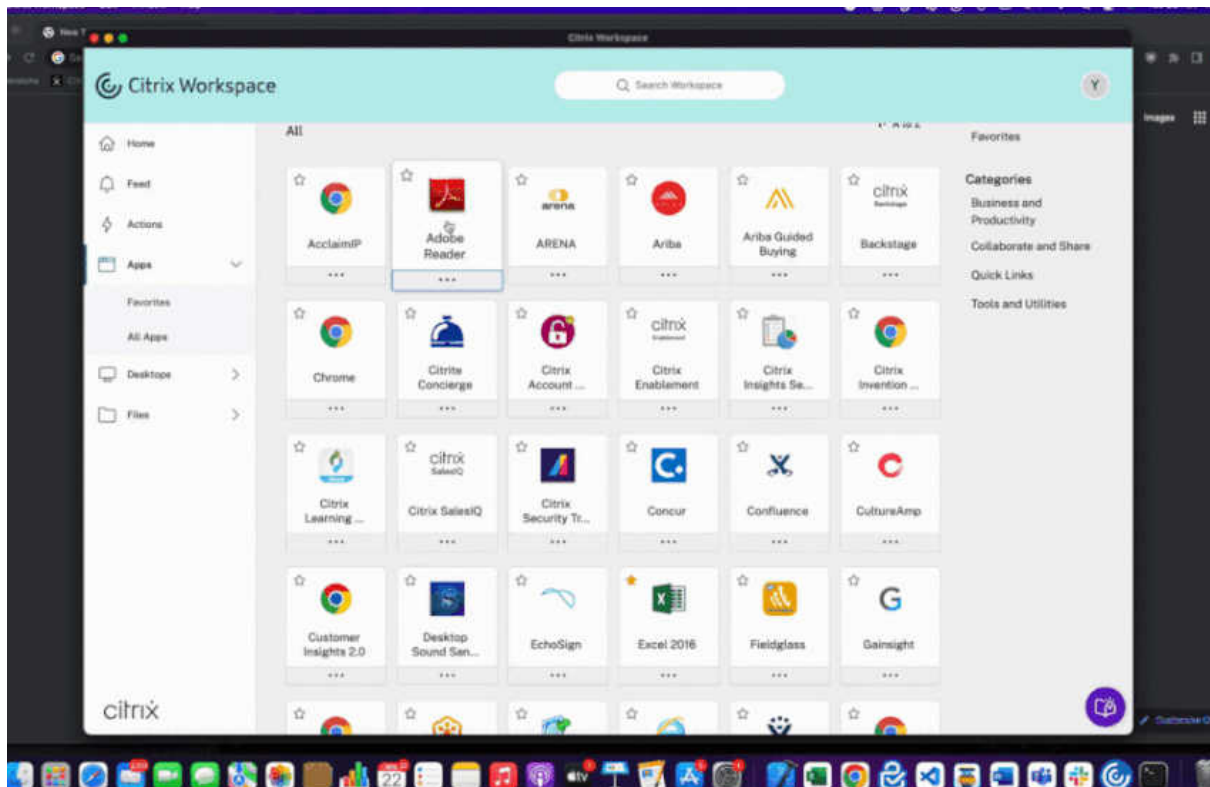
Die Verwendung der Richtlinie “Authentifizierungstoken speichern” ist zum Erzwingen der Anmeldeaufforderung nicht mehr nötig.

Unterstützung für nicht englische IME-Tastaturlayouts

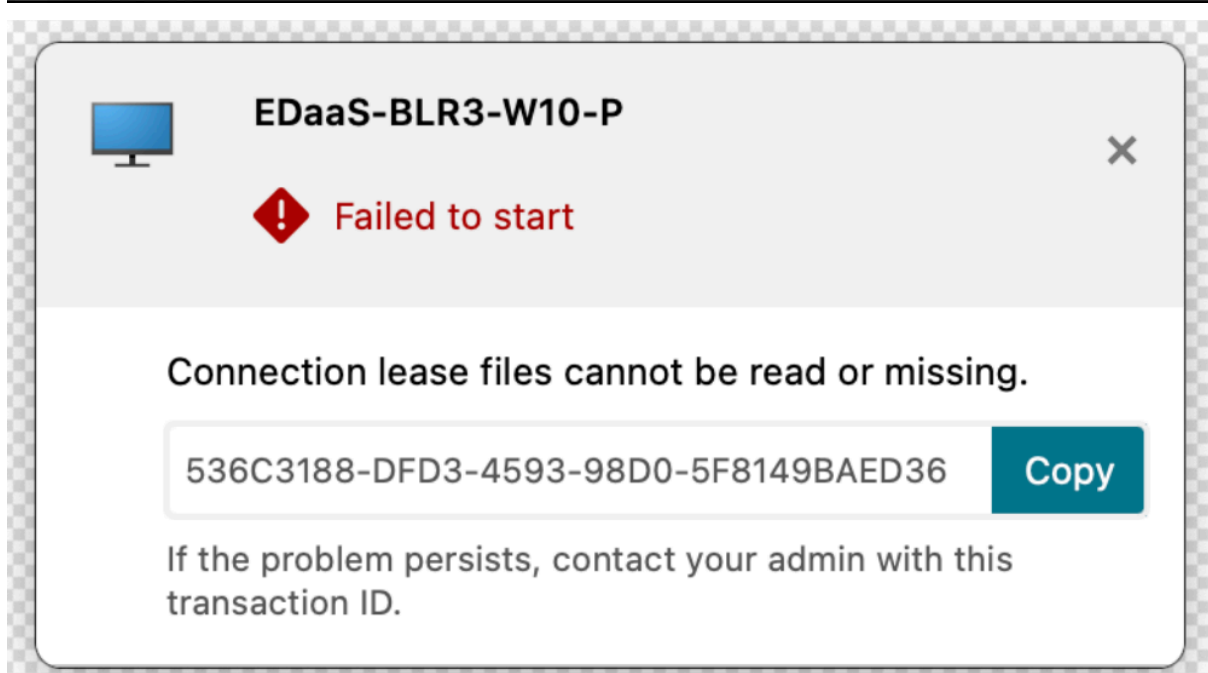
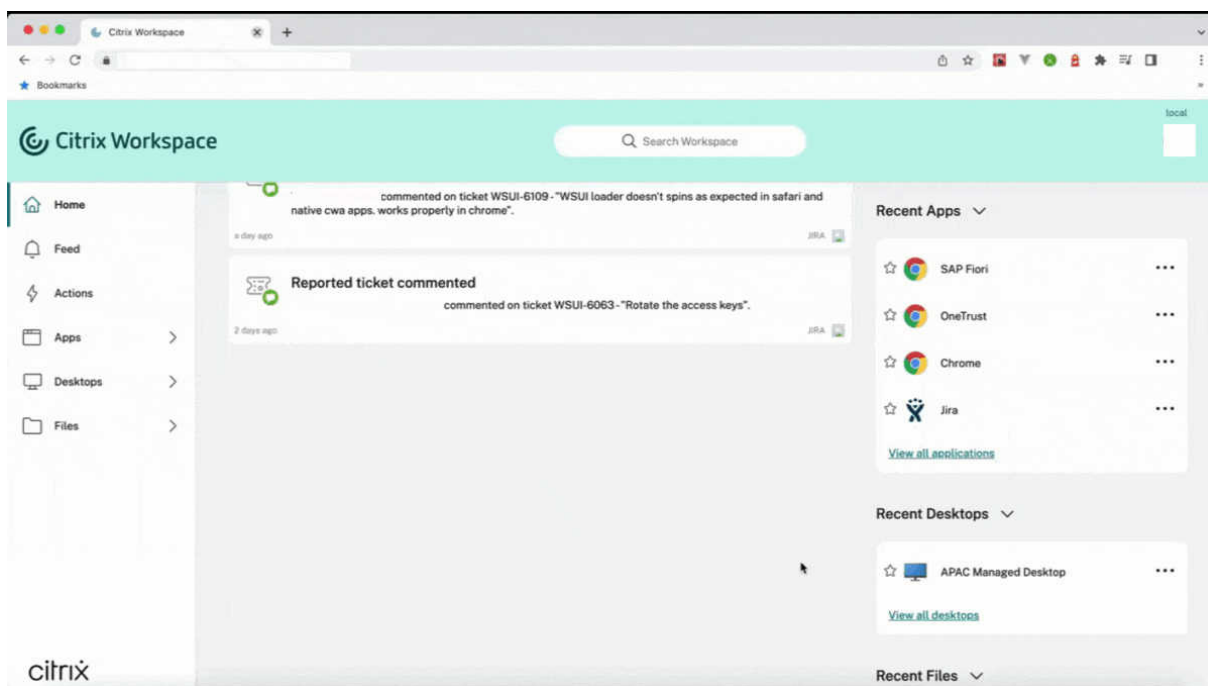
Die Unterstützung für nicht englische IME-Tastaturlayouts funktioniert ohne Unterbrechung weiter, wenn die Carbon-APIs zusammen mit den Cocoa-APIs auslaufen.

Verbessertes Startverhalten virtueller Apps und Desktops [Technical Preview]

Das Öffnen von Citrix-Ressourcen wurde verbessert und ist ab Release 2301 noch benutzerfreundlicher und informativer.



Die Benachrichtigung über den Startfortschritt wird jetzt in der unteren rechten Bildschirmcke angezeigt. Es erscheint eine Fortschrittsanzeige der Ressourcen, die gerade geöffnet werden. Wenn Sie die Benachrichtigung verwerfen, können Sie sie nicht erneut aufrufen. Nach dem Sitzungsstart ist die Benachrichtigung noch einige Sekunden zu sehen. Wenn die Sitzung nicht gestartet werden kann, enthält die Benachrichtigung eine Fehlermeldung.



Hinweis:

Dieses Feature ist für Workspace (Cloud)- und StoreFront-Sitzungen verfügbar.

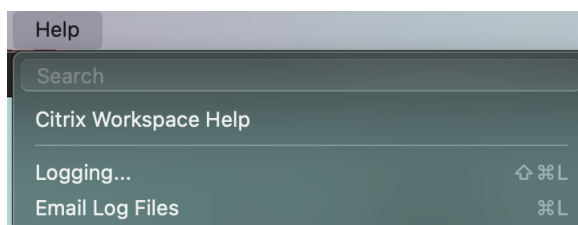
Sie können Feedback zu dieser Technical Preview mit diesem [Podio-Formular](#) geben.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Feature Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Beachten Sie, dass Beta Builds nicht in Produktionsumgebungen bereitgestellt werden dürfen.

Protokollsammlung

Protokollsammlung vereinfacht das Sammeln von Protokollen für die Citrix Workspace-App. Die Protokolle helfen Citrix bei der Fehlerbehebung und erleichtern bei komplizierten Problemen den Support. Benutzer können jetzt über das Menü **Hilfe** schnell Protokolle sammeln, indem sie zu **Hilfe** gehen und die Option **Protokollierung...** oder **Protokolldateien per E-Mail senden** auswählen. Dieses Feature verbessert die Benutzererfahrung während des Protokollerfassungsprozesses.



- **Protokollierung...:** Wenn Sie auf diese Option klicken, gelangen Sie zu **Einstellungen > Erweitert > Protokollierung**.
- **Protokolldateien per E-Mail senden:** Wenn Sie auf diese Option klicken, können Sie die neuesten Protokolle sammeln.

Unterstützung für die Synchronisation von mehr Tastaturlayouts

Ab Version 2304 unterstützt die Citrix Workspace-App für Mac die Synchronisierung des Tastaturlayouts für die folgenden Layouts oder Eingabemethoden-Editoren (IME):

- Englisch ABC
- Englisch ABC - Indien
- Chinesisch, traditionell: Zhuyin - traditionell
- Chinesisch, traditionell: Sucheng - Traditionell
- Google Japanese IME
- Sougou Chinese IME

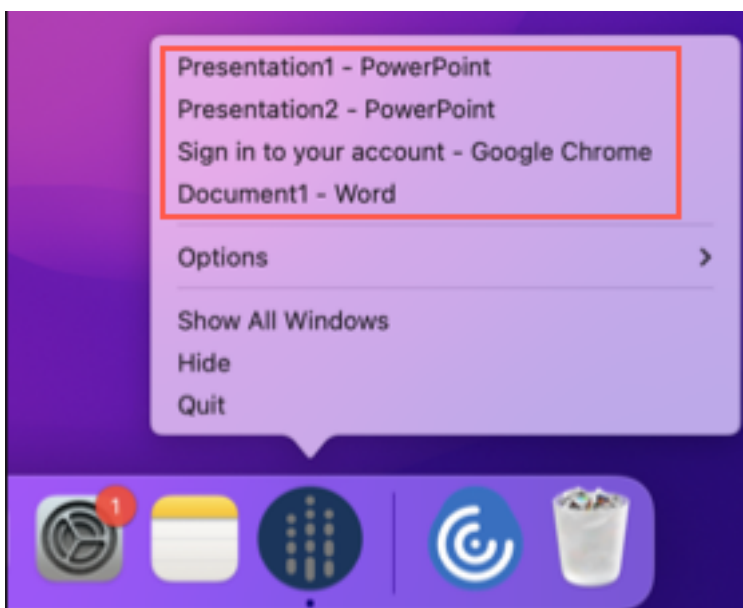
Verbesserung der automatischen Updates

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.

Anzeige geöffneter Apps im Dock mit nativen App-Symbolen

Bisher hat das Klicken auf virtuelle Apps in der Citrix Workspace-App den **Citrix Viewer** ausgelöst, in dem die Apps verfügbar waren. Wenn Sie viele Apps öffnen, werden die Apps oder Instanzen im **Citrix Viewer** geöffnet. Zum Anzeigen der geöffneten Apps klicken Sie mit der rechten Maustaste auf das **Citrix Viewer**-Symbol.

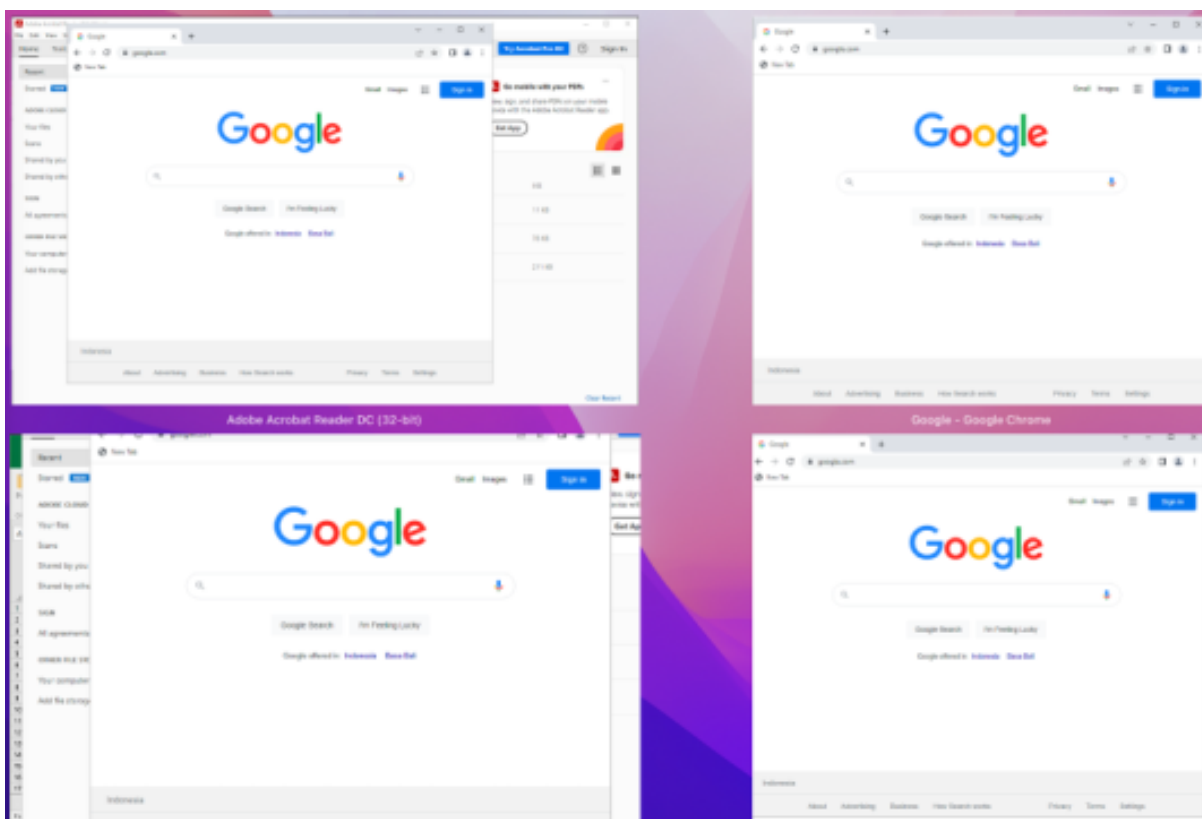


Ab diesem Release werden virtuelle Apps, die Sie öffnen, im Dock (rechts unten im Bildschirm) mit den entsprechenden Symbolen angezeigt und sind leicht identifizierbar. Sie können dann über das Dock auf die virtuelle App zugreifen. Wenn Sie mehrere Instanzen einer App öffnen, werden diese im Dock nicht dupliziert, sondern in einer Instanz im Dock angeordnet.

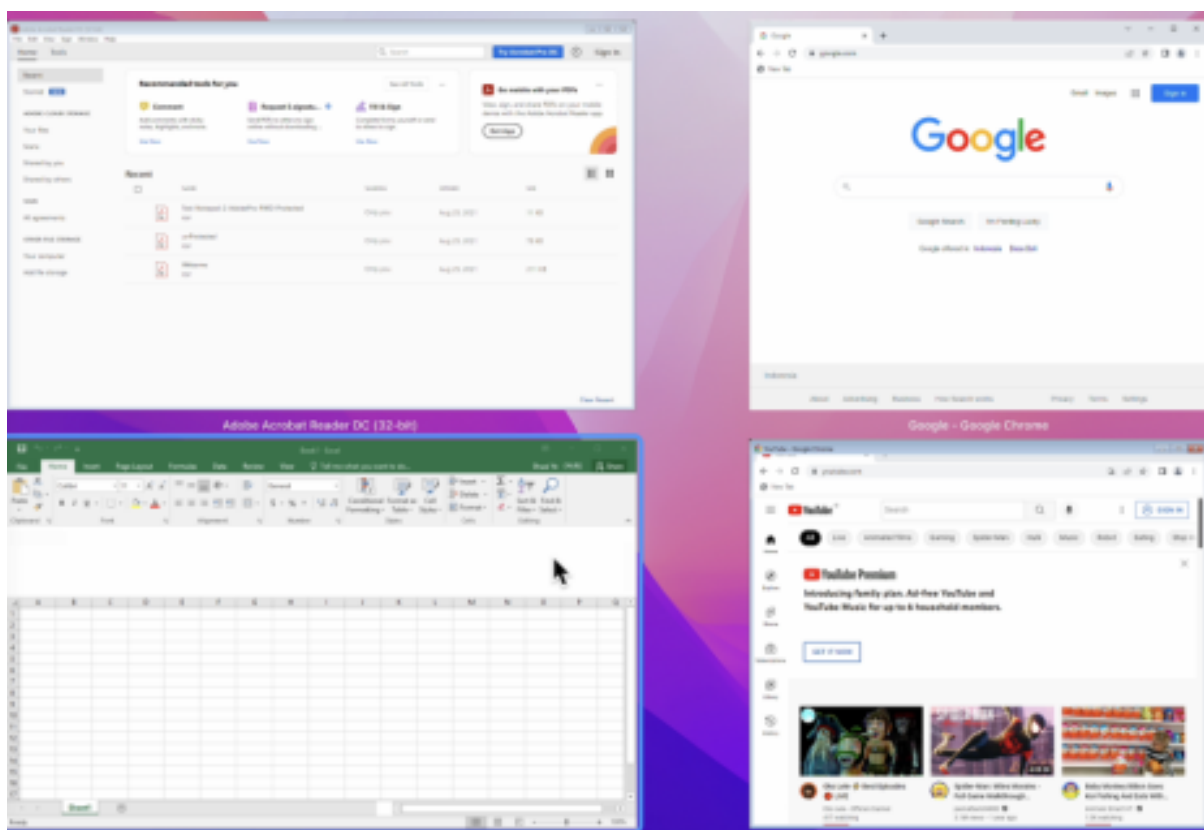


Verbessertes Mission Control- und App Expose-Erlebnis

Bisher führte die Verwendung des Features **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung zu einer großen Zahl überlappender Fenster.



Wenn Sie ab diesem Release das Feature **Mission Control** oder **App Expose** in einer virtuellen App-Sitzung verwenden und viele Fenster öffnen, überlappen sich die Fenster nicht und stehen übersichtlich zur Verfügung.



Videoauflösungen einschränken

Wenn Benutzer Clientendpunkte mit niedrigerer Leistung verwenden, können Administratoren die Auflösung eingehender oder ausgehender Videos reduzieren, um die Videocodierung und -decodierung auf diesen Endpunkten zu verbessern. Ab Version 2304 der Citrix Workspace-App für Mac können Sie diese Auflösungen über die Clientkonfigurationsoptionen einschränken.

