



Citrix Workspace-App 2203.1 LTSR für Windows

Contents

Info zu diesem Release	2
Behobene Probleme	3
Bekannte Probleme	22
Hinweise zu Drittanbietern	23
Systemanforderungen und Kompatibilität	23
Installation und Deinstallation	32
Bereitstellen	45
Aktualisieren	53
Erste Schritte	62
Konfigurieren	82
Single Sign-On für die Citrix Workspace-App konfigurieren	184
Authentifizieren	188
Sichere Kommunikation	208
Storebrowse	219
Citrix Workspace-App Desktop Lock	229
Software Development Kit (SDK) und API	235
Referenz für ICA-Einstellungen	237

Info zu diesem Release

March 6, 2024

Neue Features in 2203.1 LTSR

Citrix Workspace-App 2203.1 CU6 is the most recent Long Term Service Release (LTSR) of Citrix Workspace-App for Windows.

Hinweis:

Dieses Release unterstützt Features, die in der Citrix Workspace-App 2002 für Windows bis Citrix Workspace-App 2202 für Windows enthalten waren, mit Ausnahme derer, die sich auf im Abschnitt [Ausnahmen](#) aufgeführte Komponenten beziehen.

Verbesserung der Audioumleitung

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

Microsoft Teams-Optimierung

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

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.

Behobene Probleme

June 14, 2024

Citrix Workspace-App 2203.1 LTSR CU6 Hotfix 1 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU6

- Bei Verwendung der Citrix Workspace-App für Windows Version 2203.1 LTSR CU6 kann es zu einem Startfehler kommen, da `wfica32.exe` nicht mehr reagiert. [CVADHELP-24770]
- Benutzerdefinierte virtuelle Treiberschlüssel werden bei der Deinstallation der Citrix Workspace-App für Windows möglicherweise nicht beibehalten. [CVADHELP-24513]

Citrix Workspace app 2203.1 LTSR CU6 for Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU5

Sitzung / Verbindung

- Wenn das Verbindungsleasing für einen Cloud-Store aktiviert war, startete die Citrix Workspace-App für Windows Sitzungen erfolgreich, auch wenn das Sitzungslimit überschritten wurde. [CVADHELP-23771]
- `qlaunch` schlägt möglicherweise zum ersten Mal fehl, wenn `selfservicemode` auf `false` gesetzt ist. [CVADHELP-24414]
- Wenn die WPAD-Proxyeinstellungen auf einer Clientmaschine konfiguriert sind und die Sitzungszuverlässigkeit aktiviert ist, reagiert der Prozess `wfica32.exe` nicht mehr. [CVADHELP-23873]
- Wenn der Name der ICA-Datei oder des Ordners, in dem sich diese befindet, Unicode-Zeichen enthält, können Sitzungen möglicherweise nicht gestartet werden. Dieses Problem tritt nur beim Hybridstart auf. [CVADHELP-23843]
- Die Citrix Workspace-App für Windows Version 2212 erfüllt möglicherweise nicht die in der Proxy-PAC-Datei festgelegten Bedingungen. [CVADHELP-22503]

Benutzererfahrung

- Wenn Sie die Storekonfiguration mithilfe der Gruppenrichtlinienobjektvorlage oder über die Befehlszeile ändern, wird möglicherweise ein weißer Bildschirm angezeigt. [CVADHELP-23801]

- Die Aktualisierungsfunktion schlägt möglicherweise bei Cloudspeichern mit benutzerdefinierten Domänen fehl. [CVADHELP-23733]
- Wenn mehrere Konten über GPO konfiguriert werden und Sie ein deaktiviertes Konto aktivieren, wechselt die Citrix Workspace-App immer zur Ansicht aller Konten statt zum ausgewählten Einzelkonto. [CVADHELP-24018]
- Wenn Sie Google Japanese IME mit dem Citrix IME-Modus “Beste Benutzererfahrung” aktiviert haben, können Sie Textfelder in PowerPoint möglicherweise nicht mit der **Löschtaste** löschen. [CVADHELP-23605]
- Wenn eine HDX-Sitzung im Vollbildmodus im Fokus steht und der Endpunkt mit **Ctrl+Alt+Del** gesperrt ist, können Benutzer nach dem Entsperren möglicherweise nichts eingeben. [CVADHELP-24512]
- Sie stellen möglicherweise fest, dass die App auch nach dem Schließen der Citrix Workspace-App geöffnet wird, wenn Sie eine App auf der Registerkarte markieren, dann die Citrix Workspace-App schließen und dann die **Eingabetaste** drücken. [CVADHELP-22700]

Systemausnahmen

- Beim Upgrade des VDA auf Citrix Virtual Apps and Desktops 2308 oder höher reagiert die Citrix Workspace-App möglicherweise nicht mehr, wenn Fenster für veröffentlichte Anwendungen im Seamlessmodus gestartet werden. [CVADHELP-23976]
- Wenn die veröffentlichte Anwendung auf nicht englischen Clientmaschinen einen Unicode-Titel hat, ist `wfica32.exe` nicht mit den Analytics-Komponenten kompatibel. [CVADHELP-24471]

Seamlessfenster

- Wenn Sie eine Anwendung auf einen anderen Monitor verschieben und minimieren, wird die Anwendung in der maximierten Ansicht möglicherweise nicht richtig geöffnet. Sie können versuchen, die Anwendung zu schließen und erneut zu öffnen. [CVADHELP-23703]

Installation, Deinstallation, Upgrade

- Benutzerdefinierte virtuelle Treiberschlüssel werden bei der Deinstallation der Citrix Workspace-App möglicherweise nicht beibehalten. [CVADHELP-24513]

Probleme bei Clientgeräten

- Ein Verbundgerät wie das **biometrische Bloomberg-Tastaturmodul 5** stellt möglicherweise keine automatische Verbindung her, auch wenn die automatische Umleitung von Client-USB-Geräten aktiviert ist. [CVADHELP-22673]

Benutzeroberfläche

- Citrix Workspace listet die veröffentlichten Ressourcen möglicherweise für kurze Zeit nicht auf, wenn eine Verbindung zu einer GSLB-URL (Global Server Load Balancing) hergestellt wird. Dieses Problem tritt auf, wenn der eingerichtete StoreFront-Server auf Probleme stößt, die zu einer GSLB-gesteuerten virtuellen IP-Adressänderung (VIP) am Endpunkt führen. [CVADHELP-22467]
- Möglicherweise können Sie keinen Store hinzufügen, wenn die Top-Level-Domain (TLD) der Store-URL weniger als zwei Zeichen lang oder keine TLD vorhanden ist. [CVADHELP-23973]

Anmeldung und Authentifizierung

- Die Citrix Workspace-App mit SAML2- und FAS-Authentifizierung meldet sich beim Entsperren der Sitzung möglicherweise nicht automatisch an, auch wenn **WSCReconnectMode** for Workspace Control so eingestellt ist, dass bei der **Windows-Anmeldung erneut eine Verbindung hergestellt wird**, und die Richtlinie **Automatische Authentifizierung für Citrix Workspace** aktiviert ist. [CVADHELP-23018]

Citrix Workspace-App 2203.1 LTSR CU5 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU4

HDX Plug-n-Play

- Wenn Sie neue und vorhandene USB-Geräte auf Ablehnen einrichten, wird die folgende Anforderung möglicherweise weiterhin angezeigt:

Citrix Workspace hat mindestens ein an Ihren Computer angeschlossenes Gerät erkannt. Klicken Sie hier, um die Geräte in der Sitzung zu verbinden.

[CVADHELP-23506]

Installation, Deinstallation, Upgrade

- Nach dem Neustart eines Clientendpunkts schlägt die regelmäßige automatische Prüfung auf Updates vor der Anmeldung möglicherweise fehl. [CVADHELP-23054]
- Wenn Sie nach Abschluss der Installation der Citrix Workspace-App einen Store per GPO oder über die Befehlszeile konfigurieren, wird möglicherweise ein schwerer Fehler gemeldet. [CVADHELP-23345]

Tastatur

- In einem Double-Hop-Szenario funktioniert **Alt+Tab** möglicherweise nicht auf macOS-Clients. [CVADHELP-23085]

Sitzung/Verbindung

- Wenn Sie im [Cacheumleitungsmodus](#) eine Verbindung zu einem Desktop herstellen und ADC [hohe Verfügbarkeit](#) fehlschlägt, können Sie möglicherweise keine erneute Verbindung im Cacheumleitungsmodus zu einem Desktop herstellen. [CVADHELP-22881]
- Nach einem Upgrade auf eine neuere Version können Sie die Citrix Workspace-App möglicherweise nicht mit der API aus dem ICO SDK starten. [CVADHELP-22940]
- Wenn der Self-Service-Modus auf **False** gesetzt und die Desktop-Sperre aktiviert ist, können Sie möglicherweise keinen Store hinzufügen und keinen Desktop starten. [CVADHELP-23052]
- Der Inhalt veröffentlichter Anwendungen kann für Benutzer sporadisch einfrieren. Das Problem tritt auf, wenn die TCP-Verbindung vor der UDP-Verbindung hergestellt wird und die EDT-MTU-Erkennung beim Umschalten von TDP zu UDP nicht ausgelöst wird. [CVADHELP-23253]
- Wenn Sie sich von einem Endpunkt abmelden, reagiert der Prozess wfica32.exe möglicherweise nicht mehr und blockiert die Abmeldung. [CVADHELP-23617]

Benutzererfahrung

- Sie können sich möglicherweise nicht per Single Sign-On bei der Citrix Workspace-App anmelden oder die Authentifizierungsaufforderung in Cloud-Stores nicht sehen. Das Problem tritt auf, wenn das Konto erstmals per GPO oder über die Befehlszeile konfiguriert wurde, der Self-Service-Modus auf "false" gesetzt ist und die Richtlinie "Automatische Authentifizierung" für Citrix Workspace aktiviert ist. [CVADHELP-22641]

- Citrix VPN wird möglicherweise abgemeldet, wenn Sie sich von der Citrix Workspace-App abmelden, selbst wenn das VPN über den Registrierungswert **1** für **DisableIconHide** entkoppelt wurde. [CVADHELP-22916]
- Das Hinzufügen eines Store-Kontos kann lange dauern oder auf einem Endpunkt ohne Internetzugang fehlschlagen bzw. wenn der Global App Config-Server nicht erreichbar ist. [CVADHELP-22999]
- Die ausführbare SelfService-Datei wird möglicherweise ausgeführt, obwohl der Citrix Workspace-App kein Konto hinzugefügt wurde. [CVADHELP-23124]

Benutzeroberfläche

- Wenn Sie einen veröffentlichten Desktop öffnen, dessen Name Unicode-Zeichen enthält, wird der Desktop Viewer-Name möglicherweise unkenntlich angezeigt. Das Problem tritt nur im Internet Explorer-Modus in Microsoft Edge auf. [CVADHELP-22925]

Citrix Workspace-App 2203.1 LTSR CU4 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU3

Inhaltsumleitung

- Mit diesem Fix können Sie einen Ping-Test verhindern und die automatische Umleitung von URLs von Host zu Client zulassen.
 - Um den Ping-Test bei einer Host-zu-Client-Umleitung zu verhindern, legen Sie den folgenden Registrierungsschlüssel fest:
HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA
Bezeichnung: OverridePingCheck
Typ: REG_DWORD
Wert: 1
 - Um die automatische Umleitung von URLs bei einer Host-zu-Client-Umleitung zuzulassen, legen Sie den folgenden Registrierungsschlüssel fest:
HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA
Name: OverridePreventAutoRedirect
Typ: REGREG_DWORD
Wert: 1

[CVADHELP-22824]

Installation, Deinstallation, Upgrade

- Das Upgrade der Citrix Workspace-App für Windows bis Version 1912 CU2, die mit der Option **App Protection aktivieren** installiert wurde, kann mit folgender Fehlermeldung fehlschlagen: **Starten von Dienst 'AppProtection Service'(entryprotectsvc) fehlgeschlagen. Überprüfen Sie, ob Sie ausreichende Privilegien zum Starten der Systemdienste haben.**

[CVADHELP-22404]

- Der Befehl `CitrixReceiverUpdater.exe` kann **Autoupdate**-Einstellungen wie **AutoUpdateStream** möglicherweise nicht aktualisieren, wenn die Einstellungen für automatische Updates zuvor unter **Erweiterte Einstellungen > Citrix Workspace-Updates** geändert wurden.

[CVADHELP-22840]

Sitzung/Verbindung

- Es kann zu Verzögerungen beim Hinzufügen eines Stores kommen, ausgelöst durch Anforderungen zur Zertifikatsperrüberprüfung für das Zertifikat des Stores. Um dieses Problem zu umgehen, können Sie die Überprüfung der Zertifikatsperre mithilfe des folgenden Registrierungsschlüssels auslassen:

- HKEY_LOCAL_MACHINE/Software/wow6432node/Citrix/Receiver

Name: SkipStoreCertificateRevocationCheck

Typ: DWORD

Wert: 1

Oder

- HKEY_CURRENT_USER/Software/Citrix/Receiver

Name: SkipStoreCertificateRevocationCheck

Typ: DWORD

Wert: 1

[CVADHELP-21931]

- Die Sitzung wird möglicherweise unterbrochen, wenn Sie auf **Desktop Viewer** klicken und die Größe eines veröffentlichten Desktops fortlaufend ändern. [CVADHELP-22063]

- Versuche, mit der automatischen Wiederverbindung von Clients die Verbindung zu bestimmten nicht-englischsprachigen Desktop-Versionen wiederherzustellen, können fehlschlagen, und es wird eine Fehlermeldung angezeigt. [CVADHELP-22507]
- Bei Thinwire-H.265 im Vollbildmodus kann es bei der Citrix Workspace-App 2203.1 LTSR CU3 für Windows zum Fallback auf H.264 kommen. [CVADHELP-22919]

Systemausnahmen

- Der Prozess msedgewebview2.exe kann zu einer hohen CPU-Auslastung führen, wenn selfservice ausgeführt wird. [CVADHELP-21610]
- Der Prozess wfica32.exe wird möglicherweise unerwartet beendet, während eine Benutzersitzung mit HDX-Webcamumleitung ausgeführt wird. [CVADHELP-22249]
- Der Prozess wfica32.exe wird möglicherweise unerwartet beendet, wenn die Sitzung heruntergefahren wird. [CVADHELP-22329]

Benutzererfahrung

- Die Einstellungen für die Desktopverknüpfung pro Anwendung haben möglicherweise standardmäßig hohe Priorität. Wenn Sie zudem die Desktopverknüpfungen auf der Clientseite auf **False** setzen, wird dies möglicherweise nicht wirksam. Mit diesem Fix und dem Festlegen des folgenden Registrierungsschlüssels überschreiben die Einstellungen zur Desktopverknüpfung auf dem Client die anwendungsspezifischen Einstellungen.

Legen Sie den folgenden Registrierungsschlüssel fest, um die Einstellungen zur Desktopverknüpfung zu überschreiben:

HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Name: ProviderSettingOverride

Typ: REG_SZ

Wert: True

[CVADHELP-15550]

- In Umgebungen mit hoher Latenz kann sich der Mauszeiger in der Citrix Workspace-App sprunghaft bewegen, wenn die Einstellung **Relative Maus verwenden** aktiviert ist.

Um den Fix zu aktivieren, ändern Sie die Datei default.ica in StoreFront unter C:\inetpub\wwwroot\Citrix\StoreFront\default.ica

Fügen Sie `RelMouseSyncTimeout=xxx(min 10 to max 1000)` zum Abschnitt `[WFClient]` hinzu.

Oder

Legen Sie auf dem Endpunkt den folgenden Registrierungsschlüssel fest:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Mod

Name: RelMouseSyncTimeout

Typ: STRING

Wert: 10 bis 1000

[CVADHELP-21829]

- Der Versuch, MSG-Dateien durch Kopieren und Einfügen aus dem lokalen Microsoft Outlook in einen veröffentlichten Explorer zu verschieben, schlagen möglicherweise fehl. [CVADHELP-22542]

Benutzeroberfläche

- Wenn Sie sich bei der Citrix Workspace-App anmelden, werden Apps und Desktops möglicherweise nicht angezeigt, die mehreren über GPO oder die Befehlszeile konfigurierten Konten entsprechen. Dieses Problem tritt auf, wenn der Registrierungsschlüsselwert von [CurrentAccount](#) unter Computer\HKEY_LOCAL_MACHINE\Software\wow6432Node\Citrix\Dazzle auf [AllAccount](#) gesetzt ist. [CVADHELP-21124]
- Wenn der Parameter **AllowAddStore** auf den Wert **N** festgelegt ist und ein HTTP-Store per GPO oder mithilfe der Befehlszeilenschnittstelle hinzugefügt wird, wird möglicherweise die folgende Fehlermeldung angezeigt:

Keine Verbindung zum Server möglich.

[CVADHELP-22184]

- Bei Cloudstores können Sie möglicherweise kein Konto unter Verwendung von Umleitungs-URLs hinzufügen. [CVADHELP-22438]
- Möglicherweise wird ein anderer Store-Name als der von Ihnen angegebene in der Citrix Workspace-App angezeigt. [CVADHELP-22452]
- Nach dem Upgrade auf Citrix Workspace-App für Windows 2203 LTSR wird möglicherweise ein weißer Bildschirm angezeigt. Dieses Problem tritt auf, wenn Sie zum ersten Mal einen Store hinzufügen und konfigurieren und gleichzeitig die Self-Service-Benutzeroberfläche aktualisieren und öffnen. [CVADHELP-22696]

Citrix Workspace-App 2203.1 LTSR CU3 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU2

Probleme bei Clientgeräten

- Wenn der Standard-USB-Richtlinienwert **Bei Sperrung entfernen** Großbuchstaben enthält, wird das USB-Gerät (z. B. Unterschriftenfelder) möglicherweise nicht von einem gesperrten Client getrennt. [CVADHELP-21492]

HDX Realtime

- Wird während eines Microsoft Teams-Anrufs eine Microsoft Outlook-Erinnerung angezeigt, erscheint auf dem geteilten Microsoft Teams-Bildschirm ein schwarzes Quadrat. [CVADHELP-19222]

Installation, Deinstallation, Upgrade

- Der lokale App-Zugriff funktioniert möglicherweise nicht bei Benutzergeräten mit italienischem Betriebssystem. [CVADHELP-21986]
- Versuche, die Citrix Workspace-App zu installieren, schlagen unter Windows Server 2012 R2 möglicherweise fehl. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX477888](#). [CVADHELP-22116]

Tastatur

- Wenn Sie die Taste **Druck S-Abf** gedrückt halten, empfängt die serverseitig veröffentlichte Anwendung möglicherweise kontinuierlich VK_SNAPSHOT WM_KEYUP-Ereignisse (Bildschirm-Snapshot aufgenommen). [CVADHELP-21209]

Anmeldung und Authentifizierung

- Wenn **Selfservicemode** auf "false" gesetzt ist, werden hinzugefügte Stores nach dem Öffnen der Citrix Workspace-App möglicherweise nicht korrekt aktualisiert. Daher wird das Authentifizierungsfenster nicht angezeigt. [CVADHELP-20593]
- Das Inaktivitätstimeout läuft möglicherweise nicht ab, wenn Sie die Citrix Workspace-App beenden, bevor der eingestellte Timeout-Wert erreicht wurde. Dies kann dazu führen, dass Sie die Citrix Workspace-App später ohne Angabe von Anmeldeinformationen starten können. [CVADHELP-20912]

- Versuche, Anwendungen mit dem Befehl **storebrowse** aufzulisten, schlagen möglicherweise fehl, wenn als Citrix Gateway-URL `**.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E { NSG_URL }` verwendet wird. [CVADHELP-21910]

Seamlessfenster

- In einer Seamless-Sitzung bleiben Maus und Tastatur des Benutzergeräts möglicherweise zeitweise hängen, wenn die Anwendung ihr Fenster zuerst deaktiviert und dann wieder aktiviert. [CVADHELP-21031]
- Wenn Sie mit dem Windows-Feature **Aero Snap** ein maximiertes Fenster von einem Monitor auf einen größeren Monitor verschieben, auf dem Windows 11 ausgeführt wird, verschwindet die Sitzung möglicherweise. [CVADHELP-21173]
- Wenn Sie eine veröffentlichte App im Seamlessmodus öffnen, werden möglicherweise andere lokale Apps oder Seamless-Apps im Vordergrund angezeigt und verdecken die veröffentlichte App. [CVADHELP-20742, CVADHELP-21277]
- Eine veröffentlichte Anwendung wird möglicherweise nicht sichtbar geöffnet, wenn Sie die Anwendung starten. [CVADHELP-21618]

Sitzung/Verbindung

- Die COM-Portumleitung ist möglicherweise während des Sitzungsroamings blockiert. [CVADHELP-20959]
- Wenn die Einstellung **Relative Maus verwenden** in einer Benutzersitzung aktiviert ist, funktioniert der Linksklick auf dem Touchpad möglicherweise nicht. [CVADHELP-21223]
- In einer isolierten Umgebung versucht die Citrix Workspace-App möglicherweise, eine Verbindung zum Global App Config-Server herzustellen, selbst wenn die Richtlinie **Global App Config Service** über ein GPO deaktiviert wurde. Dies führt zu einer Verzögerung durch das Hinzufügen eines Kontos. [CVADHELP-21319]
- Citrix Analytics kann keine netzwerkbezogenen Kennzahlen von Endbenutzern empfangen. Dieses Problem tritt auch dann auf, wenn folgende Voraussetzungen erfüllt sind:
 - App- bzw. Desktopsitzungen werden länger als 15 Minuten mit der Citrix Workspace-App ausgeführt.
 - Für den Store bzw. das verwendete Konto ist CAS aktiviert.

Hinweis:

Netzwerkbezogene CAS-Ereignisse werden nicht für den browserbasierten Start von Apps und Desktops gesendet. Sie werden nur gesendet, wenn Sie die App oder den Desktop webgestützt aus dem Store öffnen, der über die native Citrix Workspace-App hinzugefügt wurde.

[CVADHELP-21448]

- Veröffentlichte Apps, die auf einem veröffentlichten Desktop ausgeführt werden, können möglicherweise nicht gestartet werden und die Citrix Workspace-App bleibt hängen. [CVADHELP-21604]
- Versuche, auf die Citrix Workspace-App für Windows zuzugreifen, schlagen möglicherweise fehl, wenn das VPN getrennt oder erneut verbunden wird. [CVADHELP-21662]
- Der Windocker.exe-Prozess kann fälschlicherweise ausgehende Netzwerkanforderungen an mehrere IP-Adressen generieren. [CVADHELP-21728]
- Die Verwendung der automatischen Wiederverbindung von Clients kann das Herstellen einer Verbindung zu einer Sitzung verzögern. [CVADHELP-21738]
- Wenn Sie mehrere Stores über ein Gruppenrichtlinienobjekt (GPO) oder eine Befehlszeile konfigurieren, wird einer der Stores möglicherweise nicht vollständig konfiguriert. [CVADHELP-22034]
- Citrix Analytics-Dateidownloadereignisse wie Dateinamen und Dateipfadattribute sind möglicherweise leer. [CVADHELP-22194]

Systemausnahmen

- Wenn Sie eine veröffentlichte Anwendung bei aktivierter Richtlinie **Adaptives Audio** starten, wird der wfica32-Prozess möglicherweise unerwartet beendet. [CVADHELP-20999]
- Einige Binärdateien der Citrix Workspace-App sind möglicherweise nicht signiert, was zu Sicherheitsproblemen führt. [CVADHELP-21159]

Benutzererfahrung

- Wenn Sie einen Desktop minimieren und dann wieder maximieren, wird die Position der Symbolleiste möglicherweise nicht beibehalten. [CVADHELP-21258]
- Wenn Sie die Verbindung zu einer Sitzung im Vollbildmodus trennen und wieder herstellen, wird die Position der Symbolleiste möglicherweise nicht beibehalten. [CVADHELP-21324]

- Wenn Sie SSON in einer Umgebung ohne aktiven Zugriff auf externe Websites verwenden, kann es zu Verzögerungen beim Auflisten von Apps und beim Starten von Apps oder Desktops kommen. Das Problem tritt ab Citrix Workspace-App Version 2210.5 und ab Citrix Workspace-App Version 2203 CU2 auf. [CVADHELP-21786]

Benutzeroberfläche

- Es kann vorkommen, dass Sie der Citrix Workspace-App einen ausgeblendeten Store nicht hinzufügen können. Das Problem tritt auf, wenn Sie versuchen, einen Citrix Gateway-FQDN hinzuzufügen, für den eine Smartcard-Authentifizierung erforderlich ist, oder wenn der Name des StoreFront-Stores ein Leerzeichen enthält, z. B. <https://servername.company.com?Store Service>. [CVADHELP-21516]
- Nachdem ein Store hinzugefügt und das Store-Authentifizierungstoken auf **true** gesetzt wurde, reagiert Citrix Workspace möglicherweise nicht mehr mit einem weißen Bildschirm und das Store-Authentifizierungstoken wird auf **False** gesetzt. [CVADHELP-21582]
- Das Authentifizierungs-Popupfenster wird möglicherweise oben links anstatt in der Mitte des Bildschirms angezeigt. [CVADHELP-21835]
- Die WebView-Statusleiste wird möglicherweise unten in der Citrix Workspace-App angezeigt, wenn Sie mit der Maus auf eine veröffentlichte App oder ein Desktopsymbol zeigen. [CVADHELP-22108]
- Wenn Sie eine native Citrix Workspace-App öffnen und mit der rechten Maustaste auf die Self-Service-Benutzeroberfläche klicken, wird möglicherweise ein Kontextmenü angezeigt. [CVADHELP-22131]

Citrix Workspace-App 2203.1 LTSR CU2 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR CU1

Installation, Deinstallation, Upgrade

- Wenn Sie die Citrix Workspace-App als Systembenutzer mit bestimmten Anwendungen von Drittanbietern installieren, werden möglicherweise falsche Fehlermeldungen in den Installationsprotokollen angezeigt. [CVADHELP-20695]

Tastatur

- Wenn Sie auf einem Surface Pro-Gerät die Bildschirmtastatur im Desktop Viewer auswählen, wird die Tastatur möglicherweise nicht angezeigt. [CVADHELP-20564]

Anmeldung und Authentifizierung

- Mit diesem Fix können Sie die Webview-Authentifizierungsaufforderung bei Verwendung der Single Sign-On-Authentifizierung unterdrücken.

Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/AuthManager oder HKEY_CURRENT_USER/SOFT

Name: HideAuthPrompt

Typ: REG_SZ

Wert: True

[CVADHELP-20799]

Sitzung/Verbindung

- Die Citrix Workspace-App Version 2109 und höher ignoriert möglicherweise die Einstellungen in der Datei default.ica auf dem StoreFront-Server. [CVADHELP-20017]
- Wenn Sie einen internen Standardbeacon als StoreFront-Store-URL (z. B. <https://example.com/Citrix/Store/discovery>) in der Citrix Workspace-App konfigurieren, können die an diese URLs gesendeten HTTP-HEAD-Anforderungen zu 404 Fehlern führen. [CVADHELP-20329]
- Versuche, eine veröffentlichte Anwendung über die Citrix Workspace-App auf einem Endpunkt mit mehr als acht Monitoren zu starten, schlagen möglicherweise mit der folgenden Fehlermeldung fehl:

Diese Version von Workspace unterstützt die ausgewählte Verschlüsselung nicht. Wenden Sie sich an den Administrator.

[CVADHELP-20555]

- Wenn der Browsername (BrowserName) einer veröffentlichten Anwendung Multibytezeichen enthält, kann die Anwendung möglicherweise nicht gestartet werden. Das Problem tritt in Internet Explorer Version 11 und Microsoft Edge im Internet Explorer-Modus auf. [CVADHELP-20684]
- Bei Verwendung der Citrix Workspace-App für Windows 2106 oder höher funktioniert der ausgehende ICA-Proxy möglicherweise nicht. [CVADHELP-20824]
- Die Citrix Workspace-App fordert Sie auf, ein Zertifikat auszuwählen, auch wenn nur ein Zertifikat vorhanden ist. Dieses Problem tritt bei der Authentifizierung beim Workspace-Store (Cloudstore) auf.

Sie können die Zertifikataufforderung unterdrücken, indem Sie die folgende Registrierung hinzufügen:

- Auf 32-Bit-Systemen:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/Dazzle oder HKEY_CURRENT_USER/SOFTWARE/Citrix/Dazzle

Name: SuppressCertSelectionPrompt

Typ: REG_SZ

Wert: True

- Auf 64-Bit-Systemen:

HKEY_LOCAL_MACHINE/Software/Wow6432Node/Citrix/Dazzle oder HKEY_CURRENT_USER/Software

Name: SuppressCertSelectionPrompt

Typ: REG_SZ

Wert: True

[CVADHELP-20844]

- Wenn die Client-USB-Geräteumleitung in einer bestehenden Sitzung deaktiviert ist und Sie eine neue Sitzung mit aktivierter Umleitung starten, funktioniert die Umleitung möglicherweise nicht. [CVADHELP-20858]

Systemausnahmen

- Citrix Authentication Manager (AuthManSvr.exe) wird während der Anmeldung möglicherweise unerwartet beendet. [CVADHELP-17233]
- In dem wfica32.exe-Prozess kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. [CVADHELP-20558]
- Wenn Sie ein Audiogerät trennen, kann eine Zugriffsverletzung beim wfica32.exe-Prozess auftreten, und der Prozess wird unerwartet beendet. Das Problem tritt nach dem Upgrade der Citrix Workspace-App für Windows auf Version 2203.1 LTSR CU1 auf. [CVADHELP-21123]
- Der Citrix Desktop Viewer (CDViewer.exe) wird möglicherweise unerwartet beendet, wenn die ICA-Dateigröße 4096 Byte ist. [CVADHELP-21128]

Benutzererfahrung

- Die Citrix Workspace-App zeigt möglicherweise ein verschwommenes Bild an, wenn Sie die Tasten Umschalt+F2 mehrmals in einer Benutzersitzung drücken und Desktop Viewer deaktiviert ist. [CVADHELP-20467]

- Wenn Sie eine VDA-Maschine starten und sich zum ersten Mal an einer Benutzersitzung anmelden, müssen Sie die Maus möglicherweise explizit verschieben, um den Cursor anzuzeigen. [CVADHELP-20818]
- Wenn Sie eine Seamlessanwendung im Windows 10-Kioskmodus starten, reagiert der Mauszeiger nicht ordnungsgemäß und Schriftarten werden möglicherweise verzerrt angezeigt. [CVADHELP-20860]

Benutzeroberfläche

- Die Citrix Workspace-App reagiert nach dem Start möglicherweise nicht mehr. [CVADHELP-20317]
- Versuche, auf die Citrix Workspace-App für Windows zuzugreifen, schlagen möglicherweise fehl, wenn das VPN getrennt oder erneut verbunden wird. [CVADHELP-20376]
- Wenn Sie zwei Stores vom gleichen StoreFront-Server über ein Gruppenrichtlinienobjekt hinzufügen, schlägt die Konfiguration des zweiten Stores möglicherweise zeitweise fehl. [CVADHELP-20655]
- Wenn Sie einen deaktivierten Store über das Gruppenrichtlinienobjekt hinzufügen und einen anderen Store vom gleichen StoreFront-Server über die GUI hinzufügen, wird möglicherweise ein Ladebildschirm angezeigt und das Hinzufügen eines Kontos schlägt fehl. [CVADHELP-20776]

Citrix Workspace-App 2203.1 LTSR CU1 für Windows

Im Vergleich zu Citrix Workspace-App 2203.1 LTSR

Inhaltsumleitung

- Wenn Desktop Viewer auf den Vollbildmodus eingestellt ist und der Standardbrowser auf dem Endpunktgerät maximiert ist, bringt die Funktion zur bidirektionalen Inhaltsumleitung das Fenster des lokalen Standardwebrowsers möglicherweise nicht in den Vordergrund. Das Problem tritt auf, wenn der lokale Standardwebbrowser nicht Internet Explorer ist. [CVADHELP-19041]

HDX RealTime

- Wenn Sie während eines Peer-to-Peer-Anrufs mit HDX-Optimierung für Microsoft Teams die App-Fensterfreigabe sehr oft starten und beenden, kann die Freigabe fehlschlagen und Sie können möglicherweise Desktop-Bildschirm oder App-Fenster nicht freigeben und keine Anrufe tätigen oder empfangen, bis Sie die Citrix Workspace-App neu starten. [CVADHELP-20162]

Installation, Deinstallation, Upgrade

- Der Citrix Workspace Updater-Dienst wird möglicherweise nicht gestartet, was zu einem Installationsfehler führt. Das Problem tritt auf, wenn der Client nicht mit dem Internet verbunden ist. [CVADHELP-19613]

Tastatur

- Wenn Sie nach dem Starten einer HDX-Sitzung das Vordergrundfenster in ein lokales Anwendungsfenster ändern, werden Systemtasten wie **Windows** und **Alt-Tab** möglicherweise von der Citrix-Sitzung anstelle des lokalen PC-Desktops verarbeitet, obwohl die Citrix Sitzung im Hintergrund ausgeführt wird. [CVADHELP-19778]

Anmeldung und Authentifizierung

- Nachdem Sie sich mit der Citrix Workspace-App angemeldet haben, wird möglicherweise eine falsche Anmeldeaufforderung mit dieser Meldung angezeigt:

Sie müssen sich anmelden, um auf Citrix Workspace zugreifen zu können.

[CVADHELP-19676]

Seamlessfenster

- Wenn Sie einen Monitor anschließen oder trennen, ist das Seamlessfenster möglicherweise falsch positioniert. [CVADHELP-19168]

Sitzung/Verbindung

- RDP-Sitzungen können möglicherweise nicht in der Citrix Workspace-App 1912 LTSR CU6 für Windows gestartet werden, wenn die Smartcard-Umleitung über RDP aktiviert ist. [CVADHELP-19430]
- Wenn Sie zum ersten Mal mit der Citrix Workspace-App für Windows Version 2112 oder höher auf einen VDA zugreifen, wird möglicherweise die folgende Sicherheitsmeldung angezeigt:

Eine Onlineanwendung versucht, auf Informationen zuzugreifen, die auf einem Gerät gespeichert sind, das an den HDX-Dateizugriff Ihres Computers angeschlossen ist.

In früheren Versionen wurde diese Nachricht nur beim ersten Zugriff auf jede veröffentlichte Ressource in einer Bereitstellungsgruppe und nicht bei jedem VDA angezeigt.

[CVADHELP-19636]

- Versuche, Desktops oder Anwendungen auf einem Tablet über die Citrix Workspace-App zu starten, schlagen möglicherweise fehl. Das Problem tritt auf, wenn die Client-IP-Adresse nicht abgerufen werden kann. [CVADHELP-19703]
- Das Konfigurieren von Stores mit Geo-DNS-URL über das Gruppenrichtlinienobjekt oder die Befehlszeile schlägt möglicherweise fehl, wenn Sie `AllowAddStore=N` während der Installation der Citrix Workspace-App festgelegt haben. [CVADHELP-19853]
- Bei Verwendung der Citrix Workspace-App 2204.1 oder höher wird die Sitzung möglicherweise getrennt. Das Problem tritt auf, wenn es eine Einschränkung bezüglich der Ausführung unsignierter Binärdateien (z. B. wfica.ocx) gibt. [CVADHELP-20053]

Systemausnahmen

- Das Ziehen und Ablegen eines Fensters in einer HDX-Sitzung kann langsam sein und dazu führen, dass der Prozess wfica32.exe unerwartet beendet wird. [CVADHELP-19482]
- Die **AppLocker**-Regel im Gruppenrichtlinienobjekt blockiert die Integration des Citrix Gateway-Plug-Ins in Citrix Workspace. Es werden mehrere temporäre Dateien im Format VPNXXXX.tmp im temporären Ordner erstellt. Die Dateien werden auch dann erstellt, wenn der Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client den Wert **DisableIconHide** hat. [CVADHELP-19709]
- Mit diesem Fix wird ein seltenes Problem mit Speicherverlusten im wfica32.exe-Prozess behoben, das bei der Citrix Workspace-App für Windows auftritt. [CVADHELP-19904]
- Microsoft Office-Anwendungen werden möglicherweise unerwartet beendet, wenn der Softwareschutzdienst aufgrund fehlerhafter App Protection-Komponenten nicht gestartet werden kann. [CVADHELP-20667]

Benutzererfahrung

- Ziehen und Ablegen von Dateien vom Benutzergerät auf eine veröffentlichte Anwendung funktioniert möglicherweise beim ersten Mal. Anschließend schlägt es fehl und die Anwendung reagiert nicht. [CVADHELP-17211]
- Wenn Sie ein Fenster in einer HDX-Sitzung ziehen und ablegen, dauert es einige Zeit, bis das Fenster wiederhergestellt ist und das Taskleistensymbol angezeigt wird. [CVADHELP-19440]
- Drag & Drop funktioniert möglicherweise nicht, wenn Sie in einer Seamlesssitzung ein Dialogfeld mit der **Esc-Taste** schließen. [CVADHELP-19604]
- Beim Update der Citrix Workspace-App 2006 oder einer älteren Version werden die Gateway- und Beacon-Konfigurationen der vorhandenen Stores möglicherweise gelöscht und dieselben

Konfigurationen werden erneut hinzugefügt, selbst wenn die Store-Konfigurationen im Gruppenrichtlinienobjekt nicht geändert werden. [CVADHELP-19839]

- Bei Zugriff auf eine Webstore-URL über die Citrix Workspace-App für Windows kann es vorkommen, dass das Workspace-Fenster nach jedem Aktualisierungsintervall im Vordergrund statt im Hintergrund angezeigt wird. [CVADHELP-19885]
- Die Citrix Workspace-App sendet möglicherweise weiterhin Daten an <https://rttf.citrix.com>, auch wenn das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) deaktiviert wurde. [CVADHELP-20016]

Benutzeroberfläche

- Wenn Sie in der Citrix Workspace-App für Windows Store-URLs mithilfe des Gruppenrichtlinienobjekts hinzufügen, wird möglicherweise die folgende Fehlermeldung angezeigt:

Verbindung zum Server nicht möglich.

Dieses Problem tritt auf, wenn einer der Stores deaktiviert und nicht erreichbar ist.