Hinweis:

Benutzer mit eingeschränkter Auflösung beeinflussen die Videoqualität der gesamten Videokonferenz. Das liegt daran, dass der Microsoft Teams-Server für alle Konferenzteilnehmer die niedrigste gemeinsame Auflösung verwenden muss.

Mit der Citrix Workspace-App 2304 sind Anrufeinschränkungen auf dem Client standardmäßig deaktiviert. Zur Aktivierung müssen Administratoren die folgenden clientseitigen Konfigurationen mit dem defaults-Befehl festlegen:

```
defaults write com.citrix.HdxRtcEngine <Name> -<Type> <Value>
```

| 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 |
| MaxScreenShareFrame | Ganzzahl | NEIN | 1-15 |

Unterstützung für horizontales Scrollen

Bisher unterstützte die Citrix Workspace-App für Mac nur vertikales Scrollen auf einem Trackpad. Ab Release 2305 wird auch horizontales Scrollen unterstützt.

Verbesserte Unterstützung der Audioechounterdrückung

Die Citrix Workspace-App unterstützt die Echounterdrückung in adaptivem Audio und Legacyaudiocodecs. Dieses Feature wurde für Anwendungsfälle von Echtzeitaudio entwickelt und verbessert die Benutzererfahrung. Citrix empfiehlt, adaptives Audio zu verwenden.

USB-Umleitung

Mit HDX USB-Geräteumleitung können USB-Geräte zum und vom Benutzergerät umgeleitet werden. Benutzer können eine Verbindung zu einem Speicherstick auf einem lokalen Computer herstellen und dann remote von einem virtuellen Desktop oder einer desktopgehosteten Anwendung darauf zugreifen.

In einer Sitzung können Benutzer Plug-and-Play-Geräte, einschließlich PTP-Geräte (Picture Transfer Protocol), verwenden. Beispiel:

- Digitalkameras, MTP-Geräte (Media Transfer Protocol) wie digitale Audio-Player und tragbare Medienplayer
- POS-Geräte und andere Geräte wie 3D SpaceMouse, Scanner, Unterschriftenfelder und so weiter.

Hinweis:

Double-Hop-USB wird bei Sitzungen mit über Desktop gehosteten Anwendungen nicht unterstützt.

USB-Umleitung ist auf folgenden Clients verfügbar:

- Windows
- Linux
- Mac

Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Um festzulegen, welche USB-Geräte einem virtuellen Desktop verfügbar gemacht werden, aktualisieren Sie die Liste der für die Umleitung unterstützten USB-Geräte. Weitere Informationen finden Sie weiter unten.

Tipp

Wenn aus Sicherheitsgründen eine Trennung zwischen Benutzergerät und Server erforderlich ist, informieren Sie die Benutzer darüber, welche Typen von USB-Geräten zu vermeiden sind.

Die beliebtesten USB-Geräte können über optimierte virtuelle Kanäle umgeleitet werden und liefern hervorragende Leistung und Bandbreiteneffizienz über ein WAN. Optimierte virtuelle Kanäle sind normalerweise die beste Option, insbesondere in Umgebungen mit hoher Latenz.

Hinweis:

Für die Umleitung von USB-Geräten gilt: die Citrix Workspace-App für Mac behandelt ein SMART-Board ebenso wie eine Maus.

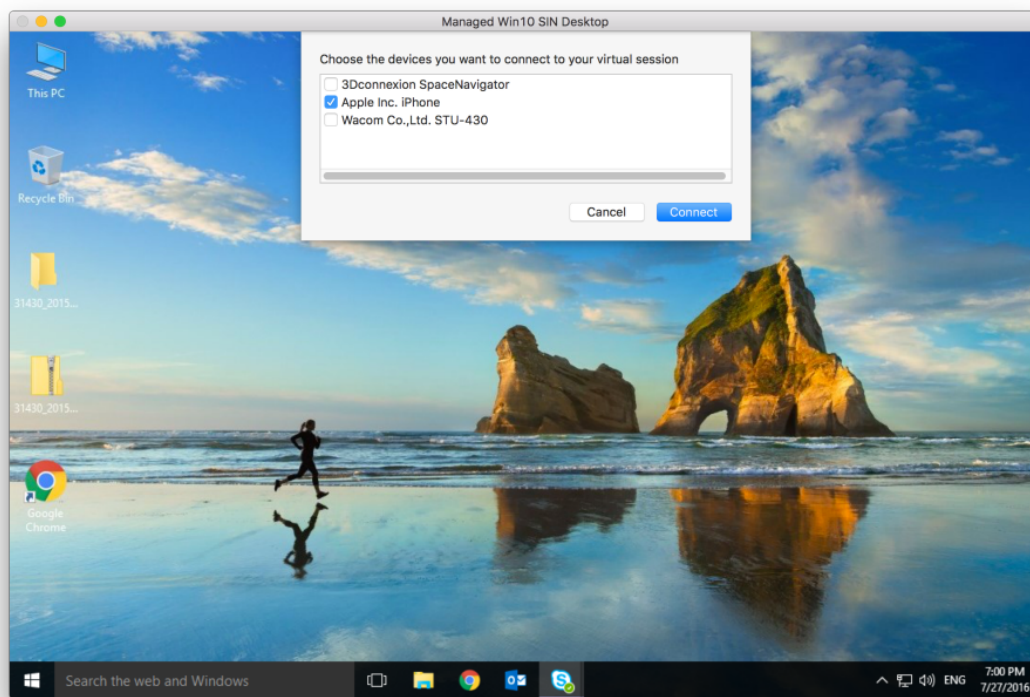
Das Produkt unterstützt optimierte virtuelle Kanäle mit USB 3.0-Geräten und USB 3.0-Anschlüssen. Beispielsweise wird ein virtueller CDM-Kanal zur Anzeige von Dateien in einer Kamera und zur Bereitstellung von Audio für ein Headset verwendet. Das Produkt unterstützt zudem die generische USB-Umleitung von USB 3.0-Geräten, die mit einem USB 2.0-Port verbunden sind.

Einige erweiterte gerätespezifischen Features, z. B. HID-Schaltflächen (Human Interface Device) auf einer Webcam, funktionieren möglicherweise mit dem optimierten virtuellen Kanal nicht wie erwartet. Verwenden Sie den virtuellen Kanal für generisches USB als Alternative.

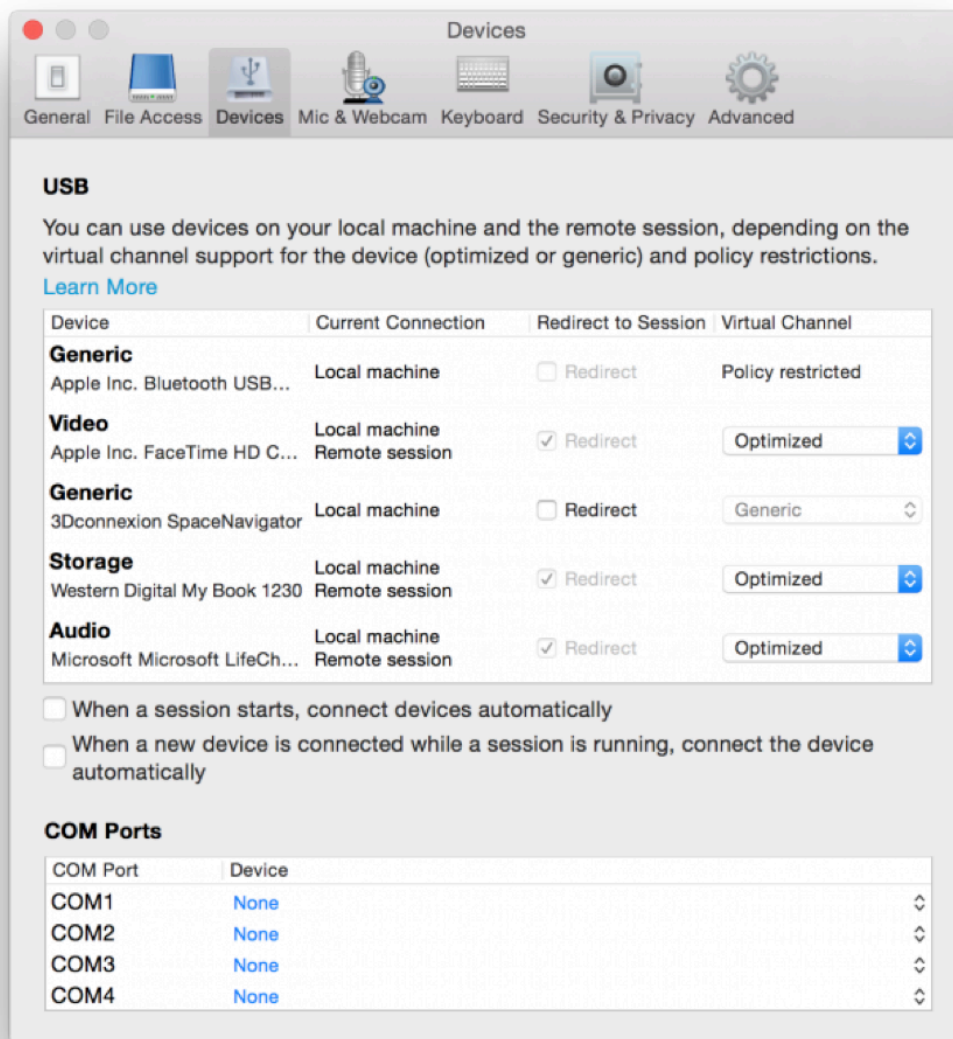
Einige Geräte werden standardmäßig nicht umgeleitet und sind nur in der lokalen Sitzung verfügbar. Es wäre beispielsweise nicht angemessen, eine über internes USB direkt angeschlossene Netzwerkkarte umzuleiten.

Verwenden von USB-Umleitung

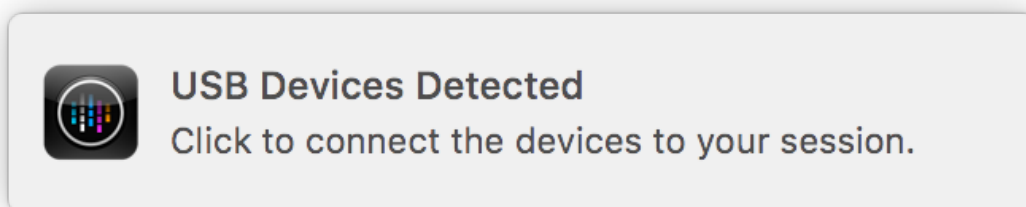
1. Verbinden Sie das USB-Gerät mit dem Gerät, auf dem die Citrix Workspace-App für Mac installiert ist.
2. Sie werden aufgefordert, die auf dem lokalen System verfügbaren USB-Geräte auszuwählen.



3. Wählen Sie das Gerät aus, das Sie verbinden möchten, und klicken Sie auf **Verbinden**. Schlägt die Verbindung fehl, wird eine Fehlermeldung angezeigt.
4. Im Fenster **Einstellungen** auf der Registerkarte **Geräte** wird das verbundene USB-Gerät im USB-Bereich angezeigt:



5. Wählen Sie für das USB-Gerät den virtuellen Kanaltyp (Generisch oder Optimiert) aus.
6. Eine Meldung wird angezeigt. Klicken Sie, um das USB-Gerät mit Ihrer Sitzung zu verbinden:



Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen. Wenn Sie mit der Citrix Workspace-App für Mac arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, erscheinen unmittelbar im USB-Menü von Desktop Viewer.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, kann das Problem u. U. dadurch behoben werden, dass das Gerät erst nach dem Beginn der virtuellen Sitzung angeschlossen wird.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Menü **Sicheres Entfernen**, bevor Sie das USB-Gerät entfernen.

Unterstützte USB-Geräte

Da Apple die Einstellung von Kernel Extensions (KEXT) angekündigt hat, wurde die Citrix Workspace-App für Mac auf das neue von Apple bereitgestellte USB-Framework für den Benutzermodus `IOUSBHost` migriert. In diesem Artikel werden die unterstützten USB-Geräte aufgeführt.

USB-Geräte, die mit der USB-Umleitung kompatibel sind

Die folgenden USB-Geräte funktionieren nahtlos mit der USB-Umleitung:

- 3DConnexion SpaceMouse
- Massenspeichergeräte
- Kingston DataTraveler USB-Speicherstick
- Externe HDD von Seagate
- Speicherstick von Kingston/Transcend, 32 GB/64 GB
- NIST PIV-Smartcard/-Lesegerät
- YubiKey

USB-Geräte, bei denen die USB-Umleitung fehlschlägt

Die externe SSD-Festplatte von Transcend ist nicht mit der USB-Umleitung kompatibel.

Nicht verifizierte USB-Geräte

Es gibt viele Geräte, von Citrix nicht verifiziert, für eine erfolgreiche USB-Umleitung mit der Citrix Workspace-App für Mac. Hier sind einige dieser Geräte:

- Andere Festplatten

- Spezielle Tasten auf der Tastatur und an Headsets, die ein benutzerdefiniertes HID-Protokoll verwenden

Unterstützung für Massenspeichergeräte

Wir haben festgestellt, dass nicht alle Arten von Massenspeichergeräten erfolgreich umgeleitet werden können. Für Geräte, die nicht umgeleitet werden können, gibt es einen optimierten virtuellen Kanal namens Clientlaufwerkzuordnung. Mit der Clientlaufwerkzuordnung kann der Zugriff auf die Massenspeichergeräte durch die Richtlinien auf dem Delivery Controller gesteuert werden.

Unterstützung für isochrone Geräte

Die generische USB-Umleitung bietet keine Unterstützung für die isochrone Klasse von USB-Geräten in der Citrix Workspace-App für Mac. Der isochrone Modus der Datenübertragung in einer USB-Spezifikation zeigt Geräte an, die die Zeitstempeldaten mit konstanter Geschwindigkeit streamen. Zum Beispiel: WebCams, USB-Kopfhörer und so weiter

Unterstützung für Verbundgeräte

Ein USB-Verbundgerät ist ein einzelnes Gadget, das mehr als eine Funktion ausführen kann. Zum Beispiel: Multifunktionsdrucker, iPhone usw. Derzeit unterstützt die Citrix Workspace-App für Mac keine Umleitung von Verbundgeräten in die Citrix Virtual Apps and Desktops- und Citrix DaaS-Sitzung.

Alternativen für nicht unterstützte USB-Geräte

Es gibt optimierte virtuelle Kanäle für Geräte, die nicht durch die generische USB-Umleitung unterstützt werden. Diese virtuellen Kanäle sind im Vergleich zur generischen USB-Umleitung auf Geschwindigkeit optimiert. Hier sind einige Beispiele:

- **Webcamumleitung:** Optimiert für rohen Webcamdatenverkehr. Das Microsoft Teams Optimization Pack hat eine eigene Methode zur Webcamumleitung. Daher fällt es nicht unter den virtuellen Kanal der Webcamumleitung.
- **Audioumleitung:** Optimiert für die Übertragung von Audiostreams.
- **Clientlaufwerkzuordnung:** Optimiert für die Umleitung von Massenspeichergeräten in die Citrix Virtual Apps and Desktops- und Citrix DaaS-Sitzung (früher Citrix Virtual Apps and Desktops Service). Zum Beispiel: Speichersticks, Festplatten, DVD ROM/RW und so weiter.

Enlightened Data Transport (EDT)

Standardmäßig ist das EDT-Protokoll in der Citrix Workspace-App für Mac aktiviert.

Die Citrix Workspace-App für Mac liest die **EDT-Einstellungen** in der Datei default.ica und wendet sie entsprechend an.

Um EDT zu deaktivieren, führen Sie den folgenden Befehl in einem Terminal aus:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

Sitzungszuverlässigkeit und automatische Wiederverbindung von Clients

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Auf dem Client friert der Bildschirm ein, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Wichtig

- Benutzer der Citrix Workspace-App für Mac können die Servereinstellung nicht außer Kraft setzen.
- Wenn die Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden.

Hinweis:

Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und Citrix Gateway gesendet werden.

Verwenden von Sitzungszuverlässigkeitsrichtlinien

Mit der Richtlinieneinstellung **Sitzungszuverlässigkeit - Verbindungen** können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.

Der Standardwert für die Einstellung **Sitzungszuverlässigkeit - Timeout** ist 180 Sekunden (drei Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Bedienkomfort erhöhen soll. Daher wird der Benutzer nicht zur erneuten Authentifizierung aufgefordert.

Tipp

Eine Verlängerung des Timeouts für die Sitzungszuverlässigkeit kann dazu führen, dass ein Benutzer abgelenkt wird und sich vom Gerät entfernt. Dann besteht das Risiko, dass unbefugte Benutzer Zugang zu der Sitzung erhalten.

Eingehende Sitzungszuverlässigkeitsverbindungen verwenden standardmäßig Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer" geändert.

Sie können die Einstellung für die Citrix-Richtlinie **Authentifizierung bei automatischer Wiederverbindung von Clients** so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wieder verbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, sobald der mit der Option **Sitzungszuverlässigkeit - Timeout** festgelegte Zeitraum abläuft. Anschließend wird über die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients versucht, die Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Hinweis:

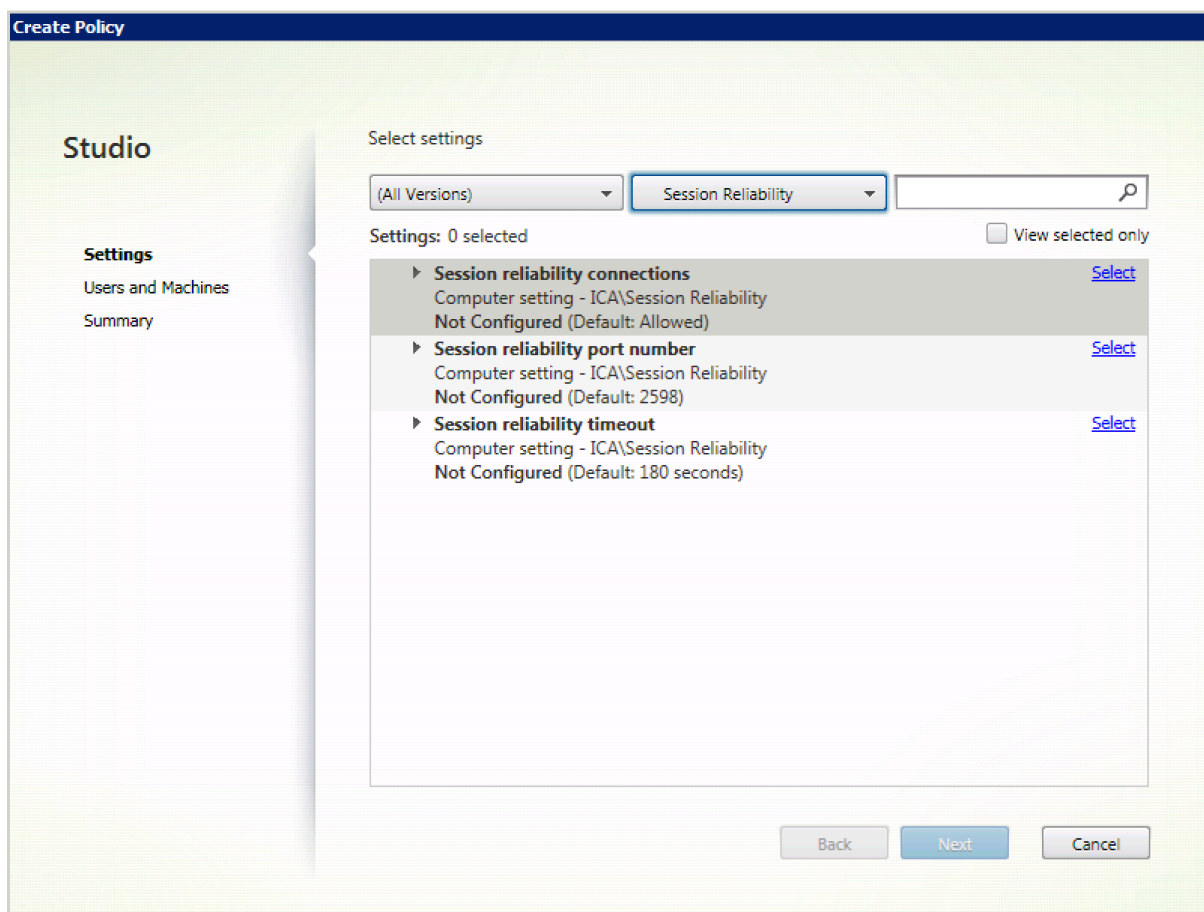
Die Sitzungszuverlässigkeit ist standardmäßig auf dem Server aktiviert. Sie deaktivieren dieses Feature, indem Sie die vom Server verwaltete Richtlinie konfigurieren.

Konfigurieren der Sitzungszuverlässigkeit in Citrix Studio

Standardmäßig ist die Sitzungszuverlässigkeit aktiviert.

Deaktivieren der Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Verbindungen**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Konfigurieren des Timeouts für die Sitzungszuverlässigkeit

Die Standardeinstellung für das Sitzungszuverlässigkeitstimeout ist 180 Sekunden.

Hinweis:

Die Richtlinie für das Sitzungszuverlässigkeitstimeout kann nur mit XenApp und XenDesktop 7.11 und höher festgelegt werden.

Ändern des Timeouts für die Sitzungszuverlässigkeit:

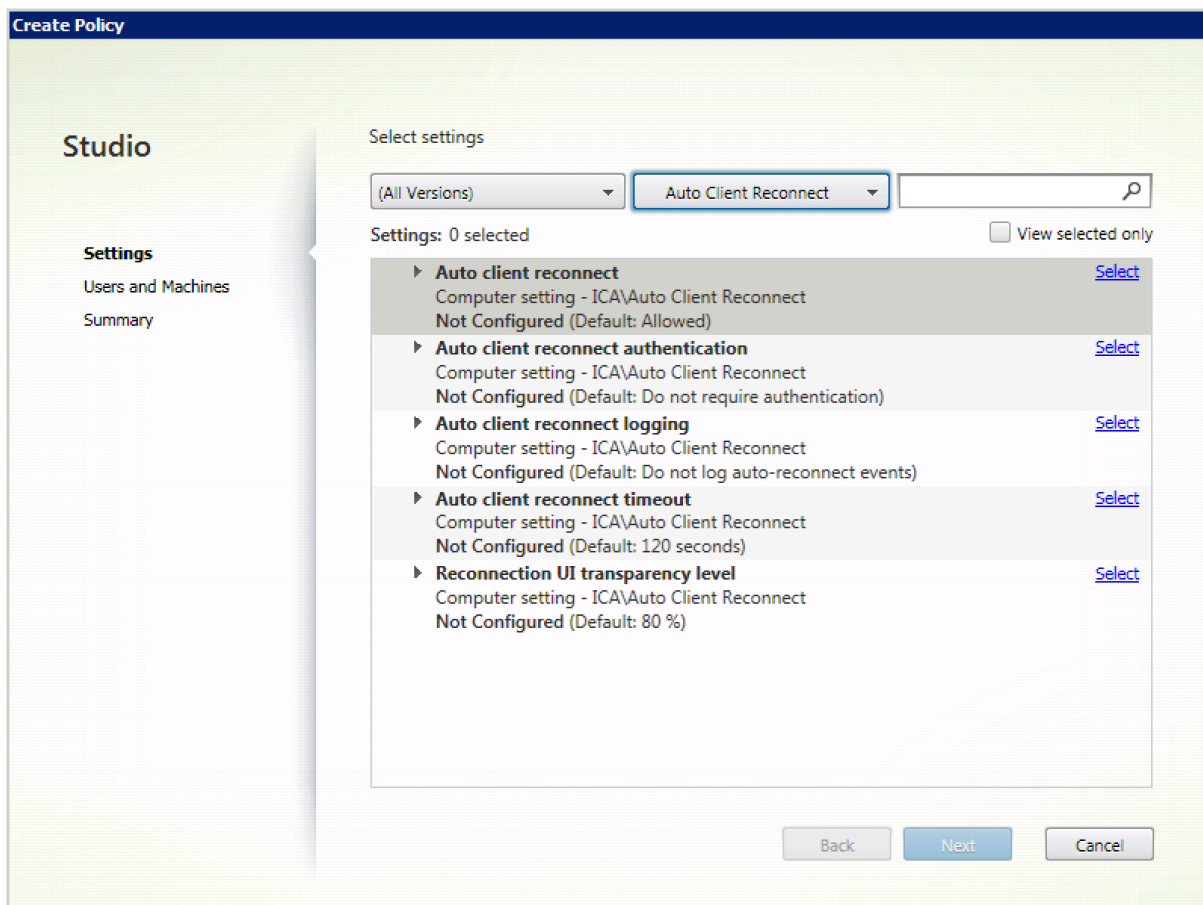
1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Timeout**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Konfigurieren der automatischen Wiederverbindung von Clients mit Citrix Studio

Die automatische Wiederverbindung von Clients ist standardmäßig aktiviert.

Deaktivieren der automatischen Wiederverbindung von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Client automatisch wieder verbinden**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Konfigurieren des Timeouts für die automatische Wiederverbindung von Clients

Die Standardeinstellung für das Timeout für die automatische Wiederverbindung von Clients ist 120 Sekunden.

Hinweis:

Die Richtlinie für das Timeout für die automatische Wiederverbindung von Clients kann nur mit XenApp und XenDesktop 7.11 und höher festgelegt werden.

Ändern des Timeouts beim automatischen Wiederverbinden von Clients:

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Client automatisch wieder verbinden**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Einschränkungen:

Auf einem Terminalserver-VDA verwendet die Citrix Workspace-App für Mac unabhängig von den Benutzereinstellungen 120 Sekunden als Timeoutwert.

Konfigurieren der Transparenz für die Benutzeroberfläche beim Wiederverbinden

Bei Verbindungen mit Sitzungszuverlässigkeit und bei der automatischen Wiederverbindung von Clients wird die Sitzungsbenutzeroberfläche angezeigt. Die Transparenzstufe der Benutzeroberfläche kann mit einer Richtlinie in Citrix Studio angepasst werden.

Standardmäßig ist die Transparenz der Benutzeroberfläche beim Wiederverbinden auf 80 % festgelegt.

Ändern der Transparenzstufe für die Benutzeroberfläche beim Wiederverbinden:

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Transparenzstufe für Benutzeroberfläche bei Wiederverbindung**.
3. Bearbeiten Sie den Wert.
4. Klicken Sie auf **OK**.

Interaktion zwischen automatischer Wiederverbindung von Clients und Sitzungszuverlässigkeit

Es gibt Herausforderungen rund um die Mobilität im Zusammenhang mit dem Wechsel zwischen Zugriffspunkten, Netzwerkunterbrechungen und Anzeigetimeouts aufgrund von Latenz. Sie erschweren die Aufrechterhaltung der Verbindungsintegrität für aktive Citrix Workspace-App für Mac-Sitzungen. Mit den verbesserten Technologien für Sitzungszuverlässigkeit und automatische Wiederverbindung von Citrix wird dieses Problem behoben.

Mit diesem Feature können Benutzer nach Netzwerkunterbrechungen die Verbindung zu Sitzungen automatisch wiederherstellen. Diese über Richtlinien in Citrix Studio aktivierten Features können die Benutzererfahrung verbessern.

Hinweis:

Timeoutwerte für die automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit können mit der Datei **default.ica** in StoreFront geändert werden.

Automatische Wiederverbindung von Clients

Die automatische Wiederverbindung von Clients kann mit einer Richtlinie in Citrix Studio aktiviert oder deaktiviert werden. Standardmäßig ist dieses Feature aktiviert. Informationen zum Ändern

dieser Richtlinie finden Sie im Abschnitt zum automatischen Wiederverbinden von Clients weiter oben in diesem Artikel.

In StoreFront können Sie mit der Datei default.ica das Verbindungstimeout für die automatische Wiederverbindung von Clients ändern. Die Standardeinstellung des Timeouts ist 120 Sekunden (zwei Minuten).

| Einstellung | Beispiel | Standard |
|-----------------------------|---------------------------------|----------|
| TransportReconnectRetryMaxT | TransportReconnectRetryMaxT=120 | 120 |

Sitzungszuverlässigkeit

Die Sitzungszuverlässigkeit kann mit einer Richtlinie in Citrix Studio aktiviert oder deaktiviert werden. Standardmäßig ist dieses Feature aktiviert.

Verwenden Sie die Datei **default.ica** in StoreFront, um das Verbindungstimeout für die Sitzungszuverlässigkeit zu ändern. Die Standardeinstellung des Timeouts ist 180 Sekunden (drei Minuten).

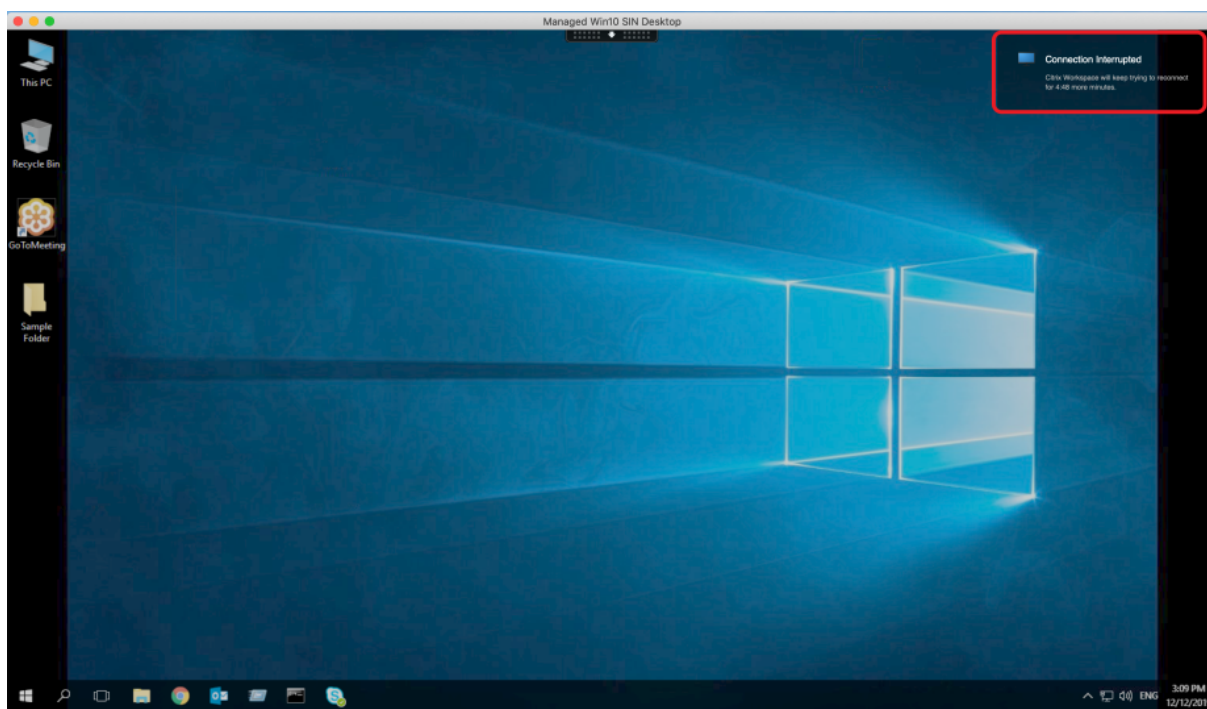
| Einstellung | Beispiel | Standard |
|-----------------------|---------------------------|----------|
| SessionReliabilityTTL | SessionReliabilityTTL=120 | 180 |

Funktionsweise von Sitzungszuverlässigkeit und automatischer Wiederverbindung von Clients

Wenn automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit für die Citrix Workspace-App für Mac aktiviert sind, berücksichtigen Sie Folgendes:

- Wenn eine Wiederverbindung erfolgt, ist das Sitzungsfenster ausgegraut. Ein Countdowntimer zeigt die verbleibende Zeit bis zur Wiederverbindung der Sitzung an. Wenn der Countdowntimer für die Sitzung abläuft, wird die Sitzung getrennt.

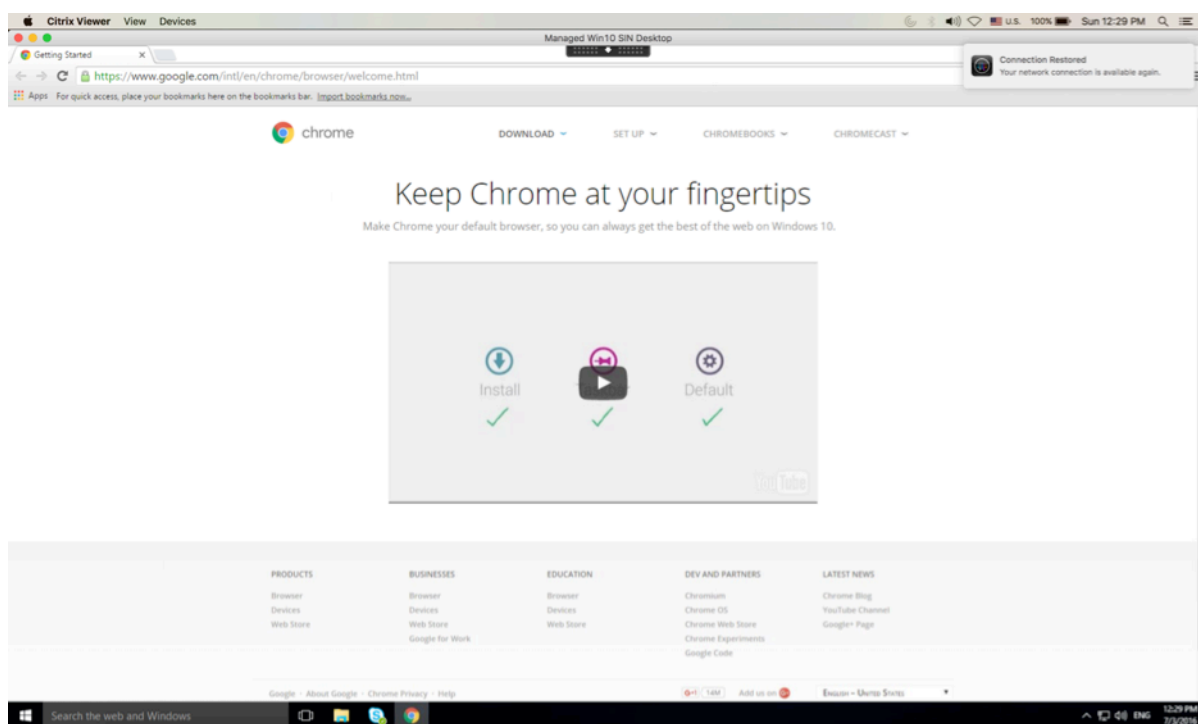
Standardmäßig beginnt die Anzeige des Wiederverbindungscountdowns bei 5 Minuten. In diesem Zeitwert sind die Werte der beiden Timer für automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit, 2 und 3 Minuten, zusammengefasst. In der Abbildung unten sehen Sie die Meldung mit dem Countdowntimer, die oben rechts im Sitzungsfenster angezeigt wird:



Tipp

Sie können die für eine inaktive Sitzung verwendete Graustufe mit einer Befehlszeile ändern. Beispiel: `com.citrix.receiver.nomas NetDisruptBrightness 80`. Der Standardwert ist 80. Der Höchstwert ist 100 (transparentes Fenster) und der Mindestwert kann 0 sein (schwarzes Fenster).

- Bei der erfolgreichen Wiederverbindung einer Sitzung (oder wenn eine Sitzung getrennt wird) werden Benutzer benachrichtigt. Die Benachrichtigung wird oben rechts im Sitzungsfenster angezeigt:



- In einem Sitzungsfenster, das durch Sitzungszuverlässigkeit und automatische Wiederverbindung von Clients gesteuert wird, wird eine Informationsmeldung zum Status der Sitzungsverbindung angezeigt. Klicken Sie auf **Wiederverbindung abbrechen**, um zu einer aktiven Sitzung zu wechseln.

Hintergrundunschärfe und Hintergrundersatz für Citrix Optimized Microsoft Teams

Citrix Optimized Microsoft Teams in der Citrix Workspace-App für Mac unterstützt jetzt Hintergrundunschärfe und das Ersetzen des Hintergrunds. Sie können das Feature verwenden, indem Sie in einer Besprechung oder einem Anruf **Mehr > Hintergrundeffekte anwenden** wählen.

Verbesserte Unterstützung für Notchdisplays

Ab Release 2301 unterstützt die Citrix Workspace-App für Mac auch Macs mit Notchdisplay. Macs unterstützen ein natives Notchdisplay im Vollbildmodus für Retina-Displays und Multimonitoranzeigen. Der Sitzungsbereich auf dem Notchdisplay ist jetzt noch größer und bietet Kunden mehr Bildschirmfläche. Diese Verbesserung unterstützt auch eine hohe DPI-Skalierung. Die Mausposition wird auf allen externen Monitoren korrekt angezeigt.

Hinweis:

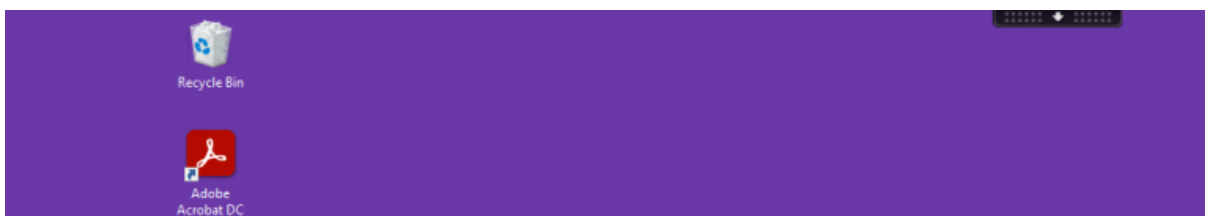
Stellen Sie sicher, dass die Option **Scale to fit below built-in camera** im Citrix Viewer nicht ausgewählt ist. Die Option ist standardmäßig deaktiviert und nur auf Macs mit Notchdisplay verfü-

bar.

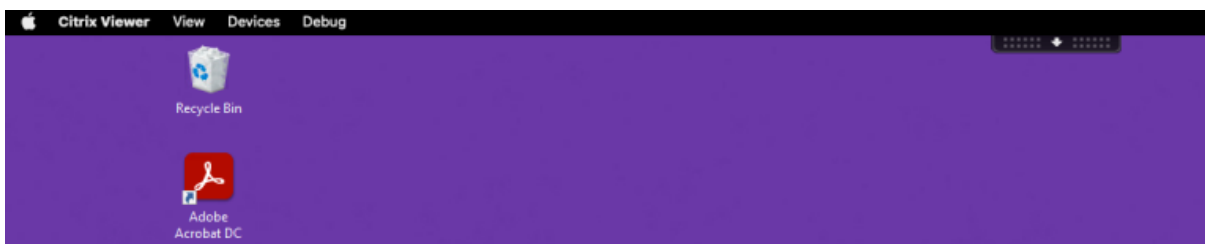
Verbesserte Unterstützung der Menüleiste

Ab Release 2301 wird die macOS-Option **Automatically hide and show the menu bar in full screen** vollständig durch die Citrix Workspace-App unterstützt. Für Versionen vor macOS 13 müssen Sie unter **System Preferences > Dock & Menu Bar** die Option **Automatically hide and show the menu bar in full screen** deaktivieren. Für macOS 13 und neuere Versionen müssen Sie unter **System Preferences > Desktop & Dock** die Option **Automatically hide and show the menu bar in full screen** deaktivieren. Sie können diese Option entweder aktivieren oder deaktivieren. Diese Verbesserung unterstützt auch eine hohe DPI-Skalierung. Die Mausposition wird auf allen externen Monitoren korrekt angezeigt.

Die folgende Abbildung zeigt ein Fenster mit ausgeblendeter Menüleiste.



Die folgende Abbildung zeigt ein Fenster mit angezeigter Menüleiste.



Verbesserter Energiesparmodus für optimierte Microsoft Teams-Anrufe

Bisher ging die Citrix Workspace-App oder der optimierte Microsoft Teams-Bildschirm gelegentlich in den Energiesparmodus über, wenn in einer Besprechung mit optimiertem Microsoft Teams keine Maus- oder Tastaturinteraktion stattfand.

Ab Release 2305 gehen die Citrix Workspace-App oder der optimierte Microsoft Teams-Bildschirm nicht in den Energiesparmodus über, wenn in einer Besprechung mit optimiertem Microsoft Teams keine Maus- oder Tastaturinteraktion auftritt.

Unterstützung für Integrationskamera

Mit der Integrationskamera (Continuity Camera) können Sie Ihr iPhone jetzt als Webcam verwenden. Platzieren Sie Ihr iPhone dabei so, dass die Kamera für das Mac-Gerät verfügbar ist. Sie müssen **Web-**

cam > Automatic Camera Selection auswählen, damit das iPhone auf dem Mac-Gerät automatisch als externe Kamera angezeigt wird. Sie können manuell zu jeder anderen Kamera wechseln, indem Sie beispielsweise **Webcam > FaceTime HD Camera** auswählen. Die Integrationskamera funktioniert kabelgebunden oder drahtlos und liefert ein qualitativ hochwertiges Bild.

Voraussetzungen

- Das Feature wird auf Mac-Geräten mit macOS Version 13 unterstützt.
- Das Feature wird auf iOS-Geräten mit iOS Version 16 unterstützt.
- Sie müssen auf dem iOS- und Mac-Gerät mit demselben Apple-Konto in der Citrix Workspace-App angemeldet sein.
- Für eine Kabelverbindung muss das iPhone über USB mit dem Mac-Gerät verbunden sein.
- Für eine drahtlose Verbindung müssen sich iPhone und Mac-Gerät in der Nähe befinden, und auf den Geräten muss Bluetooth und WLAN aktiviert sein.

Einige Vorzüge der Funktion:

- **Folgemodus:** Der Sprecher bleibt im Bild, auch wenn er sich bewegt.
- **Porträtmodus:** Der Bildhintergrund wird unscharf dargestellt.
- **Studiolicht:** Sorgt für einen hellen Effekt auf dem Bild. Der Hintergrund wird abgeblendet und das Bild erscheint heller.
- **Schreibtischansicht:** Das iPhone unterteilt den Feed der Ultra-Weitwinkelkamera in zwei Fenster. Schreibtisch und Gesichter werden gleichzeitig dargestellt.
- **Bildschirmfreigabe:** Das iPhone unterteilt den Feed der Ultra-Weitwinkelkamera in zwei Fenster. Schreibtisch und Gesichter werden gleichzeitig dargestellt. Die in den Videokonferenz-Apps verfügbare Funktion zur Bildschirmfreigabe kann verwendet werden, um den Schreibtisch-Feed zu teilen.