[CVADHELP-19751]

- Durch diesen Fix wird eine Anmeldeseite angezeigt, wenn Sie sich von der Citrix Workspace-App für Windows abmelden. Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

- Auf 32-Bit-Systemen:

HKEY/LOCAL/MACHINE/Software/Citrix/Dazzle

Name: ShowSignInPageOnLogOff

Typ: REG_SZ

Wert: True

- Auf 64-Bit-Systemen:

HKEY/LOCAL/Software/Wow6432Node/Citrix/Dazzle

Name: ShowSignInPageOnLogOff

Typ: REG_SZ

Wert: True

[CVADHELP-19967]

- Die Benachrichtigung über den Akkustatus und das automatische Tastatur-Popupdialogfeld werden möglicherweise nicht in der Sitzung angezeigt, wenn die Richtlinie **Automatische Tastaturanzeige** in DDC aktiviert ist. [CVADHELP-19987]

- Wenn Sie die Citrix Workspace-App nach dem Hinzufügen der Store-URL zum ersten Mal starten, wird die folgende Fehlermeldung angezeigt:

In der Citrix Workspace-App ist beim Initialisieren von Microsoft Edge WebView2 ein Fehler aufgetreten. Starten Sie die App neu.

Dieses Problem tritt auf, wenn Sie die Store-URL über ein GPO oder die Befehlszeile hinzufügen und nach “discovery” einen Schrägstrich verwenden (z. B. <https://sales.example.com/Citrix/Store/discovery/>;0n;Store).

[CVADHELP-20214]

- Die **Desktop Viewer**-Symbolleiste ist möglicherweise nicht sichtbar, wenn Sie den virtuellen Desktop von einem Store des benutzerdefinierten Portals aus öffnen. [CVADHELP-20253]

Citrix Workspace-App 2203.1 LTSR für Windows

Sitzung/Verbindung

- Die Citrix ADC-Appliance antwortet möglicherweise nicht mehr, wenn bestimmte Bedingungen von der Citrix Workspace-App für Windows ausgelöst werden. [HDX-39683]
- Wenn Sie versuchen, zur der in der Citrix Workspace-App für Windows eingestellten bevorzugten Webcam umzuleiten, wird die Einstellung möglicherweise nicht wie konfiguriert ausgeführt.

Durch diesen Fix ist die bevorzugte Webcam die einzige verfügbare Webcam in der Benutzersitzung. Dies ermöglicht eine bessere Steuerung, wenn mehrere Webcams in der Benutzersitzung verfügbar sind.

[HDX-38214]

- Mit diesem Fix können Sie **TWITaskbarGroupingMode** in `HKEY_CURRENT_USER` oder `HKEY_LOCAL_MACHINE` auf **GroupNone** festlegen. Der Schlüssel **TWITaskbarGroupingMode** ist beispielsweise unter folgendem Pfad verfügbar: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows`. [CVADHELP-19106]
- Versuche, eine Citrix Gateway-URL hinzuzufügen, schlagen möglicherweise gelegentlich mit folgender Fehlermeldung fehl:

Authentication Service cannot be contacted.

[CVADHELP-19415]

Bekannte Probleme

March 6, 2024

Bekannte Probleme in Release 2203.1 LTSR CU6

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 2203.1 LTSR CU5

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 2203.1 LTSR CU4

- Sie können Sitzungen möglicherweise nicht starten, wenn der Name der ICA-Datei oder des Ordners, in den die ICA-Datei heruntergeladen wurde, Unicode- oder nicht-englische Zeichen enthält. Das Problem tritt nur auf, wenn Sie per Browser auf einen Store zugreifen und sich authentifizieren und anschließend eine App oder einen Desktop über die native Citrix Workspace-App starten. [CVADHELP-23843]

Bekannte Probleme in Release 2203.1 LTSR CU3

- Bei Thinwire-H.265 im Vollbildmodus kann es bei der Citrix Workspace-App 2203.1 LTSR CU3 für Windows zum Fallback auf H.264 kommen. [CVADHELP-22919]

Bekannte Probleme in Release 2203.1 LTSR CU2

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 2203.1 LTSR CU1

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 2203.1 LTSR

- Die Installation der Citrix Workspace-App für Windows im Offlinemodus schlägt möglicherweise fehl, wenn das Installationsprogramm Microsoft Edge WebView2 auf dem System nicht findet. Installieren Sie als Problemumgehung **MicrosoftEdgeWebView2RuntimeInstallerX86.exe** als Administrator und versuchen Sie dann, die Citrix Workspace-App für Windows zu installieren. [RFIN-26329]
- Die Benachrichtigung über den Akkustatus und das automatische Tastatur-Popupdialogfeld werden möglicherweise nicht in der Sitzung angezeigt, wenn die Richtlinie **Automatische Tastaturanzeige** in DDC aktiviert ist. [HDX-39558]
- Wenn Sie ein USB-Gerät anschließen oder auf Dateien zugreifen, zeigt die Citrix Workspace-App möglicherweise das veraltete Dialogfeld **Citrix Workspace - Sicherheitswarnung** an. [LCM-10369]

Hinweise zu Drittanbietern

June 14, 2023

Die Citrix Workspace-App 2203.1 LTSR für Windows enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

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

Systemanforderungen und Kompatibilität

April 22, 2024

Anforderungen

Hardwareanforderungen

- Mindestens 1 GB RAM.
- Die folgende Tabelle enthält Informationen zum mindestens erforderlichen Speicherplatz für die Installation der Citrix Workspace-App.

Betriebssystemversion	Erforderliche Mindestversion von Microsoft Edge WebView2 Runtime	Unterstützte Höchstversion von Microsoft Edge WebView2 Runtime
Windows 10 und Windows 11	92	Nicht zutreffend (unterstützt die neueste Version)
Windows Server 2012 R2	92	109
Windows Server 2016, 2019 und 2022	92	Nicht zutreffend (unterstützt die neueste Version)

Hinweis:

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

Softwareanforderungen

- Microsoft Edge WebView2 Runtime
- .NET 4.8
- Aktuelle Version von Microsoft Visual C++ Redistributable

Anforderungen für Microsoft Edge WebView2 In der folgenden Tabelle sind die unterstützten Mindest- und Höchstversionen von Microsoft Edge WebView2 Runtime für verschiedene Windows-Betriebssysteme aufgeführt:

Betriebssystemversion	Erforderliche Mindestversion von Microsoft Edge WebView2 Runtime	Unterstützte Höchstversion von Microsoft Edge WebView2 Runtime
Windows 10 und Windows 11	92	Nicht zutreffend (unterstützt die neueste Version)
Windows Server 2012 R2	92	109
Windows Server 2016, 2019 und 2022	92	Nicht zutreffend (unterstützt die neueste Version)

- Die Citrix Workspace-App ist in der [Evergreen Bootstrapper](#)-Version von Microsoft Edge WebView2 Runtime enthalten.

- Das Citrix Workspace-App-Installationsprogramm kann Microsoft Edge WebView2 Runtime während der Installation der Citrix Workspace-App installieren. Für diese Installation müssen Sie jedoch mit dem Internet verbunden sein. Alternativ können Sie zunächst das geeignete Offline-Paket von [Microsoft Edge WebView2 Runtime Evergreen Standalone Installer](#) installieren, bevor Sie die Citrix Workspace-App installieren.
- Das Gerät muss Zugriff auf die folgenden URLs haben:
 - https://*.dl.delivery.mp.microsoft.com zum Download von Microsoft Edge WebView2 Runtime während der Installation der Citrix Workspace-App. Weitere Informationen finden Sie unter [Allow list for Microsoft Edge endpoints](#).
 - <https://msedge.api.cdp.microsoft.com> zur Suche nach einem Microsoft Edge WebView2 Runtime Update
- Informationen zum Verwalten der automatischen Aktualisierung von Microsoft Edge WebView2 Runtime finden Sie in der Microsoft-Dokumentation unter [Update policies](#). Die automatische Aktualisierung eignet sich beispielsweise für nicht persistente virtuelle Desktops, die in den Ausgangszustand zurückversetzt werden, wenn ein Benutzer sich abmeldet.

Hinweis:

Wenn Sie die Citrix Workspace-App als Nicht-Administrator installieren oder aktualisieren und Microsoft Edge WebView2 Runtime nicht vorhanden ist, wird die Installation mit der folgenden Meldung unterbrochen:

Sie müssen als Administrator angemeldet sein, um die folgenden Voraussetzungspakete installieren zu können:

Edge Webview 2 Runtime

.NET-Anforderungen Die Citrix Workspace -App erfordert .NET 4.8. Sie können die Apps und Desktops über die Benutzeroberfläche der Citrix Workspace-App oder über die Befehlszeile abonnieren und starten.

Wenn Sie versuchen, die Citrix Workspace-App 1904 oder höher zu installieren oder als Upgrade bereitzustellen und die erforderliche Version von .NET Framework nicht auf Ihrem Windows-System vorliegt, lädt das Citrix Workspace-App-Installationsprogramm die erforderliche Version von .NET Framework herunter und installiert sie.

Hinweis:

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

- **Sie müssen mit dem Internet verbunden sein, um .NET Framework herunterladen und installieren zu können. Ist dies nicht der Fall, kann der Administrator diese Anforderungen über eine Bereitstellungsmethode wie z. B. SCCM installieren.**

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

Hinweis:

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

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

Hinweis:

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

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

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

Kompatibilitätsmatrix

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

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

Hinweis:

- Die Citrix Workspace-App 2203.1 LTSR für Windows ist die letzte Version, die das Betriebssystem Windows Server 2012 R2 unterstützt.
- Die Citrix Workspace-App 2203.1 LTSR für Windows wird nicht unter Windows 7 und Windows 8.1 unterstützt.
- Das Citrix Gateway Plug-In für die Endpunktanalyse (EPA) wird für Citrix Workspace unterstützt. In der nativen Citrix Workspace-App wird es nur unterstützt, wenn die nFactor-

Authentifizierung verwendet wird. Weitere Informationen finden Sie unter [Konfigurieren des EPA-Scans für die Vor- und Nachauthentifizierung als Faktor in der Multifaktorauthentifizierung \(nFactor\)](#) in der Dokumentation zu Citrix ADC.

Betriebssystem

Windows 11

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

Unterstützung für Windows 10 Enterprise (LTSC 2021) ab Version 2203.1 LTSR CU1 und höher

Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019)

Windows 10 (Home Edition*, Pro)

Windows Server 2022

Windows Server 2019

Windows Server 2016

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

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

Mit dem Betriebssystem Windows 10 hat Microsoft eine neue Methode zum Erstellen, Bereitstellen und Verwalten von Windows eingeführt: [Windows als Dienst](#). Neue Features werden in Feature-Updates (Hauptversionen wie 20H2, 21H1, 21H2) zusammengefasst. Fehlerbehebungen und Sicherheitsfixes werden in Qualitätsupdates verpackt. Diese Updates können mit vorhandenen Verwaltungstools wie SCCM bereitgestellt werden.

Hinweis:

- Die Installation von Citrix-Softwareversionen, die vor der Version für den halbjährlichen Kanal veröffentlicht wurden, wird nicht empfohlen.
- Sobald eine Windows 10-Version ihr Dienstende erreicht, wird sie von Microsoft nicht länger unterstützt. Citrix unterstützt die eigene Software nur für Betriebssysteme, die vom Hersteller unterstützt werden. Weitere Informationen zum Dienstende von Windows 10-Versionen finden Sie im [Informationsblatt zum Lebenszyklus von Windows](#).

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

Windows 10-Versionennummer	Buildnummer	Version der Citrix Workspace-App
22H2	19045	2203.1 CU1 und höher
21H2	19044	2112.1 und später
21H1	19043.928	2106 und höher
20H2	19042.508	2012 und höher
2004	19041.113	2006.1 und höher
1909	18363.418	1911 und höher
1903	18362.116	1909 und höher
1809	17763.107	1812 und höher
1803	17134.376	1808 und höher

Hinweis:

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

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

Windows 11-Versionennummer	Buildnummer	Version der Citrix Workspace-App
23H2	22631	2203,1 CU6
22H2	22621	2203.1 CU1 und höher
21H2	22000	2203.1 und höher

Überprüfen auf freien Speicherplatz Die folgende Tabelle enthält Informationen zum mindestens erforderlichen Speicherplatz für die Installation der Citrix Workspace-App.

Installationstyp	Erforderlicher Speicherplatz
Neuinstallation	572 MB

Installationstyp	Erforderlicher Speicherplatz
Upgrade	350 MB

Die Citrix Workspace-App prüft, ob genügend Speicherplatz zum Abschließen der Installation verfügbar ist. Die Überprüfung erfolgt sowohl bei einer Neuinstallation als auch bei einem Upgrade.

Hinweis:

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

Verbindungen, Zertifikate und Authentifizierung

Verbindungen

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 10.5 und höher

Zertifikate

Hinweis:

Die Citrix Workspace-App für Windows ist digital signiert. Die digitale Signatur ist mit einem Zeitstempel versehen. Das Zertifikat ist also auch nach Ablauf gültig.

- Privat (selbstsigniert)
- Stamm
- Platzhalter
- Zwischenzertifikat

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway vorhanden ist, installieren Sie das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Benutzergerät, mit dem auf Citrix-Ressourcen zugegriffen wird.

Hinweis:

Wenn das Zertifikat des Remotegateways sich beim Herstellen der Verbindung nicht verifizieren lässt, wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Die Warnung wird angezeigt, wenn das Stammzertifikat im lokalen Schlüsselspeicher fehlt. Wenn der Benutzer weiterarbeitet, werden die Apps angezeigt, können jedoch nicht gestartet werden.

Stammzertifikate

Für in Domänen eingebundene Computer können Sie ZS-Zertifikate mit der administrativen Gruppenrichtlinienobjektvorlage verteilen und als vertrauenswürdig einstufen.

Für nicht domänengebundene Computer können Unternehmen ein benutzerdefiniertes Installationspaket erstellen und damit das Zertifikat der Zertifizierungsstelle verteilen und installieren. Wenden Sie sich bei Fragen an den Systemadministrator.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden für einen Server in derselben Domäne verwendet.

Die Citrix Workspace-App unterstützt Zertifikate mit Platzhalterzeichen. Verwenden Sie Zertifikate mit Platzhalterzeichen gemäß den jeweils gültigen Sicherheitsrichtlinien Ihres Unternehmens. Eine Alternative zu Zertifikaten mit Platzhalterzeichen sind Zertifikate, die eine Liste der Servernamen und die SAN-Erweiterung (Subject Alternative Name) enthalten. Private und öffentliche Zertifizierungsstellen stellen diese Zertifikate aus.

Zwischenzertifikate

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter [Konfigurieren von Zwischenzertifikaten](#).

Authentifizierung

Authentifizierung bei StoreFront

	Workspace für Web	StoreFront Services-Site (nativ)	StoreFront, Citrix Virtual Apps and Desktops (nativ), Citrix DaaS	Citrix Gateway bei Workspace für Web	Citrix Gateway bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zweistufige Authentifizierung (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Ja*
Smartcard	Ja	Ja		Ja	Ja
Benutzerzertifikat				Ja (Citrix Gateway Plug-In)	Ja (Citrix Gateway Plug-In)

* Mit oder ohne Citrix Gateway als installiertes Plug-In auf dem Gerät.

Hinweis:

Die Citrix Workspace-App unterstützt die zweistufige Authentifizierung (Domäne plus Sicherheitstoken) über Citrix Gateway beim nativen StoreFront-Service.

Zertifikatsperrliste

Mit der Zertifikatsperrliste (Certificate Revocation List, CRL) kann die Citrix Workspace-App überprüfen, ob das Zertifikat des Servers widerrufen wurde. Durch die Überprüfung des Zertifikats wird die kryptografische Authentifizierung für den Server und die allgemeine Sicherheit der TLS-Verbindung zwischen Benutzergerät und Server verbessert.

Sie können die Überprüfung der Zertifikatsperrlisten in mehreren Stufen einstellen. Sie können die Citrix Workspace-App beispielsweise so konfigurieren, dass nur die lokale Zertifikatsperrliste oder die

lokale und die Netzwerkzertifikatsperrliste überprüft werden. Sie können die Überprüfung der Zertifikate auch so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Wenn Sie die Überprüfung der Zertifikate auf Ihrem lokalen Computer konfigurieren, beenden Sie die Citrix Workspace-App und stellen Sie sicher, dass alle Citrix Workspace-Komponenten einschließlich **Connection Center** geschlossen sind.

Weitere Informationen finden Sie unter [TLS \(Transport Layer Security\)](#).

Installation und Deinstallation

May 23, 2024

Sie können die Citrix Workspace-App wie folgt installieren:

- Download des Installationspakets [CitrixWorkspaceApp.exe](#) von der [Downloadseite](#) oder
- Download von der Downloadseite Ihres Unternehmens (falls verfügbar).

Sie können das Paket mit den folgenden Schritten installieren:

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

Installation mit Administrator- und Nicht-Administrator-Rechten:

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

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

	Installationsordner	Installationstyp
Administrator	C:\Programme (x86)\Citrix\ICA Client	Installation pro System
Benutzer	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Installation pro Benutzer

Hinweis:

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

Verwenden eines Windows-basierten Installationsprogramms

Sie können die Citrix Workspace-App für Windows manuell installieren, indem Sie das Installationspaket [CitrixWorkspaceApp.exe](#) mit einer der folgenden Methoden ausführen:

- Installationsmedium
- Netzwerkfreigabe
- Windows-Explorer
- Befehlszeilenoberfläche

Standardmäßig sind die Installationsprotokolle unter `%temp%\CTXReceiverInstallLogs*.logs`.

1. Starten Sie die Datei [CitrixWorkspaceApp.exe](#) und klicken Sie auf **Start**.
2. Lesen und akzeptieren Sie die Lizenzvereinbarung und fahren Sie mit der Installation fort.
3. Wenn Sie die Installation auf einer domänengebundenen Maschine mit Administratorrechten durchführen, wird ein Dialogfeld für Single Sign-On angezeigt. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).
4. Folgen Sie dem Windows-basierten Installationsprogramm, um die Installation abzuschließen.

Nach Abschluss der Installation werden Sie von der Citrix Workspace-App aufgefordert, ein Konto hinzuzufügen. Informationen zum Hinzufügen eines Kontos finden Sie unter [Konten hinzufügen oder Server wechseln](#).

Verwenden von Befehlszeilenparametern

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

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

- Name der Installationsdatei,
- Installationsbefehle und

- Installationseigenschaften.

Die verfügbaren Installationsbefehle und -eigenschaften lauten wie folgt:

`CitrixWorkspaceApp.exe [commands] [properties]`

Liste der Befehlszeilenparameter

Die Parameter werden wie folgt klassifiziert:

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

Allgemeine Parameter

- `/?` oder `/help` - Listet alle Installationsbefehle und -eigenschaften auf.
- `/silent` - Deaktiviert Installationsdialogfelder und Eingabeaufforderungen während der Installation.
- `/noreboot` - Unterdrückt die Aufforderungen zum Neustart während der Installation. Wenn Sie die Neustartaufforderung unterdrücken, werden USB-Geräte, die im ausgesetzten Zustand sind, nicht erkannt. Die USB-Geräte werden erst nach dem Neustart des Geräts aktiviert.
- `/includeSSON` - Erfordert die Installation mit Administratorrechten. Gibt an, dass die Citrix Workspace-App mit der Single Sign-On-Komponente installiert wird. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).
- `/rcu` - Der Switch `/rcu` ist nur wirksam, wenn ein Upgrade von einer nicht unterstützten Version der Software durchgeführt wird. Gibt an, dass Installation oder Upgrade der Citrix Workspace-App durch Deinstallation der vorhandenen Version erfolgt. Der Switch `/rcu` bereinigt auch vorhandene oder ältere Einstellungen.

Hinweis:

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

- Der Switch `/forceinstall` ist wirksam, wenn vorhandene Konfigurationen oder Einträge der Citrix Workspace-App bereinigt werden. Verwenden Sie den Switch in folgenden Szenarios:
 - Sie führen ein Upgrade von einer nicht unterstützten Citrix Workspace-App-Version aus.
 - Die Installation oder das Upgrade schlägt fehl.

Installationsparameter

/AutoUpdateCheck

Gibt an, dass Citrix Workspace für Windows erkennt, wenn ein Update verfügbar ist.

Hinweis:

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

- Auto (Standardeinstellung): Sie werden benachrichtigt, wenn ein Update zur Verfügung steht. Beispiel: `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto`.
- Manual: Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates. Beispiel: `CitrixWorkspaceApp.exe /AutoUpdateCheck=manual`.
- Disabled - Das Feature für automatische Updates ist deaktiviert. Beispiel: `CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled`.

/AutoUpdateStream

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

- LTSR - Die automatische Aktualisierung auf des Long Term Service Release erfolgt nur kumulativ. Beispiel: `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`.
- Current - Die automatische Aktualisierung erfolgt auf die neueste Version der Citrix Workspace-App handelt. Beispiel: `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`.

/DeferUpdateCount

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

- -1 (Standard) –Ermöglicht das Ignorieren von Benachrichtigungen beliebig oft. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0 –Gibt an, dass Sie pro verfügbares Update nur eine Benachrichtigung erhalten. Sie werden nicht erneut an das Update erinnert. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Jede andere Nummer “n”- Ermöglicht das “n”-malige Ignorieren von Benachrichtigungen. Die Option **Später erinnern** wird gemäß der festgelegten Zahl “n”angezeigt. Beispiel: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

/AURolloutPriority

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

- Auto (Standard) - Sie erhalten Updates während des Bereitstellungszeitraums wie von Citrix konfiguriert. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast – Sie erhalten Updates zu Beginn des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium - Sie erhalten Updates nach Ablauf der Hälfte des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow – Sie erhalten Updates gegen Ende des Bereitstellungszeitraums. Beispiel: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

/includeappprotection

Bietet mehr Sicherheit, da Clients besser vor Bildschirmerfassungs- und Keylogging-Malware geschützt sind.

- `CitrixWorkspaceApp.exe /includeappprotection`

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

/InstallEmbeddedBrowser

Schließt die Binärdateien für den Citrix Enterprise Browser aus. Führen Sie die Befehlszeilenoption `/InstallEmbeddedBrowser=N` aus, um das Citrix Enterprise Browser-Feature auszuschließen.

INSTALLDIR

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

ADDLOCAL

Installiert die angegebenen Komponenten. Beispiel: `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SSON,SELSERVICE,DesktopViewer,WebHelper,WorkspaceHub,USB,AppProtection`.

Hinweis:

Standardmäßig werden `ReceiverInside`, `ICA_Client` und `AM` bei der Installation der Citrix Workspace-App installiert.

Der Befehl `ADDLOCAL` installiert die angegebenen Komponenten.

`ReceiverInside`, `ICA_Client` und `AM` sind Voraussetzungen und werden standardmäßig bei der Installation der Citrix Workspace-App installiert.

- `ReceiverInside` - Installiert die Citrix Workspace-App (erforderlich) sowie die Funktionalität für die Taskleiste und für automatische Updates.
- `ICA_Client` - Installiert die HDX-Komponenten.
- `AM` - Installiert die Komponenten des Authentifizierungsmanagers.

Je nach Anforderung und Umgebung können Sie auch die folgenden Module installieren:

- `SSON` - Installiert die für Single Sign-On erforderlichen Komponenten.
- `SELFERVICE` - Installiert das Self-Service-Plug-In. Auf diese Weise können Sie über das Fenster der Citrix Workspace-App oder über eine Befehlszeile auf virtuelle Desktops und Anwendungen zugreifen. Wenn `SELFERVICE` nicht installiert ist, können Sie über das Internet (`Receiver für Web`) auf die Anwendungen und Desktops zugreifen.
- `DesktopViewer` - Installiert Desktop Viewer zum Anzeigen virtueller Apps und Desktops.
- `WebHelper` - Installiert die WebHelper-Komponente. Diese Komponente ruft die ICA-Datei aus StoreFront ab und leitet sie an die HDX Engine weiter. Außerdem werden die Umgebungsparameter überprüft und für StoreFront freigegeben. Diese Komponente wird beim Starten der Sitzung über den Browser verwendet.
- `WorkspaceHub` - Citrix Ready Workspace Hub-Komponente, die Citrix Casting aktiviert.
- `USB` - Installiert die USB-Unterstützung.
- `AppProtection` - Installiert die App Protection-Komponente.

HDX-Parameter

ALLOW_BIDIRCONTENTREDIRECTION

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

- 0 (Standard) –Gibt an, dass die bidirektionale Inhaltsumleitung deaktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1 –Gibt an, dass die bidirektionale Inhaltsumleitung aktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`.

FORCE_LAA

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

- 0 (Standard) –Die Komponente für den lokalen App-Zugriff ist nicht installiert. Beispiel: `CitrixWorkspaceApp.exe FORCE_LAA =0.`
- 1 –Gibt an, dass die clientseitige Komponente für den lokalen App-Zugriff installiert ist. Beispiel: `CitrixWorkspaceApp.exe FORCE_LAA =1.`

LEGACYFTAICONS

Legt fest, ob Sie für Dokumente oder Dateien, die Dateitypzuordnungen für abonnierte Anwendungen haben, Symbole anzeigen möchten.

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

ALLOW_CLIENHOSTEDAPPSURL

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

- 0 (Standard) –Deaktiviert die URL-Umleitungsfunktion auf einem Benutzergerät. Beispiel: `CitrixWorkspaceApp.exe ALLOW_CLIENHOSTEDAPPSURL=0.`
- 1 –Aktiviert die URL-Umleitung auf einem Benutzergerät. Beispiel: `CitrixWorkspaceApp.exe ALLOW_CLIENHOSTEDAPPSURL=1.`

Parameter für Einstellungen und Benutzeroberfläche

ALLOWADDSTORE

Ermöglicht es Ihnen, die Stores (HTTP oder https) basierend auf dem angegebenen Parameter zu konfigurieren.

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

ALLOWSAVEPWD

Ermöglicht Ihnen, die Anmeldeinformationen für den Store lokal zu speichern. Dieser Parameter gilt nur für Stores, die das Citrix Workspace-App-Protokoll verwenden.

- S (Standard) –Ermöglicht das Speichern von Kennwörtern nur für sichere Stores, die mit HTTPS konfiguriert sind. Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`.
- N –Das Speichern von Kennwörtern ist nicht zulässig. Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`.
- A –Ermöglicht das Speichern von Kennwörtern für sichere Stores (HTTPS) und nicht sichere Stores (HTTP). Beispiel: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`.

STARTMENUDIR

Gibt das Verzeichnis für die Verknüpfungen im Startmenü an.

- `<Directory Name>` –Standardmäßig werden Anwendungen unter **Start > Alle Programme** angezeigt. Sie können den relativen Pfad für die Verknüpfungen im Ordner `\Programs` angeben. Beispiel: Geben Sie `STARTMENUDIR=\Workspace` an, um Verknüpfungen unter **Start > Alle Programme > Workspace** zu platzieren.

DESKTOPDIR

Gibt das Verzeichnis für Verknüpfungen auf dem Desktop an.

Hinweis:

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

- `<Directory Name>` –Sie können den relativen Pfad für Verknüpfungen angeben. Beispiel: Geben Sie `DESKTOPDIR=\Workspace` an, um Verknüpfungen unter **Start > Alle Programme > Workspace** zu platzieren.

SELFSERVICEMODE

Steuert den Zugriff auf die Self-Service-Benutzeroberfläche der Citrix Workspace-App.

- `True` –Der Benutzer hat Zugriff auf die Self-Service-Benutzeroberfläche. Beispiel: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- `False` –Gibt an, dass der Benutzer keinen Zugriff auf die Self-Service-Benutzeroberfläche hat. Beispiel: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

ENABLEPRELAUNCH

Steuert den Vorabstart von Sitzungen. Weitere Informationen finden Sie unter [Dauer des Anwendungsstarts](#).

- `True` - Gibt an, dass Sitzungsvorabstart aktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- `False` - Gibt an, dass Sitzungsvorabstart deaktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

DisableSetting

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

- `0` (Standard) –Die Optionen **Verknüpfungen** und **Wiederverbinden** werden auf der Seite “Erweiterte Einstellungen” angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=0`.
- `1` –Nur die Option **Wiederverbinden** wird auf der Seite “Erweiterte Einstellungen” angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=1`.
- `2` –Nur die Option **Verknüpfungen** wird auf der Seite “Erweiterte Einstellungen” angezeigt. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=2`.

- 3 – Die Optionen **Verknüpfungen** und **Wiederverbinden** werden beide auf der Seite “Erweiterte Einstellungen” ausgeblendet. Beispiel: `CitrixWorkspaceApp.exe DisableSetting=3`.

EnableCEIP

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

- True (Standard) – Sie nehmen am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teil. Beispiel: `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False – Sie nehmen nicht am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teil. Beispiel: `CitrixWorkspaceApp.exe EnableCEIP=False`.

EnableTracing

Steuert die Funktion **Always-On-Ablaufverfolgung**.

- True (Standard) – Aktiviert die Funktion **Always-On-Ablaufverfolgung**. Beispiel: `CitrixWorkspaceApp.exe EnableTracing=true`.
- False – Deaktiviert die Funktion **Always-On-Ablaufverfolgung**. Beispiel: `CitrixWorkspaceApp.exe EnableTracing=false`.

CLIENT_NAME

Gibt den Namen an, mit dem das Benutzergerät beim Server identifiziert wird.

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

ENABLE_DYNAMIC_CLIENT_NAME

Ermöglicht, dass der Clientname mit dem Computernamen übereinstimmt. Wenn Sie den Computernamen ändern, ändert sich auch der Clientname.

- Yes (Standard) – Erlaubt, dass der Clientname mit dem Computernamen übereinstimmt. Beispiel: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No – Erlaubt nicht, dass der Clientname mit dem Computernamen übereinstimmt. Geben Sie einen Wert für die Eigenschaft `CLIENT_NAME` ein. Beispiel: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

Authentifizierungsparameter

ENABLE_SSON

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

- Yes (Standard) –Gibt an, dass Single Sign-On aktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLE_SSON=Yes`.
- No –Gibt an, dass Single Sign-On deaktiviert ist. Beispiel: `CitrixWorkspaceApp.exe ENABLE_SSON=No`.

ENABLE_KERBEROS

Gibt an, ob die HDX Engine die Kerberos-Authentifizierung verwenden muss. Dies ist nur erforderlich, wenn Sie die Single Sign-On-Authentifizierung aktivieren. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung mit Kerberos](#).

- Yes –Gibt an, dass die HDX Engine die Kerberos-Authentifizierung verwenden muss. Beispiel: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No –Gibt an, dass die HDX Engine keine Kerberos-Authentifizierung verwendet. Beispiel: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

Zusätzlich zu den oben genannten Eigenschaften können Sie auch die Store-URL angeben, die mit der Citrix Workspace-App verwendet wird. Sie können bis zu 10 Stores hinzufügen. Verwenden Sie dazu die folgende Eigenschaft:

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

Werte:

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

- **storedescription** - Beschreibung des Stores, z. B. `HR App Store`.

Beispiele für eine Installation über die Befehlszeile

Angeben der Citrix Gateway Store-URL:

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

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

Hinweis:

- Die mit dieser Methode konfigurierte Citrix Gateway Store-URL unterstützt keine PNA-Dienste-Sites, die Citrix Gateway verwenden.
- Bei mehreren vorhandenen Stores muss die Citrix Gateway-Store-URL an erster Position in der Liste stehen. Die Konfiguration von Citrix Gateway-Store-URLs ist auf eine beschränkt.

Installieren aller Komponenten ohne Benutzereingriffe und Angeben von zwei Anwendungsstores:

```
CitrixWorkspaceApp.exe /silent  
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;  
HR App Store"  
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/  
discovery;on;Backup HR App Store"
```

Hinweis:

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

Zurücksetzen der Citrix Workspace-App

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

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

- Alle konfigurierten Konten und Stores.
- Apps, die vom Self-Service-Plug-In bereitgestellt werden, ihre Symbole und Registrierungskchlüssel.

- Vom Self-Service-Plug-In erstellte Dateitypzuordnungen.
- Zwischengespeicherte Dateien und gespeicherte Kennwörter.
- Benutzerspezifische Registrierungseinstellungen.
- Maschinenspezifische Installationen und Registrierungseinstellungen.
- Citrix Gateway-Registrierungseinstellungen für die Citrix Workspace-App.

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

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"-cleanUser
```

Verwenden Sie für eine unbeaufsichtigte Zurücksetzung folgenden Befehl:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"/silent -cleanUser
```

Hinweis:

Verwenden Sie den Großbuchstaben U im Parameter.

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

- Installation der Citrix Workspace-App oder des Plug-Ins.
- Maschinenspezifische ICA-Sperreinstellungen.
- Administrative Gruppenrichtlinienobjektvorlage für die Citrix Workspace-App.

Deinstallieren

Verwenden des Windows-basierten Deinstallationsprogramms:

Sie können die Citrix Workspace-App mit dem Windows-Hilfsprogramm "Programme und Funktionen"(Programme hinzufügen/entfernen) deinstallieren.

Hinweis:

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

Verwenden der Befehlszeilenschnittstelle:

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

```
CitrixWorkspaceApp.exe /uninstall
```

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

```
CitrixWorkspaceApp.exe /silent /uninstall
```

Hinweis:

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

Bereitstellen

April 22, 2024

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

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

Verwenden von Active Directory und Beispielskripts

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

Verwenden von Skripts mit Active Directory:

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

Skripts bearbeiten

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

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

Skripts

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

Bereitstellungstyp	Bereitstellen	Entfernen
Pro Computer	<code>CheckAndDeployWorkspacePerMachine.bat</code>	<code>CheckAndRemoveWorkspacePerMachine.bat</code>
Pro Benutzer	<code>CheckAndDeployWorkspacePerUser.bat</code>	<code>CheckAndRemoveWorkspacePerUser.bat</code>

Hinzufügen von Startskripts:

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

Bereitstellen der Citrix Workspace-App für Windows:

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

Entfernen der Citrix Workspace-App für Windows:

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

Verwenden von Workspace für Web

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

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

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

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

Hinweis:

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

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

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

Verwenden von System Center Configuration Manager 2012 R2

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

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

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

Hinzufügen der Citrix Workspace-App zur SCCM-Bereitstellung

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

Hinweis:

Benutzer können die Informationen sehen, die Sie hier angeben.

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

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

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

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

Das Dialogfeld "Erkennungsregel" wird angezeigt.

- Wählen Sie als **Einstellungstyp** die Option "Dateisystem".
- Wählen Sie folgende Einstellungen unter **Geben Sie die Datei oder den Ordner an, um diese Anwendung zu erkennen**:
 - **Typ**: Wählen Sie im Dropdownmenü die Option **Datei**.
 - **Pfad**: `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`
 - **Datei- oder Ordnername**: `receiver.exe`
 - **Eigenschaft**: Wählen Sie im Dropdownmenü die Option **Version**.
 - **Operator**: Wählen Sie im Dropdownmenü **größer oder gleich**.
 - **Wert**: Geben Sie **4.3.0.65534** ein.

Hinweis:

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

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

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

Hinweis:

Legen Sie keine Anforderungen und Abhängigkeiten für diesen Bereitstellungstyp fest.

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

Es wird dann ein Erfolg gemeldet.

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

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

Hinzufügen von Verteilungspunkten

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

Der Assistent für die Verteilung von Inhalt wird angezeigt.

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

Das Dialogfeld “Verteilungspunkte hinzufügen” wird angezeigt.

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

Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

4. Klicken Sie auf **Schließen**.

Bereitstellen der Citrix Workspace-App im Softwarecenter

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

Der Assistent zur Softwarebereitstellung wird angezeigt.

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

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

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

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

Im **Abschlussfenster** wird eine Erfolgsmeldung angezeigt.

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

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

Erstellen von Gerätesammlungen

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

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

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

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

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

Klicken Sie auf **Weiter**.

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

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

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

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

Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

6. Klicken Sie auf **Schließen**.

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

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

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

Hinweis:

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

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

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

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

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

Hinweis:

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

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

Aktualisieren

April 22, 2024

Manuelle Aktualisierung

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

Automatisches Update

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

Hinweis:

- Wenn Sie einen ausgehenden Proxy mit SSL-Interception konfiguriert haben, fügen Sie eine Ausnahme zum Workspace-Server für automatische Updates <https://downloadplugins.citrix.com/> hinzu, damit Sie Updates von Citrix erhalten.
- Automatische Updates sind für Versionen vor Citrix Workspace-App für Windows 2104 und Citrix Workspace-App 1912 LTSR CU4 nicht verfügbar.
- Ihr System muss über eine Internetverbindung verfügen, um Updates zu erhalten.
- Standardmäßig sind Citrix Workspace-App-Updates auf dem VDA deaktiviert. Dies umfasst RDS-Server mit mehreren Benutzern, VDI-Maschinen und Maschinen mit Remote-PC-Zugriff.
- Citrix Workspace-App-Updates sind auf Maschinen deaktiviert, auf denen Desktop Lock installiert ist.
- Workspace für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
- Citrix Workspace-App-Updates können auf LTSR-Updates beschränkt werden.
- Citrix HDX RTME für Windows ist in Citrix Workspace-App-Updates enthalten. Sie erhalten eine Benachrichtigung, wenn HDX RTME-Updates für das LTSR und das aktuelle Release der Citrix Workspace-App verfügbar sind.
- Ab Version 2105 haben die Citrix Workspace-App-Update-Protokolle neue Pfade. Die Workspace Update-Protokolle sind in C:\Program Files(x86)\Citrix\Logs. Informationen zur Protokollierung finden Sie unter [Protokollsammlung](#).
- Nicht-Administratoren können die Citrix Workspace-App auf einer vom Administrator installierten Instanz aktualisieren. Klicken Sie dazu im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Nach Updates suchen**. Die Option **Nach Updates suchen** ist auf vom Benutzer oder vom Administrator installierten Instanzen der Citrix Workspace-App verfügbar.

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

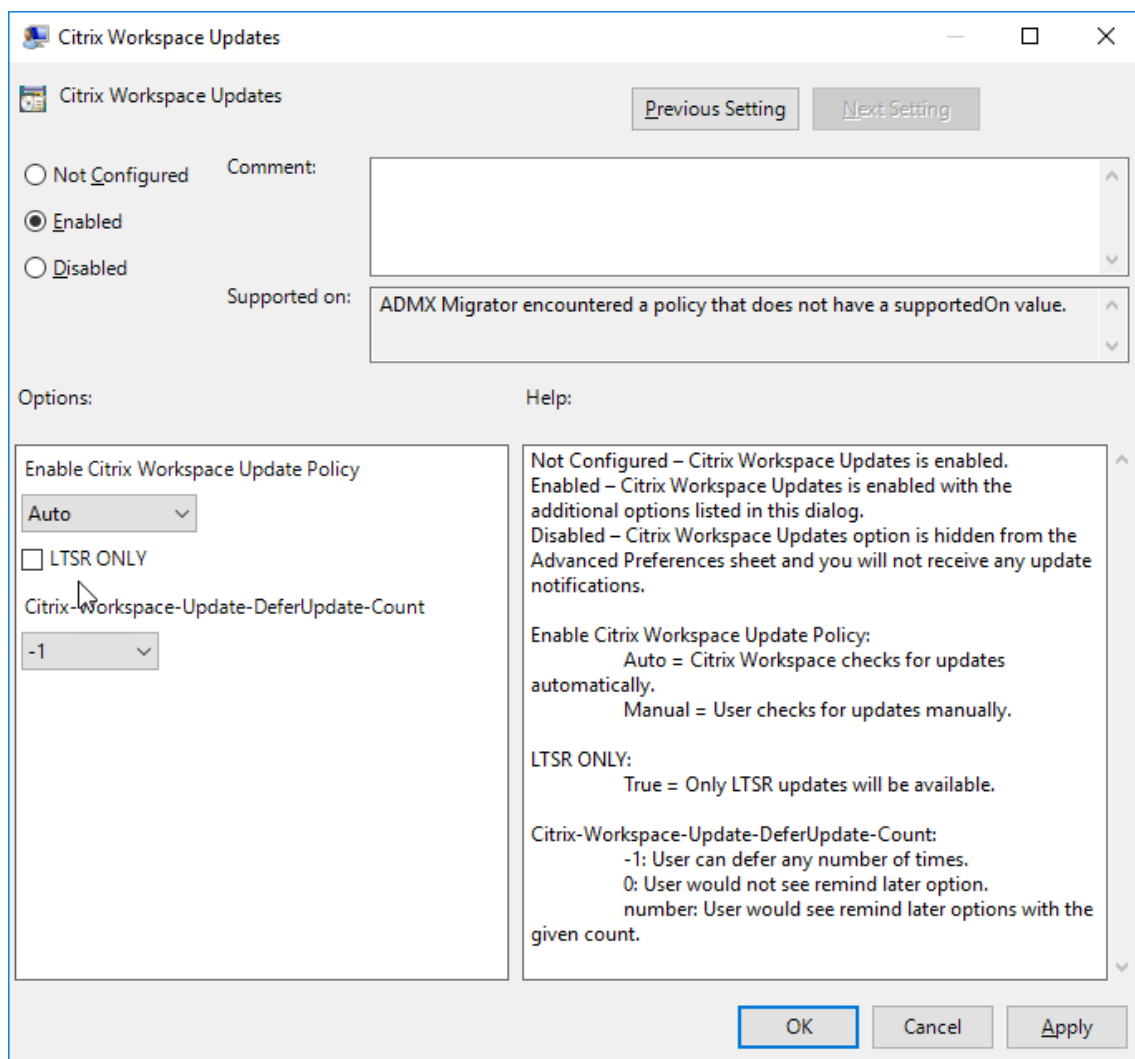
Erweiterte Konfiguration für automatische Updates (Citrix Workspace-Updates)

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

1. Administrative Gruppenrichtlinienobjektvorlage
2. Befehlszeilenoberfläche
3. Grafische Benutzeroberfläche (GUI)
4. StoreFront

Konfigurieren von Citrix Workspace-Updates mit der administrativen Gruppenrichtlinienobjektvorlage

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



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

Hinweis:

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

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

- Auto: Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).

- Manual: Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates.
5. Aktivieren Sie **Nur LTSR**, um Updates nur für LTSR zu erhalten.
 6. Wählen Sie in der Dropdownliste **Citrix-Workspace-Update-DeferUpdate-Count** einen Wert zwischen -1 und 30:
 - Beim Wert 0 wird die Option **Später erinnern** angezeigt. Die Eingabeaufforderung **Update verfügbar** wird angezeigt, wenn bei der automatischen Suche ein Update gefunden wird.
 - Beim Wert -1 wird die Option **Später erinnern** mit der Eingabeaufforderung **Update verfügbar** angezeigt. Sie können die Update-Benachrichtigung beliebig oft verschieben.
 - Der gewählte Wert (1-30) legt fest, wie oft die Option **Später erinnern** mit der Aufforderung **Update verfügbar** angezeigt werden muss. Sie können die Updatebenachrichtigung gemäß dem in diesem Feld definierten Wert verschieben. Die Aufforderung **Update verfügbar** wird zwar weiterhin angezeigt, jedoch ohne die Option **Später erinnern**.

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

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

Set the Delay in Checking for Update

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Options:

Delay Group: Fast (selected), Medium, Slow

Help:

This policy is used to set the preference when the Citrix Workspace-update is rolled-out to the users.

- (fast)- Available updates are rolled-out to the users at the beginning of delivery period.
- (Medium)- Available updates are rolled-out to the users at mid-delivery period
- (Slow)- Available updates are rolled-out to the users at the end of delivery period.

OK Cancel Apply

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

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

Hinweis:

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

Konfigurieren von Citrix Workspace-App-Updates über die Befehlszeilenschnittstelle

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

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

Mit Befehlszeilenparametern nach der Installation der Citrix Workspace-App:

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

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

Beispiel:

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

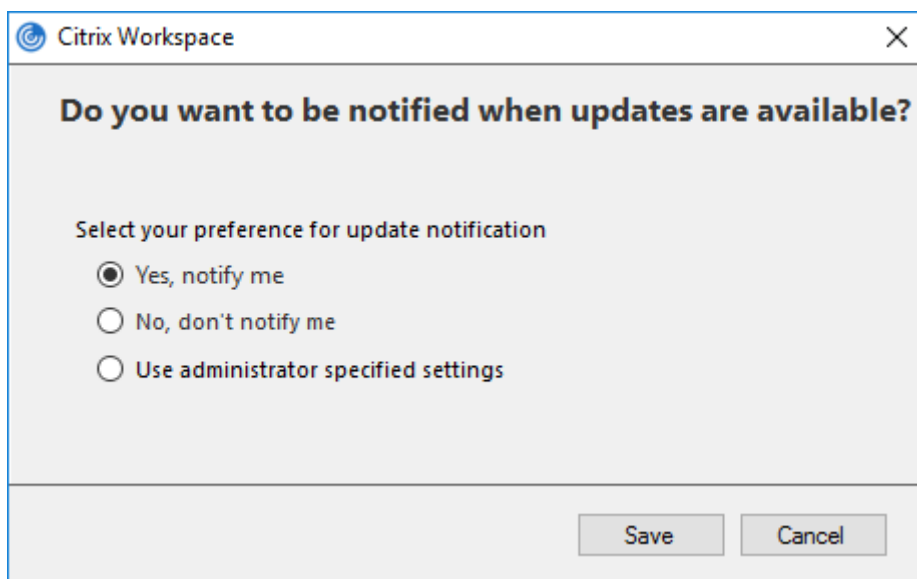
Hinweis:

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

Konfigurieren von Citrix Workspace-Updates über die grafische Benutzeroberfläche

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

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen** > **Citrix Workspace-Updates**.
3. Wählen Sie die Benachrichtigungseinstellung aus und klicken Sie auf **Speichern**.

**Hinweis:**

Sie können die über das Symbol der Citrix Workspace-App verfügbare Seite “Erweiterte Einstellungen” ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

Citrix Workspace-App-Updates mit StoreFront konfigurieren

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

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

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

```
1 <properties>
2     <clear/>
3 </properties>
4 <!--NeedCopy-->
```

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

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
```

```
7      description="" published="true" updaterType="Citrix"
      remoteAccessType="None">
8
9      <annotatedServices>
10
11      <clear />
12
13      <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15      <metadata>
16
17      <plugins>
18
19      <clear />
20
21      </plugins>
22
23      <trustSettings>
24
25      <clear />
26
27      </trustSettings>
28
29      <properties>
30
31      <property name="Auto-Update-Check" value="auto" />
32
33      <property name="Auto-Update-DeferUpdate-Count" value
34      = "1" />
35
36      <property name="Auto-Update-LTSR-Only" value
37      = "FALSE" />
38
39      <property name="Auto-Update-Rollout-Priority" value=
40      "fast" />
41
42      </properties>
43
44      </metadata>
45
46      </annotatedServiceRecord>
47
48      </annotatedServices>
49
50      <metadata>
51
52      <plugins>
53
54      <clear />
55
56      </plugins>
57
58      <trustSettings>
```

```
56
57     <clear />
58
59 </trustSettings>
60
61 <properties>
62
63     <clear />
64
65 </properties>
66
67 </metadata>
68
69 </account>
70
71 <!--NeedCopy-->
```

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

- **Auto-update-Check:** Gibt an, dass die Citrix Workspace-App ein Update automatisch erkennt, wenn es verfügbar ist.
- **Auto-update-LTSR-only:** Gibt an, dass das Update nur für LTSR gilt.
- **Auto-update-Rollout-Priority:** Gibt den Bereitstellungszeitraum an, in dem Sie das Update erhalten können.
- **Auto-update-DeferUpdate-Count:** Gibt an, wie oft Sie die Benachrichtigungen für die Updates ignorieren können.

Erste Schritte

April 22, 2024

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

Voraussetzungen:

Stellen Sie sicher, dass alle im Abschnitt [Systemanforderungen](#) aufgeführten Anforderungen erfüllt sind.

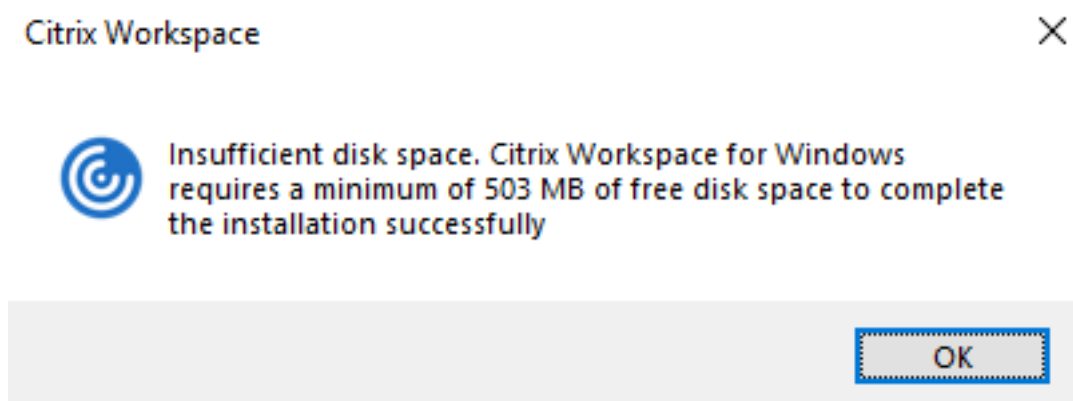
Überprüfen auf freien Speicherplatz

Weitere Informationen zum vor der Installation erforderlichen Speicherplatz finden Sie in der folgenden Tabelle:

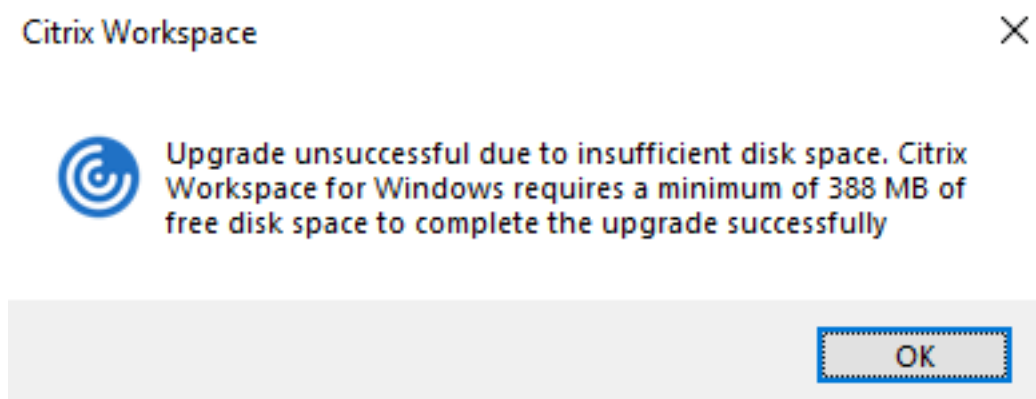
Installationstyp	Mindestens erforderlicher Speicherplatz
Neuinstallation	572 MB
Upgrade	350 MB

Die Citrix Workspace-App prüft, ob genügend Speicherplatz zum Abschließen der Installation verfügbar ist. Die Überprüfung erfolgt sowohl bei einer Neuinstallation als auch bei einem Upgrade.

Wenn bei einer Neuinstallation nicht genügend Speicherplatz vorhanden ist, wird die Installation beendet und das folgende Dialogfeld wird angezeigt:



Wenn bei einem Upgrade der Citrix Workspace-App nicht genügend Speicherplatz vorhanden ist, wird die Installation beendet und das folgende Dialogfeld wird angezeigt:



Hinweis:

- Das Installationsprogramm prüft den verfügbaren Speicherplatz erst, nachdem Sie das Installationspaket extrahiert haben.
- Wenn bei einer automatischen Installation nicht genug Speicherplatz vorhanden ist, wird das Dialogfeld nicht angezeigt, aber die Fehlermeldung wird im Protokoll `CTXInstall\`

`_TrolleyExpress-*.log` aufgezeichnet.

Bevor Sie die Citrix Workspace-App verwenden, müssen Sie Folgendes konfigurieren:

- [StoreFront](#)
- [Citrix Gateway Store](#)
- [Store-URL zur Citrix Workspace-App hinzufügen](#)
- [Clientlaufwerkzuordnung](#)
- [Domain Name Service-Namensauflösung](#)

Administrative Gruppenrichtlinienobjektvorlage

Wir empfehlen die administrative Gruppenrichtlinienobjektvorlage zum Konfigurieren von Regeln für Folgendes:

- Netzwerkrouting
- Proxyserver
- Konfiguration vertrauenswürdiger Server
- Benutzerouting
- Remote-Benutzergeräte
- Benutzererfahrung.

Sie können die Vorlagendateien `receiver.admx` / `receiver.adml` für Domänenrichtlinien und lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Der Import ist nützlich, wenn Sie Citrix Workspace-App-Einstellungen auf mehrere verschiedene Benutzergeräte im Unternehmen anwenden möchten. Wenn Sie nur ein einziges Benutzergerät ändern möchten, importieren Sie die Vorlagendatei mit dem lokalen Gruppenrichtlinien-Editor auf dem Gerät.

Citrix empfiehlt die Verwendung der administrativen Gruppenrichtlinienobjektvorlage von Windows für die Konfiguration der Citrix Workspace-App.

Im Installationsverzeichnis befinden sich die Dateien `CitrixBase.admx` und `CitrixBase.adml` sowie administrative Vorlagendateien (`receiver.adml` oder `receiver.admx`'receiver.adml').

Hinweis:

Die ADMX- und ADML-Dateien dienen zur Verwendung mit Windows Vista, Windows Server 2008 und anderen höheren Versionen von Windows.

Beispiel: `<installation directory>\Online Plugin\Configuration.`

Wird die Citrix Workspace-App ohne den VDA installiert, sind die ADMX/ADML-Dateien normalerweise im Verzeichnis `C:\Program Files\Citrix\ICA Client\Configuration.`

In der folgenden Tabelle finden Sie Informationen zu den Vorlagendateien der Citrix Workspace-App und deren Speicherorten.

Hinweis:

Citrix empfiehlt, dass Sie die GPO-Vorlagendateien verwenden, die mit der aktuellen Version der Citrix Workspace-App bereitgestellt werden.

Dateityp	Dateispeicherort
receiver.adm	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[MUIculture]

Hinweis:

- Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, geht möglicherweise die Richtlinie **ICA-Dateisignierung aktivieren** verloren.
- Fügen Sie beim Upgrade der Citrix Workspace-App dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Frühere Einstellungen werden nach dem Import beibehalten. Weitere Informationen finden Sie im folgenden Verfahren:

Hinzufügen der receiver.admx/adml-Vorlagendateien zum lokalen Gruppenrichtlinienobjekt:

Sie können ADM-Vorlagendateien zum Konfigurieren von lokalen und domänenbasierten Gruppenrichtlinienobjekten verwenden. Weitere Informationen zum Verwalten von ADMX-Dateien finden Sie in [diesem Microsoft MSDN-Artikel](#).

Kopieren Sie nach der Installation der Citrix Workspace-App die folgenden Vorlagendateien:

Dateityp	Kopieren von	Kopieren nach
receiver.admx	Installation Directory\ICA Client\ Configuration\ receiver.admx	%systemroot%\ policyDefinitions
CitrixBase.admx	Installation Directory\ICA Client\ Configuration\ CitrixBase.admx	%systemroot%\ policyDefinitions
receiver.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture]receiver. adml	%systemroot%\ policyDefinitions\ [MUICulture]
CitrixBase.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture] CitrixBase.adml	%systemroot%\ policyDefinitions\ [MUICulture]

Hinweis:

Fügen Sie die Dateien CitrixBase.admx/CitrixBase.adml dem Ordner `\PolicyDefinitions` hinzu, um die Vorlagendateien unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace** anzuzeigen.

StoreFront

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

Hinweis:

Wenn Sie die Option **Alle Stores anzeigen** auswählen, wird möglicherweise die alte StoreFront-Benutzeroberfläche angezeigt.

StoreFront konfigurieren:

Installieren und konfigurieren Sie StoreFront, wie in der [StoreFront-Dokumentation](#) beschrieben. Die Citrix Workspace-App benötigt eine HTTPS-Verbindung. Auf einem HTTP-konfigurierten StoreFront definieren Sie den Registrierungsschlüssel wie unter [Verwenden von Befehlszeilenparametern](#) beschrieben.

Hinweis:

Citrix stellt eine Vorlage bereit, mit der Sie eine Download-Site für die Citrix Workspace-App für Windows erstellen können.

Citrix Gateway Store

Hinzufügen oder Festlegen eines Citrix Gateways mit der administrativen Gruppenrichtlinienobjektvorlage:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **StoreFront**.
3. Wählen Sie **Citrix Gateway-URL\StoreFront-Kontenliste**.
4. Bearbeiten Sie die Einstellungen.
 - Storename: der angezeigte Name des Stores
 - Store-URL: die URL des Stores
 - #Storename: der Name des Stores hinter dem Citrix Gateway
 - Storeaktivierungszustand: der Zustand des Stores (Ein oder Aus)
 - Storebeschreibung: eine Beschreibung des Stores
5. Fügen Sie die Citrix Gateway-URL hinzu oder geben Sie sie ein. Geben Sie den Namen der URL durch Semikolon getrennt ein:

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

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

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

Hinweis:

Bei der Neuinstallation der Citrix Workspace-App Version 1808 und höher ist ein Zurücksetzen

nicht erforderlich. Bei Upgrades auf Version 1808 oder höher müssen Sie die Citrix Workspace-App zurücksetzen, damit die Änderungen wirksam werden.

Einschränkungen:

- Die Citrix Gateway-URL muss als Erste aufgeführt werden, gefolgt von den StoreFront-URLs.
- Mehrere Citrix Gateway-URLs werden nicht unterstützt.
- Eine mit dieser Methode konfigurierte Citrix Gateway-URL unterstützt nicht die PNA-Dienst-Site hinter Citrix Gateway.

Wiederverbindung über Workspace Control verwalten

Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt. Beispielsweise können Krankenhausärzte mit Workspace Control von einer Arbeitsstation zu einer anderen wechseln, ohne ihre Anwendungen auf jedem einzelnen Gerät neu starten zu müssen. In der Citrix Workspace-App können Sie Workspace Control auf Clientgeräten durch Ändern der Registrierung verwalten. Für domänengebundene Clientgeräte können Sie für Workspace Control auch die Gruppenrichtlinie verwenden.

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Erstellen Sie **WSCReconnectModeUser** und ändern Sie den vorhandenen Registrierungsschlüssel **WSCReconnectMode** im Masterdesktopimage oder auf dem Citrix Virtual Apps-Server. Der veröffentlichte Desktop kann das Verhalten der Citrix Workspace-App ändern.

WSCReconnectMode-Schlüsseleinstellungen für die Citrix Workspace-App:

- 0 = keine Wiederverbindung mit vorhandenen Sitzungen
- 1 = Wiederverbindung bei Anwendungsstart
- 2 = Wiederverbindung bei Anwendungsaktualisierung
- 3 = Wiederverbindung bei Anwendungsstart oder Anwendungsaktualisierung
- 4 = Wiederverbindung beim Öffnen der Citrix Workspace-Benutzeroberfläche
- 8 = Wiederverbindung beim Anmelden an Windows
- 11 = Kombination von 3 und 8

Workspace Control deaktivieren Erstellen Sie den folgenden Schlüssel, um Workspace Control zu deaktivieren:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 Bit)

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle (32-Bit)

Name: **WSCReconnectModeUser**

Typ: REG_SZ

Wertdaten: 0

Ändern Sie den folgenden Schlüssel vom Standardwert 3 auf 0

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 Bit)

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectMode**

Typ: REG_SZ

Wertdaten: 0

Hinweis:

Wenn Sie keinen Schlüssel erstellen möchten, können Sie auch den Schlüssel **WSCReconnectAll** auf "false" festlegen.

Ändern des Timeouts der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird. Um den Timeoutzeitraum zu ändern, erstellen Sie einen REG_DWORD-Wert **SI_INACTIVE_MS** in **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA_CLIENT\Engine**. Sie können den REG_DWORD-Wert auf 4 festlegen, wenn die Statusanzeige eher ausgeblendet werden soll.

Anpassen des Speicherorts für Anwendungsverknüpfungen über die Befehlszeile

Über die Integration in das Startmenü und den Nur-Desktopverknüpfungsmodus können Sie Verknüpfungen für veröffentlichte Anwendungen im **Windows-Startmenü** oder auf dem Windows-Desktop platzieren. Benutzer müssen Anwendungen nicht über die Citrix Workspace-Benutzeroberfläche abonnieren. Die Integration in das Startmenü und die Verwaltung von Desktopverknüpfungen bieten eine nahtlose Desktopeinfahrung für Benutzergruppen. Dies gilt auch für Benutzer, die einen gleichförmigen Zugriff auf einen bestimmten Anwendungssatz benötigen.

Das Flag heißt **SelfServiceMode** und ist standardmäßig auf **True** festgelegt. Wenn der Administrator das Flag **SelfServiceMode** auf **False** festlegt, können Sie nicht auf die Self-Service-Benutzeroberfläche zugreifen. Der Zugriff auf abonnierte Apps ist stattdessen über das Startmenü und über Desktopverknüpfungen möglich. Dies wird als Nur-Verknüpfungsmodus bezeichnet.

Benutzer und Administratoren können das Einrichten von Verknüpfungen über mehrere Registrierungseinstellungen anpassen.

Arbeiten mit Verknüpfungen

- Benutzer können Apps nicht entfernen. Alle Apps sind verbindlich, wenn das Flag **SelfServiceMode** auf "false" festgelegt ist (= Nur-Verknüpfungsmodus). Wenn Sie ein Verknüpfungssymbol vom Desktop entfernen, wird das Symbol wieder angezeigt, sobald der Benutzer über das Citrix Workspace-App-Symbol im Infobereich die Option **Aktualisieren** auswählt.
- Benutzer können nur einen Store konfigurieren. Die Optionen "Konto" und "Einstellungen" sind nicht verfügbar, damit der Benutzer keine weiteren Stores konfiguriert. Der Administrator kann einem Benutzer besondere Privilegien zum Hinzufügen mehrerer Konten erteilen, indem er die Gruppenrichtlinienobjektvorlage verwendet. Administratoren können auch spezielle Berechtigungen bereitstellen, indem sie manuell den Registrierungsschlüssel "HideEditStoresDialog" auf der Clientmaschine hinzufügen. Wenn der Administrator einem Benutzer dieses Privileg erteilt, steht diesem die Option "Einstellungen" im Infobereich zur Verfügung, mit der er Konten hinzufügen und entfernen kann.
- Benutzer können Apps nicht über die **Windows-Systemsteuerung** entfernen.
- Sie können Desktopverknüpfungen über eine anpassbare Registrierungseinstellung hinzufügen. Desktopverknüpfungen werden nicht standardmäßig hinzugefügt. Starten Sie nach dem Bearbeiten der Registrierungseinstellungen die Citrix Workspace-App neu.
- Verknüpfungen werden im Startmenü standardmäßig mit einem Kategoriepfad erstellt: UseCategoryAsStartMenuPath.

Hinweis:

In Windows 8/8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder unter dem Stammordner angezeigt. Sie werden jedoch nicht in den mit Citrix Virtual Apps definierten Unterordnern für Kategorien angezeigt.

- Sie können während der Installation das Flag [/DESKTOPDIR="Dir_name"] hinzufügen, um alle Verknüpfungen in einem Ordner zusammenzufassen. CategoryPath wird für Desktopverknüpfungen unterstützt.
- Die automatische Neuinstallation geänderter Apps ist ein Feature, das über den Registrierungsschlüssel **AutoReInstallModifiedApps** aktiviert werden kann. Wenn

`AutoReInstallModifiedApps` aktiviert ist, werden alle auf dem Server durchgeführten Änderungen an Attributen veröffentlichter Anwendungen und Desktops auf der Clientmaschine angezeigt. Wenn `AutoReInstallModifiedApps` deaktiviert ist, werden Attribute von Anwendungen und Desktops nicht aktualisiert und gelöschte Verknüpfungen werden auf dem Client bei einer Aktualisierung nicht wiederhergestellt. Standardmäßig ist `AutoReInstallModifiedApps` aktiviert.

Anpassen des Speicherorts für Anwendungsverknüpfungen über den Registrierungs-Editor

Hinweis:

- Standardmäßig verwenden Registrierungsschlüssel das Format **Zeichenfolge**.
- Ändern Sie Registrierungsschlüssel, bevor Sie einen Store konfigurieren. Wenn Sie oder ein Benutzer die Registrierungsschlüssel anpassen möchten, müssen Sie oder der Benutzer folgende Schritte ausführen:
 1. Setzen Sie die Citrix Workspace-App zurück.
 2. Konfigurieren Sie die Registrierungsschlüssel.
 3. Konfigurieren Sie dann den Store neu.

Registrierungsschlüssel für 32-Bit-Maschinen

Registrierungsschlüssel: `WCSupported` **Wert:** `True`

Schlüsselpfad:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID + \Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

Registrierungsschlüssel: `WSCReconnectAll` **Wert:** `True`

Schlüsselpfad:

```
1 - `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
2 - `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID + \Properties`
3 - `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
4 - `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`
```

Registrierungsschlüssel: `WSCReconnectMode` **Wert:** `3`

Schlüsselpfad:

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Registrierungsschlüssel: WSCReconnectModeUser Wert: Registrierung während der Installation nicht erstellt.

Schlüsselpfad:

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Registrierungsschlüssel für 64-Bit-Maschinen:

Registrierungsschlüssel: WSCSupported Wert: True

Schlüsselpfad:

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Registrierungsschlüssel: WSCReconnectAll Wert: True

Schlüsselpfad:

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Registrierungsschlüssel: WSCReconnectMode Wert: 3

Schlüsselpfad:

- 1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
- 2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties

```
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Registrierungsschlüssel: WSCReconnectModeUser **Wert:** Registrierung während der Installation nicht erstellt.

Schlüsselpfad:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Benutzerkonten

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

- Konfigurieren der e-mail-basierten Kontenermittlung
- Provisioningdatei
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

Wichtig

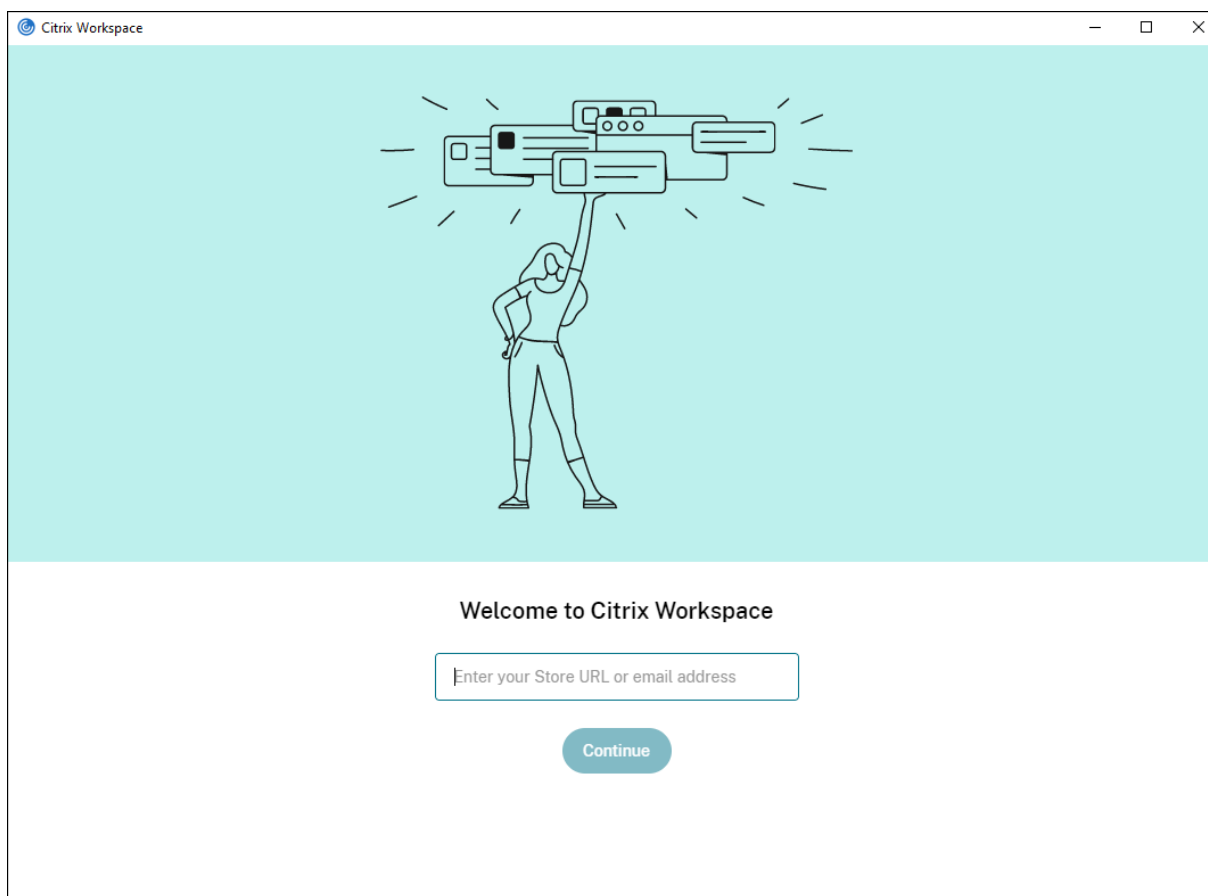
Citrix empfiehlt, die Citrix Workspace-App nach der Installation neu zu starten.

- Ein Neustart stellt sicher, dass Benutzer Konten hinzufügen können.
- Die Citrix Workspace-App kann zudem USB-Geräte erkennen, die während der Installation im ausgesetzten Zustand waren.

Die erfolgreiche Installation wird in einem Dialogfeld bestätigt. Danach wird der Bildschirm **Konto hinzufügen** angezeigt. Als Erstbenutzer müssen Sie im Dialogfeld **Konto hinzufügen** eine E-Mail- oder eine Serveradresse eingeben, um ein Konto einzurichten.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

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



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

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

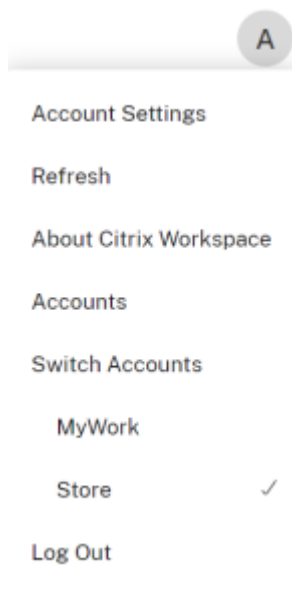
CitrixGatewayFQDN?MyStoreName:

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

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

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

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



Konfigurieren der e-mail-basierten Kontenermittlung

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

Weitere Informationen finden Sie unter [Konfigurieren der e-mail-basierten Kontenermittlung](#).

Bereitstellen von Provisioningdateien für Benutzer

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

Sie können mit StoreFront Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, um eine automatische Konfiguration

der Citrix Workspace-App zu ermöglichen. Nach der Installation der Citrix Workspace-App öffnen Benutzer einfach die Datei, um die App zu konfigurieren. Wenn Sie Workspace für Web konfigurieren, können Benutzer auch Provisioningdateien für die Citrix Workspace-App von den Sites abrufen.

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

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

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

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


CitrixGatewayFQDN?MyStoreName:

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

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

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

Wenn ein Benutzer Angaben für ein neues Konto macht, versucht die Citrix Workspace-App, die Verbindung zu überprüfen. Im Erfolgsfall fordert die Citrix Workspace-App den Benutzer auf, sich bei dem Konto anzumelden.

Öffnen Sie zur Verwaltung von Konten die Homepage der Citrix Workspace-App, klicken Sie auf den  und dann auf **Konten**.

Automatisches Freigeben von mehreren Store-Konten

Warnung

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

Wenn Sie mehrere Store-Konten haben, können Sie die Citrix Workspace-App für Windows so konfigurieren, dass beim Erstellen einer Sitzung automatisch Verbindungen zu allen Konten hergestellt werden. Automatisches Anzeigen aller Konten beim Öffnen der Citrix Workspace-App:

32-Bit-Systeme:

Schlüsselpfad: `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`

Schlüsselname: `CurrentAccount`

Wert: `AllAccount`

Typ: REG_SZ

64-Bit-Systeme:

Schlüsselpfad: `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle`

Schlüsselname: `CurrentAccount`

Wert: `AllAccount`

Typ: REG_SZ

Clientlaufwerkzuordnung

Die Citrix Workspace-App für Windows unterstützt die Gerätezuordnung auf Benutzergeräten, sodass sie in einer Sitzung zur Verfügung stehen. Benutzer haben folgende Möglichkeiten:

- Zugreifen auf lokale Laufwerke, Drucker und COM-Ports
- Ausschneiden und Einfügen zwischen der Sitzung und der lokalen Windows-Zwischenablage
- Wiedergeben von Audiodateien (Systemklänge und WAV-Dateien), die in der Sitzung abgespielt werden

Während der Anmeldung informiert die Citrix Workspace-App den Server über die verfügbaren Clientlaufwerke, COM- und LPT-Ports. Standardmäßig werden Clientlaufwerke Serverlaufwerksbuchstaben

zugeordnet. Für Clientdrucker werden Druckerwarteschlangen erstellt, sodass die Clientdrucker direkt mit der Sitzung verbunden zu sein scheinen. Diese Zuordnungen stehen nur dem aktuellen Benutzer während der aktuellen Sitzung zur Verfügung. Sie werden bei der Abmeldung des Benutzers gelöscht und bei seiner nächsten Anmeldung neu erstellt.

Mit den Einstellungen der Richtlinie für die Umleitung können Sie Benutzergeräte zuordnen, die nicht automatisch bei der Anmeldung zugeordnet werden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

Deaktivieren von Benutzergerätozuordnungen

Sie können die Benutzergerätozuordnung einschließlich Optionen für Laufwerke, Drucker und Ports mit dem **Windows-Servermanager** einstellen. Weitere Informationen über verfügbare Optionen finden Sie in der Dokumentation zu den Remotedesktopdiensten.

Umleiten von Clientordnern

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wenn auf dem Server nur die Clientlaufwerkzuordnung aktiviert ist, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner (und nicht das komplette Dateisystem auf dem Benutzergerät) werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt. Weitere Informationen, u. a. zur Konfiguration der Umleitung von Clientordnern für Benutzergeräte, finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

Zuordnen von Clientlaufwerken zu serverseitigen Laufwerksbuchstaben

Durch die Clientlaufwerkzuordnung werden Laufwerksbuchstaben auf der Hostseite auf Laufwerke umgeleitet, die auf dem Benutzergerät vorhanden sind. Beispiel: In einer Citrix Benutzersitzung kann das Laufwerk H dem Laufwerk C auf dem Benutzergerät, auf dem die Citrix Workspace-App für Windows ausgeführt wird, zugeordnet werden.

Die Clientlaufwerkzuordnung ist in die Standardfunktionen von Citrix zur Geräteumleitung integriert. Im Dateimanager, Windows Explorer und in den Anwendungen werden diese Zuordnungen genauso wie andere Netzwerkzuordnungen angezeigt.

Der Server, auf dem virtuelle Desktops und Anwendungen ausgeführt werden, kann während der Installation so konfiguriert werden, dass Clientlaufwerke automatisch einem festgelegten Satz von Laufwerksbuchstaben zugeordnet werden. In der Standardinstallation werden Laufwerksbuchstaben angefangen mit V und dann absteigend Clientlaufwerksbuchstaben zugeordnet. Ein Laufwerksbuchstabe wird jeder Festplatte und jedem CD-ROM-Laufwerk zugeordnet. (Diskettenlaufwerken werden die vorhandenen Laufwerksbuchstaben zugewiesen.) Diese Methode ergibt die folgenden Laufwerkzuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Zugriff vom Server möglich als
A	A
B	B
C	V
D	U

Der Server kann so konfiguriert werden, dass zwischen den Laufwerksbuchstaben des Servers und des Clients keine Konflikte entstehen. Dazu werden die Laufwerksbuchstaben des Servers in höhere Laufwerksbuchstaben geändert.

Im folgenden Beispiel werden die Serverlaufwerke C und D in M und N geändert, sodass Clientgeräte direkt auf ihre Laufwerke C und D zugreifen können. Diese Methode führt zu den folgenden Laufwerkzuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Zugriff vom Server möglich als
A	A
B	B
C	C
D	D

Der Laufwerksbuchstabe, durch den das Serverlaufwerk C ersetzt wird, wird während des Setups festgelegt. Alle anderen Festplatten- und CD-Laufwerksbuchstaben werden durch aufeinander folgende Laufwerksbuchstaben ersetzt (zum Beispiel: C > M, D > N, E > O). Bei diesen Laufwerksbuchstaben darf es keine Konflikte mit bereits existierenden Laufwerkszuordnungen im Netzwerk geben. Wenn Sie das Netzlaufwerk einem bereits vorhandenen Laufwerksbuchstaben eines Servers zuordnen, ist die Netzlaufwerkzuordnung ungültig.