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 Mac und sendet die Daten automatisch an Citrix und Google Analytics. | Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Citrix Workspace-App zu verbessern. |

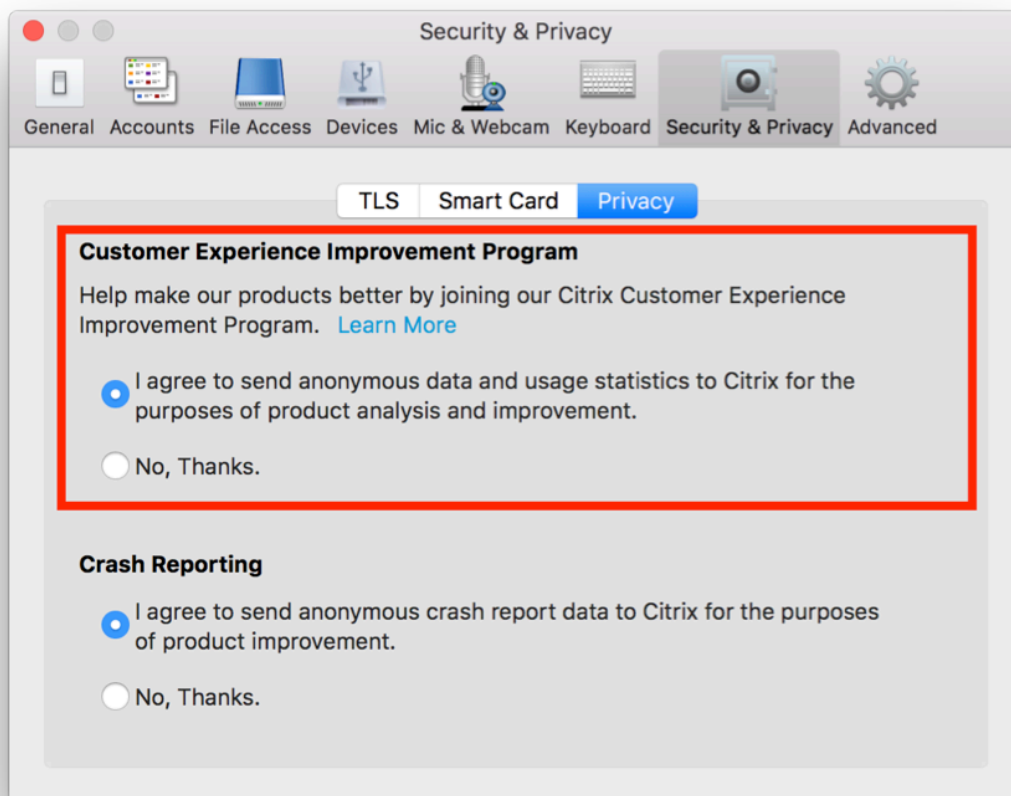
Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix. Ihre Daten sind gemäß dem [Citrix Services Security Exhibit](#), verfügbar im [Citrix Trust Center](#), geschützt.

Citrix verwendet Google Analytics, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu sammeln. Sie können prüfen, wie Google die für [Google Analytics gesammelten Daten verwendet](#).

Führen Sie die folgenden Schritte aus, um das Senden von CEIP-Daten an Citrix und Google Analytics zu deaktivieren:

1. Wählen Sie im Fenster **Einstellungen** die Option **Sicherheit und Datenschutz**.
2. Wählen Sie die Registerkarte **Datenschutz**.
3. Wählen Sie **Nein, danke**, um CEIP zu deaktivieren und die Teilnahme abzulehnen.
4. Klicken Sie auf **OK**.



Alternativ können Sie CEIP deaktivieren, indem Sie folgenden Terminalbefehl ausführen:

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```

Hinweis:

Es werden keine Daten für Benutzer in der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK) gesammelt.

Folgende Datenelemente werden von Google Analytics erfasst:

| Betriebssystemversion | Version der Workspace-App | Generischen USB-Umleitung - Nutzung | Storekonfiguration |
|-------------------------------------|---|---|---------------------------------|
| Citrix Enterprise Browser - Nutzung | Citrix Virtual Apps and Desktops- Sitzungsstartstatus | Einstellung für automatische Aktualisierung | Status für automatische Updates |

| | | | |
|---|---|--|---|
| Sitzungsstartmethode | Deinstallationsinformal | Inaktivitätstimeout - Featurenutzung | E-Mail-Ermittlung - Featurenutzung |
| Benutzerdefinierter Webstore - Featurenutzung | Einstellungen für die Wiederverbindung | Global App Configuration Service - Nutzung | Tastaturbelegung wiederherstellen - Nutzung |
| Kennwort löschen - Featurenutzung | Auto-Updatekanal | Verbindungsleasedetail | |

Hinweis:

- Citrix Enterprise Browser hieß früher "Citrix Workspace Browser".

Anwendungsbereitstellung

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops und Citrix DaaS, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen zu erhöhen:

Webzugriffsmodus

Ohne jegliche Konfiguration bietet die Citrix Workspace-App für Mac im Webzugriffsmodus browserbasierten Zugriff auf Anwendungen und Desktops. Benutzer greifen einfach über einen Browser auf Workspace für Web zu und wählen die gewünschten Anwendungen zur Verwendung aus. Im Webzugriffsmodus werden keine Appverknüpfungen im App-Ordner auf den Benutzergeräten platziert.

Self-Service-Modus

Fügen Sie der Citrix Workspace-App für Mac ein StoreFront-Konto hinzu, oder legen Sie fest, dass die Citrix Workspace-App auf eine StoreFront-Site verweist. Anschließend können Sie einen Self-Service-Modus konfigurieren, mit dem die Benutzer die Anwendungen über die Citrix Workspace-App für Mac 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. Wenn Benutzer eine Anwendung auswählen, wird eine Verknüpfung für die Anwendung im App-Ordner auf dem Benutzergerät platziert.

Wenn Benutzer auf eine StoreFront 3.0-Site zugreifen, erhalten sie eine Vorschau der Citrix Workspace-App für Mac.

Wenn Sie Anwendungen auf einer Citrix Virtual Apps-Farm veröffentlichen, können Sie die Erfahrung für Benutzer verbessern, die auf diese Anwendungen über StoreFront-Stores zugreifen. Stellen Sie sicher, dass Sie aussagekräftige Beschreibungen für die veröffentlichten Apps angeben. In Citrix Workspace-App für Mac sind diese Beschreibungen für Benutzer sichtbar.

Konfigurieren des Self-Service-Modus

Wie bereits erwähnt, fügen Sie der Citrix Workspace-App für Mac ein StoreFront-Konto hinzu oder Sie legen fest, dass die Citrix Workspace-App für Mac auf eine StoreFront-Site verweist. So können Sie den Self-Service-Modus konfigurieren, mit dem die Benutzer die Anwendungen über die Benutzeroberfläche der Citrix Workspace-App für Mac abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

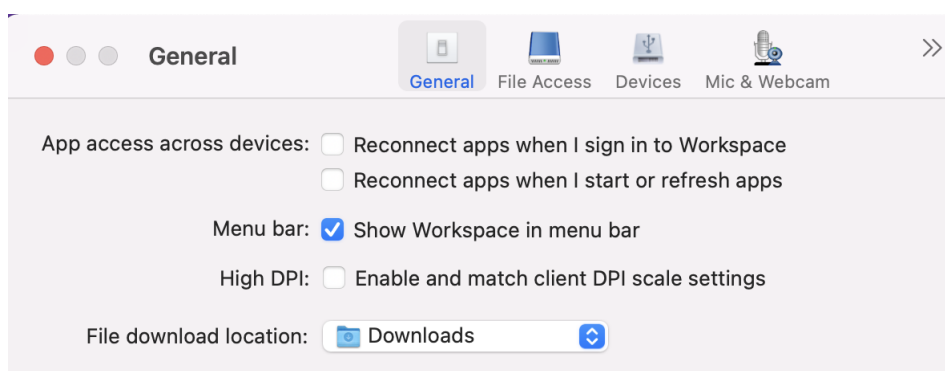
Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

- Sie können automatisch eine App für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge ****KEYWORDS: Auto**** an die Beschreibung anhängen, während Sie die App in Citrix Virtual Apps veröffentlichen. Wenn Benutzer sich bei dem Store anmelden, wird die App automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Anwendungen werden den Benutzern angekündigt bzw. häufig verwendete Anwendungen sind leichter zu finden, wenn Sie sie in der Citrix Workspace-App für Mac unter "Highlights" auführen. Um Apps für Mac in der Liste "Highlights" aufzuführen, hängen Sie die Zeichenfolge ****KEYWORDS: Featured**** an die App-Beschreibung an.

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

Unterstützung für hohe DPI-Werte

Sie können die DPI-Skalierungseinstellungen des Clients jetzt aktivieren und anpassen, indem Sie die Sitzungssymbolleiste starten und zu **Einstellungen > Allgemeines > Hoher DPI-Wert** gehen. Die Option "Hoher DPI-Wert" ist standardmäßig deaktiviert.



Citrix Workspace-Updates

Konfigurieren mit der GUI

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

1. Navigieren Sie in der Citrix Workspace-App für Mac zum Dialogfeld **Einstellungen**.
2. Klicken Sie im Bereich **Erweitert** auf **Updates**. Das Dialogfeld "Citrix Workspace-App-Updates" wird angezeigt.
3. Wählen Sie eine der folgenden Optionen:
 - Ja, benachrichtigen
 - Nein, nicht benachrichtigen
 - Vom Administrator festgelegte Einstellungen verwenden
4. Schließen Sie das Dialogfeld, um die Änderungen zu speichern.

Konfigurieren von Citrix Workspace-Updates mit StoreFront

Administratoren können Citrix Workspace-App-Updates mit StoreFront konfigurieren. Die Citrix Workspace-App für Mac verwendet diese Konfiguration nur für Benutzer, die "Vom Administrator festgelegte Einstellungen verwenden" ausgewählt haben. Mit den folgenden Schritten führen Sie die manuelle Konfiguration durch.

1. Öffnen Sie die Datei `web.config` in einem Texteditor. Der Standardspeicherort ist `C:\inetpub\wwwroot\Citrix\Roaming\web.config`
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:
`<properties>`
`<clear />`
`</properties>`
3. Fügen Sie das Tag für automatische Updates nach dem Tag `<clear />` ein.

auto-update-Check

Die Funktion "auto-update-Check" legt fest, dass die Citrix Workspace-App für Mac ermitteln kann, ob Updates verfügbar sind.

Gültige Werte:

- Auto: Benutzer erhalten Benachrichtigungen, wenn Updates verfügbar sind.
- Manual: Benutzer erhalten keine Benachrichtigungen, wenn Updates verfügbar sind. Die Benutzer müssen manuell nach Updates suchen, indem sie **Nach Updates suchen** wählen.
- Disabled: Citrix Workspace-Updates werden deaktiviert.

auto-update-DeferUpdate-Count

Legt fest, wie oft Benutzer zum Update aufgefordert werden, bevor das Update auf die aktuelle Version der Citrix Workspace-App für Mac erzwungen wird. Der Standardwert ist 7.

Gültige Werte:

- -1 — Der Benutzer wird später erinnert, wenn ein Update verfügbar ist.
- 0 – Der Benutzer wird gezwungen, auf die aktuelle Version der Citrix Workspace-App für Mac zu aktualisieren, wenn das Update verfügbar ist.
- Positive Ganzzahl – Male, die der Benutzer an das Update erinnert wird, bevor das Update erzwungen wird. Citrix empfiehlt, diesen Wert höchstens auf 7 festzulegen.

auto-update-Rollout-Priority

Legt fest, wie schnell ein Gerät erkennt, dass ein Update verfügbar ist.

Gültige Werte:

- Auto – Das Citrix Workspace-Updates-System entscheidet, wann Benutzern verfügbare Updates bereitgestellt werden.
- Fast – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten hohen Priorität zur Verfügung gestellt.
- Medium – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten mittleren Priorität zur Verfügung gestellt.
- Slow – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten niedrigen Priorität zur Verfügung gestellt.

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert. Wenn Sie dieses Feature aktivieren, wird das Clienttastaturlayout automatisch mit den virtuellen Apps und Desktops synchronisiert.

Um die Tastaturlayoutsynchronisierung zu aktivieren, gehen Sie zu **Einstellungen > Tastatur** und wählen Sie "Lokales Tastaturlayout statt des Remoteserver-Tastaturlayouts verwenden".

Hinweis:

1. Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Benutzer, die in der japanischen, chinesischen oder koreanischen Sprache arbeiten, können den IME des Servers verwenden. Sie müssen die Option für das lokale Tastaturlayout deaktivieren, indem sie die entsprechende Option unter **Einstellungen > Tastatur** deaktivieren. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.
2. Das Feature funktioniert in Sitzungen nur dann, wenn der Umschalter im Client aktiviert und das entsprechende Feature auf dem VDA aktiviert ist. Das Menüelement **Clienttastaturlayout verwenden** wird unter **Geräte > Tastatur > International** hinzugefügt, um den aktivierten Status anzuzeigen.

Ab Version 2210 unterstützt die Citrix Workspace-App für Mac drei Synchronisierungsmodi für das Tastaturlayout:

- **Nur einmal beim Sitzungsstart synchronisieren** - Basierend auf dem CTXIME-Wert in der Datei [Config](#) wird das Clienttastaturlayout beim Start der Sitzung mit dem Server synchronisiert. Änderungen, die Sie während der Sitzung am Clienttastaturlayout vornehmen, werden nicht sofort wirksam. Um die Änderungen zu übernehmen, melden Sie sich von der App ab und wieder an. Der Modus "Nur einmal beim Sitzungsstart synchronisieren" ist das Standardtastaturlayout für die Citrix Workspace-App für Mac.
- **Dynamische Synchronisierung zulassen** - Diese Option synchronisiert das Clienttastaturlayout mit dem Server, wenn Sie das Clienttastaturlayout ändern.
- **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

Voraussetzungen

- Aktivieren Sie die Unicode-Tastaturlayoutzuordnung auf dem Windows VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX226335](#).
- Aktivieren Sie die dynamische Tastaturlayoutsynchronisierung auf dem Linux VDA. Weitere Informationen finden Sie unter [Dynamische Tastaturlayoutsynchronisierung](#).
- Wenn Sie Windows Server 2016 oder Windows Server 2019 verwenden, gehen Sie zum Registrierungspfad **HKEY_LOCAL_MACHINE\Software\Citrix\ICA\Icalme**, fügen Sie einen **DWORD**-Wert mit dem Schlüsselnamen **DisableKeyboardSync** hinzu und legen Sie den Wert **0** fest.

Konfigurieren des Tastaturlayouts

Die Citrix Workspace-App für Mac bietet Optionen zum Konfigurieren der drei Synchronisierungsmodi für das Tastaturlayout.

Konfigurieren der Tastaturlayoutsynchronisierung mit der grafischen Oberfläche:

1. Klicken Sie über das Citrix Workspace-App-Symbol in der Menüleiste auf das Kontosymbol oben rechts und gehen Sie zu **Einstellungen > Tastatur**.

Die Seite "Einstellungen für die Synchronisierung des Tastaturlayouts" wird angezeigt.

2. Wählen Sie eine der folgenden Optionen:
 - **Nur einmal beim Sitzungsstart synchronisieren** - Synchronisiert das Tastaturlayout nur einmal beim Sitzungsstart mit dem VDA. Der Tastatureingabemodus "Unicode" ist die empfohlene Option für "Nur einmal beim Sitzungsstart synchronisieren".
 - **Dynamische Synchronisierung zulassen** - Synchronisiert das Tastaturlayout dynamisch mit dem VDA, wenn die Clienttastatur in einer Sitzung geändert wird. Der Tastatureingabemodus "Unicode" ist die empfohlene Option für den Modus Dynamische Synchronisierung zulassen.
 - **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout unabhängig vom im Client ausgewählten Tastaturlayout. Der Tastatureingabemodus "Scancode" ist die empfohlene Option für den Modus **Nicht synchronisieren**. Stellen Sie sicher, dass das Clienttastaturlayout mit dem Tastaturlayout auf dem VDA identisch ist, wenn Sie Unicode für die Option **Nicht synchronisieren** wählen.

Einschränkungen

- Die Verwendung der unter **Unterstützte Tastaturlayouts in Mac** aufgeführten Tastaturlayouts funktioniert, während das Feature aktiviert ist. Wenn Sie für das Clienttastaturlayout ein nicht kompatibles Layout wählen, wird das Layout möglicherweise auf dem VDA synchronisiert, die Funktionalität kann jedoch nicht bestätigt werden.
- Bei Remote-Apps, die mit erhöhten Rechten ausgeführt werden, kann keine Synchronisierung mit dem Clienttastaturlayout erfolgen. Um dieses Problem zu umgehen, ändern Sie das Tastaturlayout manuell auf dem VDA oder deaktivieren Sie die Benutzerkontensteuerung (UAC).
- Wenn ein Benutzer in einer RDP-Sitzung arbeitet, kann das Tastaturlayout nicht mit den **Alt** + **Shift**-Tastenkombinationen geändert werden, wenn RDP als App bereitgestellt wird. Als Workaround können Benutzer das Tastaturlayout mit der Sprachenleiste in der RDP-Sitzung ändern.

Tastaturlayoutunterstützung für Windows VDA

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|--|-----------------------|
| Englisch | ABC | Alle |
| Englisch | ABC - Indien | Alle |
| Englisch | U.S. | Alle |
| Englisch | U.S. International - PC | Alle |
| Englisch | Dvorak | Alle |
| Englisch | Dvorak - Linkshänder | Alle |
| Englisch | Dvorak - Rechtshänder | Alle |
| Englisch | Englisch (Großbritannien u. Nordirland) | Alle |
| Englisch | Englisch (Großbritannien u. Nordirland) - PC | Alle |
| Englisch | Englisch (Kanada) | Alle |
| Englisch | Englisch (Australien) | Alle |
| Englisch | Irish | Alle |
| Französisch | Französisch | Alle |
| Französisch | Französisch - Numerisch | Alle |
| Französisch | Französisch (Kanada) - CSA | 11, 12 |
| Französisch | Kanadisch - CSA | 13 |
| Französisch | Französisch (Schweiz) | Alle |
| Französisch | Französisch - PC | Alle |
| Deutsch | Deutsch | Alle |
| Deutsch | Deutsch (Österreich) | Alle |
| Deutsch | Deutsch (Schweiz) | Alle |
| Spanisch | Spanisch | Alle |
| Spanisch | Spanisch - ISO | 10, 11 |
| Spanisch | Spanisch — Legacy | 12, 13 |
| Spanisch | Spanisch (Mexiko) | Alle |
| Schwedisch | Schwedisch | Alle |
| Schwedisch | Schwedisch - Legacy | 12, 13 |

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|-----------------------------------|-----------------------|
| Schwedisch | Schwedisch - Pro | 10, 11 |
| Tschechisch | Tschechisch | Alle |
| Dänisch | Dänisch | Alle |
| Finnisch | Finnisch | Alle |
| Ungarisch | Ungarisch | Alle |
| Italienisch | Italienisch | Alle |
| Italienisch | Italienisch - Schreibmaschine | 10, 11 |
| Italienisch | Italienisch - QZERTY | 12, 13 |
| Griechisch | Griechisch | Alle |
| Niederländisch | Belgisch | Alle |
| Niederländisch | Niederländisch | Alle |
| Russisch | Russisch | Alle |
| Russisch | Russisch - PC | Alle |
| Kroatisch | Kroatisch - PC | Alle |
| Slowakisch | Slowakisch | Alle |
| Slowakisch | Slowakisch - QWERTY | Alle |
| Türkisch | Türkisch F | Alle |
| Türkisch | Türkisch Q | Alle |
| Portugiesisch | Brasilianisch | Alle |
| Portugiesisch | Brasilianisch - ABNT2 | Alle |
| Portugiesisch | Brasilianisch - Legacy | 12, 13 |
| Portugiesisch | Brasilianisch - Pro | 10, 11 |
| Portugiesisch | Portugiesisch | Alle |
| Ukrainisch | Ukrainisch - PC | 10, 11 |
| Ukrainisch | Ukrainisch | 12, 13 |
| Belarussisch | Belarussisch | Alle |
| Slowenisch | Slowenisch | Alle |
| Estnisch | Estnisch | Alle |

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|--|-----------------------|
| Lettisch | Lettisch | Alle |
| Polnisch | Polnisch - Pro | 10, 11 |
| Polnisch | Polnisch | 12, 13 |
| Isländisch | Isländisch | Alle |
| Norwegisch | Norwegisch | Alle |
| Japanisch | Katakana | Alle |
| Japanisch | Katakana - halbe Breite | Alle |
| Japanisch | Romaji | Alle |
| Japanisch | Romaji - volle Breite | Alle |
| Japanisch | Hiragana | Alle |
| Japanisch | Alphanumerisch (Google) | Alle |
| Japanisch | Hiragana (Google) | Alle |
| Japanisch | Katakana (Google) | Alle |
| Japanisch | Katakana - halbe Breite (Google) | Alle |
| Japanisch | Alphanumerisch - volle Breite (Google) | Alle |
| Koreanisch | Koreanisch - 2-Set | Alle |
| Chinesisch - vereinfacht | Pinyin - vereinfacht | Alle |
| Chinesisch - vereinfacht | Sogou Pinyin | Alle |
| Chinesisch - traditionell | Pinyin - traditionell | Alle |
| Chinesisch - traditionell | Cangjie - traditionell | Alle |
| Chinesisch - traditionell | Zhuyin - traditionell | Alle |
| Chinesisch - traditionell | Sucheng - traditionell | Alle |

Tastaturlayoutunterstützung für Linux VDA, Französisch - Schweiz

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|--|-----------------------|
| Englisch | ABC | Alle |
| Englisch | ABC - Indien | Alle |
| Englisch | U.S. | Alle |
| Englisch | U.S. International - PC | Alle |
| Englisch | Dvorak | Alle |
| Englisch | Dvorak - Linkshänder | Alle |
| Englisch | Dvorak - Rechtshänder | Alle |
| Englisch | Englisch (Großbritannien u. Nordirland) | Alle |
| Englisch | Englisch (Großbritannien u. Nordirland) - PC | Alle |
| Englisch | Englisch (Kanada) | Alle |
| Englisch | Englisch (Australien) | Alle |
| Englisch | Irish | Alle |
| Französisch | Französisch | Alle |
| Französisch | Französisch - Numerisch | Alle |
| Französisch | Französisch (Kanada) - CSA | 11, 12 |
| Französisch | Kanadisch - CSA | 13 |
| Französisch | Französisch (Schweiz) | Alle |
| Französisch | Französisch - PC | Alle |
| Deutsch | Deutsch | Alle |
| Deutsch | Deutsch (Österreich) | Alle |
| Deutsch | Deutsch (Schweiz) | Alle |
| Spanisch | Spanisch | Alle |
| Spanisch | Spanisch - ISO | 10, 11 |
| Spanisch | Spanisch — Legacy | 12, 13 |
| Spanisch | Spanisch (Mexiko) | Alle |
| Bulgarisch | Bulgarisch | 10, 11, 12 |
| Bulgarisch | Bulgarisch - Standard | 13 |

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|-----------------------------------|-----------------------|
| Schwedisch | Schwedisch | Alle |
| Schwedisch | Schwedisch - Legacy | 12, 13 |
| Schwedisch | Schwedisch - Pro | 10, 11 |
| Tschechisch | Tschechisch | Alle |
| Dänisch | Dänisch | Alle |
| Finnisch | Finnisch | Alle |
| Ungarisch | Ungarisch | Alle |
| Italienisch | Italienisch | Alle |
| Italienisch | Italienisch - Schreibmaschine | 10, 11 |
| Italienisch | Italienisch - QZERTY | 12, 13 |
| Griechisch | Griechisch | Alle |
| Belgisch | Belgisch | Alle |
| Niederländisch | Niederländisch | Alle |
| Rumänisch | Rumänisch - Standard | Alle |
| Russisch | Russisch | Alle |
| Russisch | Russisch - PC | Alle |
| Kroatisch | Kroatisch - PC | Alle |
| Slowakisch | Slowakisch | Alle |
| Slowakisch | Slowakisch - QWERTY | Alle |
| Türkisch | Türkisch F | Alle |
| Türkisch | Türkisch Q | Alle |
| Portugiesisch | Brasilianisch | Alle |
| Portugiesisch | Brasilianisch - ABNT2 | Alle |
| Portugiesisch | Brasilianisch - Legacy | 12, 13 |
| Portugiesisch | Brasilianisch - Pro | 10, 11 |
| Portugiesisch | Portugiesisch | Alle |
| Ukrainisch | Ukrainisch - PC | 10, 11 |
| Ukrainisch | Ukrainisch | 12, 13 |

| Sprache auf dem Mac | Eingangsquelle auf dem Mac | Mac OS-Version |
|----------------------------|--|-----------------------|
| Belarussisch | Belarussisch | Alle |
| Slowenisch | Slowenisch | Alle |
| Estnisch | Estnisch | Alle |
| Polnisch | Polnisch - Pro | 10, 11 |
| Polnisch | Polnisch | 12, 13 |
| Isländisch | Isländisch | Alle |
| Norwegisch | Norwegisch | Alle |
| Japanisch | Katakana | Alle |
| Japanisch | Katakana - halbe Breite | Alle |
| Japanisch | Romaji | Alle |
| Japanisch | Romaji - volle Breite | Alle |
| Japanisch | Hiragana | Alle |
| Japanisch | Alphanumerisch (Google) | Alle |
| Japanisch | Hiragana (Google) | Alle |
| Japanisch | Katakana (Google) | Alle |
| Japanisch | Katakana - halbe Breite (Google) | Alle |
| Japanisch | Alphanumerisch - volle Breite (Google) | Alle |
| Koreanisch | Koreanisch - 2-Set | Alle |
| Chinesisch - vereinfacht | Pinyin - vereinfacht | Alle |
| Chinesisch - vereinfacht | Sogou Pinyin | Alle |
| Chinesisch - traditionell | Pinyin - traditionell | Alle |
| Chinesisch - traditionell | Cangjie - traditionell | Alle |
| Chinesisch - traditionell | Zhuyin - traditionell | Alle |
| Chinesisch - traditionell | Sucheng - traditionell | Alle |

Standardmäßig ist das Feature für die Tastaturlayoutsynchronisierung aktiviert. Um nur dieses Feature zu steuern, öffnen Sie die Datei **Config** im Ordner **~/Library/Application Support/Citrix Receiver/**, suchen Sie die Einstellung **EnableIMEEnhancement** und aktivieren oder deaktivieren Sie das

Feature, indem Sie den Wert auf “true” oder “false” festlegen.

Hinweis:

Die Einstellungsänderung wird nach einem Neustart der Sitzung wirksam.

Verbesserungen des Tastatureingabemodus

Die Citrix Workspace-App für Mac bietet Optionen zum Konfigurieren des Tastatureingabemodus.

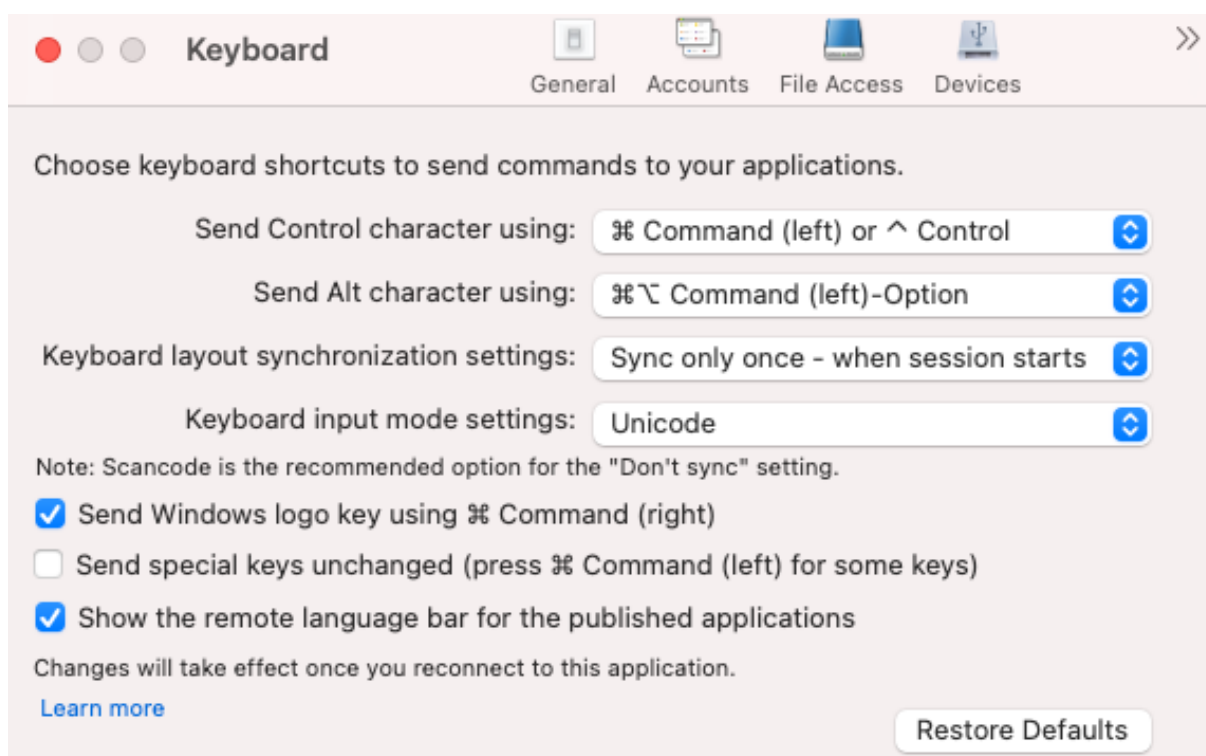
Gehen Sie wie folgt vor, um den Tastatureingabemodus über die GUI zu konfigurieren:

1. Klicken Sie über das Citrix Workspace-App-Symbol in der Menüleiste auf das Kontosymbol oben rechts und gehen Sie zu **Einstellungen > Tastatur**.

Die Einstellungen für den Tastatureingabemodus werden angezeigt.

2. Wählen Sie eine der folgenden Optionen:
 - **Scancode:** Sendet die Tastenposition von der clientseitigen Tastatur an den VDA, welcher das entsprechende Zeichen generiert. Wendet serverseitiges Tastaturlayout an
 - **Unicode:** Sendet die Taste von der clientseitigen Tastatur an den VDA, welcher das gleiche Zeichen auf dem VDA generiert. Wendet clientseitiges Tastaturlayout an.

Diese Erweiterung ist standardmäßig aktiviert.



Angenommen, Sie verwenden das Tastaturlayout USA international und der VDA das russische Tastaturlayout. Wenn Sie **Scancode** auswählen und die Taste neben der **Feststelltaste** drücken, wird der

Scancode "1E" an den VDA gesendet. Der VDA verwendet dann "1E", um das Zeichen "ϕ" anzuzeigen. Wenn Sie **Unicode** wählen und die Taste neben **Feststelltaste** drücken, wird das Zeichen "а" an den VDA gesendet. Obwohl der VDA das russische Tastaturlayout verwendet, erscheint das Zeichen "а" auf dem Bildschirm.

Citrix empfiehlt den folgenden Tastatureingabemodus für die verschiedenen Tastaturlayoutsynchronisierungsoptionen:

- Scancodemodus für die Option **Nicht synchronisieren**.
- Modus "Unicode" für **Dynamische Synchronisierung zulassen** und **Nur einmal beim Sitzungsstart synchronisieren**

Hinweis:

Änderungen an der Tastaturkonfiguration werden wirksam, sobald Sie die Verbindung zur Anwendung wieder herstellen.

Sie können die Konfiguration des Tastatureingabemodus in der Citrix Workspace-App ändern. Um eine optimale Leistung zu erzielen, sollten Sie die von Citrix empfohlenen Modi die für verschiedene Szenarien, physische Tastaturen und Clientgeräte verwenden.

Sprachenleiste

Sie können die Anzeige der Remotesprachenleiste in Anwendungssitzungen über die grafische Benutzeroberfläche ein- und ausblenden. Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt. In früheren Releases konnten Sie diese Einstellung nur über Registrierungsschlüssel auf dem VDA ändern. Ab der Citrix Workspace-App für Mac Version 1808 können Sie die Einstellungen im Dialogfeld **Einstellungen** ändern. 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.

Anzeigen/Ausblenden der Remotesprachenleiste

1. Öffnen Sie "Einstellungen".
2. Klicken Sie auf "Tastatur".
3. Aktivieren oder deaktivieren Sie "Remotesprachenleiste für die veröffentlichten Anwendungen anzeigen".

Hinweis:

Die Änderungen werden sofort wirksam. Sie können die Einstellungen in einer aktiven Sitzung ändern. Die Remotesprachenleiste wird in Sitzungen mit nur einer Eingabesprache nicht angezeigt.

Citrix Casting

Mit Citrix Casting können Sie Ihren Mac-Bildschirm an Citrix Ready Workspace Hub-Geräte in der Nähe übertragen. Die Citrix Workspace-App für Mac unterstützt das Spiegeln Ihres Mac-Bildschirms per Citrix Casting auf Monitoren, die mit einem Workspace Hub verbunden sind.

Weitere Informationen finden Sie in der Dokumentation zu [Citrix Ready Workspace Hub](#).

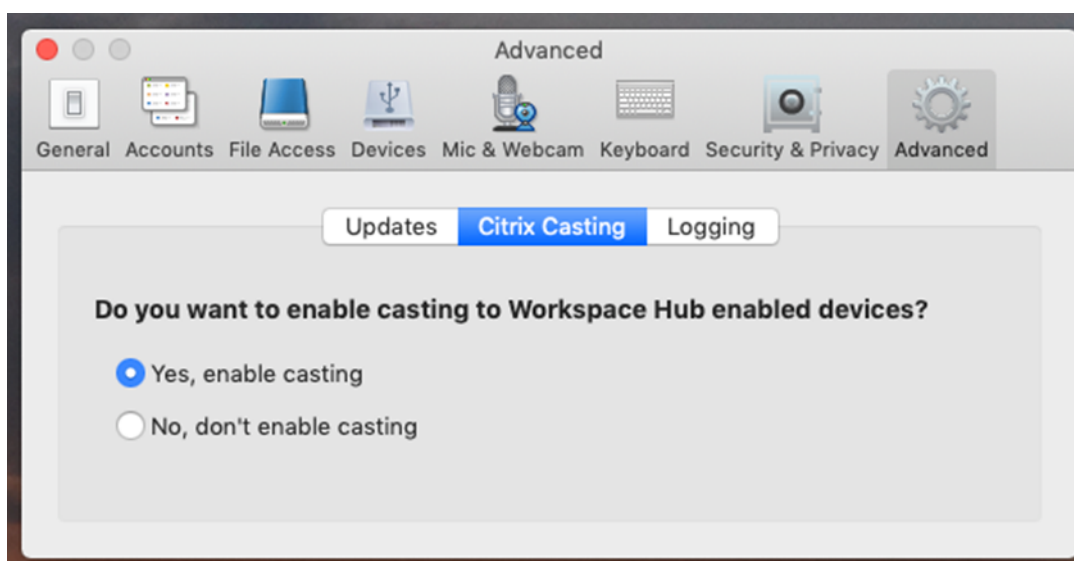
Voraussetzungen

- Aktuelle unterstützte Version der Citrix Workspace-App.
- Bluetooth ist zur Hub-Erkennung auf dem Gerät aktiviert.
- Citrix Ready Workspace Hub und Citrix Workspace-App müssen sich im selben Netzwerk befinden.
- Stellen Sie sicher, dass Port 55555 zwischen dem Gerät mit ausgeführter Citrix Workspace-App und dem Citrix Ready Workspace Hub nicht blockiert ist.
- 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.
- Stellen Sie für Citrix Casting sicher, dass Port 1494 nicht blockiert ist.

Citrix Casting aktivieren

Citrix Casting ist standardmäßig deaktiviert. Aktivieren von Citrix Casting mit der Citrix Workspace-App für Mac:

1. Gehen Sie zu **Einstellungen**.
2. Wählen Sie **Erweitert** und anschließend **Citrix Casting**.
3. Wählen Sie **Ja, Casting aktivieren**.



Beim Start von Citrix Casting wird eine Benachrichtigung angezeigt und in der Menüleiste erscheint ein Citrix Casting-Symbol.

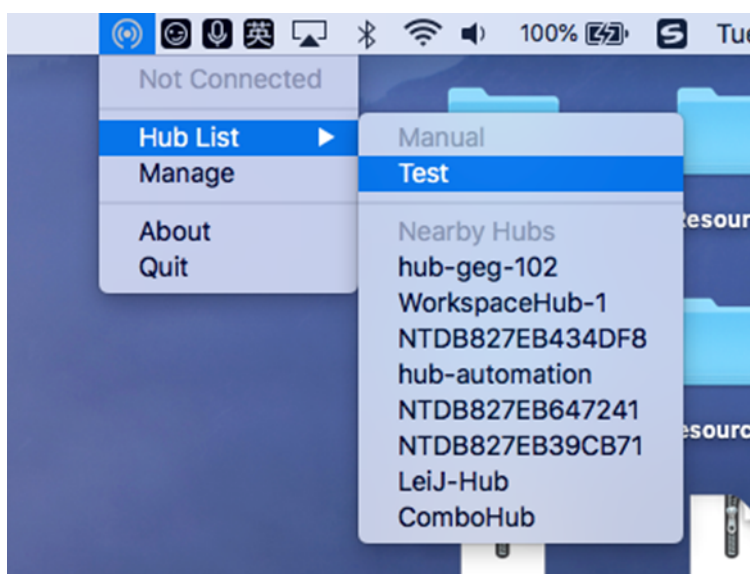
Hinweis:

Nach dem Aktivieren wird Citrix Casting stets automatisch mit der Citrix Workspace-App für Mac gestartet. Sie können das Feature jedoch unter **Einstellungen > Erweitert > Citrix Casting** mit **Nein, Casting nicht aktivieren** wieder deaktivieren.

Automatisches Ermitteln von Workspace-Hub-Geräten

Automatisches Verbinden mit Workspace Hubs:

1. Melden Sie sich auf Ihrem Mac bei der Citrix Workspace-App an und stellen Sie sicher, dass Bluetooth eingeschaltet ist. Bluetooth wird verwendet, um nahegelegene Workspace Hubs zu erkennen.
2. Wählen Sie in der Menüleiste das Symbol für **Citrix Casting**. Alle Citrix Casting-Funktionen werden über dieses Menü verwendet.
3. Im Untermenü **Hub-Liste** werden alle in der Nähe befindlichen Workspace Hubs angezeigt, die sich im selben Netzwerk befinden. Hubs werden in absteigender Reihenfolge gemäß ihrer Nähe zum Mac und mit dem konfigurierten Workspace Hub-Namen aufgelistet. Alle automatisch ermittelten Hubs werden unter **Hubs in der Nähe** angezeigt.
4. Wählen Sie den Namen des Hubs aus, mit dem Sie sich verbinden möchten.



Um die Auswahl eines Workspace Hubs während der Verbindung abbrechen, wählen Sie **Abbrechen**. Sie können **Abbrechen** auch verwenden, wenn die Netzwerkverbindung schlecht ist und der Verbindungsaufbau ungewöhnlich lange dauert.

Hinweis:

Es kann vorkommen, dass der gewünschte Hub nicht im Menü angezeigt wird. Prüfen Sie das Menü **Hub-Liste** nach einem Moment erneut oder fügen Sie den Hub manuell hinzu. Die Workspace Hub-Daten werden periodisch an Citrix Casting übertragen.

Manuelles Ermitteln von Workspace-Hub-Geräten

Wenn Sie das Citrix Ready Workspace Hub-Gerät im Menü **Hub-Liste** nicht finden können, fügen Sie die IP-Adresse des Workspace-Hubs hinzu, um manuell darauf zuzugreifen. Workspace Hub hinzufügen:

1. Melden Sie sich auf Ihrem Mac bei der Citrix Workspace-App an und stellen Sie sicher, dass Bluetooth eingeschaltet ist. Bluetooth wird verwendet, um nahegelegene Workspace Hubs zu erkennen.
2. Wählen Sie in der Menüleiste das Symbol für **Citrix Casting**.
3. Wählen Sie die Menüoption **Verwalten**. Das Fenster **Hubs verwalten** wird angezeigt.
4. Klicken Sie auf **Hinzufügen**, um die IP-Adresse Ihres Hubs einzugeben.
5. Nachdem das Gerät hinzugefügt wurde, wird in der Spalte **Hubname** der Anzeigename des Hubs angezeigt. Verwenden Sie diesen Namen, um den Hub im Bereich **Manuell** des Untermenüs **Hubliste** zu identifizieren.

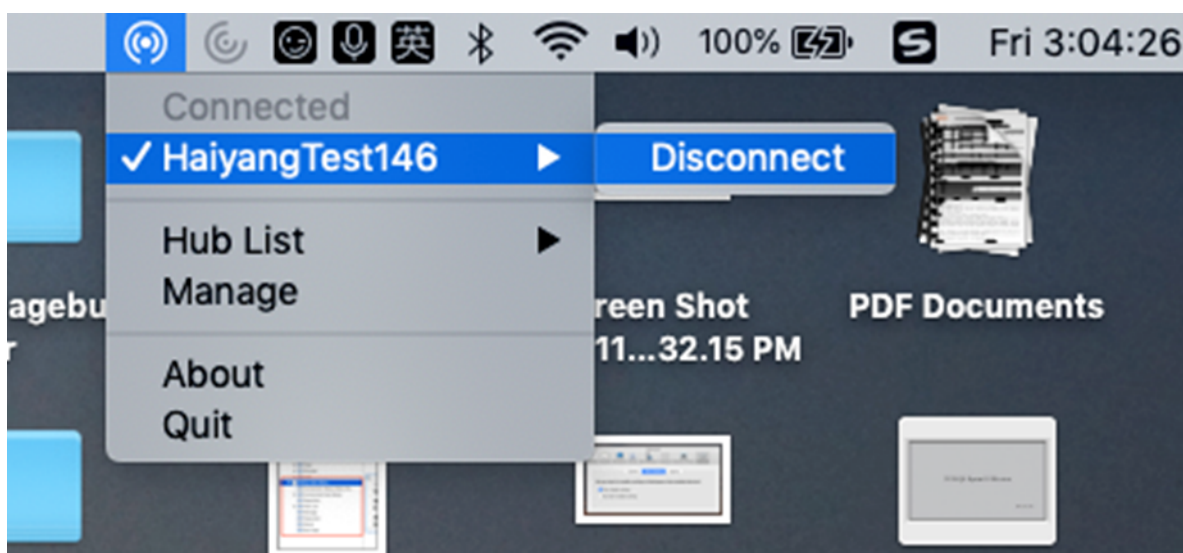
Hinweis:

Derzeit wird nur der Modus **Spiegeln** unterstützt. **Spiegeln** ist die einzige verfügbare Option in der Spalte **Anzeigemodus**.