Beim Verbinden eines Benutzergeräts mit einem Server werden die Clientzuordnungen wiederhergestellt, sofern die automatische Clientgerätszuordnung nicht deaktiviert ist. Die Clientlaufwerkzuordnung ist standardmäßig aktiviert. Sie können die Einstellungen mit dem Konfigurationstool

der Remotedesktopdienste (Terminaldienste) ändern. Außerdem können Sie mit Richtlinien genauer steuern, wie die Clientgerätszuordnung angewendet wird. Weitere Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

HDX Plug-n-Play-USB-Geräteumleitung

Die HDX Plug-n-Play USB-Geräteumleitung ermöglicht die dynamische Umleitung von Mediengeräten zum Server. Mediengeräte können Kameras, Scanner, Mediaplayer und POS-Geräte sein. Sie oder der Benutzer können die Umleitung auf einige oder alle Geräte beschränken. Bearbeiten Sie die Richtlinien auf dem Server oder wenden Sie Gruppenrichtlinien auf dem Benutzergerät an, um die Einstellungen für die Umleitung zu konfigurieren. Weitere Informationen finden Sie unter [Überlegungen zu USB und Clientlaufwerk](#) in der Citrix Virtual Apps and Desktops-Dokumentation.

Wichtig

Wenn Sie die USB-Geräteumleitung für Plug & Play-Geräte in einer Serverrichtlinie verbieten, kann der Benutzer diese Richtlinieneinstellung nicht außer Kraft setzen.

Ein Benutzer kann Berechtigungen in der Citrix Workspace-App festlegen, um die Geräteumleitung immer oder nie zuzulassen, oder bei jedem angeschlossenen Gerät benachrichtigt werden. Diese Einstellung wirkt sich nur auf Geräte aus, die eingesteckt werden, nach dem der Benutzer die Einstellung geändert hat.

Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port:

Mit der Client-COM-Portzuordnung können Geräte, die an COM-Ports des Benutzergeräts angeschlossen sind, in Sitzungen verwendet werden. Diese Zuordnungen können in gleicher Weise wie andere Netzwerkzuordnungen verwendet werden.

Sie können Client-COM-Ports von der Befehlszeile aus zuordnen. Sie können auch die Client-COM-Portzuordnung vom Remotedesktop-Konfigurationstool (Terminaldienste) oder mit Richtlinien steuern. Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

Wichtig

Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel.

1. Aktivieren Sie für Citrix Virtual Apps and Desktops-Bereitstellungen die Richtlinieneinstellung "Client-COM-Portumleitung".
2. Melden Sie sich bei der Citrix Workspace-App an.
3. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
net use comx: \\client\comz:
```

Wobei:

- x ist die Nummer des COM-Ports auf dem Server (Ports 1 bis 9 stehen für die Zuordnung zur Verfügung).
- z ist die Nummer des Client-COM-Ports, den Sie zuordnen möchten.

4. Geben Sie zur Bestätigung des Vorgangs

```
net use
```

Die Eingabeaufforderung enthält zugeordnete Laufwerke, LPT-Ports und zugeordnete COM-Ports.

Installieren Sie das Gerät für den zugeordneten Namen, um diesen COM-Port in einem virtuellen Desktop oder einer Anwendung zu verwenden. Wenn Sie beispielsweise den Port COM1 auf dem Client dem Port COM5 auf dem Server zuordnen, installieren Sie das COM-Portgerät in der Sitzung auf COM5. Verwenden Sie diesen zugeordneten COM-Port dann wie einen COM-Port auf dem Benutzergerät.

Domain Name Service-Namensauflösung

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

Wichtig:

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

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

Deaktivieren der DNS-Namensauflösung für bestimmte Benutzergeräte:

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

Achtung

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

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

Benutzerdefinierte Webstores

Mit diesem Feature können Sie über die Citrix Workspace-App für Windows auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Um dieses Feature zu verwenden, muss der Administrator die Domäne oder den benutzerdefinierten Webstore zu den zulässigen URLs im Global App Configuration Service hinzufügen.

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

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

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

Konfigurieren

May 23, 2024

Wenn Sie die Citrix Workspace-App für Windows verwenden, ermöglichen die folgenden Konfigurationen den Zugriff auf gehostete Anwendungen und Desktops.

Microsoft Teams

- [Bildschirmfreigabe](#)
- [Geschätzte Codierungsleistung](#)
- [Akustische Echounterdrückung](#)

Bildschirmfreigabe

Ab Version 2006.1 sind für Microsoft Teams mit verwendeter HDX-Optimierung neue Funktionen für das Feature zur Freigabe des eigenen Bildschirms verfügbar.

Die Inhalte, die mit Microsoft Teams freigegeben werden, sind auf den Inhalt des **Desktop Viewer**-Fensters beschränkt. Bereiche außerhalb des **Desktop Viewer**-Fensters (lokaler Clientdesktop, Apps) sind ausgeblendet.

In Windows 10 werden die folgenden Elemente nicht ausgeblendet, wenn sie das **Desktop Viewer**-Fenster überlappen:

- Startmenü, Suchmenü und Aufgabenansicht.
- Benachrichtigungsleiste und Benachrichtigungen, die auf der rechten Seite der Taskleiste angezeigt werden.
- Bei einer Konfiguration mit mehreren Monitoren und unterschiedlichen DPI-Einstellungen. Wenn eine lokale App zwei verschiedene Monitore überlappt und die DPI-Einstellung nicht mit dem DPI-Wert des Hauptmonitors übereinstimmt, der das Desktop Viewer-Fenster aufweist.
- App und Vorschau, die angezeigt werden, wenn Sie mit der Maus auf das Symbol der App in der Taskleiste zeigen.

Geschätzte Codierungsleistung

`HdxRtcEngine.exe` ist die WebRTC Media Engine, die in die Citrix Workspace-App eingebettet ist und die Microsoft Teams-Umleitung verarbeitet. Ab Citrix Workspace-App 1912 kann `HdxRtcEngine.exe` die beste Codierungsauflösung schätzen, die die CPU des Endpunkts ohne Überlastung aufrechterhalten kann. Mögliche Werte sind 240p, 360p, 480p, 720p und 1080p.

Diese Schätzung der Endpunktleistung (auch `webrtcapi.EndpointPerformance` genannt) läuft, wenn `HdxTeams.exe` initialisiert wird. Der Macroblock-Code bestimmt die beste Auflösung, die bei dem 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
Schnell	1080p (1920x1080 16:9 @ 30 F/s)	3
Mittel	720p (1280x720 16:9 @ 30 F/s)	2

Endpunktleistung	Maximale Auflösung	Registrierungsschlüsselwert
Langsam	360p (entweder 640x360 16:9 bei 30 F/s oder 640x480 4:3 bei 30 F/s)	1
Sehr langsam	240p (entweder 320x180 16:9 bei 30 F/s oder 320 x 240 4:3 bei 30 F/s)	0

Registrierungspfad in der Citrix Workspace-App:

Navigieren Sie zum Registrierungspfad HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream, und erstellen Sie folgenden Schlüssel:

Name	Typ	Werte	Beschreibung
OverridePerformance	DWORD	0;1;2;3	Erzwingen Sie die gewünschte Leistung. Der Wert muss zwischen 0 und 3 liegen, wobei 0 für "Langsam" und 3 für "Schnell" steht.

Weitere Informationen zur Optimierung von Microsoft Teams finden Sie unter [Optimierung für Microsoft Teams](#).

Akustische Echounterdrückung

Die Echounterdrückung in `HdxRtcEngine.exe` kann deaktiviert werden, um Probleme mit der Audioleistung oder der Kompatibilität mit Peripheriegeräten zu beheben, die über integrierte AEC-Funktionen verfügen.

Navigieren Sie zum Registrierungspfad HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream, und erstellen Sie folgenden Schlüssel:

Name: EnableAEC

Typ: REG_DWORD

Data: 0

(0 deaktiviert AEC. 1 aktiviert AEC. Ohne [Regkey](#) wird AEC in HdxRtcEngine standardmäßig aktiviert, unabhängig von den Hardwarefunktionen des Peripheriegeräts.)

Erweiterungen für die Microsoft Teams-Optimierung

- Ab Citrix Workspace-App 2112.1 für Windows sind die folgenden Features nur nach Rollout eines zukünftigen Updates von Microsoft Teams verfügbar.

Wenn das Update von Microsoft veröffentlicht wurde, finden Sie im Knowledge Center-Artikel [CTX253754](#) Informationen über das Dokumentationsupdate und die Ankündigung.

- **Chats und Besprechungen mit mehreren Fenstern in Microsoft Teams:** Sie können mehrere Fenster für Chats und Besprechungen in Microsoft Teams (1.4.00.16771 oder höher) nutzen, wenn die HDX-Optimierung in Citrix Virtual Apps and Desktops (2112 oder höher) verwendet wird. Das Fenster-Pop-Out ist auf verschiedenerelei Art möglich. Einzelheiten zum Ausklappen von Fenstern finden Sie unter [Microsoft Teams Pop-Out Window for Chats and Meetings](#) auf der Microsoft Office 365-Website.

Benutzer älterer Versionen der Citrix Workspace-App oder des Virtual Delivery Agent (VDA) sollten bedenken, dass Microsoft den Einzelfenstercode künftig nicht mehr unterstützen könnte. Sobald das Feature jedoch global verfügbar ist, haben Sie neun Monate Zeit für ein Upgrade auf eine VDA- bzw. Citrix Workspace-App-Version, die mehrere Fenster unterstützt (2112 und höher).

- **App-Freigabe:** Bisher konnten Apps nicht per **Bildschirmfreigabe** in Microsoft Teams freigegeben werden, wenn die HDX 3D Pro-Richtlinie in Citrix Studio aktiviert war. Ab Citrix Workspace-App 2112.1 für Windows bzw. Citrix Virtual Apps and Desktops 2112 können Sie Apps über das Feature **Bildschirmfreigabe** in Microsoft Teams freigeben. Sie können eine App freigeben, wenn die HDX 3D Pro-Richtlinie aktiviert ist.
- **Steuerung übergeben:** Über die 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. Sowohl Sie als auch der Teilnehmer können den freigegebenen Bildschirm jetzt steuern und Sie können die Kontrolle jederzeit zurückfordern.
- **Kontrolle übernehmen:** 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.

Einschränkung:

Während eines Peer-zu-Peer-Anrufs 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:** Die Citrix Workspace-App unterstützt den dynamischen Notruf. Wenn Sie Microsoft-Anrufpläne, Operator Connect und Direct Routing verwenden, haben Sie folgende Möglichkeiten:

- * Konfiguration und Übermittlung von Notrufen
- * Benachrichtigung von Sicherheitspersonal

Die Benachrichtigung erfolgt basierend auf dem aktuellen Standort der Citrix Workspace-App auf dem Endpunkt anstelle des Microsoft Teams-Clients auf dem VDA.

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.

- Ab Citrix Workspace-App 2109.1 für Windows sind die folgenden Features nur nach Rollout eines zukünftigen Updates von Microsoft Teams verfügbar.

Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

- **Unterstützung für WebRTC:** Die Citrix Workspace-App 2109.1 für Windows unterstützt WebRTC 1.0, um eine bessere Videokonferenzenerfahrung und Katalogansicht zu bieten.
- **Verbesserung der Bildschirmfreigabe:** Mit dem Feature für die Bildschirmfreigabe in Microsoft Teams können Sie einzelne Anwendungen, Fenster oder den Vollbildschirm freigeben. Citrix Virtual Delivery Agent 2109 ist eine Voraussetzung für dieses Feature.
- **Kompatibilität von App Protection:** Wenn App Protection aktiviert ist, können Sie jetzt Inhalte über Microsoft Teams mit HDX-Optimierung teilen. Mit diesem Feature können Sie ein Anwendungsfenster freigeben, das auf dem virtuellen Desktop ausgeführt wird. Citrix Virtual Delivery Agent 2109 ist eine Voraussetzung für dieses Feature.

Hinweis:

Bei aktiviertem App Protection für die Bereitstellungsgruppe ist die vollständige Monitor- oder Desktop-Freigabe deaktiviert.

- **Liveuntertitel:** Die Citrix Workspace-App 2109.1 für Windows unterstützt die Echtzeittranskription dessen, was ein Sprecher sagt, wenn Liveuntertitel in Microsoft Teams aktiviert sind.
- Die Citrix Workspace-App 2109.1 für Windows unterstützt folgende Funktionen bei optimiertem Microsoft Teams auf VM-gehosteten Apps:

- - * Peer-to-Peer-Audio- und Videoanrufe
 - * Telefonkonferenz
 - * Bildschirmfreigabe
- Folgendes gilt ab Citrix Workspace-App 2106 für Windows:
 - 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 der Bildschirme zur Freigabe auswählen. Wenn der Desktop Viewer den Fenstermodus ändert (maximieren, wiederherstellen oder minimieren), wird die Bildschirmfreigabe beendet.
- Folgendes gilt ab Citrix Workspace-App 2105 für Windows:
 - Sie können eine bevorzugte Netzwerkschnittstelle für den Medienverkehr konfigurieren. Navigieren Sie zu `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` und erstellen Sie einen Schlüssel mit dem Namen `NetworkPreference(REG_DWORD)`. Wählen Sie einen der folgenden Werte aus:
 - * 1: Ethernet
 - * 2: Wi-Fi
 - * 3: Cellular
 - * 5: Loopback
 - * 6: AnyStandardmäßig und wenn kein Wert festgelegt ist, wählt die WebRTC Media Engine die beste verfügbare Route aus.
 - Sie können das Audiogerätemodul 2 (ADM2) deaktivieren, sodass das Legacy-Audiogerätemodul (ADM) für 4-Kanal-Mikrofone verwendet wird. Das Deaktivieren von ADM2 hilft bei Problemen im Zusammenhang mit Mikrofonen in einem Anruf. Um ADM2 zu deaktivieren, navigieren Sie zu `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, erstellen Sie einen Schlüssel namens `DisableADM2(REG_DWORD)` und legen Sie den Wert auf 1 fest.
- Folgendes gilt ab Citrix Workspace-App 2103.1 für Windows:
 - Der VP9-Videocodec ist jetzt standardmäßig deaktiviert.
 - Verbesserte Konfigurationen mit Echounterdrückung, automatischer Verstärkungsregelung, Rauschunterdrückung: Wenn diese Optionen in Microsoft Teams konfiguriert sind, übernimmt das von Citrix umgeleitete Microsoft Teams die konfigurierten Werte. Andernfalls sind diese Optionen auf **Wahr** voreingestellt.

- **DirectWShow** ist jetzt der Standardrenderer.

Mit folgender Schrittfolge können Sie den Standardrenderer ändern:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zum folgenden Schlüssel Speicherort: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
3. Aktualisieren Sie den folgenden Wert: "`UseDirectShowRendererAsPrimary`"
`=dword:00000000`

Andere mögliche Werte:

- * 0: Media Foundation
- * 1: DirectShow (Standard)

4. Starten Sie die Citrix Workspace-App neu.

- Folgendes gilt ab Citrix Workspace-App 2012 für Windows:
 - Peers können jetzt den Mauszeiger des Referenten in einer Bildschirmfreigabe sehen.
 - Die **WebRTC** Media Engine beachtet jetzt den auf dem Clientgerät konfigurierten Proxyserver.
- Folgendes gilt ab Citrix Workspace-App 2009.6 für Windows:
 - Microsoft Teams zeigt zuvor verwendete Peripheriegeräte in der Liste **Bevorzugte Geräte** an.
 - Die **WebRTC** Media Engine bestimmt die an einem Endpunkt maximal mögliche Codierungsauflösung genau. Die **WebRTC** Media Engine schätzt mehrfach am Tag und nicht nur beim ersten Start.
 - Das Installationspaket der Citrix Workspace-App enthält die Klingeltöne von Microsoft Teams.
 - Verbesserungen bei Echounterdrückung - Reduzierter Echopegel, wenn ein Peer über einen Lautsprecher oder ein Mikrofon verfügt, der/das ein Echo erzeugt.
 - Verbesserungen bei der Bildschirmübertragung - Wenn Sie Ihren Bildschirm freigeben, wird nur der **Desktop Viewer**-Bildschirm im nativen Bitmap-Format erfasst. Zuvor waren lokale Clientfenster, die das Fenster des **Desktop Viewer** überlagerten, ausgeblendet.
- Folgendes gilt ab Citrix Workspace-App 2002 für Windows:
 - Wenn Sie Ihren Workspace in Microsoft Teams freigeben, wird in der Citrix Workspace-App der aktuell freigegebene Bildschirmbereich mit einem roten Rahmen markiert. Sie können nur das **Desktop Viewer**-Fenster oder ein beliebiges lokales Fenster darüber freigeben. Wenn Sie das **Desktop Viewer**-Fenster minimieren, wird die Bildschirmfreigabe angehalten.

Administratortaufgaben und -überlegungen

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

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](#). Mit dieser Liste können Sie sicherstellen, dass Ihre Firewallkonfigurationen automatisch anhand der Infrastrukturupdates aktualisiert werden. Einzelheiten zum Status der Änderungen der Infrastruktur finden Sie auf der [Statusseite von LaunchDarkly](#).

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

- LaunchDarkly-Dienst.
- APNs-Listenerdienst

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

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

Sie können den LaunchDarkly-Dienst auch über die Registrierung deaktivieren.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie auf einer 64-Bit-Maschine zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix` und auf einer 32-Bit-Maschine zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
3. Erstellen Sie eine Registrierungszeichenfolge REG_SZ mit dem Namen **EnableLDFeature** und fügen Sie sie hinzu. Legen Sie ihren Wert auf **False** fest.
4. Beenden und starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

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.

App Protection (App-Schutz) ist ein Zusatzfeature, das erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) bietet. Sie verringert das Risiko, dass Clients Keylogging und Screenshot-Malware zulassen. App Protection verhindert das Exfiltrieren von Benutzeranmeldeinformationen und anderen vertraulichen Informationen auf dem Bildschirm. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

Für App Protection müssen Sie eine Add-On-Lizenz auf dem Lizenzserver installieren. Eine Citrix Virtual Desktops-Lizenz muss ebenfalls vorhanden sein. Informationen zur Lizenzierung finden Sie unter [Konfigurieren](#) in der Dokumentation zu App Protection.

Anforderungen:

- Citrix Virtual Apps and Desktops Version 1912 oder höher.
- StoreFront Version 1912.
- Citrix Workspace-App Version 1912 oder höher

Voraussetzungen:

- App Protection muss auf dem Controller aktiviert sein. Weitere Informationen finden Sie in der Dokumentation zu [App Protection](#).

Sie können App Protection mit einem der folgenden Verfahren in die Citrix Workspace-App integrieren:

- Bei der Installation der Citrix Workspace-App über die Befehlszeilenschnittstelle oder GUI.
- Beim Starten einer App (Installation bei Bedarf).

Hinweis:

- Dieses Feature wird nur unter Desktop-Betriebssystemen wie Windows 10 und Windows 8.1 unterstützt.
- Die Citrix Workspace-App wird ab Version 2006.1 unter Windows 7 nicht unterstützt. Daher funktioniert auch App Protection unter Windows 7 nicht. Weitere Informationen finden Sie unter [Einstellung von Features und Plattformen](#).
- Das Feature wird nicht über RDP (Remote Desktop Protocol) unterstützt.

Schutz von On-Premises-HDX-Sitzungen:

Zwei Richtlinien bieten Keylogging- und Screenshotschutz in einer Sitzung. Diese Richtlinien müssen über PowerShell konfiguriert werden. Für diesen Zweck steht keine GUI zur Verfügung.

Hinweis:

Citrix DaaS unterstützt App Protection ab Version 2103 nur für StoreFront.

Informationen zur Konfiguration von App Protection in Citrix Virtual Apps and Desktops finden Sie in der Dokumentation zu [App Protection](#).

App Protection - Konfiguration in der Citrix Workspace-App

Hinweis:

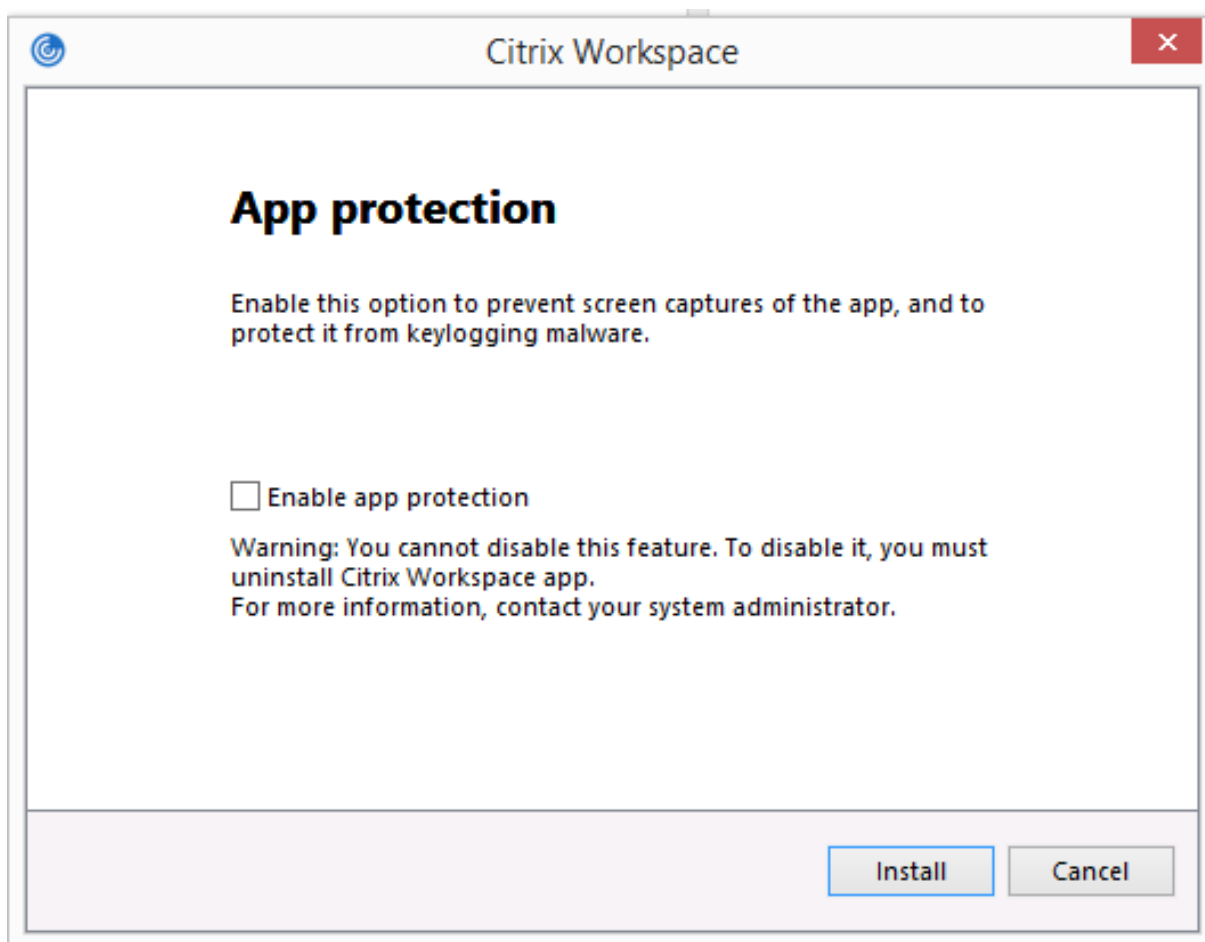
- Integrieren Sie App Protection nur dann in die Citrix Workspace-App, wenn Sie dazu vom Administrator aufgefordert werden.

- App Protection kann das Erstellen von Screenshots auf dem Gerät erschweren.

Bei der Installation der Citrix Workspace-App können Sie App Protection über eines der folgenden Verfahren integrieren:

- Grafische Benutzeroberfläche (GUI)
- Befehlszeilenoberfläche

Grafische Benutzeroberfläche (GUI) Bei der Installation der Citrix Workspace-App können Sie die App Protection-Komponente im folgenden Dialogfeld hinzufügen. Aktivieren Sie **App Protection aktivieren** und klicken Sie auf **Installieren**, um mit der Installation fortzufahren.



Hinweis:

Wenn Sie App Protection nicht bei der Installation aktivieren, werden Sie beim Starten einer geschützten App dazu aufgefordert. Installieren Sie dann die App Protection-Komponente.

Befehlszeilenoberfläche Mit der Befehlszeilenoption `/includeappprotection` fügen Sie App Protection während der Installation der Citrix Workspace-App hinzu.

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

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

Wenn Sie in früheren Versionen den Screenshot eines geschützten Fensters erstellen, wurde der gesamte Bildschirm, einschließlich der nicht geschützten Apps im Hintergrund, abgedunkelt angezeigt.

Ab Version 2008 wird beim Erstellen eines Screenshots nur das geschützte Fenster abgedunkelt. Sie können einen Screenshot des Bereichs außerhalb des geschützten Fensters erstellen.

Erwartetes Verhalten:

Das erwartete Verhalten hängt davon ab, wie Benutzer auf StoreFront zugreifen, das die geschützten Ressourcen enthält.

Hinweis:

- Citrix empfiehlt, nur die native Citrix Workspace-App zum Starten einer geschützten Sitzung zu verwenden.

• **Verhalten im Workspace für Web:**

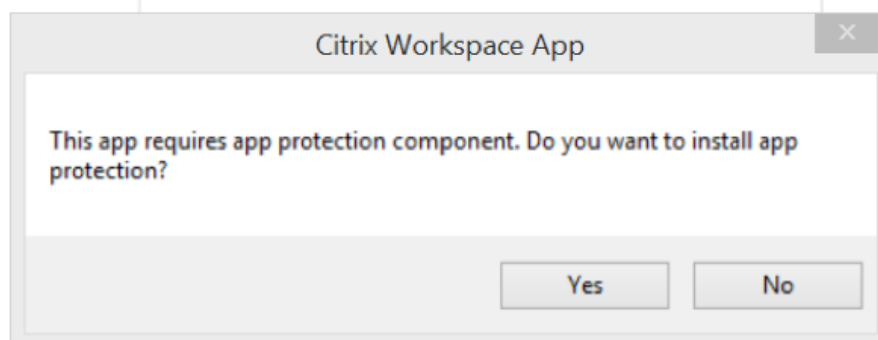
App Protection wird nicht in Konfigurationen mit Workspace für Web unterstützt. Anwendungen, die durch Richtlinien von App Protection geschützt sind, werden nicht aufgelistet. Weitere Informationen zu den zugewiesenen Ressourcen erhalten Sie von Ihrem Systemadministrator.

• **Verhalten in Versionen der Citrix Workspace-App, die App Protection nicht unterstützen:**

In der Citrix Workspace-App bis Version 1911 werden Anwendungen, die durch App Protection-Richtlinien geschützt sind, in StoreFront nicht aufgelistet.

• **Verhalten von Apps, wenn App Protection auf dem Controller konfiguriert ist:**

Wenn Sie auf einem mit App Protection konfigurierten Controller eine geschützte Anwendung starten, wird App Protection zunächst installiert. Das folgende Dialogfeld wird angezeigt:



Klicken Sie auf **Ja**, um App Protection zu installieren. Anschließend können Sie die geschützte App starten.

- **Verhalten von geschützten Sitzungen mit Remotedesktopverbindung (RDP)**
 - Die aktive geschützte Sitzung wird getrennt, sobald Sie eine RDP-Sitzung starten.
 - Der Start einer geschützten Sitzung in einer Sitzung mit Remotedesktopverbindung ist nicht möglich.

Verbesserung der Konfiguration von App Protection

Zuvor waren die Dialogfelder des Authentifizierungsmanagers und des **Self-Service-Plug-Ins** standardmäßig geschützt.

Ab Version 2012 können Sie Keyloggingschutz- und Screenshotschutz-Funktionen für den Authentifizierungsmanager und das Self-Service-Plug-In separat konfigurieren. Sie können die Funktionen mithilfe einer GPO-Richtlinie konfigurieren.

Hinweis:

Diese GPO-Richtlinie gilt nicht für ICA- und SaaS-Sitzungen. Die ICA- und SaaS-Sitzungen werden weiterhin über Delivery Controller und Citrix Gateway Service gesteuert.

App Protection für das Self-Service-Plug-In konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace**.

3. Um Keylogging- und Screenshotschutz für das Self-Service-Plug-In zu konfigurieren, wählen Sie **Self-Service > App Protection verwalten** aus.
4. Wählen Sie mindestens eine der folgenden Optionen aus:
 - **Keyloggingschutz:** Verhindert, dass Keylogger Tastenanschläge erfassen.
 - **Screenshotschutz:** Verhindert, dass Benutzer Screenshots erstellen und ihren Bildschirm teilen.
5. Klicken Sie auf **Anwenden** und **OK**.

App Protection für den Authentifizierungsmanager konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace**.
3. Um den Keylogging- und Screenshotschutz für den Authentifizierungsmanager zu konfigurieren, wählen Sie **Benutzerauthentifizierung > App Protection verwalten**.
4. Wählen Sie mindestens eine der folgenden Optionen aus:
 - **Keyloggingschutz:** Verhindert, dass Keylogger Tastenanschläge erfassen.
 - **Screenshotschutz:** Verhindert, dass Benutzer Screenshots erstellen und ihren Bildschirm teilen.
5. Klicken Sie auf **Anwenden** und **OK**.

App Protection-Fehlerprotokolle:

Ab Version 2103 werden die App Protection-Protokolle als Teil der Citrix Workspace-App-Protokolle gesammelt. Weitere Informationen zur Protokollsammlung finden Sie unter [Protokollsammlung](#).

Sie müssen keine spezielle Drittanbieter-App installieren oder verwenden, um die App Protection-Protokolle zu sammeln. DebugView kann jedoch weiterhin zur Protokollsammlung verwendet werden.

Die App Protection-Protokolle werden in der Debug-Ausgabe registriert. Führen Sie folgende Schritte aus, um diese Protokolle zu erfassen:

1. Laden Sie die App [DebugView](#) von der Microsoft-Website herunter und installieren Sie sie.
2. Starten Sie die Eingabeaufforderung, und führen Sie folgenden Befehl aus:

```
Dbgview.exe /t /k /v /l C:\logs.txt
```

Im obigen Beispiel können Sie die Protokolle in der Datei `log.txt` anzeigen.

Der Befehl gibt Folgendes an:

- `/t` –Die DebugView-App ist beim Start im Infobereich minimiert.

- /k –Kernel-Erfassung aktivieren.
- /v –Ausführliche Kernel-Erfassung aktivieren.
- /l –Ausgabe in spezieller Datei protokollieren.

App Protection deinstallieren:

Um App Protection zu deinstallieren, müssen Sie die Citrix Workspace-App von Ihrem System deinstallieren. Starten Sie das System neu, damit die Änderungen wirksam werden.

Hinweis:

App Protection wird nur bei einem Upgrade auf Version 1912 und höher unterstützt.

Bekannte Probleme oder Einschränkungen:

- Dieses Feature wird nicht unter Microsoft Server-Betriebssystemen wie Windows Server 2012 R2 oder Windows Server 2016 unterstützt.
- Dieses Feature wird nicht in Double-Hop-Szenarios unterstützt.
- Damit das Feature ordnungsgemäß funktioniert, müssen Sie auf dem VDA die Citrix-Richtlinie zur **Zwischenablagenumleitung** deaktivieren.

Anwendungskategorien

Anwendungskategorien ermöglichen Benutzern das Verwalten von Anwendungssammlungen in der Citrix Workspace-App. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder nur von einigen Benutzern in einer Bereitstellungsgruppe verwendet werden.

Weitere Informationen finden Sie unter [Erstellen von Anwendungsgruppen](#) in der Citrix Virtual Apps and Desktops-Dokumentation.

Verbesserte ICA-Dateisicherheit

Dieses Feature bietet erhöhte Sicherheit für die Handhabung von ICA-Dateien beim Starten von Citrix Virtual Apps and Desktops-Sitzungen.

Mit der Citrix Workspace-App können Sie die ICA-Datei beim Starten einer Sitzung mit virtuellen Apps und Desktops im Systemspeicher speichern statt auf dem lokalen Datenträger.

Diese Funktion zielt darauf ab, Oberflächenangriffe und Malware auszuschließen, die die ICA-Datei missbrauchen könnten, wenn sie lokal gespeichert wird. Das Feature ist auch in Sitzungen mit virtuellen Apps und Desktops verfügbar, die im Workspace für Web gestartet werden.

Konfiguration

Die ICA-Dateisicherheit wird auch unterstützt, wenn über das Internet auf Citrix Workspace oder StoreFront zugegriffen wird. Die Clienterkennung ist eine Voraussetzung für das Funktionieren des Features, wenn darauf über das Internet zugegriffen wird. Wenn Sie über einen Browser auf StoreFront zugreifen, aktivieren Sie die folgenden Attribute in der Datei web.config in StoreFront-Bereitstellungen:

StoreFront-Version	Attribut
2.x	pluginassistant
3.x	protocolHandler

Klicken Sie bei der Anmeldung am Store über den Browser auf **Workspace-App ermitteln**. Wenn die Aufforderung nicht angezeigt wird, löschen Sie die Browsercookies und versuchen Sie es erneut.

Wenn es sich um eine Workspace-Bereitstellung handelt, finden Sie die Einstellungen für die Clienterkennung unter **Kontoeinstellungen > Erweitert > Startpräferenz für Apps und Desktops**.

Sie können zusätzliche Maßnahmen ergreifen, damit Sitzungen nur mit der ICA-Datei gestartet werden, die im Systemspeicher gespeichert ist. Verwenden Sie eine der folgenden Methoden:

- Administrative Gruppenrichtlinienobjektvorlage auf dem Client
- Global App Config Service
- Workspace für Web.

Verwenden des Gruppenrichtlinienobjekts:

Gehen Sie wie folgt vor, um Sitzungsstarts von ICA-Dateien zu blockieren, die auf dem lokalen Datenträger gespeichert sind:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Clientengine**.
3. Wählen Sie die Richtlinie **Sitzungsstart mit ICA-Datei sichern** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Anwenden** und **OK**.

Verwenden des Global App Config Service:

Gehen Sie wie folgt vor, um Sitzungsstarts von ICA-Dateien zu blockieren, die auf dem lokalen Datenträger gespeichert sind:

Setzen Sie das Attribut **Block Direct ICA File Launches** auf **True**.

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

Workspace für Web verwenden:

Gehen Sie wie folgt vor, um den Download der ICA-Datei auf den lokalen Datenträger zu unterbinden, wenn Sie Workspace für Web verwenden:

Führen Sie das PowerShell-Modul aus. Siehe [Configure DisallowICADownload](#).

Hinweis:

Die Richtlinie **DisallowICADownload** ist für StoreFront-Bereitstellungen nicht verfügbar.

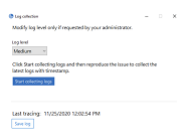
Protokollsammlung

Protokollsammlung vereinfacht das Sammeln von Protokollen für die Citrix Workspace-App. Die Protokolle helfen Citrix bei der Problembearbeitung und erleichtern bei komplizierten Problemen den Support.

Sie können Protokolle über die GUI sammeln.

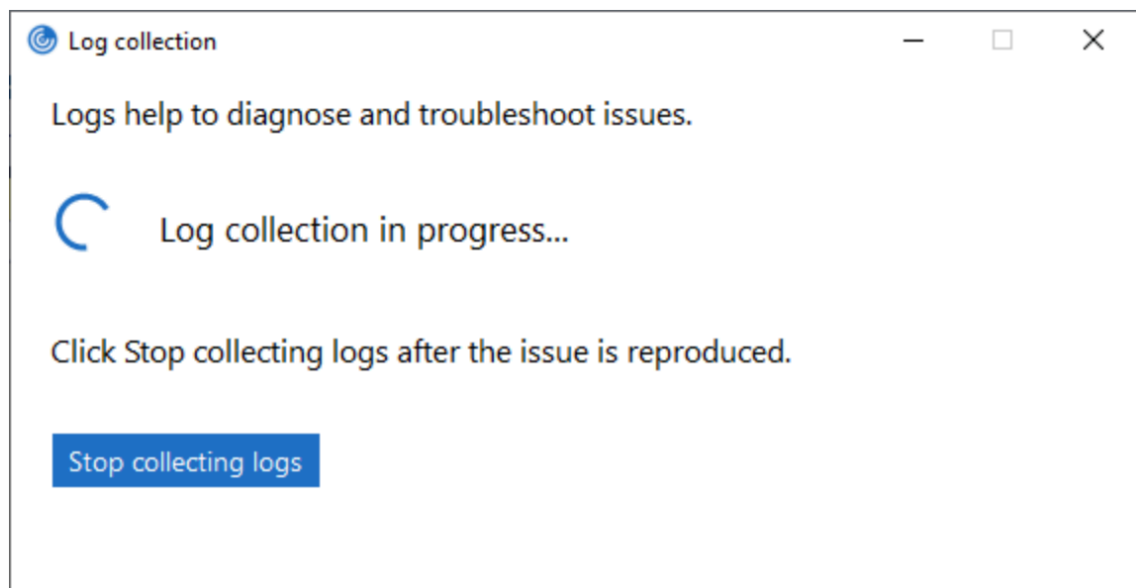
Protokolle sammeln:

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Citrix Workspace-App-Symbol und wählen Sie **Erweiterte Einstellungen**.
2. Wählen Sie **Protokollsammlung**.
Das Dialogfeld "Protokollsammlung" wird angezeigt.



3. Wählen Sie eine der folgenden Protokollebenen aus:
 - Niedrig
 - Medium
 - Ausführlich
4. Klicken Sie auf **Protokollsammlung starten**, um das Problem zu reproduzieren und die neuesten Protokolle zu sammeln.

Der Protokollsammelungsprozess wird gestartet.



5. Klicken Sie auf **Protokollsammlung stoppen**, wenn Sie das Problem reproduziert haben.
6. Klicken Sie auf **Protokoll speichern**, um die Protokolle an einem gewünschten Ort zu speichern.

Adaptiver HDX-Durchsatz

Der adaptive HDX-Durchsatz passt den Spitzendurchsatz einer ICA-Sitzung über die Ausgabepuffer intelligent an. Die Anzahl der Ausgabepuffer ist anfangs auf einen hohen Wert eingestellt. Der hohe Wert ermöglicht es insbesondere in Netzwerken mit hoher Latenz, Daten schneller und effizienter an den Client zu übertragen.

Sie erhalten damit bessere Interaktivität, schnellere Dateiübertragungen, flüssigere Videowiedergabe sowie höhere Framerate und Auflösung für eine bessere Benutzererfahrung.

Die Sitzungsinteraktivität wird ständig gemessen, um festzustellen, ob Datenströme innerhalb der ICA-Sitzung die Interaktivität beeinträchtigen. Ist dies der Fall, wird der Durchsatz verringert, um die Beeinträchtigungen durch den großen Datenstrom zu verringern und die Interaktivität wiederherzustellen.

Das Feature wird nur in der Citrix Workspace-App für Windows ab Version 1811 unterstützt.

Wichtig:

Der adaptive HDX-Durchsatz ändert die Ausgabepuffer durch Übertragung des Mechanismus vom Client auf den VDA. Das Anpassen der Anzahl der Ausgabepuffer auf dem Client, wie es im Knowledge Center-Artikel [CTX125027](#) erläutert wurde, hat daher keine Wirkung.

Adaptiver Transport

Adaptiver Transport ist ein Verfahren in Citrix Virtual Apps and Desktops und Citrix DaaS, mit dem Enlightened Data Transport (EDT) als Protokoll für ICA-Verbindungen verwendet werden kann. Weitere Informationen finden Sie unter [Adaptiver Transport](#) in der Citrix Virtual Apps and Desktops-Dokumentation.

Seite “Erweiterte Einstellungen”

Ab Version 4.10 können Sie die Verfügbarkeit und den Inhalt der Seite **Erweiterte Einstellungen** anpassen. Die Seite ist im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich zu finden. Auf diese Weise wird sichergestellt, dass Benutzer nur vom Administrator festgelegte Einstellungen auf ihren Systemen anwenden können. Optionen:

- Ausblenden der gesamten Seite “Erweiterte Einstellungen”
- Ausblenden der folgenden Einstellungen auf der Seite:
 - Datensammlung
 - Connection Center
 - Konfigurationsprüfung
 - Tastatur und Sprachenleiste
 - Hoher DPI-Wert
 - Supportinformationen
 - Verknüpfungen und Wiederverbinden
 - Citrix Casting

Erweiterte Einstellungen aus dem Kontextmenü ausblenden

Sie können die Seite “Erweiterte Einstellungen” über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App ausblenden:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Self-Service** > **Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie **Erweiterte Einstellungen deaktivieren**.
4. Wählen Sie **Aktiviert** aus, um die Option “Erweiterte Einstellungen” im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich auszublenden.

Hinweis:

Standardmäßig ist die Option **Nicht konfiguriert** ausgewählt.

Ausblenden bestimmter Einstellungen auf der Seite “Erweiterte Einstellungen”

Sie können auf der Seite **Erweiterte Einstellungen** bestimmte vom Benutzer konfigurierbare Einstellungen über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App ausblenden. Ausblenden der Einstellungen:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Self-Service > Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie für die Einstellung, die Sie ausblenden möchten.

Die folgende Tabelle listet die verfügbaren Optionen und ihre Wirkung auf:

Optionen	Aktion
Nicht konfiguriert	Anzeigen der Einstellung
Aktiviert	Ausblenden der Einstellung
Deaktiviert	Anzeigen der Einstellung

Sie können die folgenden bestimmten Einstellungen auf der Seite “Erweiterte Einstellungen” ausblenden:

- Konfigurationsprüfung
- Connection Center
- Hoher DPI-Wert
- Datensammlung
- Gespeicherte Kennwörter löschen
- Tastatur und Sprachenleiste
- Verknüpfungen und Wiederverbinden
- Supportinformationen
- Citrix Casting

Ausblenden der Option zum Zurücksetzen von Workspace auf der Seite “Erweiterte Einstellungen” mit dem Registrierungs-Editor

Sie können die Option **Workspace zurücksetzen** auf der Seite “Erweiterte Einstellungen” nur mit dem Registrierungs-Editor ausblenden.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Erstellen Sie einen Schlüsselzeichenfolgert **EnableFactoryReset** und legen Sie ihn auf eine der folgenden Optionen fest:
 - True: zeigt die Option “Workspace zurücksetzen” auf der Seite “Erweiterte Einstellungen” an.
 - False: blendet die Option “Workspace zurücksetzen” auf der Seite “Erweiterte Einstellungen” aus.

Ausblenden der Option “Citrix Workspace-Updates” auf der Seite “Erweiterte Einstellungen”

Hinweis:

Der Richtlinienpfad für die Option “Citrix Workspace-Updates” ist anders als bei anderen Optionen auf der Seite “Erweiterte Einstellungen”.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Citrix Workspace-Updates**.
3. Wählen Sie die Richtlinie **Citrix Workspace-Updates** aus.
4. Wählen Sie **Deaktiviert**, um die Einstellungen für automatische Updates auf der Seite **Erweiterte Einstellungen** auszublenden.

URL-Migration von StoreFront zu Workspace

Dieses Feature ist als Technical Preview verfügbar. Die URL-Migration von StoreFront zu Workspace ermöglicht es Ihnen, Endbenutzer nahtlos von einem StoreFront-Store zu einem Workspace-Store unter minimaler Benutzerinteraktion zu migrieren.

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

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

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

1. Konfigurieren Sie die StoreFront-zu-Workspace-Zuordnung mit dem Global App Config Service. Weitere Informationen zum Global App 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      "windows":[ 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.

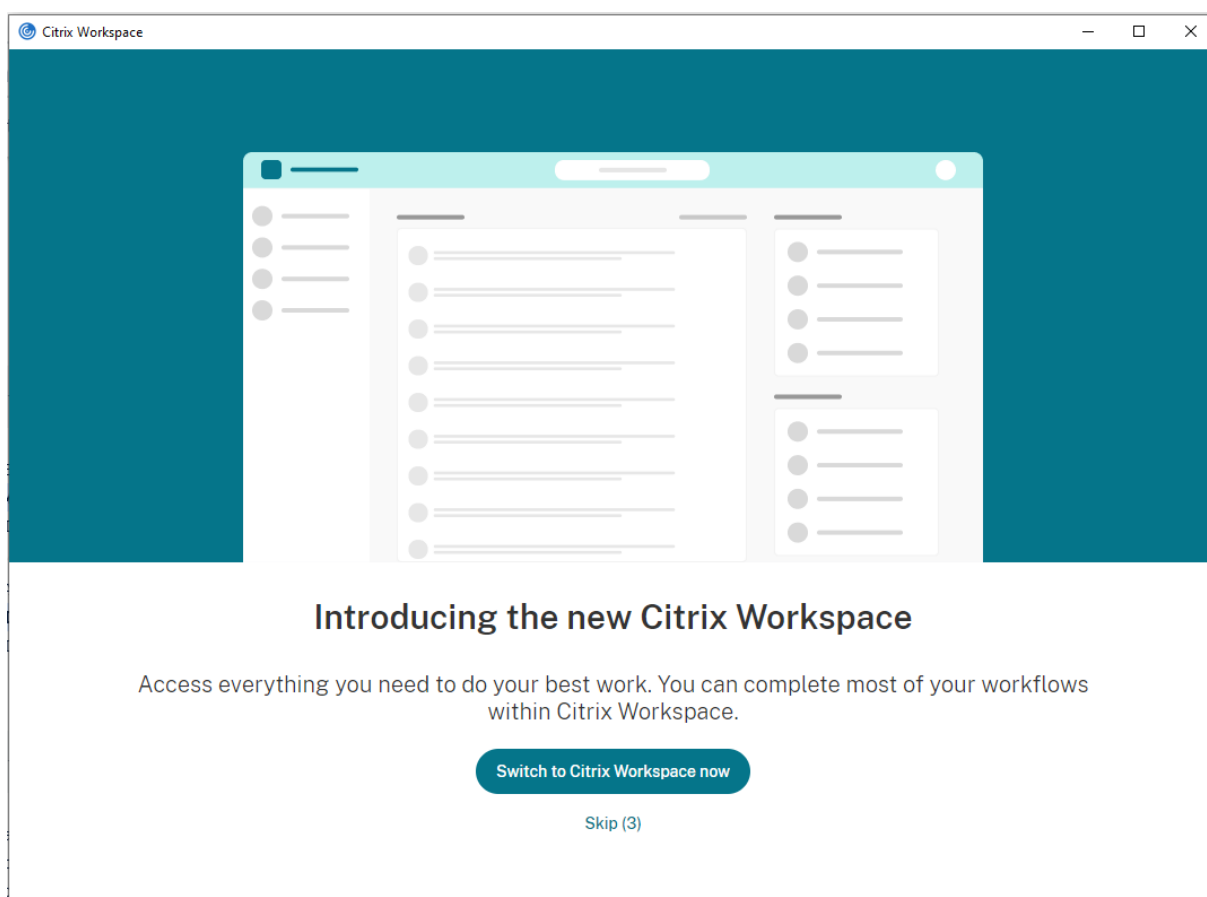
3. Geben Sie die StoreFront-URL `storefront.com` als Wert für **URL** im Abschnitt **serviceURL** an.

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 -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.

Anwendungsbereitstellung

Mit den folgenden Optionen können Sie die Benutzererfahrung bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops und Citrix DaaS verbessern.

- **Webzugriffsmodus:** Ohne jegliche Konfiguration ermöglicht die Citrix Workspace-App browserbasierten Zugriff auf Anwendungen und Desktops. Sie greifen einfach über einen Browser auf Workspace für Web zu und wählen die gewünschten Anwendungen aus. In diesem Modus werden keine Verknüpfungen auf dem Desktop der Benutzer platziert.
- **Self-Service-Modus:** Sie konfigurieren den *Self-Service-Modus* durch Hinzufügen eines StoreFront-Kontos zur Citrix Workspace-App oder durch Verweisen der Citrix Workspace-App auf eine StoreFront-Website. Im Self-Service-Modus können Sie Anwendungen über die Benutzeroberfläche der Citrix Workspace-App abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores. Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

Hinweis:

Standardmäßig können Sie in der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

- **Nur-Verknüpfungsmodus:** Administratoren können mit der Citrix Workspace-App Anwendungs- und Desktopverknüpfungen automatisch direkt in das Startmenü oder auf dem Desktop platzieren. Die Platzierung ähnelt der Citrix Workspace-App (Enterprise). Mit dem neuen *Nur-Verknüpfungsmodus* werden die veröffentlichten Anwendungen entsprechend dem gewohnten Windows-Navigationsschema angezeigt.

Weitere Informationen finden Sie unter [Bereitstellungsgruppe erstellen](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Konfigurieren des Self-Service-Modus

Sie konfigurieren den Self-Service-Modus durch einfaches Hinzufügen eines StoreFront-Kontos zur Citrix Workspace-App oder durch Verweisen der Citrix Workspace-App auf eine StoreFront-Site. Mit dieser Konfiguration können Benutzer die Anwendungen über die Citrix Workspace-Benutzeroberfläche abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

Hinweis:

Standardmäßig können Benutzer der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

Fügen Sie den Beschreibungen, die Sie für Bereitstellungsgruppenanwendungen eingeben, Schlüsselwörter hinzu:

- Um eine App verbindlich zu machen, sodass sie nicht aus der Citrix Workspace-App entfernt werden kann, hängen Sie die Zeichenfolge “KEYWORDS: Mandatory” an die Anwendungsbeschreibung an. Benutzer haben keine Option zum Kündigen des Abonnements verbindlicher Apps.
- Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, wenn Sie die Zeichenfolge “KEYWORDS: Auto” der Beschreibung anhängen. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Hängen Sie die Zeichenfolge “KEYWORDS: Featured” der Anwendungsbeschreibung an, um den Benutzern Anwendungen anzukündigen oder häufig verwendete Anwendungen in der Highlightliste von Citrix Workspace anzuzeigen.

Speicherort für App-Verknüpfung mit Gruppenrichtlinienobjektvorlage konfigurieren

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **Self-Service-Modus verwalten** aus.
 - a) Wählen Sie **Aktiviert**, um die Self-Service-Benutzeroberfläche anzuzeigen.
 - b) Wählen Sie **Deaktiviert**, um Apps manuell zu abonnieren. Diese Option blendet die Self-Service-Benutzeroberfläche aus.
4. Wählen Sie die Richtlinie **App-Verknüpfung verwalten** aus.
5. Wählen Sie die gewünschten Optionen aus.
6. Klicken Sie auf **Anwenden** und **OK**.
7. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

Speicherorte für App-Verknüpfungen mit StoreFront-Kontoeinstellungen anpassen

Sie können Verknüpfungen im Startmenü und auf dem Desktop von der StoreFront-Site aus einrichten. Die folgenden Einstellungen können im Abschnitt **<annotatedServices>** der Datei web.config in `C:\inetpub\wwwroot\Citrix\Roaming` hinzugefügt werden:

- Zum Einfügen von Verknüpfungen auf dem Desktop verwenden Sie `PutShortcutsOnDesktop`. Einstellungen: “true” oder “false” (Standardwert ist “false”).
- Zum Einfügen von Verknüpfungen im Startmenü verwenden Sie `PutShortcutsInStartMenu`. Einstellungen: “true” oder “false” (Standardwert ist “true”).
- Zum Verwenden eines Kategoriepfads im Startmenü verwenden Sie `UseCategoryAsStartMenuPath`. Einstellungen: “true” oder “false” (Standardwert ist “true”).

Hinweis:

In Windows 8, 8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden stattdessen einzeln oder unter dem Stammordner angezeigt. Die Anwendungen werden nicht in den mit Citrix Virtual Apps and Desktops definierten Unterordnern für Kategorien angezeigt.

- Zum Festlegen eines einzelnen Verzeichnisses für alle Verknüpfungen im Startmenü verwenden Sie `StartMenuDir`. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Neuinstallieren modifizierter Apps verwenden Sie `AutoReinstallModifiedApps`. Einstellungen: “true” oder “false” (Standardwert ist “true”).
- Zum Anzeigen eines einzelnen Verzeichnisses für alle Verknüpfungen auf dem Desktop verwenden Sie `DesktopDir`. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Vermeiden eines Eintrags unter “Programme hinzufügen/entfernen” verwenden Sie `DontCreateAddRemoveEntry`. Einstellungen: “true” oder “false” (Standardwert ist “false”).
- Zum Entfernen von Verknüpfungen und des Citrix Workspace-Symbols einer Anwendung, die nicht mehr im Store verfügbar ist, verwenden Sie `SilentlyUninstallRemovedResources`. Einstellungen: “true” oder “false” (Standardwert ist “false”).

Fügen Sie die Änderungen in der Datei `web.config` im **XML**-Abschnitt für das Konto hinzu. Sie finden diesen Abschnitt durch Suchen des Starttags:

```
<account id=... name="Store"
```

Der Abschnitt endet mit dem Tag `</account>`.

Vor dem Ende des Abschnitts “account” ist der Abschnitt “properties” mit den Eigenschaften:

```
<properties> <clear> <properties>
```

Eigenschaften können in diesen Abschnitt nach dem Tag `<clear />` unter Angabe des Namens und Werts (eine Eigenschaft pro Zeile) eingefügt werden. Beispiel:

```
<property name="PutShortcutsOnDesktop" value="True" />
```

Hinweis:

Wenn Eigenschaftenelemente vor dem Tag <clear /> hinzugefügt werden, sind sie u. U. ungültig. Sie können das Tag <clear /> entfernen, wenn Sie einen Eigenschaftsnamen und -wert hinzufügen.

Ausführliches Beispiel für diesen Abschnitt:

```
<properties <property name="PutShortcutsOnDesktop" value="True">  
property name="DesktopDir" value="Citrix Applications">
```

Wichtig

Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden. Weitere Informationen finden Sie in der [StoreFront](#)-Dokumentation.

Konfigurieren von Speicherorten für App-Verknüpfungen mit Einstellungen pro App in Citrix Virtual Apps and Desktops 7.x

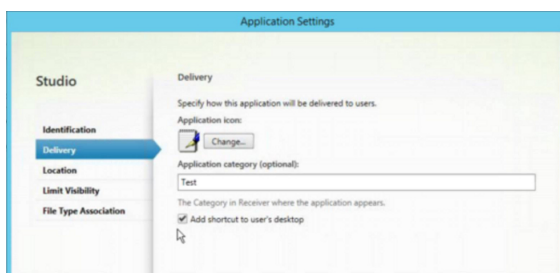
Mit der Citrix Workspace-App können Anwendungs- und Desktopverknüpfungen direkt in das Startmenü oder auf dem Desktop platziert werden. Diese Konfiguration ähnelt jedoch früheren Versionen von Workspace für Windows. Ab Release 4.2.100 kann jedoch die Platzierung der App-Verknüpfung in Citrix Virtual Apps über Einstellungen pro App gesteuert werden. Diese Funktionalität ist in Umgebungen mit nur einer Handvoll Anwendungen nützlich, die immer am gleichen Ort angezeigt werden sollen.

Speicherorte für App-Verknüpfungen mit Einstellungen pro App in XenApp 7.6 konfigurieren

Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 7.6:

1. Navigieren Sie in Citrix Studio zum Bildschirm **Anwendungseinstellungen**.
2. Wählen Sie im Bildschirm **Anwendungseinstellungen** die Option **Bereitstellung**. In diesem Bildschirm legen Sie fest, wie Anwendungen Benutzern bereitgestellt werden.
3. Wählen Sie das entsprechende Symbol für die Anwendung. Klicken Sie auf **Ändern**, um zum Speicherort des erforderlichen Symbols zu navigieren.

4. Im Feld **Anwendungskategorie** können Sie optional für die Anwendung eine Kategorie in der Citrix Workspace-App angeben. Wenn Sie beispielsweise Verknüpfungen für Microsoft Office-Anwendungen hinzufügen, geben Sie Microsoft Office ein.
5. Aktivieren Sie das Kontrollkästchen **Verknüpfung auf Benutzerdesktop hinzufügen**.
6. Klicken Sie auf OK.



Reduzieren von Enumerationsverzögerungen oder digitales Signieren von Anwendungsstubs

Mit der Citrix Workspace-App können Sie in folgenden Fällen die EXE-Stubs von einer Netzwerkfreigabe kopieren:

- Es gibt eine Verzögerung der App-Enumeration bei jeder Anmeldung. Oder:
- Anwendungsstubs müssen digital signiert werden.

Diese Funktionalität umfasst mehrere Schritte:

1. Erstellen Sie die Anwendungsstubs auf der Clientmaschine.
2. Kopieren Sie die Anwendungsstubs an einen allgemeinen Speicherort, der von einer Netzwerkfreigabe aus verfügbar ist.
3. Erstellen Sie bei Bedarf eine Positivliste oder signieren Sie die Stubs mit einem Unternehmenszertifikat.
4. Fügen Sie einen Registrierungsschlüssel hinzu, damit Workspace für Windows die Stubs durch Kopieren von der Netzwerkfreigabe erstellen kann.

Wenn **RemoveappsOnLogoff** und **RemoveAppsonExit** aktiviert sind und die App-Enumeration bei jeder Anmeldung langsam ist, lösen Sie das Problem mit dem folgenden Workaround:

1. Fügen Sie mit dem Registrierungs-Editor (regedit) Folgendes hinzu: `HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`.
2. Fügen Sie mit dem Registrierungs-Editor (regedit) Folgendes hinzu: `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`. HKEY_CURRENT_USER hat Vorrang vor HKEY_LOCAL_MACHINE.

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Ermöglichen Sie die Verwendung zuvor erstellter und in einer Netzwerkfreigabe gespeicherter EXE-Stubdateien durch den Computer:

1. Erstellen Sie auf einer Clientmaschine EXE-Stubdateien für alle Apps. Zum Erstellen von EXE-Stubdateien fügen Sie mit der Citrix Workspace-App alle Anwendungen zur Maschine hinzu. Die Citrix Workspace-App generiert die EXE-Dateien.
2. Verwenden Sie die EXE-Stubdateien aus `%APPDATA%\Citrix\SelfService`. Sie benötigen nur die Dateien mit der Erweiterung `.exe`.
3. Kopieren Sie die EXE-Dateien in eine Netzwerkfreigabe.
4. Legen Sie für jeden Clientcomputer, der gesperrt werden soll, folgende Registrierungsschlüssel fest:
 - a) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"`
 - b) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v`
 - c) `CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"`. Diese Einstellungen sind auch über `HKEY_CURRENT_USER` möglich. `HKEY_CURRENT_USER` hat Vorrang vor `HKEY_LOCAL_MACHINE`.
 - d) Beenden und starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

Anwendungsbeispiele:

In diesem Abschnitt finden Sie Anwendungsfälle für App-Verknüpfungen.

Benutzer wählen die gewünschten Apps für das Startmenü selbst aus (Self-Service)

Wenn Sie Dutzende oder sogar Hunderte von Apps haben, lassen Sie Benutzer ihre Anwendungen selbst auswählen und im **Favoriten-** und **Startmenü** hinzufügen:

Wenn Benutzer Apps selbst auswählen und dem Startmenü hinzufügen sollen ...

... konfigurieren Sie die Citrix Workspace-App im Self-Service-Modus. In diesem Modus können Sie nach Bedarf Schlüsselworteinstellungen für *obligatorische* und *automatisch bereitgestellte* Apps konfigurieren.

Wenn Benutzer die Apps für das Startmenü selbst auswählen aber auch bestimmte App-Verknüpfungen auf dem Desktop platziert werden sollen ...

... konfigurieren Sie die Citrix Workspace-App ohne Optionen und legen Sie die Einstellungen für die wenigen Apps, die auf dem Desktop platziert werden, einzeln fest. Verwenden Sie *automatisch bereitgestellte* und *obligatorische* Apps nach Bedarf.

Keine App-Verknüpfungen im Startmenü

Wenn ein Benutzer einen Familiencomputer verwendet, sind App-Verknüpfungen möglicherweise nicht erwünscht oder erforderlich. In solchen Fällen ist die einfachste Lösung der Zugriff über einen Browser. Installieren Sie die Citrix Workspace-App hierfür ohne Konfiguration und navigieren Sie zu Workspace für Web. Sie können für die Citrix Workspace-App auch Self-Service-Zugriff konfigurieren, ohne Verknüpfungen zu erstellen.

Wenn die Citrix Workspace-App nicht automatisch Anwendungsverknüpfungen im Startmenü platzieren soll ...

... konfigurieren Sie die Citrix Workspace-App mit `PutShortcutsInStartMenu=False`. Die Citrix Workspace-App platziert keine Apps ins Startmenü (selbst bei aktiviertem Self-Service-Modus), sofern Sie sie nicht einzeln über die Einstellungen platzieren.

Alle App-Verknüpfungen im Startmenü oder auf dem Desktop

Wenn Benutzer nur wenige Apps haben, platzieren Sie alle Apps im Startmenü oder auf dem Desktop oder in einem Ordner auf dem Desktop.

Wenn die Citrix Workspace-App automatisch alle Anwendungsverknüpfungen im Startmenü platzieren soll konfigurieren Sie die Citrix Workspace-App mit SelfServiceMode=False. Alle verfügbaren Apps werden dann im Startmenü angezeigt.
Wenn alle Anwendungsverknüpfungen auf dem Desktop platziert werden sollen konfigurieren Sie die Citrix Workspace-App mit PutShortcutsOnDesktop=true. Alle verfügbaren Apps werden dann auf dem Desktop angezeigt.
Wenn alle Verknüpfungen auf dem Desktop in einem Ordner platziert werden sollen konfigurieren Sie die Citrix Workspace-App mit DesktopDir=Name des Desktopordners, in dem die Anwendungen platziert werden sollen.

Einstellungen pro App in XenApp 6.5 oder 7.x

Wenn Sie die Speicherorte der Verknüpfungen für alle Benutzer gleich festlegen möchten, verwenden Sie die XenApp-Einstellungen pro App:

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden konfigurieren Sie die Citrix Workspace-App mit PutShortcutsInStartMenu=false und aktivieren Sie die Einstellungen pro App.
--	--

Apps in Kategorieordnern oder in bestimmten Ordnern

Wenn Anwendungen in bestimmten Ordnern angezeigt werden sollen, verwenden Sie die folgenden Optionen:

Wenn die von der Citrix Workspace-App im Startmenü platzierten Anwendungsverknüpfungen in den zugeordneten Kategorieordnern angezeigt werden sollen konfigurieren Sie die Citrix Workspace-App mit UseCategoryAsStartMenuPath=True.
Wenn die von der Citrix Workspace-App im Startmenü platzierten Anwendungen in einem bestimmten Ordner angezeigt werden sollen konfigurieren Sie die Citrix Workspace-App mit StartMenuDir=Startmenü-Ordnername.

Apps beim Abmelden oder Beenden entfernen

Wenn ein Endpunkt von mehreren Benutzern genutzt wird und andere Benutzer die Apps nicht sehen sollen, können Sie die Apps beim Abmelden und Beenden des Benutzers entfernen.

Wenn die Citrix Workspace-App alle Apps beim Abmelden entfernen soll konfigurieren Sie die Citrix Workspace-App mit <code>RemoveAppsOnLogoff=True</code> .
Wenn die Citrix Workspace-App alle Apps beim Beenden entfernen soll konfigurieren Sie die Citrix Workspace-App mit <code>RemoveAppsOnExit=True</code> .

Konfigurieren von lokalem App-Zugriff für Anwendungen

Lokalen App-Zugriff für Anwendungen konfigurieren:

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge `KEYWORDS:prefer="pattern"` an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

Bevor Sie eine Anwendung auf dem Computer des Benutzers installieren, sucht die Citrix Workspace-App nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Citrix Workspace-App-Fenster aus startet, startet die App die lokal installierte (bevorzugte) Anwendung.

Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über das Citrix Workspace-App-Dialogfeld deinstalliert, kündigt die Citrix Workspace-App das Abonnement; die Anwendung wird jedoch nicht deinstalliert.

Hinweis:

Das Schlüsselwort `“prefer”` wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort `“prefer”` mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge KEYWORDS:prefer="pattern" an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

Bevor Sie eine Anwendung auf dem Computer des Benutzers installieren, sucht die Citrix Workspace-App nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung über das Citrix Workspace-App-Dialogfeld startet, startet die App die lokal installierte (bevorzugte) Anwendung.

Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über die Citrix Workspace-App deinstalliert, kündigt die App das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

Hinweis:

Das Schlüsselwort "prefer" wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort "prefer" mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- prefer="ApplicationName"

Das Anwendungsnamenmuster stimmt mit jeder Anwendung überein, die den angegebenen Anwendungsnamen im Verknüpfungsdateinamen hat. Der Anwendungsname kann ein Wort oder ein Satz sein. Für Sätze sind Anführungszeichen erforderlich. Die Übereinstimmung ist nicht für Teilworte oder Dateipfade zulässig; die Groß- und Kleinschreibung wird beachtet. Das Übereinstimmungsmuster für den Anwendungsnamen ist nützlich, wenn ein Administrator manuelle Überschreibungen ausführt.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Word	\Microsoft Office\Microsoft Word 2010	Ja
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Ja
Konsole	McAfee\VirusScan Console	Ja
Virus	McAfee\VirusScan Console	Nein

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Konsole	McAfee\VirusScan Console	Ja

- prefer="\\Folder1\Folder2\...\ApplicationName"

Das Muster des absoluten Pfads stimmt mit dem gesamten Pfad der Verknüpfungsdatei und dem ganzen Anwendungsnamen unter dem Startmenü überein. Der Ordner "Programme" ist ein Unterordner des Startmenüverzeichnis und muss daher im absoluten Pfad für die Zielanwendung in diesem Ordner enthalten sein. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den absoluten Pfad ist für Überschreibungen nützlich, die programmatisch in Citrix Virtual Apps and Desktops und Citrix DaaS implementiert werden.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Programme\Microsoft Office\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Programme\Microsoft Word 2010	\Programme\Microsoft Word 2010	Ja

- prefer="Folder1\Folder2\...\ApplicationName"

Das Muster des absoluten Pfads stimmt mit dem relativen Pfad unter dem Startmenü überein. Der angegebene relative Pfad muss den Anwendungsnamen enthalten und (optional) den Ordner, in dem die Verknüpfung gespeichert ist. Die Übereinstimmung ist erfolgreich, wenn am Ende des Pfads der Verknüpfungsdatei der angegebene relative Pfad steht. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den relativen Pfad ist für Überschreibungen nützlich, die programmatisch implementiert werden.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	Nein

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Word	\Microsoft Word 2010	Nein

Informationen zu anderen Schlüsselwörtern finden Sie im Abschnitt “Zusätzliche Empfehlungen” unter [Optimieren der Benutzererfahrung](#) in der StoreFront-Dokumentation.

Virtuelles Anzeigelayout

Mit diesem Feature definieren Sie ein virtuelles Bildschirmlayout für den Remotedesktop. Außerdem können Sie einen einzelnen Clientmonitor virtuell in bis zu acht Bildschirme auf dem Remotedesktop aufteilen. Sie können die virtuellen Bildschirme auf der Registerkarte **Bildschirmlayout** im Desktop Viewer konfigurieren. Dort können Sie horizontale oder vertikale Linien ziehen, um den Bildschirm in virtuelle Bildschirme zu unterteilen. Der Bildschirm wird entsprechend den angegebenen Prozentsätzen der Auflösung des Clientbildschirms aufgeteilt.

Sie können für die virtuellen Bildschirme eine DPI festlegen, die für die DPI-Skalierung bzw. DPI-Anpassung verwendet wird. Ändern Sie nach dem Anwenden eines virtuellen Bildschirmlayouts die Größe der Sitzung oder stellen Sie erneut eine Verbindung her.

Die Konfiguration gilt nur für Desktopsitzungen mit einem Bildschirm im Vollbildmodus. Sie hat keine Auswirkungen auf veröffentlichte Anwendungen. Diese Konfiguration gilt für alle nachfolgenden Verbindungen von diesem Client.

Ab Citrix Workspace-App für Windows 2106 wird das virtuelle Anzeigelayout auch für Desktopsitzungen mit mehreren Bildschirmen im Vollbildmodus unterstützt. Das virtuelle Anzeigelayout ist standardmäßig aktiviert. In einem Szenario mit mehreren Bildschirmen wird das gleiche virtuelle Anzeigelayout auf alle Sitzungsmonitore angewendet, sofern nicht mehr als acht virtuelle Anzeigen vorhanden sind. Wird dieses Limit überschritten, wird das virtuelle Anzeigelayout ignoriert und auf keinen Sitzungsbildschirm angewendet.

Die Verbesserung für die Multimonitoranzeige kann durch Festlegen des folgenden Registrierungsschlüssels deaktiviert werden:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Name: **SplitAllMonitors**

Typ: DWORD

Werte:

1 - Aktiviert

0 - Deaktiviert

Dauer des Anwendungsstarts

Verwenden Sie das Sitzungsvorabstartfeature, um den Anwendungsstart in Zeiten mit normalem oder hohem Netzwerkverkehr zu verkürzen und die Benutzererfahrung dadurch zu verbessern. Mit dem Vorabstartfeature kann eine Vorabstart Sitzung erstellt werden. Eine Vorabstart Sitzung wird erstellt, wenn ein Benutzer sich an der Citrix Workspace-App anmeldet oder zu einem geplanten Zeitpunkt (wenn der Benutzer bereits angemeldet ist).

Die Vorabstart Sitzung verkürzt die Startzeit der ersten Anwendung. Wenn ein Benutzer eine neue Kontoverbindung in der Citrix Workspace-App für Windows hinzufügt, findet der Sitzungsvorabstart erst in der nächsten Sitzung statt. Die Standardanwendung `ctxprelaunch.exe` wird in der Sitzung ausgeführt, ist jedoch für Sie unsichtbar.

Weitere Informationen finden Sie in den Anleitungen zum Vorabstart von Sitzungen und zum Sitzungsfortbestehen unter [Verwalten von Bereitstellungsgruppen](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Der Sitzungsvorabstart ist standardmäßig deaktiviert. Geben Sie zum Aktivieren des Vorabstarts von Sitzungen den Parameter `ENABLEPRELAUNCH=true` an der Workspace-Befehlszeile an oder legen Sie den Registrierungsschlüssel `EnablePreLaunch` auf "true" fest. Die Standardeinstellung "Null" bedeutet, dass der Vorabstart deaktiviert ist.

Hinweis:

Wenn der Client zur Unterstützung der Domänen-Passthrough-Authentifizierung (SSON) konfiguriert wurde, ist Vorabstart automatisch aktiviert. Wenn Sie die Domänen-Passthrough-Authentifizierung (SSON) ohne Vorabstart verwenden möchten, legen Sie den Registrierungsschlüssel `EnablePreLaunch` auf "false" fest.

Die Registrierungsverzeichnisse sind:

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

Es gibt zwei Arten von Vorabstart:

- **Just-In-Time-Vorabstart:** Der Vorabstart wird direkt nach dem Authentifizieren der Anmeldeinformationen des Benutzers gestartet, unabhängig davon, ob es sich um eine Zeit mit hohem Netzwerkverkehr handelt. Diese Option wird normalerweise für Zeiten mit normalen Datenverkehr verwendet. Ein Benutzer kann den Just-In-Time-Vorabstart durch einen Neustart der Citrix Workspace-App auslösen.

- **Geplanter Vorabstart:** Der Vorabstart wird nach einem Zeitplan gestartet. Ein geplanter Vorabstart startet nur, wenn das Benutzergerät bereits ausgeführt wird und authentifiziert wurde. Wenn diese beiden Bedingungen zur geplanten Vorabstartzeit nicht erfüllt sind, wird keine Sitzung gestartet. Um Netzwerk- und Serverlast zu teilen, wird die geplante Sitzung innerhalb eines Zeitfensters gestartet. Ist der Vorabstart beispielsweise für 13:45 geplant, erfolgt der Sitzungsstart irgendwann zwischen 13:15 und 13:45. Normalerweise für Zeiten mit normalen Datenverkehr verwendet.

Die Konfiguration des Vorabstarts auf einem Citrix Virtual Apps-Server umfasst Folgendes:

- Erstellen, Bearbeiten oder Löschen von Vorabstartanwendungen
- Aktualisieren der Benutzerrichtlinien, die die Vorabstartanwendung steuern.

Sie können das Vorabstartfeature nicht mit der Datei `receiver.admx` anpassen. Sie können die Vorabstartkonfiguration jedoch ändern, indem Sie die Registrierungswerte ändern. Dies kann während oder nach der Installation der Citrix Workspace-App für Windows erfolgen.

- Die HKEY_LOCAL_MACHINE-Werte werden während der Clientinstallation geschrieben.
- Mit den HKEY_CURRENT_USER-Werten können Sie verschiedenen Benutzern auf derselben Maschine unterschiedliche Einstellungen bereitstellen. Die Benutzer können die HKEY_CURRENT_USER-Werte ohne Administratorrechte ändern. Sie können Skripts bereitstellen, mit denen Benutzer die Werte ändern können.

Registrierungswerte für HKEY_LOCAL_MACHINE:

Für 64-Bit-Windows-Betriebssysteme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\PreLaunch`

Für 32-Bit-Windows-Betriebssysteme: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\PreLaunch`

Name: **UserOverride**

Typ: REG_DWORD

Werte:

0 - Wert unter HKEY_LOCAL_MACHINE verwenden, selbst wenn unter HKEY_CURRENT_USER Werte vorhanden sind.

1 - Werte unter HKEY_CURRENT_USER verwenden, wenn vorhanden; sonst die Werte unter HKEY_LOCAL_MACHINE verwenden.

Name: **State**

Typ: REG_DWORD

Werte:

0 - Vorabstart deaktivieren.

1 - Just-In-Time-Vorabstart aktivieren. (Vorabstart wird gestartet, nachdem die Anmeldeinformationen des Benutzers authentifiziert wurden.)

2 - Geplanten Vorabstart aktivieren. (Vorabstart startet zu der Zeit, die unter Schedule angegeben wurde.)

Name: **Schedule**

Typ: REG_DWORD

Wert:

Uhrzeit (24-Stunden-Format) und Wochentage für geplante Vorabstarts werden im folgenden Format angegeben:

HH:MM	Mo:Di:Mi:Do:Fr:Sa:So, wobei HH und MM Stunden und Minuten sind. Mo:Di:Mi:Do:Fr:Sa:So sind die Wochentage. Um beispielsweise den geplanten Vorabstart montags, mittwochs und freitags um 13:45 zu aktivieren, stellen Sie Folgendes ein: Schedule=13:45	1:0:1:0:1:0:0. Die Sitzung startet dann zwischen 13:15 und 13:45 Uhr.
-------	---	---

Registrierungswerte für HKEY_CURRENT_USER:

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Die Schlüssel **State** und **Schedule** haben dieselben Werte wie für HKEY_LOCAL_MACHINE.

Bidirektionale Inhaltsumleitung

Die bidirektionale Inhaltsumleitung ermöglicht das Aktivieren und Deaktivieren der Client-zu-Host- und der Host-zu-Client-URL-Umleitung. Serverrichtlinien werden in Studio festgelegt und Clientrichtlinien werden in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App festgelegt.

Citrix bietet Host-zu-Client-Umleitung und lokalen App-Zugriff für die Client-zu-URL-Umleitung. Wir empfehlen jedoch, dass Sie die bidirektionale Inhaltsumleitung für domänenverbundene Windows-Clients verwenden.

Sie können die bidirektionale Inhaltsumleitung auf folgende Weise aktivieren:

1. Administrative Gruppenrichtlinienobjektvorlage

2. Registrierungs-Editor

Hinweis:

- Die bidirektionale Inhaltsumleitung funktioniert nicht in einer Sitzung, in der **Lokaler App-Zugriff** aktiviert ist.
- Die bidirektionale Inhaltsumleitung muss auf dem Server und dem Client aktiviert sein. Wenn sie auf dem Server oder auf dem Client deaktiviert ist, ist die Funktion deaktiviert.
- Wenn Sie URLs einschließen, können Sie eine URL angeben oder eine durch Semikolon getrennte Liste von URLs. Sie können ein Sternchen (*) als Platzhalter verwenden.

Aktivieren der bidirektionalen Inhaltsumleitung mit der administrativen Gruppenrichtlinienobjektvorlage:

Verwenden Sie die Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage nur für die Erstinstallation der Citrix Workspace-App für Windows.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Bidirektionale Inhaltsumleitung**.

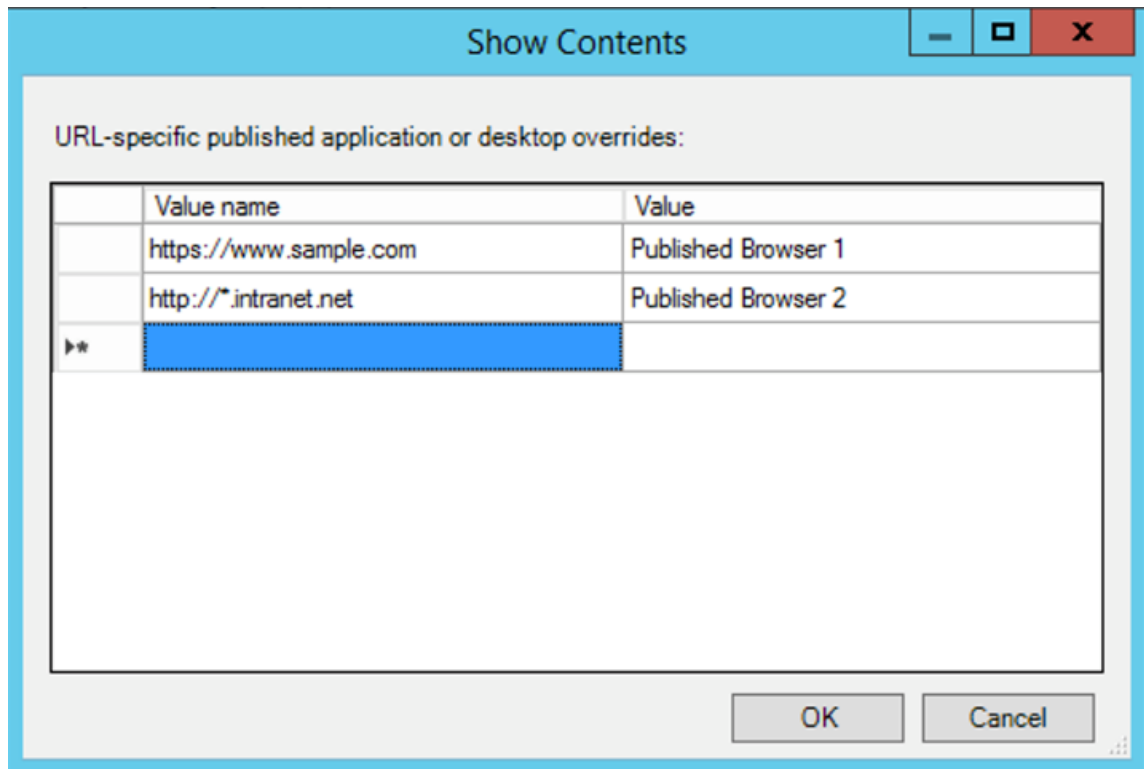
1. Geben Sie im Feld **Veröffentlichte Anwendungen oder Desktops** den Namen der Ressource ein, die zum Starten der umgeleiteten URL verwendet wird.

Hinweis:

Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (*) als Platzhalter verwenden.

2. Wählen Sie unter **Veröffentlicht als** die Option **Anwendung** oder **Desktop** aus.
3. Geben Sie im Feld **Für Umleitung an VDA zulässige URLs** die URL ein, die umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

4. Wählen Sie **URL-spezifische Außerkraftsetzungen für veröffentlichte Anwendungen oder Desktops aktivieren?**, wenn für eine URL eine Außerkraftsetzung gelten soll.
5. Klicken Sie auf **Anzeigen**, um eine Liste anzuzeigen, in der der Wertname mit einer der URLs im Feld **Für Umleitung an VDA zulässige URLs** übereinstimmen muss. Der Wert muss mit dem Namen einer veröffentlichten Anwendung übereinstimmen.



6. Geben Sie im Feld **Für Umleitung an Client zulässige URLs** die URL ein, die vom Server an den Client umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

Hinweis:

Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (*) als Platzhalter verwenden.

7. Klicken Sie auf **Anwenden** und **OK**.
8. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus.

Aktivieren der bidirektionalen Inhaltsumleitung mit der Registrierung:

Zum Aktivieren der bidirektionalen Inhaltsumleitung führen Sie den Befehl `redirector.exe /RegIE` im Installationsordner der Citrix Workspace-App aus (C:\Program Files (x86)\Citrix\ICA Client)).

Wichtig:

- Stellen Sie sicher, dass die Umleitungsregel keine Schleifenkonfiguration ergibt. Eine Schleifenkonfiguration entsteht zum Beispiel, wenn VDA-Regeln so festgelegt sind, dass eine URL wie https://www.my_company.com an den Client und an den VDA umgeleitet wird.
- Die URL-Umleitung unterstützt nur explizite URLs, also URLs, die in der Adressleiste des Browsers angezeigt werden oder die mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Wenn zwei Anwendungen mit demselben Anzeigenamen mehrere StoreFront-Konten verwenden, wird der Anzeigename im primären StoreFront-Konto für den Start der Anwendung oder einer Desktopsitzung verwendet.
- Ein neues Browserfenster wird nur geöffnet, wenn eine URL zum Client umgeleitet wird. Wenn eine URL zum VDA umgeleitet wird, und der Browser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet.
- Eingebettete Links in Dateien wie Dokumente, E-Mails, PDFs werden unterstützt.
- Stellen Sie sicher, dass auf einer Maschine nur eine der Serverdateitypzuordnungen existiert und dass die Richtlinien für die Hostinhaltsumleitung aktiviert sind. Citrix empfiehlt, entweder die Serverdateitypzuordnung oder das URL-Umleitungsfeature zu deaktivieren, damit die URL-Umleitung ordnungsgemäß funktioniert.

Einschränkung:

Kein Fallbackmechanismus ist vorhanden, wenn die Umleitung aufgrund von Problemen mit dem Sitzungsstart fehlschlägt.

Bidirektionale URL-Unterstützung mit Chromium-basierten Browsern

Die bidirektionale Inhaltsumleitung ermöglicht es Ihnen, URLs für die Umleitung vom Client zum Server und vom Server zum Client mithilfe von Richtlinien auf Server und Client zu konfigurieren.

Serverrichtlinien werden auf dem Delivery Controller festgelegt und Clientrichtlinien in der Citrix Workspace-App. Die Richtlinien werden mit der administrativen Gruppenrichtlinienobjektvorlage festgelegt.

Ab Version 2106 wird die bidirektionale URL-Umleitung für Google Chrome und Microsoft Edge unterstützt.

Voraussetzungen:

- Citrix Virtual Apps and Desktops Version 2106 oder höher.
- Erweiterung für die Browserumleitung Version 5.0.

Um den Google Chrome-Browser für die bidirektionale URL-Umleitung zu registrieren, führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App aus:

```
%ProgramFiles(x86)%\Citrix\ICA Client\Redirector.exe /regChrome /verbose
```

Hinweis:

Wenn Sie diese Befehle für Chrome-Browser verwenden, wird die [Erweiterung für die bidirektionale Inhaltsumleitung](#) automatisch aus dem Chrome Web Store installiert.

Um die Registrierung des Google Chrome-Browsers für die bidirektionale URL-Umleitung aufzuheben, führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App aus:

```
%ProgramFiles(x86)%\Citrix\ICA Client\Redirector.exe /unregChrome /verbose
```

Hinweis:

Wenn beim Zugriff auf die Seite “Browsererweiterungen” die folgende Fehlermeldung angezeigt wird, ignorieren Sie die Meldung:

```
WebSocket connection to wss://... failed.
```

Informationen zum Konfigurieren der URL-Umleitung in der Citrix Workspace-App finden Sie unter [Bidirektionale Inhaltsumleitung](#).

Abblenden des Desktop Viewer-Fensters verhindern:

Wenn Sie mehrere Desktop Viewer-Fenster verwenden, sind die nicht aktiven Desktops in der Standardeinstellung abgeblendet. Wenn Benutzer mehrere Desktops gleichzeitig anzeigen möchten, können die Informationen auf den Desktops unlesbar sein. Sie können das Standardverhalten deaktivieren und das Abblenden des **Desktop Viewer**-Fensters durch Bearbeiten der Registrierung verhindern.

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

- Erstellen Sie auf dem Benutzergerät einen REG_DWORD-Eintrag mit dem Namen **DisableDimming** in einem der folgenden Registrierungsschlüssel, abhängig davon, ob Sie ein Abblenden für den aktuellen Benutzer des Geräts oder für das Gerät selbst einstellen möchten. Ein Eintrag ist bereits vorhanden, wenn Desktop Viewer auf dem Gerät verwendet wurde:

- HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

Sie können das Abblenden steuern oder auch eine lokale Richtlinie festlegen, indem Sie denselben REG_WORD-Eintrag in einem der folgenden Schlüssel erstellen:

- HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

Überprüfen Sie vor der Verwendung dieser Schlüssel, ob der Administrator von Citrix Virtual Apps and Desktops und Citrix DaaS eine Richtlinie für dieses Feature festgelegt hat.

Stellen Sie den Eintrag auf einen Wert ungleich Null ein, z. B. 1 oder true.

Wenn keine Einträge angegeben sind, oder der Eintrag auf 0 gesetzt ist, wird das **Desktop Viewer**-Fenster abgeblendet. Bei Angabe mehrerer Einträge wird die folgende Priorität verwendet. Der erste Eintrag und Wert in der Liste legen fest, ob das Fenster abgeblendet wird:

1. HKEY_CURRENT_USER\Software\Policies\Citrix\...
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\...
3. HKEY_CURRENT_USER\Software\Citrix\...
4. HKEY_LOCAL_MACHINE\Software\Citrix\...

Citrix Casting

Der Citrix Ready Workspace Hub verbindet die digitale und die physische Umgebung zur Bereitstellung von Apps und Daten in einem sicheren, intelligenten Bereich. Das System verbindet Geräte (oder auch Dinge, z. B. mobile Apps und Sensoren) zur Schaffung einer intelligenten und reaktionsfähigen Umgebung.

Citrix Ready Workspace Hub baut auf der Raspberry Pi 3-Plattform auf. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, stellt eine Verbindung zum Citrix Ready Workspace Hub her und ermöglicht die Anzeige von Apps und Desktops auf einem größeren Display. Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.

Mit Citrix Casting können Sie sofort und sicher auf jede App auf einem Mobilgerät zugreifen und sie auf einem großen Bildschirm anzeigen.

Hinweis:

- Citrix Casting für Windows unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.

- Citrix Casting wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.

Voraussetzungen:

- Bluetooth ist zur Hub-Erkennung auf dem Gerät aktiviert.
- Citrix Ready Workspace Hub und Citrix Workspace-App müssen sich im selben Netzwerk befinden.
- Port 55555 ist zwischen dem Gerät mit ausgeführter Citrix Workspace-App und dem Citrix Ready Workspace Hub zugelassen.
- Port 1494 darf für Citrix Casting nicht blockiert sein.
- Port 55556 ist der Standardport für SSL-Verbindungen zwischen Mobilgeräten und dem Citrix Ready Workspace Hub. Sie können in den Einstellungen von Raspberry Pi einen anderen SSL-Port konfigurieren. Wenn der SSL-Port blockiert ist, können die Benutzer keine SSL-Verbindungen zum Workspace Hub herstellen.
- Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.

Konfigurieren des Citrix Casting-Starts

Hinweis:

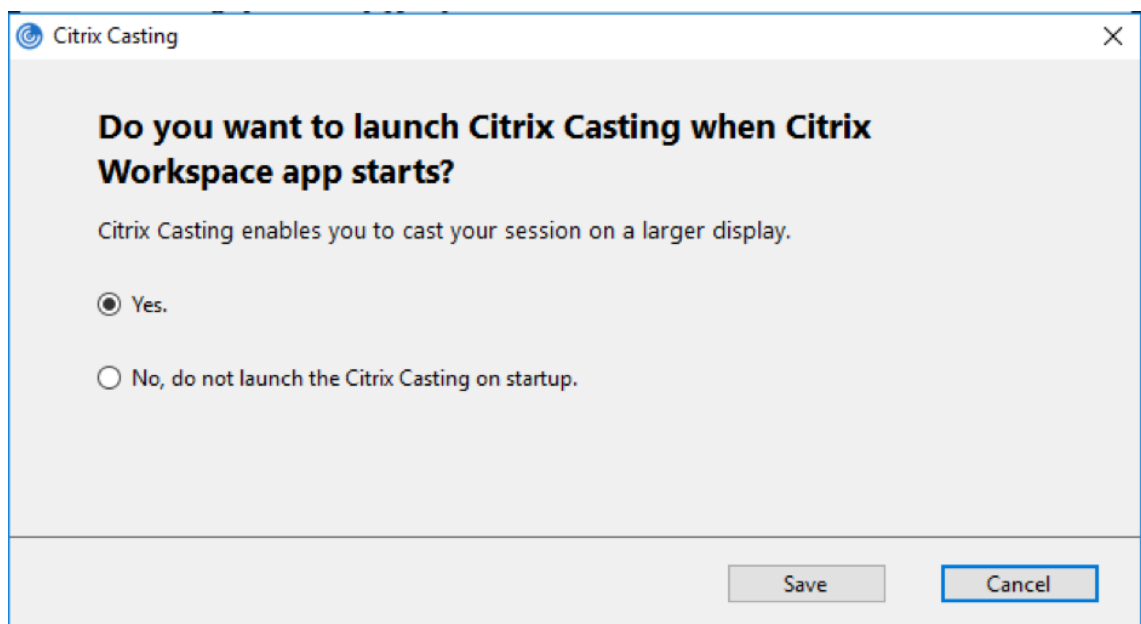
Sie können die Seite "Erweiterte Einstellungen" ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

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

Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.

2. Wählen Sie **Citrix Casting**.

Das Dialogfeld **Citrix Casting** wird angezeigt.



3. Wählen Sie eine dieser Optionen:

- Ja –Citrix Casting wird beim Start der Citrix Workspace-App ebenfalls gestartet.
- Nein, Citrix Casting beim Start nicht starten –Gibt an, dass Citrix Casting beim Start der Citrix Workspace-App nicht gestartet wird.

Hinweis:

Bei Auswahl der Option **Nein** wird die aktuelle Bildschirmcastingsitzung nicht beendet. Die Einstellung wird erst beim nächsten Start der Citrix Workspace-App wirksam.

4. Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.

Citrix Casting mit der Citrix Workspace-App verwenden

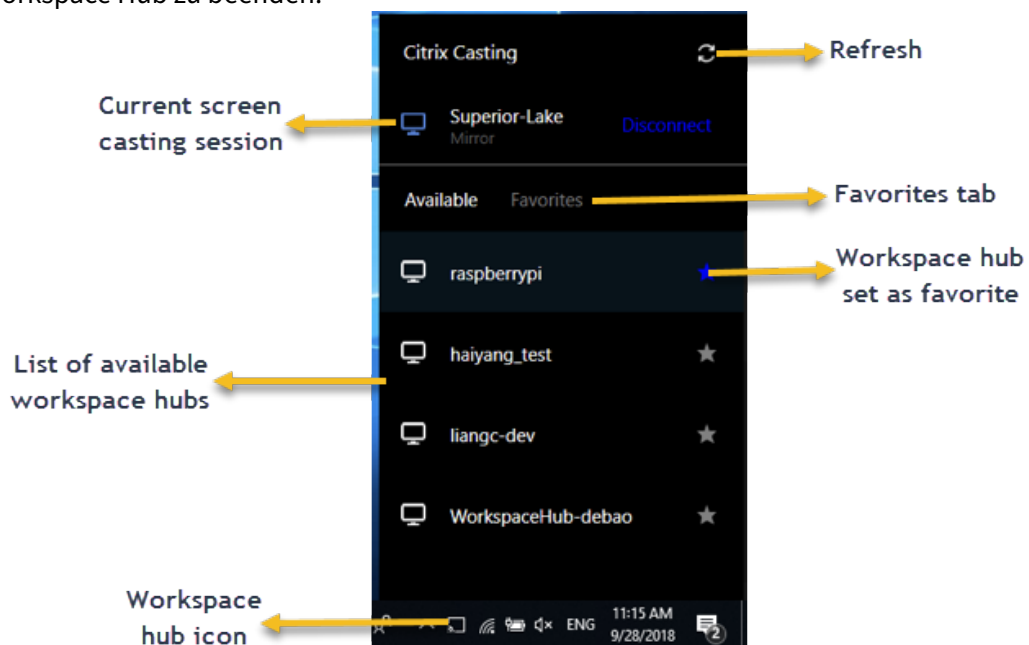
1. Melden Sie sich an der Citrix Workspace-App an und aktivieren Sie Bluetooth auf Ihrem Gerät.
Die Liste der verfügbaren Hubs wird angezeigt. Die Liste ist nach dem RSSI-Wert des Beaconpakets der Workspace Hubs sortiert.
2. Wählen Sie den Workspace Hub aus, an den Sie Ihre Anzeige übertragen möchten, und wählen Sie eine der folgenden Optionen:
 - Mit **Spiegeln** können Sie den primären Bildschirm duplizieren und die Anzeige an das verbundene Workspace Hub-Gerät übertragen.
 - Mit **Erweitern** können Sie den Bildschirm des Workspace Hub-Geräts als sekundären Bildschirm verwenden.

Hinweis:

Beim Beenden der Citrix Workspace-App wird Citrix Casting nicht beendet.

Im Infobereich von **Citrix Casting** sind folgende Optionen verfügbar:

1. Die aktuelle Bildschirmcastingsitzung wird oben angezeigt.
2. Symbol **Aktualisieren**.
3. Wählen Sie **Trennen**, um die aktuelle Bildschirmcastingsitzung auf dem Workspace Hub zu beenden.
4. Mit dem Stern fügen Sie den Workspace Hub zu **Favoriten** hinzu.
5. Klicken Sie mit der rechten Maustaste auf das Workspace Hub-Symbol im Infobereich und wählen Sie **Beenden**, um die Bildschirmcastingsitzung zu trennen und den Citrix Ready Workspace Hub zu beenden.



Checkliste bei Problemen

Prüfen Sie folgende Faktoren, wenn die Citrix Workspace-App keine verfügbaren Workspace Hubs im Umfeld erkennt oder mit ihnen nicht kommunizieren kann:

1. Citrix Workspace-App und Citrix Ready Workspace Hub sind mit demselben Netzwerk verbunden.
2. Bluetooth ist aktiviert und funktioniert ordnungsgemäß auf dem Gerät, auf dem die Citrix Workspace-App ausgeführt wird.

3. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, liegt in Reichweite des Citrix Ready Workspace Hub, also weniger als 10 Meter entfernt und nicht hinter einer Wand oder einem anderen Hindernis.
4. Öffnen Sie einen Browser in der Citrix Workspace-App und geben Sie `http://<hub_ip>:55555/device-details.xml` ein, um zu überprüfen, ob die Details des Workspace Hub-Geräts angezeigt werden.
5. Klicken Sie in Citrix Ready Workspace Hub auf **Aktualisieren** und versuchen Sie erneut, eine Verbindung zum Workspace Hub herzustellen.

Bekannte Probleme und Einschränkungen

1. Citrix Casting funktioniert nur, wenn das Gerät mit demselben Netzwerk wie der Citrix Ready Workspace Hub verbunden ist.
2. Bei Netzwerkproblemen kann es zu einer verzögerten Anzeige auf dem Workspace Hub-Gerät kommen.
3. Bei Auswahl von **Erweitern** blinkt der primäre Bildschirm, auf dem die Citrix Ready Workspace-App gestartet wird, mehrmals.
4. Im Modus **Erweitern** können Sie die sekundäre Anzeige nicht als primäre Anzeige festlegen.
5. Die Bildschirmcastingsitzung wird automatisch beendet, wenn die Anzeigeeinstellungen auf dem Gerät geändert werden. Dies kann beispielsweise auftreten, wenn Sie die Bildschirmauflösung oder Bildschirmausrichtung ändern.
6. Wenn das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, während der Bildschirmcastingsitzung gesperrt, inaktiviert oder in den Ruhezustand versetzt wird, wird beim Anmelden ein Fehler angezeigt.
7. Mehrere Bildschirmcastingsitzungen werden nicht unterstützt.
8. Die von Citrix Casting unterstützte maximale Bildschirmauflösung beträgt 1920 x 1440.
9. Citrix Casting unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.
10. Das Feature wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.
11. Unter Windows 10, Build 1607 wird Citrix Casting im Modus **Erweitert** u. U. nicht richtig positioniert.

Weitere Informationen zu Citrix Ready Workspace Hub finden Sie unter [Citrix Ready Workspace Hub](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Umleitung von USB-Verbundgeräten

USB 2.1 und höher unterstützt USB-Verbundgeräte, bei denen mehrere untergeordnete Geräte sich eine Verbindung mit demselben USB-Bus teilen. Die Geräte teilen sich Konfigurationsraum und Busverbindung, und zur Identifizierung jedes untergeordneten Geräts wird eine eindeutige

Schnittstellenzahl 00-ff verwendet. Diese Geräte sind auch nicht identisch mit einem USB-Hub, der einen neuen USB-Bus zum Anschluss anderer USB-Geräte mit jeweils eigener Adresse bereitstellt.

Auf dem Clientendpunkt gefundene Verbundgeräte können wie folgt an den virtuellen Host weitergeleitet werden:

- als einzelnes USB-Verbundgerät oder
- als Gruppe unabhängiger untergeordneter Geräte (aufgeteilte Geräte)

Wenn ein USB-Verbundgerät weitergeleitet wird, steht das gesamte Gerät dem Endpunkt nicht mehr zur Verfügung. Durch das Weiterleiten wird auch die lokale Nutzung des Geräts für alle Anwendungen auf dem Endpunkt blockiert –auch für den Citrix Workspace-Client, der für eine optimierte HDX-Remoteerfahrung erforderlich ist.

Verwenden Sie gegebenenfalls ein USB-Headset mit Audiogerät und HID-Taste für Stummschaltung und Lautstärkeregelung. Wenn das gesamte Gerät über einen generischen USB-Kanal weitergeleitet wird, kann es nicht mehr über den optimierten HDX-Audiokanal umgeleitet werden. Die Audioqualität ist jedoch am besten, wenn Audiodaten über den optimierten HDX-Audiokanal und nicht mit hostseitigen Audiotreibern über generisches USB-Remoting gesendet werden. Dieses Verhalten liegt an der “geschwätzigen”Natur der USB-Audioprotokolle.

Weitere Probleme treten auf, wenn Systemtastatur oder Zeigegerät zu einem Verbundgerät gehören, in dem auch Funktionen integriert sind, die für Remotesitzungen erforderlich sind. Wird ein komplettes Verbundgerät weitergeleitet, funktionieren Systemtastatur oder Maus am Endpunkt nur noch innerhalb der Remotedesktopsitzung oder -anwendung.

Zum Beheben dieser Probleme empfiehlt Citrix, das Verbundgerät per Splitting aufzuteilen und nur die untergeordneten Schnittstellen weiterzuleiten, die einen generischen USB-Kanal verwenden. Die übrigen untergeordneten Geräte können dadurch weiterhin von Anwendungen auf dem Clientendpunkt verwendet werden, einschließlich der Citrix Workspace-App, die ein optimiertes HDX-Erlebnis bietet. Gleichzeitig werden nur die erforderlichen Geräte weitergeleitet und der Remotesitzung zur Verfügung gestellt.

Geräteregeln:

Wie auch USB-Standardgeräte werden die Verbundgeräte von Geräteregeln, die in der Richtlinie oder der Citrix Workspace-App auf dem Clientendpunkt konfiguriert sind, für die Weiterleitung ausgewählt. Die Citrix Workspace-App entscheidet dann anhand dieser Regeln, welche USB-Geräte an die Remotesitzung weitergeleitet werden dürfen.

Jede Regel besteht aus einem Aktionsschlüsselwort (Allow, Connect oder Deny), einem Doppelpunkt (:), und null oder mehr Filterparametern, die den tatsächlichen Geräten am USB-Subsystem des Endpunkts entsprechen. Diese Filterparameter entsprechen den Metadaten des USB-Gerätedeskriptors, die von jedem USB-Gerät zur Identifizierung verwendet werden.

Geräteregeln sind als Klartext angegeben, mit einer Regel pro Zeile und einem optionalen Kommentar nach dem #-Zeichen. Regeln werden von oben nach unten (in absteigender Prioritätsreihenfolge) zugeordnet. Die erste Regel, die dem Gerät oder der untergeordneten Schnittstelle entspricht, wird angewendet. Nachfolgende Regeln, die dasselbe Gerät oder dieselbe Schnittstelle auswählen, werden ignoriert.

Beispiele für GeräteregeIn:

- ALLOW: vid=046D pid=0102 # Bestimmtes Gerät gemäß vid/pid zulassen
- ALLOW: vid=0505 class=03 subclass=01 # Jede pid für Anbieter 0505 zulassen, wenn subclass=01
- DENY: vid=0850 pid=040C # Bestimmtes Gerät (und alle untergeordneten Geräte) ablehnen
- DENY: class=03 subclass=01 prot=01 # Jedes Gerät ablehnen, dass allen Filtern entspricht
- CONNECT: vid=0911 pid=0C1C # Bestimmtes Gerät zulassen und automatisch verbinden
- ALLOW: vid=0286 pid=0101 split=01 # Dieses Gerät aufteilen und alle Schnittstellen zulassen
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Aufteilen und nur zwei Schnittstellen zulassen
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Aufteilen und Schnittstelle 2 automatisch verbinden
- DENY: vid=1050 pid=0407 split=1 intf=03 # Remoting von Schnittstelle 03 verhindern

Sie können einen der folgenden Filterparameter verwenden, um Regeln auf die erkannten Geräte anzuwenden:

Filterparameter	Beschreibung
vid=xxxx	Hersteller-ID des USB-Geräts (vierstelliger Hexadezimalcode)
pid=xxxx	Produkt-ID des USB-Geräts (vierstelliger Hexadezimalcode)
rel=xxxx	Release-ID des USB-Geräts (vierstelliger Hexadezimalcode)
class=xx	Klassencode des USB-Geräts (zweistelliger Hexadezimalcode)
subclass=xx	Unterklassencode des USB-Geräts (zweistelliger Hexadezimalcode)
prot=xx	Protokollcode des USB-Geräts (zweistelliger Hexadezimalcode)
split=1 (oder split=0)	Aufteilen (oder Nichtaufteilen) eines Verbundgeräts

Filterparameter	Beschreibung
<code>intf=xx[,xx,xx,...]</code>	Auswahl einer bestimmten Gruppe untergeordneter Schnittstellen eines Verbundgeräts (durch Kommas getrennte Liste mit zweistelligen Hexadezimalcodes)

Mit den ersten sechs Parametern werden die USB-Geräte ausgewählt, auf die die Regel angewendet werden soll. Wenn kein Parameter definiert ist, wird die Regel einem Gerät mit einem BELIEBIGEN Wert für diesen Parameter zugeordnet.

Das USB Implementers Forum (USB-IF) bietet unter [Defined Class Codes](#) eine Liste definierter Klassen-, Unterklassen- und Protokollwerte. USB-IF bietet außerdem eine Liste registrierter Hersteller-IDs. Hersteller-, Produkt-, Release- und Schnittstellen-ID eines Geräts finden Sie auch in der Windows-Geräteverwaltung oder mithilfe kostenloser Tools wie USBTreeView.

Die letzten beiden Parameter gelten (sofern vorhanden) nur für USB-Verbundgeräte. Der `split`-Parameter legt fest, ob ein Verbundgerät als aufgeteiltes Gerät oder als einzelnes Verbundgerät weitergeleitet werden soll.

- `Split=1` zeigt an, dass die ausgewählten untergeordneten Schnittstellen eines Verbundgeräts als aufgeteilte Geräte weiterzuleiten sind.
- `Split=0` zeigt an, dass das Verbundgerät nicht aufgeteilt werden darf.

Hinweis:

Ist der `split`-Parameter nicht vorhanden, wird dies als `Split=0` interpretiert.

Der `intf`-Parameter wählt die untergeordneten Schnittstellen des Verbundgeräts aus, auf die eine Aktion anzuwenden ist. Ist der Parameter nicht vorhanden, wird die Aktion auf alle Schnittstellen des Verbundgeräts angewendet.

Das folgende Headset ist ein USB-Verbundgerät mit drei Schnittstellen:

- Schnittstelle 0: Geräteendpunkte der Audioklasse
- Schnittstelle 3: Geräteendpunkte der HID-Klasse (Tasten für Lautstärkeregelung und Stumm-schaltung)
- Schnittstelle 5: Schnittstelle für Verwaltung/Aktualisierung

Folgende Regeln werden für diese Gerätetypen empfohlen:

- CONNECT: `vid=047F pid=C039 split=1 intf=03` # Eingabegerät zulassen und automatisch verbinden
- DENY: `vid=047F pid=C039 split=1 intf=00` # Audioendpunkte ablehnen

- ALLOW: vid=047F pid=C039 split=1 intf=05 # Verwaltungsschnittstelle `intf` zulassen aber nicht automatisch verbinden

Aktivieren der Richtlinie für GeräteregeIn:

Die Citrix Workspace-App für Windows enthält mehrere StandardgeräteregeIn, mit denen unerwünschte Geräteklassen herausgefiltert werden und eine vom Kunden häufig verwendete Klasse zugelassen wird.

Sie finden diese StandardgeräteregeIn in der Systemregistrierung für:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (32-Bit-Windows) oder
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (64 Bit Windows), im Wert der mehrteiligen Zeichenfolge **DeviceRules**.

In der Citrix Workspace-App für Windows können Sie diese Standardregeln jedoch mit der Richtlinie **USB-GeräteregeIn** überschreiben.

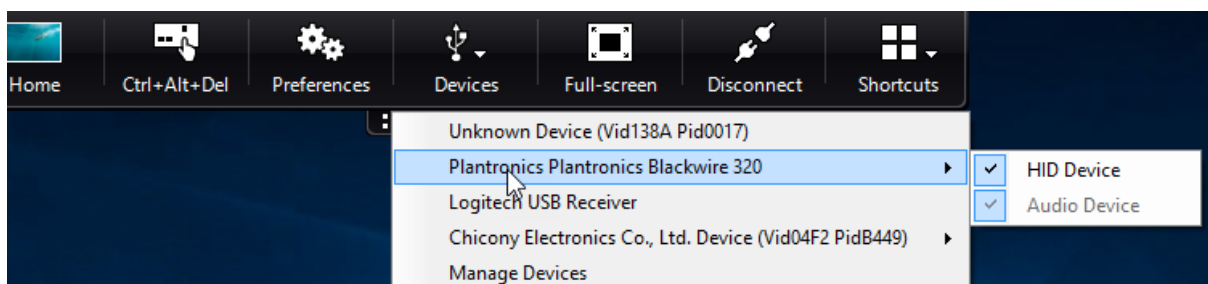
Aktivieren der Richtlinie für GeräteregeIn für die Citrix Workspace-App für Windows:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Remoting von Clientgeräten > Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-GeräteregeIn**.
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-GeräteregeIn** die gewünschten USB-GeräteregeIn ein (oder bearbeiten Sie sie direkt).
6. Klicken Sie auf **Anwenden** und **OK**.

Citrix empfiehlt, die voreingestellten Standardregeln auf dem Client vor dem Erstellen dieser Richtlinie zu sichern, indem Sie die Originalregeln kopieren und dann neue Regeln einfügen, um das Verhalten nach Wunsch zu ändern.

USB-Geräte anschließen:

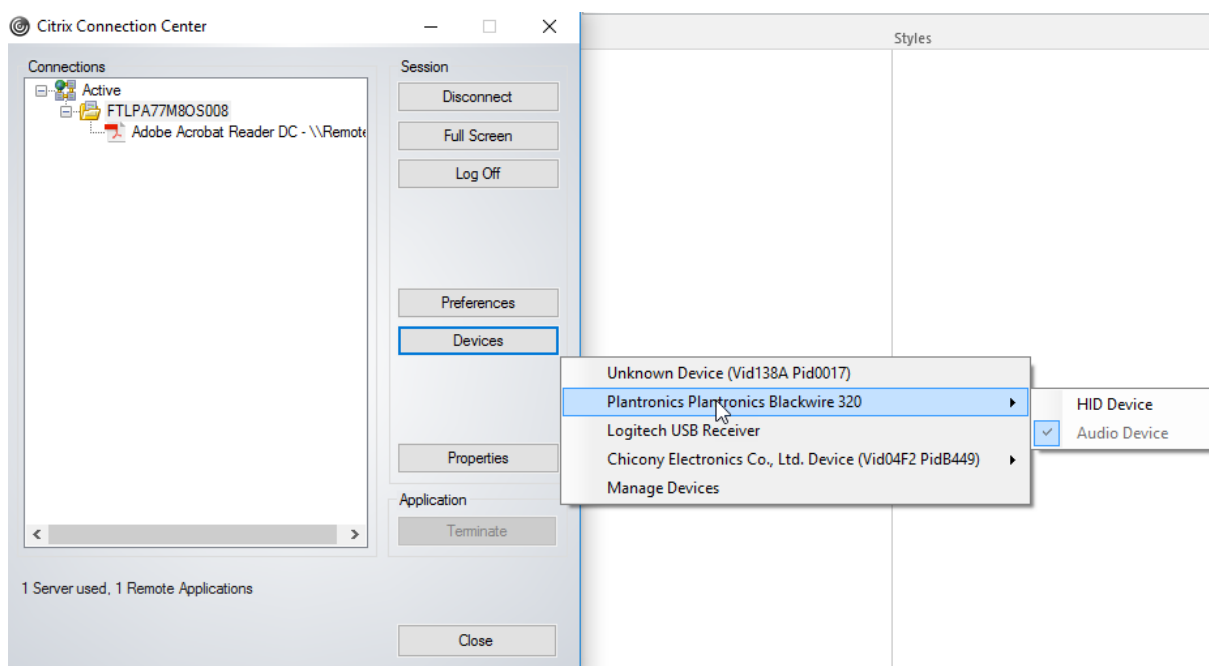
In einer Desktopsitzung werden per Splitting aufgeteilte USB-Geräte im Desktop Viewer unter **Geräte** angezeigt. Darüber hinaus werden aufgeteilte USB-Geräte unter **Einstellungen > Geräte** angezeigt.



Hinweis:

Das Schlüsselwort CONNECT aktiviert das automatische Verbinden eines USB-Geräts. Wenn Sie das Schlüsselwort CONNECT jedoch beim Aufteilen eines USB-Verbundgeräts für die generische USB-Umleitung nicht verwenden, müssen Sie das Gerät im Desktop Viewer oder Connection Center manuell auswählen, um ein zugelassenes Gerät zu verbinden.

In einer Anwendungssitzung werden per Splitting aufgeteilte USB-Geräte im **Connection Center** angezeigt.



Automatisches Verbinden einer Schnittstelle:

Das Schlüsselwort CONNECT, das in der Citrix Workspace-App für Windows 2109 eingeführt wurde, ermöglicht das automatische Umleiten von USB-Geräten. Die CONNECT-Regel kann die ALLOW-Regel ersetzen, wenn der Administrator zulässt, dass ein Gerät oder ausgewählte Schnittstellen sich automatisch in der Sitzung verbinden.

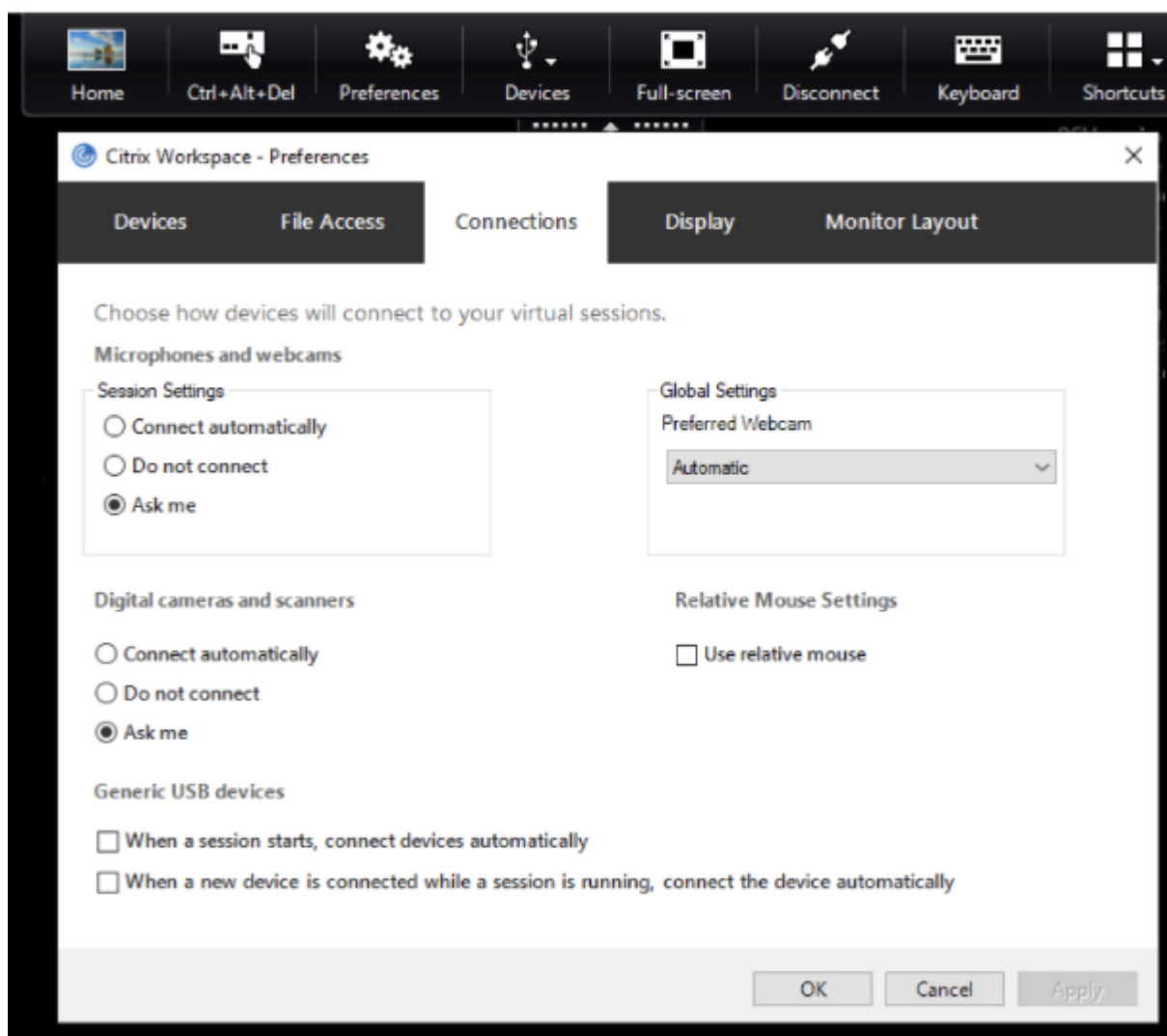
1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.

2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Remoting von Clientgeräten > Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-Geräteregeln**.
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-Geräteregeln** das USB-Gerät hinzu, für das Sie das automatische Verbinden aktivieren möchten.

Beispiel: `CONNECT: vid=047F pid=C039 split=01 intf=00,03` ermöglicht das Aufteilen eines Verbundgeräts, das automatische Verbinden der Schnittstellen 00 und 03 und die Beschränkung anderer Schnittstellen dieses Geräts.
6. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

Einstellungen für die automatische Verbindung von USB-Geräten ändern:

Die Citrix Workspace-App verbindet mit CONNECT-Aktion gekennzeichnete USB-Geräte automatisch gemäß den Einstellungen, die für die aktuelle Desktopressource festgelegt sind. Sie können die Einstellungen in der Symbolleiste des **Desktop Viewer** ändern, wie in der folgenden Abbildung dargestellt.



Mit den beiden Kontrollkästchen unten im Fenster legen Sie fest, ob Geräte sich automatisch verbinden oder auf eine manuelle Verbindung in der Sitzung warten müssen. Diese Einstellungen sind nicht standardmäßig aktiviert. Sie können die Einstellungen ändern, falls generische USB-Geräte automatisch verbunden werden müssen.

Ein Administrator kann die Benutzereinstellungen auch überschreiben, indem er die entsprechenden Richtlinien über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App bereitstellt. Maschinen- und Benutzerrichtlinien finden Sie unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Remoting von Clientgeräten > Generisches USB-Remoting**. Die entsprechenden Richtlinien sind als "Vorhandene USB-Geräte" bzw. "Neue USB-Geräte" gekennzeichnet.

Ändern der Standardeinstellung für aufgeteilte Geräte:

Standardmäßig werden Verbundgeräte von der Citrix Workspace-App für Windows nur dann aufgeteilt, wenn sie in den Geräteregelexplizit mit *Split=1* gekennzeichnet sind. Dieses Standard-

verhalten lässt sich jedoch ändern, um alle Verbundgeräte aufzuteilen, die nicht mit *Split=0* in einer zugeordneten Geräteregelel gekennzeichnet sind.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices** (Geräte teilen).
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

Hinweis:

Citrix empfiehlt, aufzuteilende Geräte oder Schnittstellen über explizite Geräteregelel festzulegen, anstatt die Standardeinstellung zu ändern. Diese Einstellung wird in einem zukünftigen Release ausgemustert.

Einschränkung:

Citrix empfiehlt, Schnittstellen für eine Webcam nicht per Splitting aufzuteilen. Als Workaround können Sie das Gerät über die generische USB-Umleitung an ein einzelnes Gerät weiterleiten. Verwenden Sie zur Leistungsverbesserung den optimierten virtuellen Kanal.

Bloomberg-Tastaturen

Die Citrix Workspace-App unterstützt die Verwendung einer Bloomberg-Tastatur in einer Citrix Virtual Apps and Desktops-Sitzung. Die erforderlichen Komponenten werden mit dem Plug-In installiert. Sie können das Feature für Bloomberg-Tastaturen zusammen mit der Citrix Workspace-App für Windows installieren oder über die Registrierung aktivieren.

Im Vergleich zu Standardtastaturen bieten Bloomberg-Tastaturen bessere Funktionen, mit denen Benutzer auf Finanzmarktdaten zugreifen und Transaktionen durchführen können.

Die Bloomberg-Tastatur besteht aus mehreren USB-Geräten, die in einem Gehäuse zusammengefasst sind:

- Tastatur
- Fingerabdruckleser
- Audiogerät
- USB-Hub zum Anschluss all dieser Geräte an das System
- HID-Tasten für das Audiogerät, z. B. zum Stummschalten und zur Lautstärkeregelung

Zusätzlich zu den Standardfunktionen dieser Geräte unterstützt das Audiogerät diverse Tasten und Tastatur-LEDs und eine Steuerung der Tastatur.

Um die Spezialfunktionen in einer Sitzung zu verwenden, müssen Sie das Audiogerät als USB-Gerät umleiten. Dadurch wird das Audiogerät für die Sitzung verfügbar, es kann jedoch nicht mehr lokal verwendet werden. Die Spezialfunktionen können zudem nur von einer Sitzung und nicht von mehreren Sitzungen gemeinsam genutzt werden.

Mehrere Sitzungen mit Bloomberg-Tastaturen sind nicht empfehlenswert. Die Tastatur funktioniert nur in Einzelsitzungen.

Konfigurieren der Bloomberg-Tastatur 5:

Sie müssen verschiedene Schnittstellen der Bloomberg-Tastatur konfigurieren. In der Citrix Workspace-App für Windows 2109 wird ein neues CONNECT-Schlüsselwort eingeführt, das die automatische Verbindung von USB-Geräten beim Sitzungsstart und Anschließen von Geräten ermöglicht. Das Schlüsselwort CONNECT kann anstelle des Schlüsselworts ALLOW verwendet werden, wenn ein Benutzer ein USB-Gerät oder eine Schnittstelle automatisch verbinden möchte. Im folgenden Beispiel wird das Schlüsselwort CONNECT verwendet.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices** (Geräte teilen).
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-Geräteregeln** die folgenden Regeln hinzu, falls sie noch nicht vorhanden sind.
 - CONNECT: vid=1188 pid=A101 # Biometrisches Bloomberg-Modul 5
 - DENY: vid=1188 pid=A001 split=01 intf=00 # Primäre Bloomberg-Tastatur 5
 - CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg-Tastatur 5 - Eingabegerät
 - DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg-Tastatur 5 - Audiokanal
 - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg-Tastatur 5 - Audio-Eingabegerät

Hinweis:

Zeilenumbruch oder Semikolon können verwendet werden, um Regeln zu trennen, sodass ein- oder mehrzeilige Registrierungswerte gelesen werden können.

6. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

7. Wählen Sie im Fenster **Einstellungen** die Registerkarte **Verbindungen** und aktivieren Sie ein oder beide Kontrollkästchen, um Geräte automatisch zu verbinden. Das Fenster **Einstellungen** kann über die Desktopsymbolleiste oder den Verbindungsmanager geöffnet werden.

Mit diesem Verfahren wird die Bloomberg-Tastatur 5 einsatzbereit. Mit den DENY-Regeln in der Schrittfolge erzwingen Sie, dass die primäre Tastatur und der Audiokanal nicht über generisches USB, sondern über einen optimierten Kanal umgeleitet werden. Mit den CONNECT-Regeln aktivieren Sie die automatische Umleitung des Fingerabdruckmoduls, von Sondertasten auf der Tastatur und von Tasten zur Audiosteuerung.

Konfigurieren der Bloomberg-Tastatur 4 oder 3:

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Gehen Sie zu folgenden Schlüsseln in der Registrierung:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

2. Führen Sie einen der folgenden Schritte aus:

- Zum Aktivieren dieses Features müssen Sie den Eintrag mit Typ DWORD und dem Namen **EnableBloombergHID** auf den Wert 1 setzen.
- Zum Deaktivieren dieses Features setzen Sie den Wert auf 0.

Unterstützung für die Bloomberg-Tastatur 3 ist im Online-Plug-In für Windows ab Version 11.2 verfügbar.

Unterstützung für die Bloomberg-Tastatur 4 ist für Windows Receiver 4.8 und höher verfügbar.

Prüfung auf aktivierte Unterstützung für Bloomberg-Tastaturen:

- Um festzustellen, ob die Bloomberg-Tastaturunterstützung im Online-Plug-In aktiviert ist, prüfen Sie, ob die Bloomberg-Tastaturgeräte im Desktop Viewer angezeigt werden. Wenn der Desktop Viewer nicht verwendet wird, können Sie die Registrierung auf der Maschine überprüfen, auf der das Online-Plug-In ausgeführt wird.
- Bei nicht aktivierter Unterstützung für Bloomberg-Tastaturen wird Folgendes im Desktop Viewer angezeigt:
 - zwei Geräte für die Bloomberg-Tastatur 3, angezeigt als **Bloomberg Fingerprint Scanner** und **Bloomberg Keyboard Audio**.

- ein Gerät mit Richtlinienumleitung für die Bloomberg-Tastatur 4. Dieses Gerät wird als **Bloomberg LP Keyboard 2013** angezeigt.
- Bei aktivierter Unterstützung für Bloomberg-Tastaturen werden zwei Geräte im Desktop Viewer angezeigt. Ein Gerät wird wie zuvor als **Bloomberg Fingerprint Scanner** angezeigt und ein Gerät als **Bloomberg Keyboard Features**.
- Bei nicht installiertem Treiber für den Bloomberg-Fingerabdruckscanner wird der zugehörige Eintrag möglicherweise nicht im Desktop Viewer angezeigt. Fehlt der Eintrag, steht der Bloomberg-Fingerabdruckscanner möglicherweise nicht für die Umleitung zur Verfügung. Sie können weiterhin den Namen des anderen Bloomberg-Geräts suchen, falls die Unterstützung für Bloomberg-Tastaturen aktiviert ist.
- Sie können auch anhand des Werts in der Registrierung überprüfen, ob die Unterstützung aktiviert ist:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

Ist der Wert nicht vorhanden oder auf 0 (null) gesetzt, werden Bloomberg-Tastaturen nicht unterstützt. Wird der Wert 1 angezeigt, ist die Unterstützung aktiviert.

Aktivieren der Unterstützung für Bloomberg-Tastaturen:

Hinweis:

Mit Citrix Receiver für Windows 4.8 wurde Unterstützung für zusammengesetzte Geräte über die Richtlinie **Geräte teilen** eingeführt. Für die Bloomberg-Tastatur 4 müssen Sie jedoch anstelle der Richtlinie das Bloomberg-Tastaturfeature verwenden.

Die Unterstützung der Bloomberg-Tastatur ändert die Art und Weise, wie bestimmte USB-Geräte zu einer Sitzung umgeleitet werden. Diese Unterstützung ist nicht standardmäßig aktiviert.

- Um die Unterstützung während der Installation zu aktivieren, legen Sie an der Befehlszeile der Installation die Eigenschaft **ENABLE_HID_REDIRECTION** auf den Wert "TRUE" fest. Beispiel:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="
TRUE"
```