Trennen des Workspace Hub-Geräts

Sie können die aktuelle Sitzung trennen und den Citrix Ready Workspace Hub automatisch oder manuell beenden.

- Schließen Sie den Laptop, um die Bildschirmcasting-Sitzung automatisch zu trennen.
- Bildschirmcasting-Sitzung manuell trennen:
 1. Wählen Sie das Symbol für **Citrix Casting**.
 2. Wählen Sie in der Liste der Hubs den Namen Ihres Workspace Hubs aus. Auf der rechten Seite wird die Option **Trennen** angezeigt.
 3. Wählen Sie **Trennen**, um den Hub zu beenden.



Bekannte Probleme

- Es gibt geringe Latenzprobleme beim Anzeigen des gespiegelten Bildschirms. Schlechte Netzwerkbedingungen können die Latenz noch verstärken.
- Wenn SSL in einem Citrix Ready Workspace Hub aktiviert ist und das Zertifikat des Hubs nicht vertrauenswürdig ist, wird eine Warnmeldung angezeigt. Um das Problem zu beheben, fügen Sie das Zertifikat mit dem Schlüsselbundtool zur Liste der vertrauenswürdigen Zertifikate hinzu.

Clientseitige Mikrofoneingabe

Die Citrix Workspace-App für Mac unterstützt die mehrfache clientseitige Mikrofoneingabe. Lokal installierte Mikrofone können für Folgendes verwendet werden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Die Citrix Workspace-App für Mac bietet Unterstützung für digitale Diktate.

Sie können Mikrofone, die an das Gerät angeschlossen sind, verwenden. Wählen Sie hierfür eine der folgenden Optionen in den Einstellungen für **Mikrofon und Webcam** unter **Citrix Workspace-App für Mac > Einstellungen** aus:

- Mikrofon und Webcam verwenden
- Mikrofon und Webcam nicht verwenden
- Jedes Mal fragen

Wenn Sie **Immer fragen** auswählen, müssen Sie jedes Mal beim Herstellen einer Verbindung in einem Dialogfeld bestätigen, dass Sie das Mikrofon in dieser Sitzung verwenden möchten.

Windows-Sondertasten

Die Citrix Workspace-App für Mac stellt diverse Optionen und vereinfachte Methoden für den Ersatz von Sondertasten bereit, u. a. Ersatz von Funktionstasten in Windows-Anwendungen durch Mac-Tasten. Auf der Registerkarte **Tastatur** konfigurieren Sie die gewünschten Optionen wie folgt:

- Mit **Control-Zeichen senden mit** können Sie auswählen, ob Sie die Befehl-Zeichentaste-Tastenkombinationen als Ctrl+-Zeichentaste-Tastenkombinationen in einer Sitzung senden. Wenn Sie "Befehl oder Control" im Kontextmenü auswählen, können Sie bekannte Befehl-Zeichentaste- oder Ctrl-Zeichentaste-Tastenkombinationen auf dem Mac als Strg+Zeichentaste-Tastenkombinationen an den PC senden. Wenn Sie Befehl auswählen, müssen Sie Ctrl+Zeichentastekombinationen verwenden.
- Mit **Alt-Zeichen senden mit** können Sie auswählen, wie die Alt-Taste in einer Sitzung repliziert wird. Wenn Sie die Befehl-Option auswählen, können Sie Befehl-Option-Tastenkombinationen als Alt-Tastenkombinationen in einer Sitzung senden. Sie können auch Befehl auswählen und die Befehl-Taste als Alt-Taste verwenden.
- Mit **Windows-Logo-Taste mit Befehl (rechts) senden** können Sie die Windows-Logo-Taste durch Druck der Befehl-Taste an der rechten Seite der Tastatur an Remotedesktops und -anwendungen senden. Wenn diese Option deaktiviert ist, hat die rechte Befehl-Taste dieselbe Funktion wie die linke Befehl-Taste gemäß den zwei obigen Einstellungen im Dialogfeld "Einstellungen". Sie können die Windows-Logo-Taste jedoch mit dem Menü "Tastatur" senden. Wählen Sie **Tastatur > Windows-Tastenkombination senden > Start**.

- Mit **Sondertasten unverändert senden** deaktivieren Sie die Konvertierung von Sondertasten. Beispiel: Die Kombination Option-1 (auf der Zehnertastatur) entspricht der Sondertaste F1. Sie können dieses Verhalten ändern und diese Sondertaste so einstellen, dass sie 1 (die Zahl 1 auf der Zehnertastatur) in der Sitzung darstellt. Damit die Sondertaste 1 darstellt, aktivieren Sie das Kontrollkästchen “Sondertasten unverändert senden”. Standardmäßig ist dieses Kontrollkästchen nicht aktiviert, daher wird Option-1 als F1 an die Sitzung gesendet.

Funktions- und andere Sondertasten werden mit dem Menü **Tastatur** an eine Sitzung gesendet.

Wenn die Tastatur eine Zehnertastatur enthält, können Sie die folgenden Tastaturanschläge verwenden:

| PC-Taste oder Aktion | Mac-Optionen |
|----------------------|--|
| Einfügen | 0 (die Zahl 0) auf der Zehnertastatur. Die Num-Taste muss deaktiviert sein. Sie können die Aktion mit der Clear -Taste ein- und ausschalten; Option-Hilfe |
| Löschen | Dezimalstelle auf der Zehnertastatur. Die Num-Taste muss deaktiviert sein. Sie können die Aktion mit der Clear -Taste ein- und ausschalten; Clear |
| F1 bis F9 | Option-1 bis 9 (die Zahlen 1 bis 9) auf der Zehnertastatur |
| F10 | Option-0 (die Zahl 0) auf der Zehnertastatur |
| F11 | Option-Minuszeichen auf der Zehnertastatur |
| F12 | Option-Pluszeichen auf der Zehnertastatur |

Windows-Tastenkombinationen

In Remotesitzungen werden die meisten Mac-Tastenkombinationen für die Texteingabe erkannt, z. B. Option-G für die Eingabe des Copyrightsymbols ©. Einige Tastaturanschläge in einer Sitzung werden jedoch nicht in der Remoteanwendung oder auf dem Remotedesktop angezeigt. Sie werden vom Mac-Betriebssystem interpretiert, was dazu führen kann, dass Tasten stattdessen Mac-Antworten auslösen.

Sie möchten vielleicht auch bestimmte Windows-Tasten verwenden, z. B. Einfügen, die auf vielen Mac-Tastaturen nicht vorhanden ist. Genauso zeigen einige Windows 8-Tastenkombinationen Charms und App-Befehle an und docken Apps an und wechseln sie. Mac-Tastaturen imitieren diese Tastenkombinationen nicht. Die Tastenkombinationen können jedoch über das Menü **Tastatur** an den Remot-

edesktop oder die Remoteanwendung gesendet werden.

Tastaturen und die Konfiguration der Tasten können sich stark zwischen Computern unterscheiden. Die Citrix Workspace-App für Mac bietet daher mehrere Auswahlen an, um sicherzustellen, dass Tastaturanschläge richtig an gehostete Anwendungen und Desktops weitergeleitet werden. Diese Tastaturanschläge sind in der Tabelle aufgeführt. Das Standardverhalten wird beschrieben. Wenn Sie die Standardwerte angepasst haben (mit der Citrix Workspace-App oder anderen Einstellungen), werden möglicherweise andere Kombinationen von Tastaturanschlägen weitergeleitet, und der Remote-PC-Zugriff weist ein anderes Verhalten auf.

Wichtig

Bestimmte Tastenkombinationen, die in der Tabelle aufgelistet sind, sind nicht auf neueren Mac-Tastaturen verfügbar. In den meisten Fällen kann die Tastatureingabe mit dem Menü Tastatur zur Sitzung gesendet werden.

In der Tabelle verwendete Konventionen:

- Buchstabentasten sind großgeschrieben; dies gibt nicht an, dass die Umschalt-Taste gleichzeitig gedrückt werden soll.
- Bindestriche zwischen Tastaturanschlägen geben an, dass Tasten gleichzeitig gedrückt werden müssen (z. B. Strg-C).
- Mit Zeichentasten werden Texteingaben erzeugt. Dazu gehören alle Buchstaben, Zahlen und Satzzeichen. Sondertasten erzeugen keine Eingabe, sondern dienen als Modifikator oder Steuertaste. Zu den Sondertasten gehören die Control-, Alt-, Umschalt-, Befehl- und Option-Taste sowie die Pfeiltasten und Funktionstasten.
- Menüanweisungen beziehen sich auf die Menüs in der Sitzung.
- Abhängig von der Konfiguration des Benutzergeräts funktionieren einige Tastenkombinationen nicht erwartungsgemäß und alternative Kombinationen sind aufgeführt.
- “Fn” bezieht sich auf die Fn-Taste (Funktion) der Mac-Tastatur. Die Funktionstaste bezieht sich auf die Tasten F1 bis F12 auf der PC- oder Mac-Tastatur.

| Windows-Taste oder Tastenkombination | Mac-Äquivalent |
|--------------------------------------|---|
| Alt+Zeichentaste | Cmd-Option-Zeichen (z. B. zum Senden von Alt-C verwenden Sie Cmd-Option-C) |
| Alt+Sondertaste | Option-Sondertaste (z. B. Option-Tab); Cmd-Option-Sondertaste (z. B. Cmd-Option-Tab) |
| Strg+Zeichentaste | Cmd-Zeichentaste (z. B. Cmd-C); Ctrl-Zeichentaste (z. B. Ctrl-C) |
| Strg+Sondertaste | Ctrl-Sondertaste (z. B. Ctrl-F4); Cmd-Zeichentaste (z. B. Cmd-F4) |

| Windows-Taste oder Tastenkombination | Mac-Äquivalent |
|---|--|
| Strg/Alt/Umschalt/Windows-Logo + Funktionstaste | Wählen Sie Tastatur > Funktionstaste senden > Ctrl/Alt/Umschalt/Cmd-Funktionstaste. |
| Strg+Alt | Ctrl-Option-Cmd |
| Strg+Alt+Entf | Strg-Option-Fn-Cmd-Löschen; Wählen Sie Tastatur > Strg+Alt+Entf senden. |
| Löschen | Delete; Wählen Sie Tastatur > Taste senden > Entfernen ; Fn-Rücktaste (Fn-Delete auf einigen US-Tastaturen) |
| Ende | Ende; Fn-Rechtspfeil |
| Esc | Esc; Wählen Sie Tastatur > Taste senden > Esc. |
| F1 bis F12 | F1 bis F12; Wählen Sie Tastatur > Funktionstaste senden > F1 bis F12. |
| Home | Pos1; Fn-Linkspfeil |
| Einfügen | Wählen Sie Tastatur > Taste senden > Einfügen. |
| Num | Löschen |
| Bild ab | Bild ab; Fn-Abwärtspfeil |
| Bild auf | Bild auf; Fn-Aufwärtspfeil |
| Leertaste | Wählen Sie Tastatur > Taste senden > Leertaste. |
| Tabulator | Wählen Sie Tastatur > Taste senden > Tabulator. |
| Windows-Logo | Rechte Cmd-Taste (Tastatureinstellung standardmäßig aktiviert); Wählen Sie Tastatur > Windows-Tastenkombination senden > Start. |
| Tastenkombinationen zum Anzeigen von Charms | Wählen Sie Tastatur > Windows-Tastenkombination senden > Charms. |
| Tastenkombinationen zum Anzeigen von App-Befehlen | Wählen Sie Tastatur > Windows-Tastenkombination senden > App-Befehle. |

| Windows-Taste oder Tastenkombination | Mac-Äquivalent |
|---|--|
| Tastenkombinationen zum Andocken von Apps | Wählen Sie Tastatur > Windows-Tastenkombination senden > Andocken. |
| Tastenkombinationen zum Wechseln von Apps | Wählen Sie Tastatur > Windows-Tastenkombination senden > Apps wechseln. |

Verwenden eines Eingabemethoden-Editors (IME) und internationaler Tastaturlayouts

Mit der Citrix Workspace-App für Mac können Sie einen Eingabemethoden-Editor (IME) auf dem Benutzergerät oder dem Server verwenden.

Wenn der clientseitige Eingabemethoden-Editor (IME) aktiviert ist, können Benutzer an der Einfügemarke statt in einem Fenster Text eingeben.

Mit der Citrix Workspace-App für Mac können Benutzer auch das gewünschte Tastaturlayout angeben.

Aktivieren des clientseitigen Eingabemethoden-Editors

1. Klicken Sie auf der Menüleiste Citrix Viewer auf **Tastatur > International > Client-IME verwenden.**
2. Stellen Sie sicher, dass der serverseitige IME auf direkte Eingabe oder den alphanumerischen Modus eingestellt ist.
3. Geben Sie mit dem Mac-IME Text ein.

Explizites Angeben des Anfangspunkts für die Texteingabe

- Klicken Sie auf der Menüleiste Citrix Viewer auf **Tastatur > International > Kompositionszichen verwenden.**

Verwenden des serverseitigen Eingabemethoden-Editors

- Stellen Sie sicher, dass der clientseitige IME auf den alphanumerischen Modus eingestellt ist.

Zugeordnete serverseitige IME-Eingabemodustasten

Die Citrix Workspace-App für Mac stellt Tastaturzuordnungen für serverseitige Windows-IME-Eingabemodustasten bereit, die nicht auf Mac-Tastaturen verfügbar sind. Auf Mac-Tastaturen ist die

Optionstaste den folgenden serverseitigen IME-Eingabemodustasten zugeordnet, abhängig vom serverseitigen Gebietsschema:

| Serverseitiges Systemgebietsschema | Serverseitige IME-Eingabemodustaste |
|------------------------------------|--|
| Japanisch | Kanji-Taste (Alt + Hankaku/Zenkaku auf der japanischen Tastatur) |
| Koreanisch | Rechte Alt-Taste (Umschalten Hanguk/English auf der koreanischen Tastatur) |

Verwenden internationaler Tastaturlayouts

- Stellen Sie sicher, dass die Tastaturlayouts auf der Client- und Serverseite auf dasselbe Gebietsschema wie die Standardeingabesprache auf der Serverseite eingestellt sind.

Mehrere Monitore

Benutzer können die Citrix Workspace-App für Mac im Vollbildmodus über mehrere Monitore hinweg ausführen.

1. Öffnen Sie den Citrix Viewer.
2. Klicken Sie in der Menüleiste auf **Ansicht** und wählen Sie je nach Anforderung eine der folgenden Optionen aus:
 - **Zu Vollbild wechseln** - Vollbild nur auf dem Hauptmonitor.
 - **Alle Displays in Vollbild verwenden** - Vollbild auf allen angeschlossenen Monitoren.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die Monitore.

Der Bildschirm ist nun auf alle Monitore erweitert.

Einschränkungen

- Der Vollbildmodus wird nur auf einem Monitor oder auf allen Monitoren unterstützt. Diese Funktion kann über ein Menüelement festgelegt werden.
- Citrix empfiehlt die Verwendung von maximal 2 Monitoren. Die Verwendung von mehr als 2 Monitoren kann die Sitzungsleistung beeinträchtigen oder Probleme mit der Benutzerfreundlichkeit verursachen.
- Der Vollbildmodus ist auf Macs mit Einkerbung (Notch) nicht verfügbar.

Desktop-Symbolleiste

Benutzer können jetzt im Fenstermodus und im Vollbildmodus auf die **Desktopsymbolleiste** zugreifen. Zuvor konnte die Symbolleiste nur im Vollbildmodus angezeigt werden. Darüber hinaus wurden folgende Änderungen an der Symbolleiste vorgenommen:


- Die Schaltfläche **Home** wurde von der Symbolleiste entfernt. Diese Funktion kann mit den folgenden Befehlen ausgeführt werden:
 - **Cmd-Tab**: Wechseln zur vorherigen aktiven Anwendung.
 - **Ctrl-Left Arrow**: Wechseln zum vorherigen Bereich.
 - Sie können mit dem integrierten Trackpad oder den Magic Mouse-Gesten zu einem anderen Bereich wechseln.
 - Wenn Sie den Cursor im Vollbildmodus an den Rand des Bildschirms bewegen, wird ein Dock angezeigt, in dem Sie Anwendungen aktivieren können.
- Die Schaltfläche für den **Fenstermodus** wurde von der Symbolleiste entfernt. Wenden Sie eine dieser Methoden an, um vom Vollbildmodus in den Fenstermodus zu wechseln:
 - In OS X 10.10 klicken Sie in der Dropdown-Menüleiste auf die grüne Fensterschaltfläche.
 - In OS X 10.9 klicken Sie in der Dropdown-Menüleiste auf die blaue Menüschtfläche.
 - In allen Versionen von OS X können Sie in der Dropdown-Menüleiste im Menü **Ansicht** die Option **Vollbildmodus beenden** auswählen.
- Unterstützung für das Ziehen zwischen Fenstern im Vollbildmodus mit mehreren Monitoren.

Workspace Control

Mit Workspace Control folgen Desktops und Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Arbeitsstation zu einer anderen gehen, ohne ihre Desktops und Anwendungen auf jedem einzelnen Gerät neu starten zu müssen.

Die Richtlinien und die Clientlaufwerkzuordnung ändern sich entsprechend, wenn Benutzer zu einem anderen Benutzergerät wechseln. Die angewendeten Richtlinien und Zuordnungen hängen vom Benutzergerät ab, an dem Sie momentan an einer Sitzung angemeldet sind. Beispielsweise kann sich ein Mitarbeiter im Gesundheitswesen von einem Gerät in der Notaufnahme abmelden und sich bei einer Arbeitsstation im Röntgenlabor anmelden. Die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen, die für die Sitzung im Röntgenlabor geeignet sind, werden für die Sitzung im Röntgenlabor wirksam.

Konfigurieren der Workspace Control-Einstellungen

1. Klicken Sie im Fenster der Citrix Workspace-App für Mac auf den Abwärtspfeil  und wählen Sie **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Allgemein**.
3. Wählen Sie eine der folgenden Optionen:

- Beim Anmelden an Citrix Workspace Anwendungen wiederverbinden. Benutzer können eine Verbindung mit getrennten Anwendungen wiederherstellen, wenn sie Citrix Workspace starten.
- Verbindungen zu Anwendungen wiederherstellen, wenn ich Anwendungen starte oder aktualisiere. Benutzer können eine Verbindung mit getrennten Apps wiederherstellen, wenn sie die Apps starten oder im Menü der Citrix Workspace-App für Mac "Apps aktualisieren" auswählen.


Zuordnen von Clientlaufwerken

Mit der Clientlaufwerkzuordnung greifen Sie auf lokale Laufwerke auf dem Benutzergerät in Sitzungen zu, z. B. CD-Laufwerke, DVDs und USB-Sticks. Wenn eine Serverkonfiguration die Clientlaufwerkzuordnung zulässt, können Benutzer auf lokal gespeicherte Dateien zugreifen und diese in Sitzungen bearbeiten. Benutzer können sie auch speichern, entweder auf einem lokalen Laufwerk oder auf einem Laufwerk auf dem Server.

Die Citrix Workspace-App für Mac überwacht die Verzeichnisse, in denen Hardwaregeräte wie CDs, DVDs und Memory Sticks (USB) normalerweise auf dem Benutzergerät bereitgestellt werden, und ordnet neue Hardwaregeräte in der Sitzung automatisch dem nächsten verfügbaren Laufwerksbuchstaben auf dem Server zu.

Sie können den Lese- und Schreibzugriff für zugeordnete Laufwerke in den Citrix Workspace-App für Mac-Einstellungen konfigurieren.

Konfigurieren des Lese- und Schreibzugriffs für zugeordnete Laufwerke

1. Klicken Sie auf der Homepage der Citrix Workspace-App für Mac auf den Abwärtspfeil  und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf **Dateizugriff**.
3. Wählen Sie das Niveau für den Lese- und Schreibzugriff für zugeordnete Laufwerke unter den folgenden Optionen aus:
 - Lesen und Schreiben
 - Lesezugriff
 - Kein Zugriff
 - Jedes Mal fragen
4. Melden Sie sich von offenen Sitzungen ab und erneut an, um die Änderungen anzuwenden.