- Um die Unterstützung nach der Installation des Online-Plug-Ins zu aktivieren, bearbeiten Sie die Windows-Registrierung auf dem System, auf dem das Online-Plug-In ausgeführt wird:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu folgendem Schlüssel:
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. Wenn der Wert **EnableBloombergHID** vorhanden ist, ändern Sie den Wert zu 1.
4. Wenn der Wert **EnableBloombergHID** nicht vorhanden ist, erstellen Sie einen DWORD-Wert namens EnableBloombergHID und geben Sie als Wert 1 an.

Deaktivieren der Unterstützung für die Bloomberg-Tastatur:

Sie können die Unterstützung für die Bloomberg-Tastatur im Online-Plug-In wie folgt deaktivieren:

1. Öffnen Sie den Registrierungs-Editor auf dem System, auf dem das Online-Plug-In ausgeführt wird.
2. Navigieren Sie zu folgendem Schlüssel:
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. Wenn der Wert **EnableBloombergHID** vorhanden ist, ändern Sie den Wert zu 0 (null).

Wenn der Wert **EnableBloombergHID** nicht vorhanden ist, ist die Unterstützung für die Bloomberg-Tastatur nicht aktiviert. In diesen Fällen müssen Sie keine Registrierungswerte ändern.

Bloomberg-Tastaturen ohne aktivierte Unterstützung verwenden:

- Sie können die Tastatur auch bei nicht aktivierter Bloomberg-Tastaturunterstützung im Online-Plug-In verwenden. Sie können dann jedoch nicht die Spezialfunktionen für mehrere Sitzungen freigeben und benötigen unter Umständen mehr Netzwerkbandbreite für Audiodaten.
- Die Standardtasten von Bloomberg-Tastaturen stehen wie bei jeder anderen Tastatur zur Verfügung. Sie müssen keine besondere Aktion ergreifen.
- Zur Verwendung der Bloomberg-Spezialtasten müssen Sie das Audiogerät der Bloomberg-Tastatur in die Sitzung umleiten. Wenn Sie den Desktop Viewer verwenden, werden der Herstellername und der Geräte name der USB-Geräte sowie **Bloomberg Keyboard Audio** für das Audiogerät der Bloomberg-Tastatur angezeigt.
- Um den Fingerabdruckleser zu verwenden, müssen Sie das Gerät zu "Bloomberg Fingerprint Scanner" umleiten. Wenn die Treiber für den Fingerabdruckleser nicht lokal installiert sind, zeigt das Gerät nur an:
 - ob das Online-Plug-In eine automatische Verbindung von Geräte erlaubt, oder
 - dass der Benutzer auswählen kann, ob Geräte verbunden werden sollen.

Wenn die Bloomberg-Tastatur vor dem Einrichten der Sitzung verbunden ist und die Treiber für den Fingerabdruckleser nicht lokal vorhanden sind, wird der Fingerabdruckleser nicht angezeigt und kann in der Sitzung nicht verwendet werden.

Hinweis:

Bei Verwendung von Bloomberg 3 kann der Fingerabdruckleser von einer einzelnen Sitzung oder dem lokalen System verwendet, aber nicht freigegeben werden. Bloomberg 4 darf nicht umgeleitet werden.

Bloomberg-Tastaturen nach dem Aktivieren der Unterstützung verwenden:

- Wenn Sie die Unterstützung für Bloomberg-Tastaturen im Online-Plug-In aktivieren, können Sie die Spezialtastenfunktionen in mehreren Sitzungen verwenden. Außerdem ist weniger Netzwerkbandbreite für Audiodaten erforderlich.
- Bei aktivierter Unterstützung der Bloomberg-Tastatur kann das Audiogerät der Bloomberg-Tastatur nicht umgeleitet werden. Stattdessen wird ein neues Gerät zur Verfügung gestellt. Wenn Sie den Desktop Viewer verwenden, wird dieses Gerät als “Bloomberg Keyboard Features” angezeigt. Durch Umleiten dieses Geräts werden die Bloomberg-Spezialtasten in der Sitzung verfügbar.

Das Aktivieren der Unterstützung der Bloomberg-Tastatur wirkt sich nur auf die Bloomberg-Spezialtasten und das Audiogerät aus. Die Standardtasten und der Fingerabdruckleser werden wie bei nicht aktivierter Unterstützung verwendet.

DPI-Skalierung

Die Citrix Workspace-App gestattet die Steuerung der Sitzungsauflösung durch das Betriebssystem.

Sie können in einer Sitzung einen hohen DPI-Wert anwenden. Dieses Feature ist jedoch standardmäßig deaktiviert. Die Sitzungsskalierung folgt der Auflösung des Betriebssystems.

Sie können die DPI-Skalierung mit den folgenden Optionen konfigurieren:

1. Administrative Gruppenrichtlinienobjektvorlage (Konfiguration pro Maschine)
2. Erweiterte Einstellungen (Konfiguration pro Benutzer)

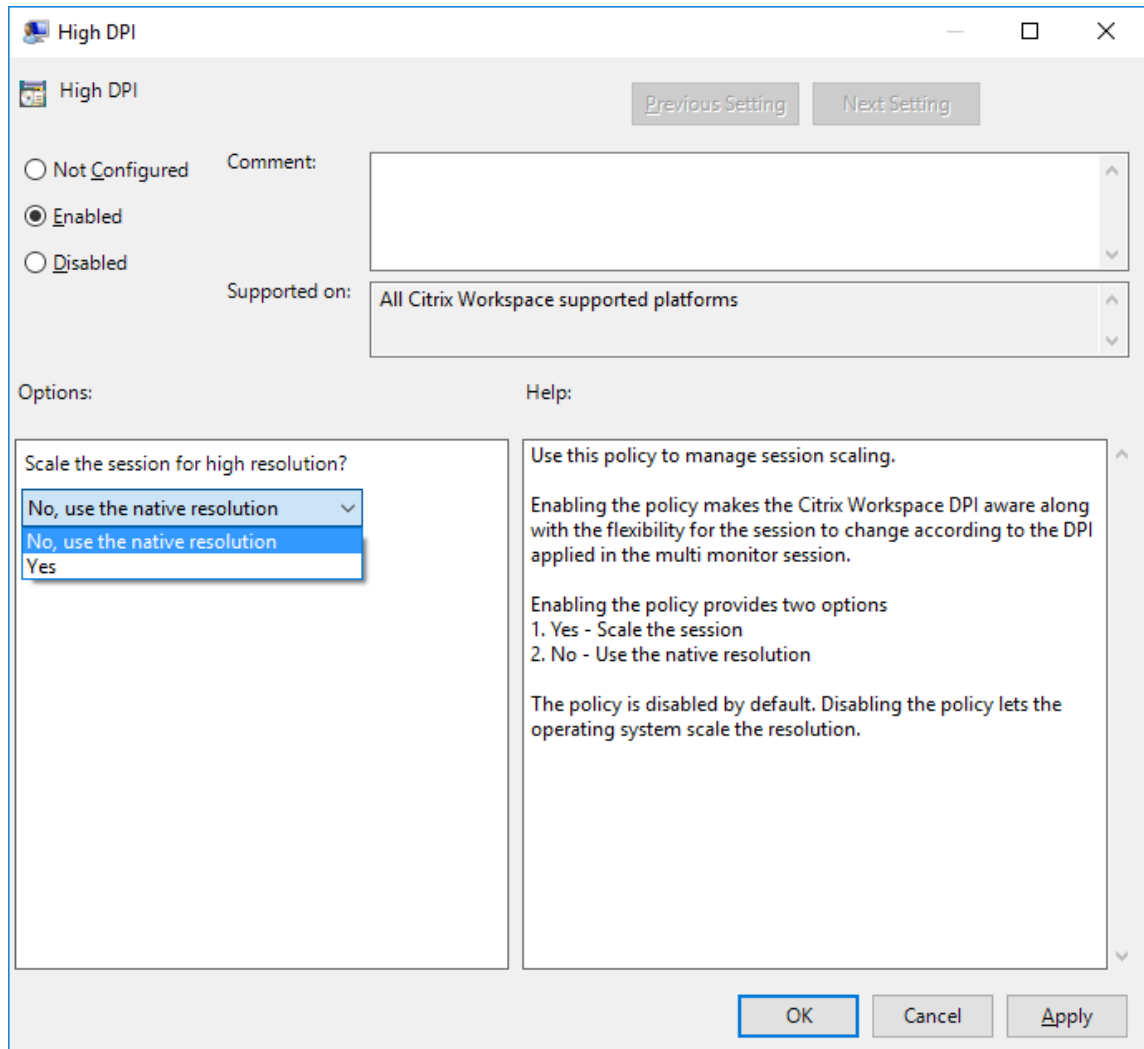
Einschränkungen:

- Auch wenn dieses Feature aktiviert ist, wurde eine leichte Unschärfe im Desktop Viewer beobachtet.
- Wenn Sie in einer Sitzung die DPI-Einstellungen ändern und die Sitzung neu starten, ist die Größe des Sitzungsfensters möglicherweise nicht angemessen. Um das Problem zu umgehen, ändern Sie die Größe des Sitzungsfensters.

DPI-Skalierung mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > DPI**
3. Wählen Sie die Richtlinie **Hoher DPI-Wert** aus.



4. Wählen Sie eine der folgenden Optionen:
 - a) Ja – Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.
 - b) Nein, native Auflösung verwenden – Gibt an, dass die Auflösung vom Betriebssystem festgelegt wird.
5. Klicken Sie auf **Anwenden und OK**.
6. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus, um die Änderungen anzuwenden.

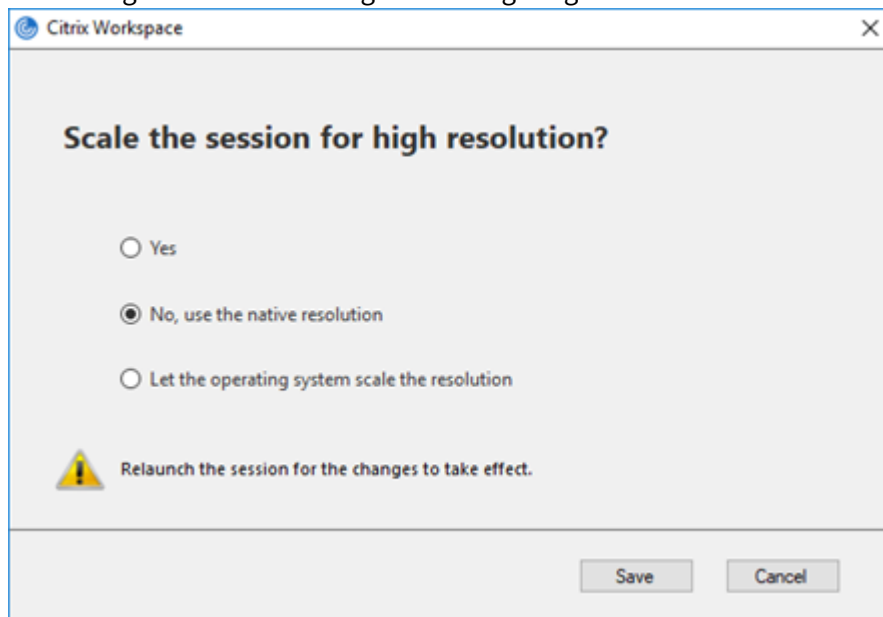
Konfiguration von DPI-Skalierung über die grafische Benutzeroberfläche:

Hinweis:

Sie können die Seite “Erweiterte Einstellungen” ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

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

Das Dialogfeld DPI-Einstellungen wird angezeigt.



3. Wählen Sie eine der folgenden Optionen:
 - a) Ja – Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.
 - b) Nein, native Auflösung verwenden - Gibt an, dass die Citrix Workspace-App den DPI-Wert auf dem VDA erkennt und ihn anwendet.
 - c) Betriebssystem die Auflösung skalieren lassen – Standardmäßig ist diese Option ausgewählt. Damit kann Windows die DPI-Skalierung verarbeiten. Diese Option bedeutet auch, dass die Richtlinie “Hoher DPI-Wert” deaktiviert ist.
4. Klicken Sie auf **Speichern**.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

DPI-Skalierungsoptionen

Es gibt drei mögliche Einstellungen für die DPI-Skalierung in der Citrix Workspace-App: Skaliert, Nicht skaliert und Betriebssystemskalierung. Die Anwendungsfälle für die verschiedenen Einstellungen sind wie folgt.

Skaliert:

Bei aktivierter Skalierung wird die Auflösung im VDA ähnlich wie bei der Betriebssystemskalierung skaliert. Diese Einstellung unterstützt jedoch gemischte DPI-Szenarien. Die Einstellung “Skaliert” entspricht der Benutzeroberflächeneinstellung **Ja** oder der Aktivierung der Richtlinie “Hoher DPI-Wert” in der GPO-Richtlinie. Die Benutzeroberflächeneinstellung **Ja** eignet sich gut für gemischte DPI-Szenarios, wenn Sie eine Verbindung zu modernen VDAs herstellen, und sie ermöglicht das Skalieren von Seamlessitzungen. Die Skalierung kann zu Unschärfe in Bildern führen, insbesondere bei Text. Bei der Verbindung zu älteren VDAs (6.5 oder für Legacygrafiken konfigurierte VDAs) kann die Leistung beeinträchtigt sein. Lokaler App-Zugriff, RTOP und andere Plug-Ins, die APIs für die Bildschirmpositionierung verwenden, sind möglicherweise nicht mit der Skalierung kompatibel. In diesem Modus wechseln Seamless-Apps zwischen den Bildschirmen, um die korrekte Skalierung beizubehalten.

Diese Einstellung wird für Benutzer unter Windows 10 empfohlen, die eine Verbindung zu modernen VDAs herstellen. Sie unterstützt gemischte DPI-Werte ohne zusätzliche Auswirkungen auf die Serverressourcen.

Nicht skaliert:

Bei der nicht skalierten Einstellung wird die volle Auflösung aller Bildschirme in der Sitzung übermittelt. Diese Auflösungen sind nicht skaliert und können zu kleinem Text und kleinen Symbolen in Apps und Desktops führen. Die Einstellung “Nicht skaliert” entspricht der Benutzeroberflächeneinstellung **Nein** bei aktivierter Richtlinie “Hoher DPI-Wert” in der GPO-Richtlinie. Die Benutzeroberflächeneinstellung **Nein** verursacht keine Unschärfe aufgrund der Skalierung, kann jedoch zu kleinem Text und kleinen Symbolen führen. Wenn Sie eine Verbindung zu einer Desktopsitzung herstellen, kann der DPI-Wert im VDA eingestellt werden, was zur gewünschten Skalierung führt. Auf RDS-Desktops oder bei Seamlessanwendungen ist diese Einstellung jedoch nicht möglich. Durch Aktivieren dieser Einstellung haben Sitzungen eine höhere Auflösung, was die Serverleistung und Skalierbarkeit beeinträchtigen kann.

Diese Einstellung wird für Desktopsitzungen empfohlen, bei denen die beste Bildqualität erforderlich ist und für die zusätzliche Serverressourcen verfügbar sind. Sie kann auch verwendet werden, wenn kleiner Text und kleine Symbole für den Benutzer kein Problem darstellen.

Betriebssystemskalierung:

Betriebssystemskalierung ist die Standardeinstellung und entspricht der Benutzeroberflächeneinstellung **Betriebssystem die Auflösung skalieren lassen**. In diesem Szenario wird für die Richtlinie “Hoher DPI-Wert” die Option “Deaktiviert” festgelegt. Gemäß dieser Einstellung übernimmt das Windows-Betriebssystem die DPI-Skalierung für eine Sitzung. Die Auflösung wird auf dem VDA basierend auf dem DPI-Wert skaliert, was zu einer geringeren Auflösung als auf dem Clientgerät führt. Dies funktioniert gut für Sitzungen mit einem Bildschirm und ist effizient, wenn Sie eine Verbindung zu 6.5-VDAs oder VDAs herstellen, die für Legacygrafiken konfiguriert sind. Diese Methode unterstützt keine gemischten DPI-Werte. Alle Bildschirme müssen dieselben DPI-Werte haben, oder die Sitzung funk-

tioniert nicht. Skalierung kann insbesondere bei Text zu unscharfer Darstellung führen. Bei Windows 10-Betriebssystemen können auch Probleme mit der Cursorgröße auftreten.

Citrix empfiehlt diese Einstellung für Benutzer mit Windows 7-Endpunkten oder für Benutzer, die eine Verbindung zu Legacy-VDA herzustellen. Sie kann auch unter Windows 10 verwendet werden, wenn keine gemischten DPI-Werte vorliegen.

Virtuelles Anzeigelayout

Mit diesem Feature definieren Sie ein virtuelles Bildschirmlayout für den Remotedesktop. Außerdem können Sie einen einzelnen Clientmonitor virtuell in bis zu acht Bildschirme auf dem Remotedesktop aufteilen. Sie können die virtuellen Bildschirme auf der Registerkarte **Bildschirmlayout** im Desktop Viewer konfigurieren. Dort können Sie horizontale oder vertikale Linien ziehen, um den Bildschirm in virtuelle Bildschirme zu unterteilen. Der Bildschirm wird entsprechend den angegebenen Prozentsätzen der Auflösung des Clientbildschirms aufgeteilt.

Sie können für die virtuellen Bildschirme eine DPI festlegen, die für die DPI-Skalierung bzw. DPI-Anpassung verwendet wird. Ändern Sie nach dem Anwenden eines virtuellen Bildschirmlayouts die Größe der Sitzung oder stellen Sie erneut eine Verbindung her.

Die Konfiguration gilt nur für Desktopsitzungen mit einem Bildschirm im Vollbildmodus. Sie hat keine Auswirkungen auf veröffentlichte Anwendungen. Diese Konfiguration gilt für alle nachfolgenden Verbindungen von diesem Client.

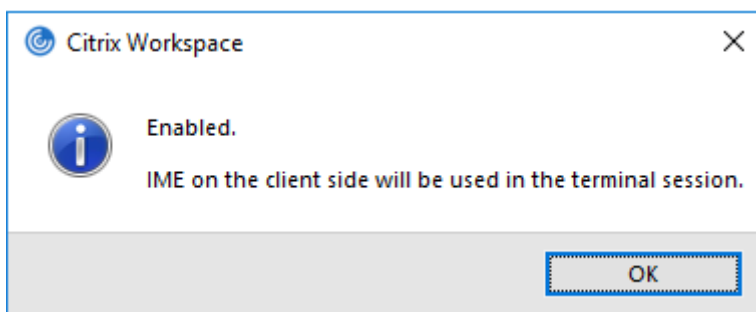
Generischer Client-IME (Eingabemethoden-Editor)

Hinweis:

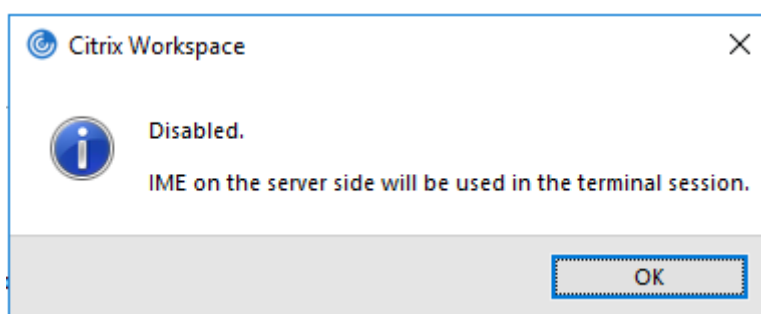
Wenn Sie mit dem Betriebssystem Windows 10 Version 2004 arbeiten, können bestimmte technische Probleme auftreten, wenn Sie das IME-Feature in einer Sitzung verwenden. Diese Probleme treten aufgrund eines Drittanbieterproblems auf. Weitere Informationen finden Sie im [Microsoft-Supportartikel](#).

Konfigurieren eines generischen Client-IME über die Befehlszeilenschnittstelle:

- Führen Sie den Befehl `wfica32.exe /localime:on` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu aktivieren.



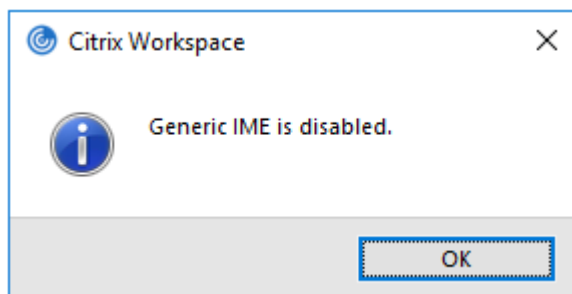
- Führen Sie den Befehl `wfica32.exe /localime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren.



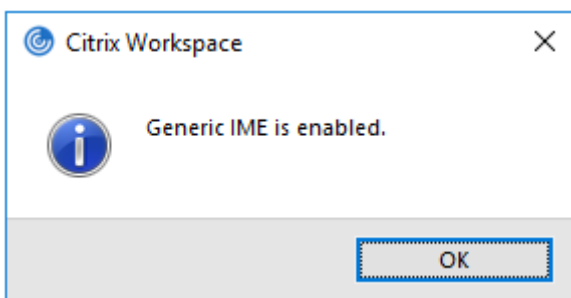
Hinweis:

Sie können mit der Befehlszeilenoption `wfica32.exe /localime:on` den generischen Client-IME und die Tastaturlayoutsynchronisierung aktivieren.

- Führen Sie den Befehl `wfica32.exe /localgenericime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren. Dieser Befehl hat keine Auswirkungen auf die Einstellungen für die Tastaturlayoutsynchronisierung.



Wenn Sie den generischen Client-IME über die Befehlszeilenschnittstelle deaktiviert haben, können Sie das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` wieder aktivieren.



Ein-/Ausschalten:

Die Citrix Workspace-App unterstützt das Ein- und Ausschalten dieses Features. Sie können das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` ein- und ausschalten. Die Einstellungen für die Tastaturlayoutsynchronisierung haben jedoch Vorrang vor der Ein-/Ausschaltfunktion. Wenn die Tastaturlayoutsynchronisierung auf **Aus** festgelegt ist, kann der generische Client-IME nicht durch Ein-/Ausschalten aktiviert werden.

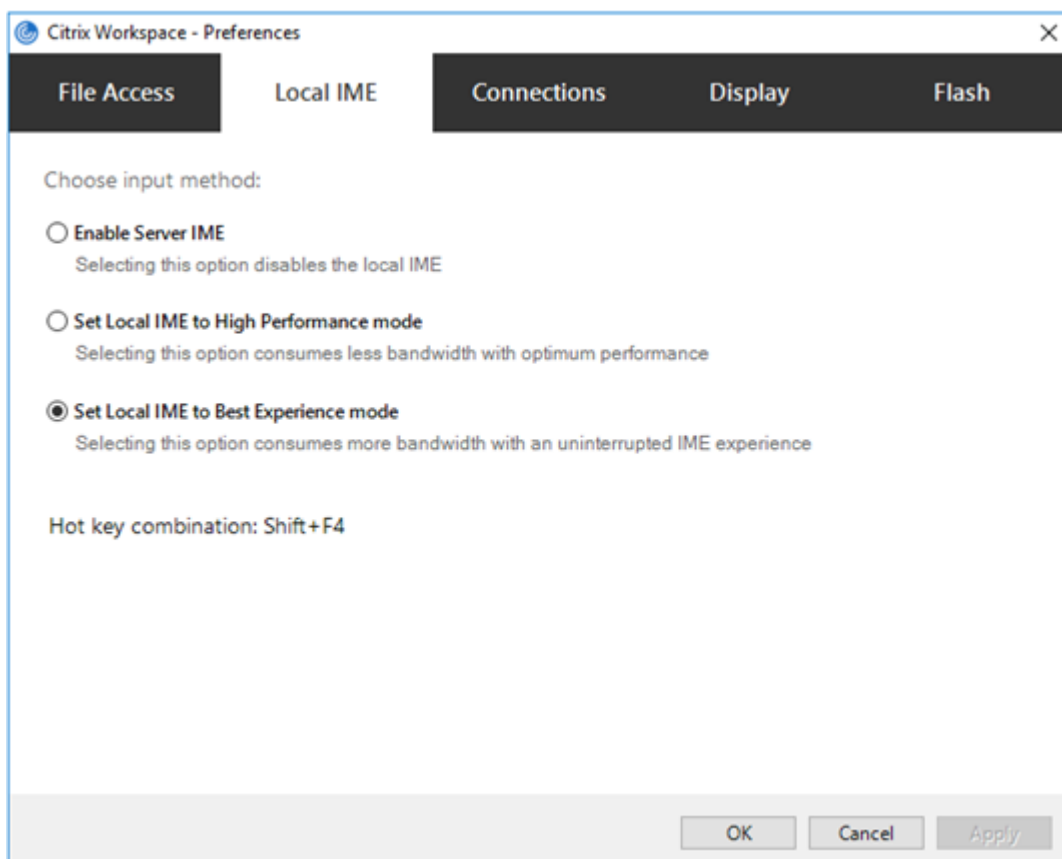
Konfigurieren eines generischen Client-IME über die grafische Benutzeroberfläche:

Der generische Client-IME erfordert VDA-Version 7.13 oder höher.

Die generische Client-IME-Features können durch Aktivieren der Tastaturlayoutsynchronisierung aktiviert werden. Weitere Informationen finden Sie unter [Tastaturlayoutsynchronisierung](#).

Die Citrix Workspace-App ermöglicht das Konfigurieren verschiedener Optionen für den generischen Client-IME. Entsprechend Ihrer Anforderungen und der Nutzung können Sie eine der Optionen auswählen.

1. Klicken Sie mit der rechten Maustaste auf das Citrix Workspace-App-Symbol im Infobereich und wählen Sie **Connection Center**.
2. Wählen Sie **Einstellungen** und **Lokaler IME**.



Für die verschiedenen IME-Modi sind die folgenden Optionen verfügbar:

1. **Server-IME aktivieren** –Deaktiviert den lokalen IME und nur die auf dem Server festgelegten Sprachen können verwendet werden.
2. **Lokalen IME auf Hochleistungsmodus einstellen** –Verwendet den lokalen IME mit beschränkter Bandbreite. Diese Option schränkt die Funktionalität des Kandidatenfensters ein.
3. **Lokalen IME-Modus für beste Erfahrung einstellen** –Verwendet den lokalen IME mit optimaler Benutzerfreundlichkeit. Diese Option verbraucht hohe Bandbreite. Diese Option ist standardmäßig ausgewählt, wenn der generische Client-IME aktiviert ist.

Die Änderungen werden nur in der aktuellen Sitzung angewendet.

Tastenkombinationen mit einem Registrierungs-Editor konfigurieren:

Wenn der generische Client-IME aktiviert ist, können Sie mit der Tastenkombination **Umschalt+F4** verschiedene IME-Modi auswählen. Die verschiedenen Optionen für die IME-Modi werden oben rechts in der Sitzung angezeigt.

Standardmäßig ist die Tastenkombination für den generischen Client-IME deaktiviert.

Navigieren Sie im Registrierungs-Editor zu `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

Wählen Sie **AllowHotKey** und ändern Sie den Standardwert in 1.

Mit der Tastenkombination **Umschalt+F4** können Sie verschiedene IME-Modi in einer Sitzung auswählen.

Die verschiedenen IME-Modi werden rechts oben in der Sitzung angezeigt, während Sie die Optionen mit der Tastenkombination durchlaufen.



Einschränkungen:

- Der generische Client-IME unterstützt keine UWP-Apps (Universelle Windows-Plattform-Anwendungen) wie Suchbenutzeroberfläche und Edge-Browser des Windows 10-Betriebssystems. Verwenden Sie als Workaround den Server-IME.
- Der generische Client-IME wird für Internet Explorer Version 11 im **geschützten Modus** nicht unterstützt. Als Workaround können Sie den geschützten Modus unter **Internetoptionen** deaktivieren. Klicken Sie zum Deaktivieren auf **Sicherheit** und deaktivieren Sie das Kontrollkästchen **Geschützten Modus aktivieren**.