Benutzerdefinierter Webstore

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

nutzerdefinierten Webstore der Liste der zulässigen URLs in der Eigenschaft `allowedWebStoreURLs` im Global App Configuration Service hinzufügen.

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

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Webstore-URL hinzuzufügen:

1. Öffnen Sie die Citrix Workspace-App und navigieren Sie zu **Konten**.
2. Klicken Sie im Fenster **Konten** auf das Symbol **+** und geben Sie die URL ein.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Webstore-URL zu löschen:

1. Öffnen Sie die Citrix Workspace-App und navigieren Sie zu **Konten**.
2. Wählen Sie im Fenster **Konten** das Konto aus, das Sie löschen möchten, und klicken Sie auf das Symbol **-**.

Inaktivitätstimeout für die Citrix Workspace-App

Die Inaktivitätstimeout-Funktion meldet Sie basierend auf einem vom Administrator festgelegten Wert von der Citrix Workspace-App ab. Administratoren können die zulässige Leerlaufzeit angeben, bevor ein Benutzer automatisch von der Citrix Workspace-App abgemeldet wird. Sie werden automatisch abgemeldet, wenn innerhalb des angegebenen Zeitintervalls im Fenster der Citrix Workspace-App keine Aktivität über Maus, Tastatur oder Berührung erfolgt. Das Inaktivitätstimeout hat keine Auswirkungen auf die bereits ausgeführten Citrix Virtual Apps and Desktops- und Citrix DaaS-Sitzungen oder die 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 angezeigt. Sie können angemeldet bleiben oder sich abmelden. Die Benachrichtigung wird angezeigt, wenn Sie Benachrichtigungen der Citrix Workspace-App in den Systemeinstellungen Ihres Mac aktiviert haben.
- Die Benachrichtigung wird nur angezeigt, wenn der konfigurierte Wert für das Inaktivitätstimeout größer als fünf Minuten ist. Wenn der konfigurierte Wert beispielsweise 6 Minuten beträgt, wird eine Benachrichtigung angezeigt, wenn 3 Minuten Inaktivität erkannt werden. Wenn der konfigurierte Wert für das Inaktivitätstimeout kleiner oder gleich 5 Minuten ist, wird der Benutzer ohne Benachrichtigung abgemeldet.
- 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.

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 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 Configuration 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 Configuration Service. Weitere Informationen zum Global App Configuration Service finden Sie unter [Global App Configuration Service](#).
2. Bearbeiten Sie die Nutzlast im App Config Service:

```
1 {
2   "serviceURL": Unknown macro: {
3     "url" }
4
5   ,
6   "settings":{
7
8     "name":"Productivity Apps", [New Store Name]
9     "description":"Provides access StoreFront to Workspace Migration",
10    "useForAppConfig":true,
11    "appSettings":
12    {
13      "macos":[ Unknown macro: {
```

```
14     "category" }
15
16   ]
17 }
18
19 }
20
21 }
22
23 <!--NeedCopy-->
```

Hinweis:

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

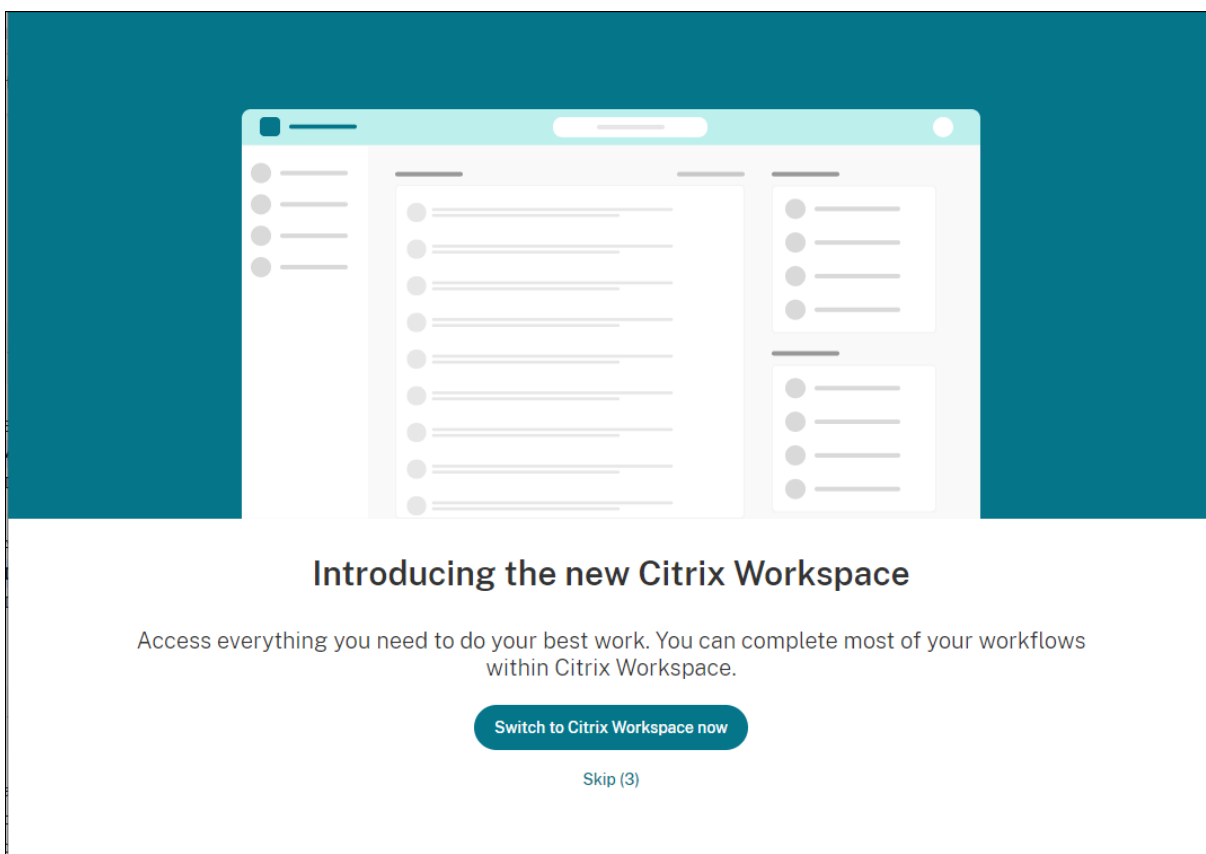
Wenn Sie eine Nutzlastkonfiguration bearbeiten, verwenden Sie **PUT** und stellen Sie sicher, dass Sie die Nutzlast aus allen unterstützten Einstellungen haben.

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.

Verbesserung für Microsoft Teams

Schnittstelle für bevorzugtes Netzwerk konfigurieren

Sie können jetzt eine bevorzugte Netzwerkschnittstelle für den Medienverkehr konfigurieren. Führen Sie den folgenden Befehl in einem Terminal aus:

```
defaults write com.citrix.HdxRtcEngine NetworkPreference -int <value>
```

Wählen Sie einen der folgenden Werte aus:

- 1: Ethernet
- 2: Wi-Fi
- 3: Cellular
- 4: VPN
- 5: Loopback
- 6: Any

Standardmäßig und wenn kein Wert festgelegt ist, wählt die WebRTC Media Engine die beste verfügbare Route aus.

Microsoft Teams

Geschätzte Codierungsleistung

`HdxRtcEngine.exe` ist die WebRTC Media Engine, die in die Citrix Workspace-App eingebettet ist und die Microsoft Teams-Umleitung verarbeitet. `HdxRtcEngine.exe` kann die beste Codierungsauflösung schätzen, die die CPU des Endpunkts ohne Überlastung aufrechterhalten kann. Mögliche Werte sind 240p, 360p, 480p, 720p und 1080p.

Die Schätzung der Leistung basiert auf Makroblockcode, um die beste Auflösung zu bestimmen, die beim jeweiligen Endpunkt erzielt werden kann. In die Codec-Aushandlung fließt die höchstmögliche Auflösung ein. Die Codec-Aushandlung kann zwischen Peers oder zwischen Peer und Konferenzserver stattfinden.

Es gibt vier Leistungskategorien für Endpunkte, jeweils mit eigener **maximal** verfügbarer Auflösung:

| Endpunktleistung | Maximale Auflösung | Registrierungsschlüsselwert |
|------------------|---|-----------------------------|
| Fast | 1080p (1920x1080 16:9 @ 30 F/s) | 3 |
| Medium | 720p (1280x720 16:9 @ 30 F/s) | 2 |
| Slow | 360p (640x360 16:9 bei 30 F/s oder 640x480 4:3 bei 30 F/s) | 1 |
| Sehr langsam | 240p (320x180 16:9 bei 30 F/s oder 320 x 240 4:3 bei 30 F/s) | 0 |

Um die Videocodierungsauflösung z. B. auf 360p festzulegen, führen Sie den folgenden Befehl im Terminal aus:

```
defaults write com.citrix.HdxRtcEngine OverridePerformance -int 1
```

Weitere Informationen zur Optimierung von Microsoft Teams finden Sie unter [Optimierung für Microsoft Teams](#).

Drucken

Sie können jetzt den universellen PDF-Druck verwenden, wenn Sie von einem MAC aus drucken. Beim automatischen Erstellen von Druckern mit dem universellen Druckertreiber brauchen Sie den Treiber

“HP Color LaserJet 2800 Series PS” nicht mehr zu installieren, wenn Sie den universellen PDF-Druck verwenden.

PostScript-Druck

Standardmäßig werden die automatisch umgeleiteten Clientdrucker mit dem Citrix UPD mit PostScript-Unterstützung erstellt.

Weitere Informationen finden Sie im Supportartikel [CTX296662](#).

Stellen Sie sicher, dass die Richtlinien “Clientdruckerumleitung”, “Verwendung universeller Druckertreiber” und die Prioritätsrichtlinien für den universellen Druckertreiber auf die Standardwerte festgelegt sind. Stellen Sie außerdem sicher, dass Sie den Druckertreiber der HP Color LaserJet 2800 PS-Serie auf dem VDA installiert haben.

Weitere Informationen zum Installieren des Treibers finden Sie im Supportartikel [CTX140208](#).

Universelles PDF-Drucken

Voraussetzungen:

- Citrix Workspace-App für Mac Version 2112 oder höher - Ermöglicht die Verwendung von PDF-Druckstreams für die Citrix Workspace-App für Mac.
- Citrix Virtual Apps and Desktops Version 2112 oder höher - Ermöglicht universelles PDF-Drucken für automatisch erstellte Clientdrucker.
- Aktivieren Sie die Richtlinie zur Clientdruckerumleitung in Citrix Studio oder in der Webkonsole.

| | | | |
|---|--|------|----------|
| ✓ | > Auto-create PDF Universal Printer User setting - ICA\Printing\Client Printers Enabled (Default: Disabled) | Edit | Unselect |
| ✓ | > Auto-create client printers User setting - ICA\Printing\Client Printers Auto-create all client printers (Default: Auto-create all client printers) | Edit | Unselect |
| ✓ | > Client printer redirection User setting - ICA\Printing Allowed (Default: Allowed) | Edit | Unselect |
| ✓ | > Universal driver preference **** User setting - ICA\Printing\Drivers EMF,XPS,PCL5c,PCL4,PDF,PS (Default: EMF;XPS;PCL5c;PCL4;PS) | Edit | Unselect |
| ✓ | > Universal print driver usage User setting - ICA\Printing\Drivers Use universal printing only if requested driver is unavailable (Default: Use u... | Edit | Unselect |

**** “PDF” needs to be added manually if absent from the Universal Driver Preference policy

Sie können per PDF drucken, nachdem Sie eine oder beide der folgenden Optionen konfiguriert haben:

1. Stellen Sie einen einzelnen PDF-Universaldrucker bereit, der in jeder Sitzung erstellt wird.
2. Verwenden Sie universellen Druckertreiber (UPD) für normale, automatisch erstellte Drucker.

Bereitstellen eines einzelnen universellen PDF-Druckers, der in jeder Sitzung erstellt wird

Um die Erstellung des **universellen PDF-Druckers** in Sitzungen von einem Mac-Client oder einem anderen PDF-fähigen Clientendpunkt aus zu ermöglichen, rufen Sie Citrix Studio oder die Webkonsole auf und aktivieren Sie die Richtlinie **Universellen PDF-Drucker automatisch erstellen**.

Wenn die Richtlinie aktiviert ist, wird der universelle PDF-Drucker in der Sitzung erstellt. Der Drucker heißt **Citrix PDF-Drucker**.

Durch die Verwendung dieses Druckers in einer Sitzung wird eine PDF-Ausgabe generiert, die an den Client geliefert und an die Anwendung auf dem Endpunkt übergeben wird, die PDFs standardmäßig handhabt. Für den macOS-Client ist diese PDF-Standardanwendung normalerweise die integrierte **Vorschauanwendung**. Es kann jedoch jede registrierte Anwendung für die Handhabung von PDFs sein, wie Adobe Acrobat Reader.

Verwenden des UPD für normale, automatisch erstellte Drucker

Um das universelle PDF-Drucken für alle umgeleiteten Clientdrucker in einer Sitzung von einem Mac-Client aus zu aktivieren, rufen Sie Citrix Studio oder eine Webkonsole auf und konfigurieren Sie die Prioritätsrichtlinie für den universellen Druckertreiber so, dass das Metadateiformat **PDF** vor **PS** in der Prioritätsliste steht.

Nachdem Sie diese Änderung vorgenommen haben, verwenden automatisch erstellte Drucker, die einen universellen Treiber mit einem PDF-fähigen Mac-Client verwenden, den universellen PDF-Treiber von Citrix statt des Treibers für HP Color LaserJet 2800 Series PS auf dem Host.

Wenn Sie einen der automatisch erstellten Drucker in einer Sitzung verwenden, wird PDF als Zwischenformat des Druckauftrags verwendet. Die Druckausgabe geht jedoch direkt an den ausgewählten, an den Client angeschlossenen Drucker.

Mobilgeräteverwaltung

December 18, 2023

Die Citrix Workspace-App unterstützt jetzt die Mobilgeräteverwaltung (MDM), mit der Administratoren die Citrix Workspace-App für Mac konfigurieren, sichern und unterstützen können, indem sie Richtlinien mit jedem MDM-Tool durchsetzen.

In MDM unterstützte Einstellungen

| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Unterstützte Version |
|--|--|----------------------|------------|-----------------|--------------|----------------------|
| Menüleiste ein-/ausblenden | Blendet das Citrix Workspace-Menü in der Menüleiste ein oder aus. | ShowHelperI | true/false | Boolescher Wert | True | 2208.1 |
| Automatischer Start der Citrix Workspace-App | Steuert, dass die Citrix Workspace-App für Mac automatisch gestartet wird, wenn ein Computer von einem Endbenutzer eingeschaltet wird. | AutoLaunchAppOnFirst | On/Off | Boolescher Wert | True | 2304 |

| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Unterstützte Version |
|--|---|--------------------|-------------|-----------------|-----------------|----------------------|
| Vorkonfigurieren der Store-URL | Ermöglicht Administratoren, die Storedetails vorzukonfigurieren und zur Workspace-App hinzuzufügen, sodass die Endbenutzer dies nicht tun müssen. | StoreURLs | <Store URL> | Zeichenfolge | Nicht verfügbar | 2210 |
| Hinzufügen eines neuen Stores durch den Endbenutzer blockieren | Verhindert, dass Endbenutzer auf ihren Endpunktggeräten einen Store in der Workspace-App hinzufügen. | BlockStoreAddition | true/false | Boolescher Wert | False | 2210 |

| | | | | | | Unterstützte |
|--|--|--------------|--------------|--------------|--------------|--------------|
| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Version |
| Automatische Updates - AutoUpdateState | Aktualisiert die Citrix Workspace-App automatisch auf die neueste Version, ohne dass Benutzer eingreifen müssen. | AutoUpdateS | Automatisch/ | Zeichenfolge | Automatisch | 2305 |
| Automatische Updates - AutoUpdateChannel | Hiermit können Administratoren sicherstellen, dass die Workspace-App GA-Updates oder Beta-Updates erhält, wenn automatische Updates aktiviert sind. | AutoUpdateCh | PROD/EAR | Zeichenfolge | PROD | 2201 |

| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Unterstützte Version |
|---|---|-----------|------------|-----------------|--------------|----------------------|
| Azure Active Directory aktivieren | Ermöglicht Administratoren das Konfigurieren und Erzwingen von Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer, die sich bei der Citrix Workspace-App authentifizieren. | enableAAD | true/false | Boolescher Wert | False | 2305 |

| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Unterstützte Version |
|---|---|--|---|---------|--------------|----------------------|
| Browser für FIDO2-Webauthentifizieren auswählen | Ermöglicht die Administration der Auswahl des Browser-typs für die Authentifizierung von Endbenutzern in der Citrix Workspace-App. Weitere Informationen zu den Werten finden Sie unter FIDO2-Authentifizierung beim Verbinden mit einem Cloudstore . | WebBrowserForSystem/SessionWithPrivateSession/EndUser/EndUserSession | System/SessionWithPrivateSession/EndUser/EndUserSession | String | Chrome | 2017.0.0.0 |

| Einstellung | Beschreibung | Schlüssel | Wert | Werttyp | Standardwert | Unterstützte Version |
|--|--|------------------------------|------------|-----------------|--------------|----------------------|
| FIDO2-Authentifizieren für HDX-Sitzungen aktivieren/deaktivieren | Ermöglicht Administratoren, die FIDO2-Authentifizieren in HDX-Sitzungen zu aktivieren oder zu deaktivieren. | Fido2Enable | true/false | Boolescher Wert | true | 2307 |
| Schnellzugriff für StoreFront | Ermöglicht Administratoren, das Schnellzugriffsmenü für On-Premises-Stores zu aktivieren oder zu deaktivieren. | ShowQuickAccessForStoreFront | true/false | Boolescher Wert | false | 2307 |

Referenzschema

```

1 <array>
2     <dict>
3         <key>ShowHelperInMenuBar</key>
4         <true/>
5         <key>AutoLaunchAppOnRestart</key>
6         <true/>
7         <key>StoreURLs</key>
8         <array>
9             <string>PROVIDE STORE URL HERE</string>
10        </array>
11        <key>BlockStoreAddition</key>

```

```
12         <false/>
13         <key>CEIPEnabled</key>
14         <true/>
15         <key>AutoUpdateArchitecture</key>`
16         <string>Universal</string>
17         <key>AutoUpdateState</key>
18         <string>Enable</string>
19         <key>AutoUpdateChannel</key>
20         <string>PROD</string>
21         <key>PayloadDisplayName</key>
22         <string>Citrix Workspace</string>
23         <key>PayloadIdentifier</key>
24         <string>com.citrix.receiver.nomas</string>
25         <key>PayloadType</key>
26         <string>com.citrix.receiver.nomas</string>
27         <key>PayloadUUID</key>
28         <string>3BE38AD3-7D95-423F-BD7B-8A4D1F5208EF</string>
29         <key>PayloadVersion</key>
30         <integer>1</integer>
31         <key>WebBrowserForAuthentication</key>
32         <string>System</string>
33         <key>Fido2Enabled</key>
34         <false/>
35         <key>ShowQuickAccessForStoreFront</key>
36         <true/>
37     </dict>
38 </array>
39
40 <!--NeedCopy-->
```

Authentifizieren

December 1, 2023

Smartcard

Die Citrix Workspace-App für Mac unterstützt die Smartcardauthentifizierung für die folgenden Konfigurationen:

- Smartcardauthentifizierung bei Workspace für Web oder StoreFront 3.12 und höher
- Citrix Virtual Apps and Desktops 7 2203 und höher.

- XenApp und XenDesktop 7.15 und höher.
- In smartcard-aktivierten Anwendungen, z. B. Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in virtuellen Desktop- oder Anwendungssitzungen verfügbar sind, digital signieren oder verschlüsseln.
- Die Citrix Workspace-App für Mac unterstützt die Verwendung von mehreren Zertifikaten mit einer Smartcard oder mit mehreren Smartcards. Wenn ein Benutzer eine Smartcard in einen Kartenleser einsteckt, sind die Zertifikate für alle Anwendungen verfügbar, die auf dem Gerät ausgeführt werden, einschließlich der Citrix Workspace-App für Mac.
- In Double-Hop-Sitzungen wird eine weitere Verbindung zwischen der Citrix Workspace-App für Mac und dem virtuellen Desktop des Benutzers hergestellt.

Info zur Smartcardauthentifizierung an Citrix Gateway

Es stehen mehrere Zertifikate zur Verfügung, wenn Sie eine Verbindung per Smartcard authentifizieren. Die Citrix Workspace-App für Mac fordert Sie auf, ein Zertifikat auszuwählen. Nach der Auswahl des Zertifikats werden Sie von der Citrix Workspace-App für Mac aufgefordert, das Smartcardkennwort einzugeben. Nach der Authentifizierung wird die Sitzung gestartet.

Wenn auf der Smartcard nur ein passendes Zertifikat ist, verwendet die Citrix Workspace-App für Mac das Zertifikat und Sie müssen keine Auswahl treffen. Sie müssen allerdings das Kennwort für die Smartcard eingeben, um die Verbindung zu authentifizieren und die Sitzung zu starten.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung

Hinweis:

Die Installation des PKCS#11-Moduls ist nicht obligatorisch. Dieser Abschnitt gilt nur für ICA-Sitzungen. Die Beschreibung gilt nicht für Citrix Workspace-Zugriff auf Citrix Gateway oder StoreFront, wenn eine Smartcard erforderlich ist.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung:

1. Wählen Sie in der Citrix Workspace-App für Mac **Einstellungen**.
2. Klicken Sie auf **Sicherheit und Datenschutz**.
3. Klicken Sie im Bereich **Sicherheit und Datenschutz** auf **Smartcard**.
4. Wählen Sie im Feld **PKCS#11** das entsprechende Modul aus. Klicken Sie auf **Weitere** und navigieren Sie zum Speicherort des PKCS#11-Moduls, wenn das gewünschte Modul nicht aufgeführt wird.
5. Wählen Sie das entsprechende Modul aus und klicken Sie auf **Hinzufügen**.

Unterstützte Leser, Middleware und Smartcardprofile

Die Citrix Workspace-App für Mac unterstützt die meisten, mit macOS kompatiblen Smartcardleser und kryptografische Middleware. Die Funktion der folgenden Smartcardleser wurde von Citrix überprüft.

Unterstützte Smartcardleser:

- Gängige Smartcardleser mit USB-Anschluss

Unterstützte Middleware:

- Clarify
- ActivIdentity (Clientversion)
- Charismathics (Clientversion)

Unterstützte Smartcards:

- PIV-Karten
- Common Access Card (CAC)
- Gemalto .NET-Karten

Folgen Sie zum Konfigurieren von Benutzergeräten den Anweisungen des macOS-kompatiblen Smartcardlesers und der kryptografischen Middleware.

Einschränkungen

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Citrix Workspace-App für Mac speichert nicht die Zertifikatauswahl des Benutzers.
- Die Citrix Workspace-App für Mac speichert nicht die Smartcard-PIN des Benutzers. PIN-Abfragen werden vom Betriebssystem gehandhabt, das möglicherweise seinen eigenen Cachingmechanismus hat.
- Die Citrix Workspace-App für Mac stellt die Verbindung mit Sitzungen nicht wieder her, wenn eine Smartcard eingesteckt ist.
- Für die Verwendung von VPN-Tunneln mit der Smartcardauthentifizierung müssen Sie das Citrix Gateway Plug-In installieren und sich über eine Webseite anmelden. Verwenden Sie Ihre Smartcards und PINs zur Authentifizierung bei jedem Schritt. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.

Bedingter Zugriff mit Azure Active Directory

Diese Authentifizierungsmethode wird nicht in der Citrix Workspace-App für Mac unterstützt.

User-Agent

Die Citrix Workspace-App sendet einen Benutzeragent in Netzwerkanforderungen, mit dem Authentifizierungsrichtlinien konfiguriert werden, einschließlich der Umleitung der Authentifizierung an andere Identitätsanbieter (IdPs).

Hinweis:

Bei der Konfiguration der Richtlinien nicht die Versionsnummern erwähnen.

| Szenario | User-Agent |
|--|---|
| <p>Allgemeine HTTP-Anforderungen — Netzwerkanforderungen der Citrix Workspace-App erhalten in der Regel einen allgemeinen User-Agent. Netzwerkanforderungen wie GET /Citrix/Roaming/Accounts und GET /AGServices/discover enthalten zum Beispiel folgenden User-Agent:</p> | <p>CitrixReceiver/23.05.0.36 MacOSX/13.4.0 com.citrix.receiver.nomas X1Class CWACapable</p> |
| <p>Cloudstore — Wenn ein Benutzer einen Cloudstore zur Citrix Workspace-App hinzufügt, werden Netzwerkanforderungen mit einem bestimmten User-Agent gesendet. Zum Beispiel Netzwerkanforderungen mit dem Pfad /core/connect/authorize. Der von der Citrix Workspace-App gesendete User-Agent ist:</p> | <p>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, wie Gecko) Citrix Workspace/23.05.0.36 MacOSX/13.4.0 com.citrix.receiver.nomas X1Class CWACapable</p> |
| <p>On-Premises-Store mit erweiterter Gateway-Authentifizierung — Wenn ein Benutzer zur Citrix Workspace-App einen On-Premises-Store mit in Gateway konfigurierter erweiterter Authentifizierung hinzufügt, werden Netzwerkanforderungen mit einem bestimmten User-Agent gesendet. Zum Beispiel Netzwerkanforderungen, deren Anforderungen Folgendes enthalten: GET /nf/auth/doWebview.do und GET /logon/LogonPoint/tmindex.html. Der von der Citrix Workspace-App gesendete User-Agent ist:</p> | <p>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, wie Gecko), CWAWEBSITEVIEW/23.05.0.36</p> |

| Szenario | User-Agent |
|--|---|
| Benutzerdefinierter Webstore — Wenn ein Benutzer einen benutzerdefinierten Webstore zur Citrix Workspace-App hinzufügt, lautet der von der Citrix Workspace-App gesendete User-Agent: | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, wie Gecko) Safari CWA/23.05.0.18 MacOSX/13.4.0 |

Sichere Kommunikation

December 1, 2023

Zum Sichern der Kommunikation zwischen der Site und der Citrix Workspace-App für Mac können Sie Verbindungen mit zahlreichen Sicherheitsverfahren integrieren, einschließlich Citrix Gateway. Weitere Informationen zur Konfiguration von Citrix Gateway mit Citrix StoreFront finden Sie in der [StoreFront-Dokumentation](#).

Hinweis:

Citrix empfiehlt das Schützen der Kommunikation zwischen StoreFront-Servern und Benutzgeräten mit Citrix Gateway.

- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das Netzwerk und vom Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App für Mac unterstützt die Protokolle SOCKS und Secure Proxy.
- Citrix Secure Web Gateway. Citrix Secure Web Gateway stellt einen einzigen sicheren, verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit.
- SSL-Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall verwenden, die die interne IP-Adresse des Servers einer externen Internetadresse wie der Netzwerkadressübersetzung (NAT) zuweist, konfigurieren Sie die externe Adresse.

Hinweis:

Ab macOS Catalina hat Apple zusätzliche Anforderungen für Stammzertifikate und Zwischenzertifikate erzwungen, die Administratoren konfigurieren müssen. Weitere Informationen finden Sie im Apple Support-Artikel [HT210176](#).

Citrix Gateway

Damit Remotebenutzer sich über Citrix Gateway mit der XenMobile-Bereitstellung verbinden können, können Sie Citrix Gateway für StoreFront konfigurieren. Die Methode für das Aktivieren des Zugriffs hängt von der in der Bereitstellung verwendeten XenMobile-Edition ab.

Wenn Sie XenMobile im Netzwerk bereitstellen, lassen Sie Verbindungen von internen oder Remotebenutzern mit StoreFront über Citrix Gateway zu, indem Sie Citrix Gateway mit StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf von XenApp veröffentlichte Anwendungen und auf von XenDesktop virtualisierte Desktops zu. Benutzer stellen eine Verbindung über die Citrix Workspace-App für Mac her.

Verbinden mit Citrix Secure Web Gateway

Wenn Citrix Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Citrix Secure Web Gateway Proxy im Relaymodus verwenden. Weitere Informationen zum Relaymodus finden Sie in der Dokumentation unter [XenApp und Citrix Secure Web Gateway](#).

Wenn Sie den Relaymodus verwenden, fungiert der Citrix Secure Web Gateway-Server als Proxy, und die Citrix Workspace-App für Mac muss Folgendes verwenden:

- Vollqualifizierter Domänenname (FQDN) des Citrix Secure Web Gateway-Servers.
- Portnummer des Citrix Secure Web Gateway-Servers. Citrix Secure Web Gateway Version 2.0 unterstützt den Relaymodus nicht.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

Beispiel: eigener_Computer.Beispiel.com ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (eigener_Computer), eine Second-Level-Domäne (Beispiel) und eine Top-Level-Domäne (com) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (example.com) wird als Domänenname bezeichnet.

Herstellen von Verbindungen über Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und Verbindungen zwischen der Citrix Workspace-App für Mac und Servern gehandhabt. Die Citrix Workspace-App für Mac unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Webserver verwendet die Citrix Workspace-App für Mac die Proxyservereinstellungen, die für den Standardwebbrowser auf dem Benutzergerät konfiguriert sind. Kon-

figurieren Sie die Proxyservereinstellungen für den Standardwebbrowser entsprechend auf dem Benutzergerät.

Herstellen einer Verbindung durch eine Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Die Citrix Workspace-App für Mac muss über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können. Die Firewall muss HTTP-Datenübertragungen für die Kommunikation zwischen Benutzergerät und Webserver zulassen (meist über den HTTP-Standardport 80 oder 443 für einen sicheren Webserver). Für die Kommunikation zwischen Citrix Workspace und dem Citrix-Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

TLS

TLS (Transport Layer Security) ist die neueste, standardisierte Version des TLS-Protokolls. 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.

Die Citrix Workspace-App für Mac unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

Hinweis:

Die Citrix Workspace-App für Mac verwendet plattformeigene Kryptografie (OS X) für Verbindungen zwischen der Citrix Workspace-App für Mac und StoreFront.

Die folgenden Verschlüsselungssammlungen sind aus Sicherheitsgründen veraltet:

- Verschlüsselungssammlungen mit dem Präfix "TLS_RSA_**"
- Verschlüsselungssammlungen RC4 und 3DES
- 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)

Die Citrix Workspace-App für Mac unterstützt nur die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Für Benutzer von DTLS 1.0 unterstützt die Citrix Workspace-App für Mac 1910 und höher nur die folgende Verschlüsselungssammlung:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Aktualisieren Sie Citrix Gateway auf Version 12.1 oder höher, wenn Sie DTLS 1.0 verwenden möchten. Andernfalls greift es basierend auf der DDC-Richtlinie auf TLS zurück.

Die folgenden Matrizen enthalten Einzelheiten zu internen und externen Netzwerkverbindungen:

| Client cipher set | VDA cipher set | Direct connections | | | | | | | | |
|-------------------|----------------|--------------------|------|----------|-----------|------|----------|-----------|------|----------|
| | | TLS | | | DTLS v1.0 | | | DTLS v1.2 | | |
| | | Open | FIPS | SP800-52 | Open | FIPS | SP800-52 | Open | FIPS | SP800-52 |
| Any | ANY | Y | Y | Y | Y | | | Y | | |
| | COM | Y | X | X | Y | | | Y | | |
| | GOV | Y | Y | Y | Y | | | Y | | |
| COM | ANY | Y | X | X | Y | | | | | |
| | COM | Y | X | X | Y | | | | | |
| | GOV | Y | X | X | Y | | | | | |
| GOV | ANY | Y | Y | Y | X | | | Y | | |
| | COM | X | X | X | X | | | X | | |
| | GOV | Y | Y | Y | X | | | Y | | |

| Client cipher set | VDA cipher set | External connections with Citrix Gateway | | | | | | | | |
|-------------------|----------------|--|------|----------|-----------|------|----------|-----------|------|----------|
| | | TLS | | | DTLS v1.0 | | | DTLS v1.2 | | |
| | | Open | FIPS | SP800-52 | Open | FIPS | SP800-52 | Open | FIPS | SP800-52 |
| Any | ANY | Y | Y | Y | Y | | | X | | |
| | COM | Y | X | X | Y | | | X | | |
| | GOV | Y | Y | Y | Y | | | X | | |
| COM | ANY | Y | X | X | Y | | | X | | |
| | COM | Y | X | X | Y | | | X | | |
| | GOV | Y | X | X | Y | | | X | | |
| GOV | ANY | Y | Y | Y | X | | | X | | |
| | COM | X | X | X | X | | | X | | |
| | GOV | Y | Y | Y | X | | | X | | |

Hinweis:

- Verwenden Sie Citrix Gateway 12.1 oder höher, damit EDT ordnungsgemäß funktioniert. Ältere Versionen unterstützen keine ECDHE-Verschlüsselungssammlungen im DTLS-Modus.
- Citrix Gateway unterstützt kein DTLS 1.2. `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` und `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` werden also nicht unterstützt. Citrix Gateway muss für die Verwendung von `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` konfiguriert sein, damit es in DTLS 1.0 ordnungsgemäß funktioniert.

Konfigurieren und Aktivieren der Citrix Workspace-App für TLS

Das Setup von TLS besteht aus zwei Hauptschritten:

1. Einrichten von SSL-Relay auf dem Citrix Virtual Apps and Desktops- und Citrix DaaS-Server (früher Citrix Virtual Apps and Desktops Service). Anschließende Abfrage und Installation des erforderlichen Serverzertifikats.
2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Installieren von Stammzertifikaten auf Benutzergeräten

Für das Sichern der Kommunikation mit TLS zwischen TLS-aktivierter Citrix Workspace-App für Mac und der Serverfarm muss auf dem Clientgerät ein Stammzertifikat vorhanden sein. Das Stammzertifikat überprüft die Signatur der Zertifizierungsstelle im Serverzertifikat.

In macOS X sind ca. 100 kommerzielle Stammzertifikate vorinstalliert. Wenn Sie jedoch ein anderes Zertifikat verwenden möchten, können Sie eines von der Zertifizierungsstelle abrufen und auf jedem Benutzergerät installieren.

Installieren Sie das Stammzertifikat je nach den Richtlinien und Verfahren Ihres Unternehmens auf jedem Gerät, anstatt die Benutzer zur Installation aufzufordern. Am einfachsten und sichersten ist es, wenn Sie die Stammzertifikate der macOS X-Schlüsselkette hinzufügen.

Hinzufügen eines Stammzertifikats zur Schlüsselkette

1. Doppelklicken Sie auf die Datei, die das Zertifikat enthält. Durch diese Aktion wird die Anwendung für die Schlüsselbundverwaltung automatisch gestartet.
2. Wählen Sie im Dialogfeld "Add Certificates" eine Option im Pop-upmenü "Keychain":
 - "login" (das Zertifikat gilt nur für den aktuellen Benutzer.)
 - "System" (das Zertifikat gilt für alle Benutzer eines Geräts.)
3. Klicken Sie auf OK.
4. Geben Sie Ihr Kennwort in das Dialogfeld "Authenticate" ein und klicken Sie auf "OK".

Das Stammzertifikat ist installiert und wird von TLS-fähigen Clients und anderen Anwendungen, die TLS einsetzen, verwendet.

Informationen über TLS-Richtlinien

In diesem Abschnitt finden Sie Informationen zur Konfiguration von Sicherheitsrichtlinien für ICA-Sitzungen über TLS. Sie können bestimmte TLS-Einstellungen, die für ICA-Verbindungen verwendet werden, in der Citrix Workspace-App für Mac konfigurieren. Diese Einstellungen werden in der Benutzeroberfläche nicht angezeigt. Für das Ändern müssen Sie einen Befehl auf dem Citrix Workspace-App für Mac-Gerät ausführen.

Hinweis:

TLS-Richtlinien werden mit anderen Methoden verwaltet – von Geräten, die von einem OS X-Server oder einer anderen Mobilgeräteverwaltungslösung gesteuert werden.

TLS-Richtlinien enthalten die folgenden Einstellungen:

SecurityComplianceMode. Stellt den Sicherheitskompatibilitätsmodus für die Richtlinie ein. Wenn Sie “SecurityComplianceMode” nicht konfigurieren, wird standardmäßig FIPS verwendet. Gültige Werte für diese Einstellung sind u. a.:

- **Keine.** Kein Kompatibilitätsmodus wird erzwungen
- **FIPS.** FIPS-Kryptografiemodule werden verwendet
- **SP800-52.** NIST SP800-52r1-Kompatibilität wird erzwungen

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. Gibt die TLS-Protokollversionen an, die bei der Protokollaushandlung akzeptiert werden. Diese Informationen werden als Array dargestellt; jede Kombination der möglichen Werte wird unterstützt. Wenn diese Einstellung nicht konfiguriert ist, werden als Standardwerte TLS10, TLS11 und TLS12 verwendet. Gültige Werte für diese Einstellung sind u. a.:

- **TLS10.** Gibt an, dass das TLS 1.0-Protokoll zugelassen ist.
- **TLS11.** Gibt an, dass das TLS 1.1-Protokoll zugelassen ist.
- **TLS12.** Gibt an, dass das TLS 1.2-Protokoll zugelassen ist.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array  
TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy. Verbessert die kryptografische Authentifizierung des Citrix Servers und die allgemeine Sicherheit der SSL/TLS-Verbindungen zwischen einem Client und einem Server. Diese Einstellung regelt den Umgang mit einer vertrauenswürdigen Stammzertifizierungsstelle beim Öffnen einer Remotesitzung über SSL mit dem Client für OS X.

Wenn diese Einstellung aktiviert ist, prüft der Client, ob das Zertifikat des Servers widerrufen wurde. Es gibt mehrere Prüfstufen für die Zertifikatsperlliste. Der Client kann beispielsweise so konfiguriert

werden, dass er nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft. Außerdem können Sie die Überprüfung der Zertifikate so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Das Prüfen der Zertifikatsperrliste ist ein fortschrittliches Feature, das von einigen Zertifikatausstellern unterstützt wird. Administratoren können Sicherheitszertifikate widerrufen (d. h. vor dem Ablaufdatum ungültig machen), wenn private Schlüssel von Zertifikaten kryptografisch kompromittiert sind oder der DNS-Name unerwartet geändert werden muss.

Gültige Werte für diese Einstellung sind u. a.:

- **NoCheck.** Es wird keine Überprüfung der Zertifikatsperrliste durchgeführt.
- **CheckWithNoNetworkAccess.** Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Es werden nur lokale Zertifikatsperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay oder Citrix Secure Web Gateway-Server vorgelegt wird, nicht wichtig.
- **FullAccessCheck.** Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Lokale Zertifikatsperrlistenpeicher und alle Verteilungspunkte werden verwendet. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay oder Citrix Secure Web Gateway-Server vorgelegt wird, nicht wichtig.
- **FullAccessCheckAndCRLRequired.** Die Prüfung der Zertifikatsperrliste wird durchgeführt, mit Ausnahme der Root-Zertifizierungsstelle. Lokale Zertifikatsperrlistenpeicher und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
- **FullAccessCheckAndCRLRequiredAll.** Die Prüfung der Zertifikatsperrliste wird durchgeführt, einschließlich der Stammzertifizierungsstelle. Lokale Zertifikatsperrlistenpeicher und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.

Hinweis:

Wenn Sie "SSLCertificateRevocationCheckPolicy" nicht festlegen, wird standardmäßig "FullAccessCheck" verwendet.

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

Konfigurieren von TLS-Richtlinien

Führen Sie zum Konfigurieren von TLS-Einstellungen auf einem nicht verwalteten Computer den Befehl **defaults** in Terminal.app aus.

defaults ist eine Befehlszeilenanwendung, mit der Sie App-Einstellungen in einer OS X-Einstellungslistendatei hinzufügen, bearbeiten und löschen können.

Ändern der Einstellungen

1. Öffnen Sie **Applications > Utilities > Terminal**.
2. Führen Sie in "Terminal" folgenden Befehl aus:

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

Dabei gilt:

<name>: Der Name der Einstellung, wie oben beschrieben.

<type>: Eine Option zum Identifizieren des Typs der Einstellung, entweder -string oder -array. Wenn der Einstellungstyp "string" ist, kann diese Einstellung ausgelassen werden.

<value>: Der Wert für die Einstellung. Wenn der Wert ein Array ist und mehrere Werte angegeben werden müssen, trennen Sie die Werte durch ein Leerzeichen.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array  
TLS11 TLS12
```

Wiederherstellen der Standardkonfiguration

Zurücksetzen einer Einstellung auf den Standard

1. Öffnen Sie **Applications > Utilities > Terminal**.
2. Führen Sie in "Terminal" folgenden Befehl aus:

```
defaults delete com.citrix.receiver.nomas <name>
```

Dabei gilt:

<name>: Der Name der Einstellung, wie oben beschrieben.

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Sicherheitseinstellungen

Mit Citrix Receiver für Mac-Version 12.3 wurden Sicherheitsverbesserungen eingeführt, u. a.:

- Verbesserte Benutzeroberfläche für die Sicherheitskonfiguration: In älteren Versionen war die Befehlszeile die bevorzugte Methode, um sicherheitsrelevante Änderungen vorzunehmen. Jetzt können Konfigurationseinstellungen für die Sitzungssicherheit einfach über die Benutzeroberfläche vorgenommen werden. Diese nahtlose Methode zum Festlegen von Sitzungseinstellungen führt zu einer besseren Benutzererfahrung.
- Anzeigen von TLS-Verbindungen: Sie können Verbindungen überprüfen, die eine bestimmte TLS-Version verwenden, sowie Verschlüsselungsalgorithmen, den Modus, die Schlüsselgröße und den SecureICA-Status. Darüber hinaus können Sie das Serverzertifikat für TLS-Verbindungen anzeigen.

Die neue Registerkarte **TLS** im erweiterten Bildschirm **Sicherheit und Datenschutz** enthält die folgenden neuen Optionen:

- Konformitätsmodus festlegen
- Kryptografiemodul konfigurieren
- Geeignete TLS-Version auswählen
- Zertifikatsperrliste auswählen
- Einstellungen für alle TLS-Verbindungen aktivieren

Im Bild unten sehen Sie die Einstellungen für **Sicherheit und Datenschutz**, auf die über die Benutzeroberfläche zugegriffen werden kann:



© 2023 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).