H.265-Videocodierung

Die Citrix Workspace-App unterstützt die Verwendung des H.265-Videoencoders für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Der H.265-Videoencoder muss auf dem VDA und in der Citrix Workspace-App unterstützt und aktiviert sein. Wenn die GPU auf dem Endpunkt H.265-Decodierung über die DXVA-Schnittstelle nicht unterstützt, wird die Einstellung der Richtlinie "H265-Decodierung für Grafiken" ignoriert und die Sitzung greift auf den H.264-Videoencoder zurück.

Voraussetzungen:

1. VDA 7.16 oder höher.
2. Aktivieren Sie auf dem VDA die Richtlinie **Optimierung für 3D-Grafikworkload**.
3. Aktivieren Sie auf dem VDA die Richtlinie **Hardwarecodierung für Videoencoder verwenden**.

Hinweis:

H.265-Codierung wird nur von der NVIDIA-GPU unterstützt.

Dieses Feature ist in der Citrix Workspace-App für Windows standardmäßig **deaktiviert**.

Citrix Workspace-App für die Verwendung von H.265-Videocodierung mit der administrativen Gruppenrichtlinienobjektvorlage von Citrix konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **H265-Decodierung für Grafiken**.
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Anwenden** und **OK**.

H.265-Videocodierung mit dem Registrierungs-Editor konfigurieren:

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 32-Bit-Betriebssystem aktivieren:

1. Starten Sie den Registrierungs-Editor, indem Sie den Befehl "regedit" ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableH265** und legen Sie seinen Wert auf 1 fest.

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 64-Bit-Betriebssystem aktivieren:

1. Starten Sie den Registrierungs-Editor, indem Sie den Befehl "regedit" ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen `EnableH265` und legen Sie seinen Wert auf 1 fest.

Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Hinweis:

- Wenn die Richtlinie **Hardwarebeschleunigung für Grafiken** in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App für Windows deaktiviert ist, werden die Einstellungen der Richtlinie **H265-Decodierung für Grafiken** ignoriert und das Feature funktioniert nicht.

- Führen Sie das Tool “HDX Monitor 3.x” aus, um festzustellen, ob der H.265-Videoencoder in den Sitzungen aktiviert ist. Weitere Informationen zu HDX Monitor 3.x finden Sie im Knowledge Center-Artikel [CTX135817](#).

Tastaturlayout und Sprachenleiste

Tastaturlayout

Hinweis:

Sie können die über das Citrix Workspace-App-Symbol im Infobereich verfügbare Seite “Erweiterte Einstellungen” ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

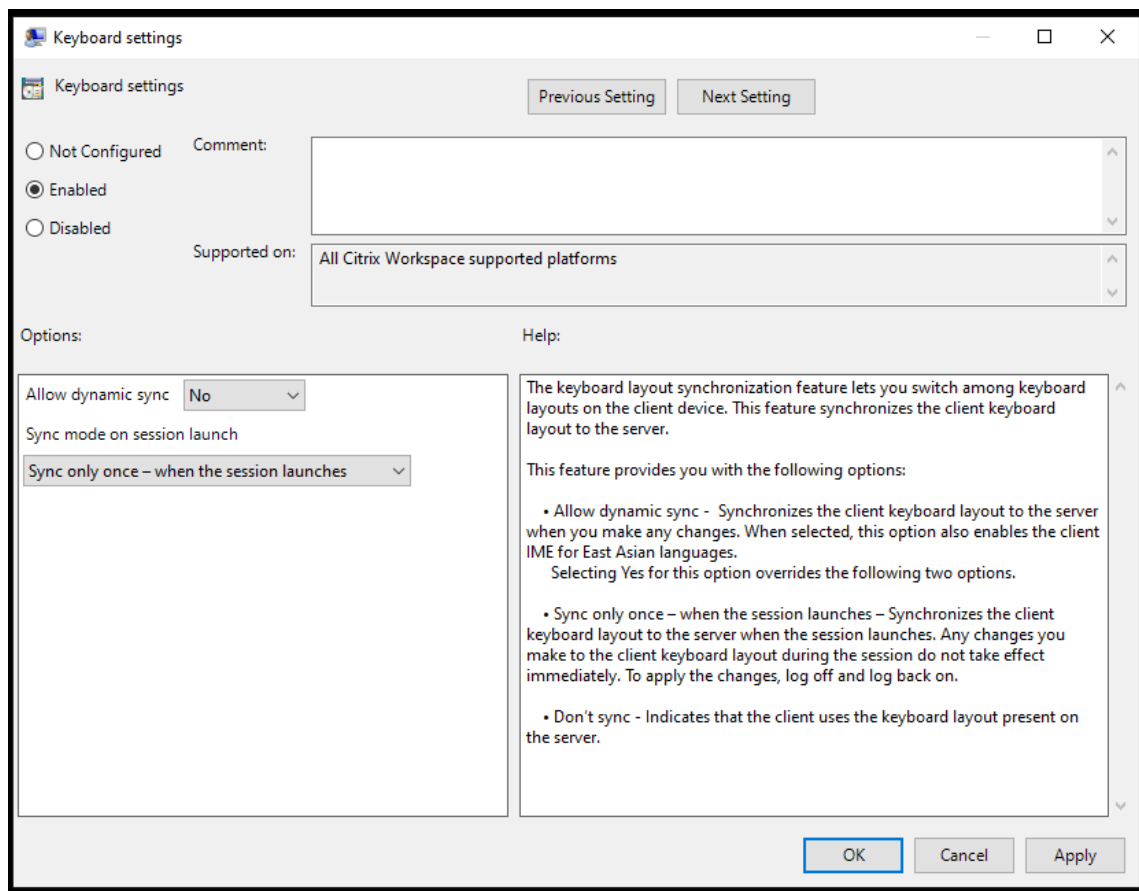
Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert. Die Tastaturlayoutsynchronisierung ermöglicht das automatische Synchronisieren des Clienttastaturlayouts mit einer Sitzung mit virtuellen Apps und Desktops.

Konfigurieren der Tastaturlayoutsynchronisierung mit der administrativen GPO-Vorlage:

Hinweis:

Die GPO-Konfiguration hat Vorrang vor der StoreFront- bzw. GUI-Konfiguration.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** oder **Benutzerkonfiguration** zu **Administrative Vorlagen > Administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Tastatureinstellungen**.



4. Wählen Sie **Aktiviert** und wählen Sie eine der folgenden Optionen:

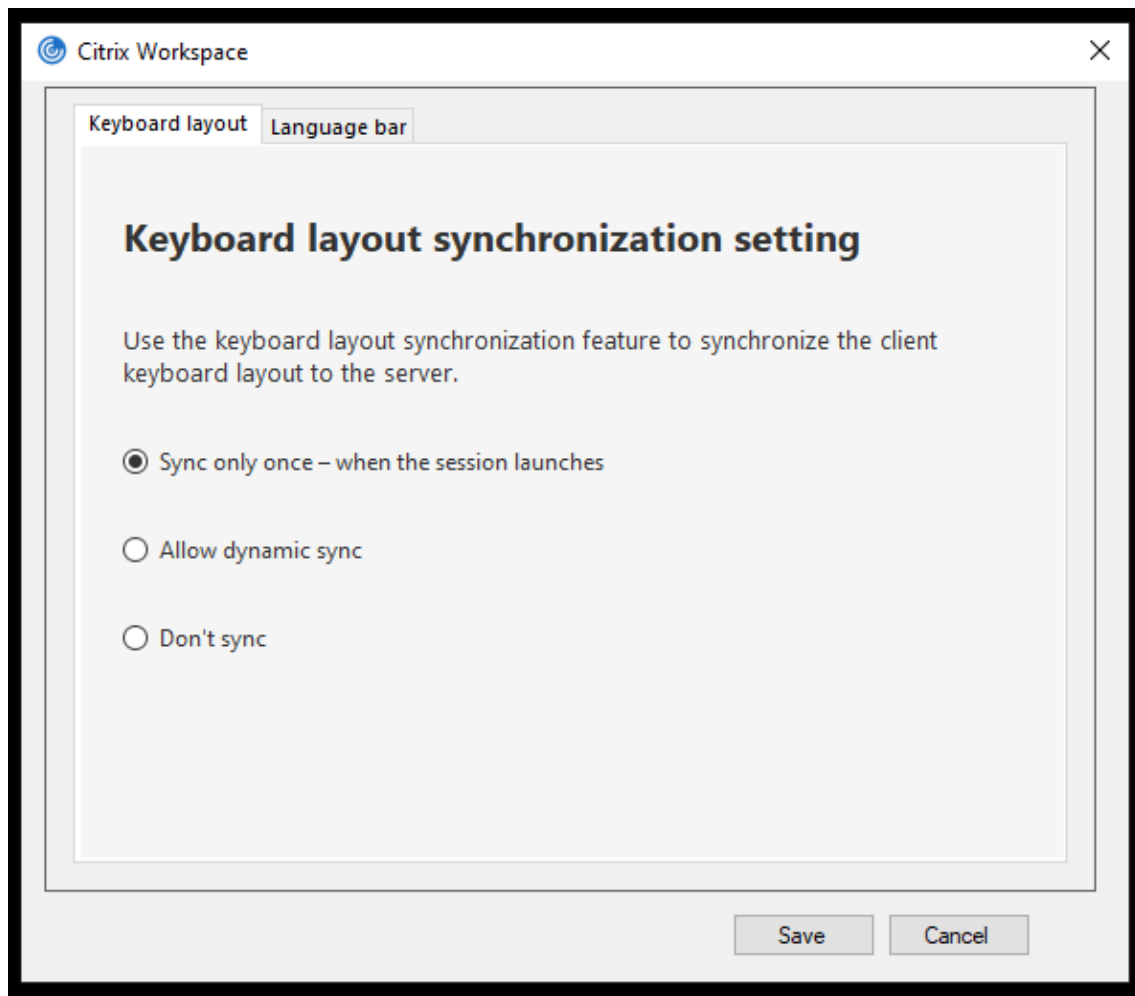
- **Dynamische Synchronisierung zulassen** - Wählen Sie im Dropdownmenü **Ja** oder **Nein**. Diese Option synchronisiert das Clienttastaturlayout mit dem Server, wenn Sie das Clienttastaturlayout ändern. Wenn diese Option ausgewählt ist, wird auch der Client-IME für ostasiatische Sprachen aktiviert.
Wenn Sie für diese Option **Ja** auswählen, werden die folgenden beiden Optionen überschrieben.
- **Synchronisierung beim Sitzungsstart** - Wählen Sie im Dropdownmenü eine der folgenden Optionen:
 - **Nur einmal beim Sitzungsstart synchronisieren** - Synchronisiert das Clienttastaturlayout beim Sitzungsstart mit dem Server. Änderungen, die Sie während der Sitzung am Clienttastaturlayout vornehmen, werden nicht sofort wirksam. Melden Sie sich ab und wieder an, um die Änderungen zu übernehmen.
 - **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

5. Wählen Sie **Übernehmen** und **OK**.

Konfigurieren der Tastaturlayoutsynchronisierung über die grafische Benutzeroberfläche:

1. Klicken Sie auf das Infobereichssymbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen > Tastatur und Sprachenleiste**.

Das Dialogfeld **Tastatur und Sprachenleiste** wird angezeigt.



2. Wählen Sie eine der folgenden Optionen:

- **Nur einmal beim Sitzungsstart synchronisieren** - Gibt an, dass das Tastaturlayout nur einmal beim Sitzungsstart mit dem VDA synchronisiert wird.
- **Dynamische Synchronisierung zulassen** - Synchronisiert das Tastaturlayout dynamisch mit dem VDA, wenn die Clienttastatur in einer Sitzung geändert wird.
- **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

3. Klicken Sie auf **Speichern**.

Konfigurieren der Tastaturlayoutsynchronisierung mit der Befehlszeilenschnittstelle (CLI):

Führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App für Windows aus.

Der Installationsordner der Citrix Workspace-App ist in der Regel unter `C:\Program files (x86)\Citrix\ICA Client`.

- Zum Aktivieren: `wfica32.exe /localime:on`
- Zum Deaktivieren: `wfica32.exe /localime:off`

Beim Verwenden der Clienttastaturlayoutoption wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Benutzer, die Japanisch, Chinesisch oder Koreanisch verwenden, den Server-IME bevorzugen, müssen sie die Clienttastaturlayoutoption durch Auswahl von **Nein** oder über den Befehl `wfica32.exe /localime:off` deaktivieren. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.

Gelegentlich wird der Wechsel des Clienttastaturlayouts nicht in einer aktiven Sitzung wirksam. Sie beheben das Problem, indem Sie sich von der Citrix Workspace-App ab- und dann wieder anmelden.

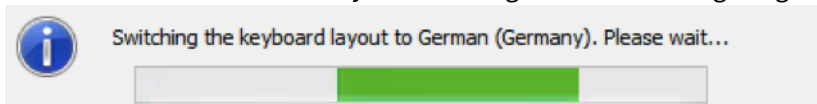
Konfigurieren der Tastatursynchronisierung auf Windows VDA

Hinweis:

Das folgende Verfahren gilt nur für Windows Server 2016 und höher. Unter Windows Server 2012 R2 und früher ist die Tastatursynchronisierung standardmäßig aktiviert.

1. Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie den DWORD-Eintrag `DisableKeyboardSync` und legen Sie seinen Wert auf 0 fest.
 - 1 deaktiviert die Synchronisierung des Tastaturlayouts.
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Nachdem Sie das Tastaturlayout für den VDA und für die Citrix Workspace-App aktiviert haben, wird beim Wechsel von Tastaturlayouts das folgende Fenster angezeigt.



Dieses Fenster zeigt an, dass das Tastaturlayout in der Sitzung auf das Clienttastaturlayout umgestellt wird.

Konfigurieren der Tastatursynchronisierung auf Linux VDA

Starten Sie die Eingabeaufforderung, und führen Sie folgenden Befehl aus:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout
   " -d "0x00000001"
2 <!--NeedCopy-->
```

Starten Sie den VDA neu, damit die Änderungen wirksam werden.

Weitere Informationen zur Tastaturlayoutsynchronisierung auf Linux VDA finden Sie unter [Dynamische Tastaturlayoutsynchronisierung](#).

Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel:

Durch die Benachrichtigung beim Wechseln des Tastaturlayouts erfahren Sie, dass die VDA-Sitzung das Tastaturlayout ändert. Der Wechsel des Tastaturlayouts dauert ungefähr zwei Sekunden. Wenn Sie die Benachrichtigung ausblenden, warten Sie einige Zeit, bevor Sie mit der Eingabe beginnen, um die Eingabe falscher Zeichen zu vermeiden.

Warnung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel mit dem Registrierungs-Editor:

1. Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie einen neuen Zeichenfolgenwertschlüssel mit dem Namen **HideNotificationWindow**.
3. Legen Sie den DWORD-Wert auf **1** fest.
4. Klicken Sie auf **OK**.
5. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Einschränkungen:

- Für Remoteanwendungen, die mit erhöhten Rechten ausgeführt werden (z. B. wenn Sie mit der rechten Maustaste auf ein Anwendungssymbol klicken und "Als Administrator ausführen" wählen), kann keine Tastaturlayoutsynchronisierung erfolgen. Als Workaround ändern Sie das Tastaturlayout manuell auf der Serverseite (VDA) oder deaktivieren Sie die Benutzerkontensteuerung (UAC).

- Wenn der Benutzer für das Tastaturlayout auf dem Client ein Layout wählt, das vom Server nicht unterstützt wird, dann wird das Synchronisierungsfeature des Tastaturlayouts aus Sicherheitsgründen deaktiviert. Ein unbekanntes Tastaturlayout wird als mögliches Sicherheitsrisiko behandelt. Um das Feature für die Tastaturlayoutsynchronisierung wiederherzustellen, muss der Benutzer sich von der Sitzung abmelden und wieder anmelden.
- In einer RDP-Sitzung können Sie das Tastaturlayout nicht mit der Tastenkombination **Alt + Shift** ändern. Als Workaround können Sie das Tastaturlayout mit der Sprachenleiste in der RDP-Sitzung ändern.

Sprachenleiste

Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt. Die Sprachenleiste wird in Sitzungen standardmäßig angezeigt.

Hinweis:

Das Feature ist in Sitzungen verfügbar, die unter einem VDA der Version 7.17 und höher ausgeführt werden.

Konfigurieren der Sprachenleiste über die administrative GPO-Vorlage:

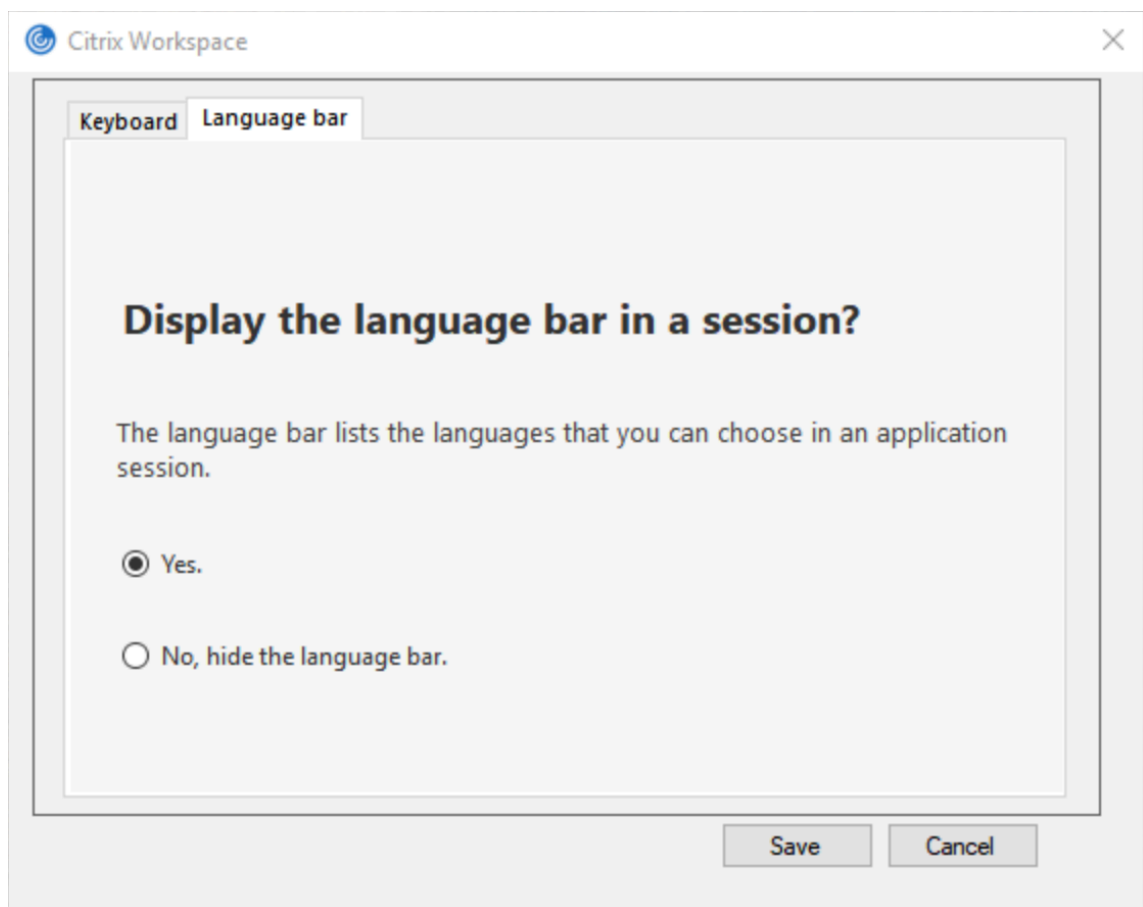
Remotesprachenleiste ein- und ausblenden: Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Anwendungssitzungen angezeigt.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** oder **Benutzerkonfiguration** zu **Administrative Vorlagen > Administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Sprachenleiste** aus.
4. Wählen Sie **Aktiviert** und wählen Sie eine der folgenden Optionen:
 - Ja - Gibt an, dass die Sprachenleiste in einer Anwendungssitzung angezeigt wird.
 - Nein, Sprachenleiste ausblenden - Gibt an, dass die Sprachenleiste in einer Anwendungssitzung ausgeblendet ist.
5. Klicken Sie auf **Anwenden** und **OK**.

Konfigurieren der Sprachenleiste über die grafische Benutzeroberfläche:

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

3. Wählen Sie die Registerkarte **Sprachenleiste**.
 4. Wählen Sie eine der folgenden Optionen:
 - a) Ja - Gibt an, dass die Sprachenleiste in einer Sitzung angezeigt wird.
 - b) Nein, Sprachenleiste ausblenden – Zeigt an, dass die Sprachenleiste in einer Sitzung ausgeblendet ist.
 5. Klicken Sie auf **Speichern**.
- Die Änderungen werden sofort wirksam.



Hinweis:

- Sie können die Einstellungen in einer aktiven Sitzung ändern.
- Die Remotesprachenleiste wird in Sitzungen mit nur einer Eingabesprache nicht angezeigt.

Ausblenden der Registerkarte “Sprachenleiste” von der Seite “Erweiterte Einstellungen”:

Sie können die Registerkarte “Sprachenleiste” von der Seite **Erweiterte Einstellungen** über die Registrierung ausblenden.

1. Öffnen Sie den Registrierungs-Editor.

2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Erstellen Sie den DWORD-Wertschlüssel **ToggleOffLanguageBarFeature** und legen Sie ihn auf **1** fest, um die Option für die Sprachenleiste auf der Seite "Erweiterte Einstellungen" auszublenden.

USB-Unterstützung

Mit der USB-Unterstützung können Sie mit zahlreichen USB-Geräten interagieren, wenn sie mit Citrix Virtual Apps and Desktops und Citrix DaaS verbunden sind. Sie können USB-Geräte an die Geräte anschließen und mit Remoting der Geräte stehen sie auf dem virtuellen Desktop zur Verfügung. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets. Benutzer von Desktop Viewer können mit einer Einstellung auf der Symbolleiste steuern, ob USB-Geräte für Citrix Virtual Apps and Desktops und Citrix DaaS verfügbar sind.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz oder hoher Geschwindigkeit unterstützt. In solchen Umgebungen können diese Geräte mit Programmpaketen wie Microsoft Office Communicator und Skype verwendet werden.

Die folgenden Gerätetypen werden direkt in Sitzungen mit virtuellen Apps und Desktops unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unter [Konfigurieren von Bloomberg-Tastaturen](#).

Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie im Knowledge Center-Artikel [CTX122615](#).

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über Citrix Virtual Apps and Desktops und Citrix DaaS unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre bei einem solchen Gerät nicht angebracht. Die folgenden USB-Gerätetypen werden standardmäßig nicht in Sitzungen mit virtuellen Apps und Desktops unterstützt:

- Bluetooth-Dongle

- Integrierte Netzwerkkarte
- USB-Hubs
- USB-Grafikadapter

Remoting ist möglich für USB-Geräte, die mit einem Hub verbunden sind, jedoch nicht für den Hub selbst.

Die folgenden USB-Gerätetypen werden standardmäßig nicht in einer Sitzung mit virtuellen Apps unterstützt:

- Bluetooth-Dongle
- Integrierte Netzwerkkarte
- USB-Hubs
- USB-Grafikadapter
- Audiogeräte
- Massenspeichergeräte

Funktionsweise der USB-Unterstützung:

Wenn ein Benutzer ein USB-Gerät anschließt, wird es mit der USB-Richtlinie überprüft, und wenn das Gerät zulässig ist, erfolgt ein Remoting zum virtuellen Desktop. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Wenn ein Benutzer ein USB-Gerät anschließt, wird eine Meldung über den Anschluss eines neuen Geräts angezeigt. Der Benutzer kann die Geräte, für die ein Remoting zum virtuellen Desktop erfolgen soll, bei jeder Verbindung auswählen. Der Benutzer kann die USB-Unterstützung auch so konfigurieren, dass für alle USB-Geräte, die vor oder während einer Sitzung angeschlossen werden, automatisch ein Remoting zu dem virtuellen Desktop erfolgt, der den Fokus hat.

Massenspeichergeräte

Nur bei Massenspeichergeräten ist der Remotezugriff neben USB-Unterstützung auch durch Clientlaufwerkzuordnung verfügbar. Sie können dies in der Citrix Workspace-App für Windows über die Richtlinie **Remoting von Clientgeräten > Clientlaufwerkzuordnung** konfigurieren. Wenn Sie diese Richtlinie anwenden, werden die Laufwerke auf dem Benutzergerät automatisch den Laufwerksbuchstaben auf dem virtuellen Desktop zugeordnet, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

Feature	Clientlaufwerkzuordnung	USB-Unterstützung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein
Sicheres Entfernen des Geräts in einer Sitzung	Nein	Ja, wenn der Benutzer im Infobereich auf Hardware sicher entfernen klickt.

Wenn Sie die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktivieren und vor dem Sitzungsstart ein Massenspeichergerät anschließen, wird es zuerst mit der Clientlaufwerkzuordnung umgeleitet, bevor eine Umleitung mit USB-Unterstützung erwogen wird. Wenn das Gerät nach dem Sitzungsstart angeschlossen wird, wird die Umleitung mit der USB-Unterstützung vor der Clientlaufwerkzuordnung erwogen.

In der Standardeinstellung zulässige USB-Geräteklassen:

Verschiedene Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln zugelassen.

Auch wenn sie in dieser Liste sind, stehen manche Klassen nur nach zusätzlicher Konfiguration für das Remoting in Sitzungen mit virtuellen Apps und Desktops zur Verfügung. Folgende USB-Geräteklassen sind möglich.

- **Audio (Geräteklasse 01):** Umfasst Audioeingabegeräte (Mikrofone), Audioausgabegeräte und MIDI-Controller. Moderne Audiogeräte verwenden im Allgemeinen isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Audio (Geräteklasse 01) ist für Citrix Virtual Apps nicht relevant, da Geräte dieser Klasse für das Remoting in Citrix Virtual Apps mit USB-Unterstützung nicht verfügbar sind.

Hinweis:

Für manche Spezialgeräte (z. B. VOIP-Telefone) ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **PID (Physical Interface Devices) (Geräteklasse 05):** Diese Geräte ähneln HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Endoskelette.
- **Bilder (Geräteklasse 06):** Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen oft die Bilderklasse, in der Bilder mit den Protokollen PTP (Picture Transfer Protocol) oder MTP (Media Transfer Protocol) zu einem Computer oder zu einem anderen Peripheriegerät übertragen werden. Kameras können auch als Massenspeichergeräte angezeigt werden. Eine

Kamera kann möglicherweise auch über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

Hinweis:

Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet und die USB-Unterstützung wird nicht benötigt.

- **Drucker (Geräteklasse 07):** Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. Multifunktionsdrucker haben ggf. einen internen Hub oder sind Composite-Geräte. In beiden Fällen verwendet das Druckererelement meistens die Druckerklasse und das Scanner- oder Faxelement verwendet eine andere Klasse, z. B. Bilder.

Drucker funktionieren normalerweise ohne USB-Unterstützung.

Hinweis

Für diese Klasse von Geräten (vor allem Drucker mit Scanfunktion) ist eine zusätzliche Konfiguration erforderlich. Anweisungen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **Massenspeicher (Geräteklasse 08):** Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke sowie über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, der auch eine Massenspeicherschnittstelle darstellt, u. a. Media Player, digitale Kameras und Mobiltelefone. Massenspeicher (Geräteklasse 08) ist für Citrix Virtual Apps nicht relevant, da Geräte dieser Klasse für das Remoting in Citrix Virtual Apps mit USB-Unterstützung nicht verfügbar sind. Bekannte Unterklassen:

- 01: Begrenzte Flashlaufwerke
- 02: Normalerweise CD- bzw. DVD-Geräte (ATAPI/MMC-2)
- 03: Normalerweise Bandgeräte (QIC-157)
- 04: Normalerweise Diskettenlaufwerke (UFI)
- 05: Normalerweise Diskettenlaufwerke (SFF-8070i)
- 06: Die meisten Massenspeichergeräte verwenden diese SCSI-Variante

Der Zugriff auf Massenspeichergeräte erfolgt oft über die Clientlaufwerkzuordnung und USB-Unterstützung wird daher nicht benötigt.

- **Content Security (Geräteklasse 0d):** Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.
- **Video (Geräteklasse 0e):** Die Videoklasse umfasst Geräte, mit denen Videos und videobezogenes Material verwendet werden. Dies können Webcams, digitale Camcorder, analoge

Videokonverter und einige Fernsehtuner sein, aber auch einige digitale Kameras, die Videostreaming unterstützen.

Wichtig

Die meisten Videostreaminggeräte verwenden isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Für manche Videogeräte (z. B. Webcams mit Bewegungserkennung) ist eine zusätzliche Konfiguration erforderlich. Anweisungen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **Personal Healthcare (Geräteklasse 0f):** Hierzu gehören Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.
- **Anwendungs- und herstellerspezifisch (Geräteklassen fe und ff):** Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese Geräte werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

In der Standardeinstellung nicht zugelassene USB-Geräteklassen

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a): Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein solches Gerät möglicherweise selbst die Verbindung zum virtuellen Desktop bereitstellt.
- HID (Human Interface Devices, Geräteklasse 03): Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktablets, Sensoren, Game Controller, Tasten und Steuerfunktionen.

Die Unterklasse 01 wird "Boot Interface"-Klasse genannt und für Tastaturen und Maus verwendet.

USB-Tastaturen (Klasse 03, Unterklasse 01, Protokoll 1) oder USB-Mäuse (Klasse 03, Unterklasse 01, Protokoll 2) werden von der USB-Standardrichtlinie nicht zugelassen. Begründung: Die meisten Tastaturen und Mäuse können auch ohne USB-Unterstützung genutzt werden. Sie werden zudem sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.

- USB-Hubs (Geräteklasse 09): Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.
- Smartcard (Geräteklasse 0b): Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.

Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.

- **Kabellose Controller (Geräteklasse e0):** Einige dieser Geräte stellen u. U. wichtigen Netzwerkzugang bereit oder schließen wichtige Peripheriegeräte an, z. B. Bluetooth-Tastaturen oder -Mäuse.

Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

- **Verschiedene Netzwerkgeräte (Geräteklasse ef, Unterklasse 04):** Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang. Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

Für Remoting verfügbare USB-Geräteliste aktualisieren

Bearbeiten Sie die Vorlagendatei für Citrix Workspace für Windows, um die USB-Geräte zu aktualisieren, die für das Remoting zu Desktops verfügbar sind. Mit diesem Update können Sie Citrix Workspace-App für Windows über eine Gruppenrichtlinie ändern. Die Datei ist in folgendem Installationsordner:

`\C:\Program Files\Citrix\ICA Client\Configuration\en`

Sie können auch die Registrierung auf jedem Benutzergerät ändern und den folgenden Registrierungsschlüssel hinzufügen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules"Wert=

Wichtig

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Standardregeln für das Produkt sind an folgendem Speicherort gespeichert:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules"Value=

Ändern Sie nicht die Produktstandardregeln.

Weitere Informationen zu den Richtlinieneinstellungen für USB-Geräte finden Sie unter [Einstellungen der Richtlinie "USB-Geräte"](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

USB-Audio konfigurieren

Hinweis:

- Wenn Sie die Citrix Workspace-App für Windows zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#). Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.
- Dieses Feature ist nur für Citrix Virtual Apps-Server verfügbar.

USB-Audiogeräte konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung** und wählen Sie **Audio über generische USB-Umleitung**.
3. Bearbeiten Sie die Einstellungen.
4. Klicken Sie auf **Anwenden** und **OK**.
5. Öffnen Sie eine Eingabeaufforderung im Administratormodus.
6. Führen Sie den folgenden Befehl aus
`gpupdate /force`.

vPrefer-Start

In älteren Releases können Sie festlegen, dass die Instanz einer auf dem VDA installierten App (= "lokale Instanz" im vorliegenden Dokument) bevorzugt vor der veröffentlichten Anwendung gestartet werden muss, indem Sie in **Citrix Studio** das Attribut `KEYWORDS:prefer="application"` festlegen.

Ab Version 4.11 können Sie in einem Double-Hop-Szenario (wenn die Citrix Workspace-App auf dem VDA ausgeführt wird, der Ihre Sitzung hostet) steuern, was die Citrix Workspace-App startet:

- die lokale Instanz einer auf dem VDA installierten Anwendung (sofern sie als lokale App verfügbar ist) oder
- eine gehostete Instanz der Anwendung.

vPrefer ist in StoreFront 3.14 und in Citrix Virtual Desktops ab Version 7.17 verfügbar.

Wenn Sie die Anwendung starten, liest die Citrix Workspace-App die Ressourcendaten auf dem StoreFront-Server und wendet die Einstellungen auf der Grundlage des **vprefer**-Flags zum Zeitpunkt der Aufzählung an. Die Citrix Workspace-App sucht in der Windows-Registrierung des VDA nach dem Installationspfad der Anwendung. Falls vorhanden, wird die lokale Instanz der Anwendung gestartet. Andernfalls wird eine gehostete Instanz gestartet.

Wenn Sie eine Anwendung starten, die nicht auf dem VDA ist, wird die gehostete Anwendung von der Citrix Workspace-App gestartet. Weitere Informationen zur Handhabung des lokalen Starts in StoreFront finden Sie unter [Steuern des lokalen Starts von Anwendungen auf veröffentlichten Desktops](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Wenn Sie nicht möchten, dass die lokale Instanz einer Anwendung auf dem VDA gestartet wird, setzen Sie **LocalLaunchDisabled** auf dem Delivery Controller mithilfe von PowerShell auf **True**. Weitere Informationen finden Sie in der Dokumentation zu [Citrix Virtual Apps and Desktops](#).

Das Feature beschleunigt den Anwendungsstart und bietet dadurch eine bessere Benutzererfahrung. Sie können es über die administrative GPO-Vorlage konfigurieren. Standardmäßig ist vPrefer nur in einem Double-Hop-Szenario aktiviert.

Hinweis:

Wenn Sie die Citrix Workspace-App zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#). Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **vPrefer**.
4. Wählen Sie **Aktiviert**.
5. Wählen Sie in der Dropdownliste neben **Apps zulassen** eine der folgenden Optionen:
 - **Alle Apps zulassen:** Mit dieser Option wird die lokale Instanz aller Apps auf dem VDA gestartet. Die Citrix Workspace-App sucht nach der installierten Anwendung (einschließlich Windows-eigener Anwendungen wie Editor, Rechner, WordPad, Eingabeaufforderung). Sie startet dann diese Anwendung auf dem VDA (und nicht die gehostete App).
 - **Installierte Apps zulassen:** Mit dieser Option wird die lokale Instanz der installierten App auf dem VDA gestartet. Wenn die App nicht auf dem VDA installiert ist, wird die gehostete App gestartet. Standardmäßig ist die Option **Installierte Apps zulassen** ausgewählt, wenn die **vPrefer**-Richtlinie auf **Aktiviert** festgelegt ist. Diese Option gilt nicht für Windows-eigene Anwendungen wie Editor oder Rechner.

- **Netzwerk-Apps zulassen:** Durch diese Option wird die Instanz von Apps gestartet, die in einem freigegebenen Netzwerk veröffentlicht ist.

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

7. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Einschränkung:

- Workspace für Web unterstützt dieses Feature nicht.

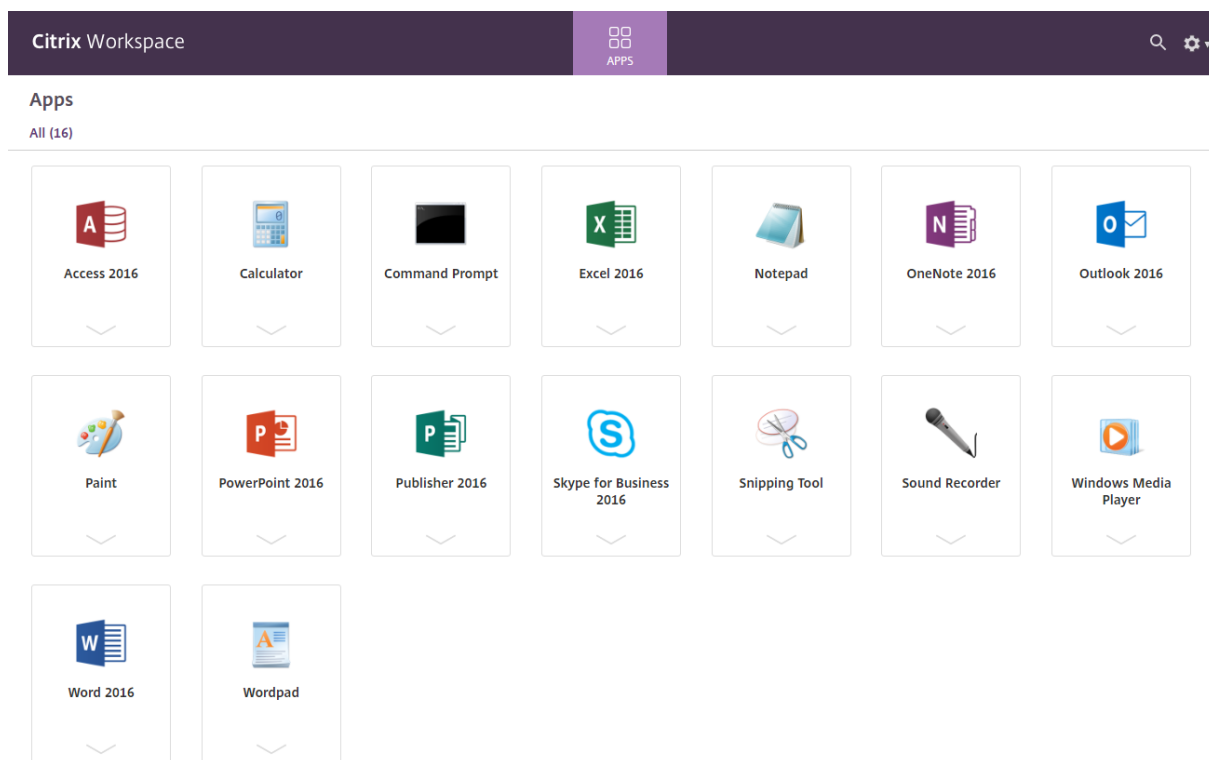
Workspacekonfiguration

Die Citrix Workspace-App für Windows unterstützt die Konfiguration von Workspace für Abonnenten, die möglicherweise einen oder mehrere in Citrix Cloud verfügbare Dienste verwenden.

Die Citrix Workspace-App zeigt nur die speziellen Workspaceressourcen an, die Benutzer verwenden dürfen. Alle in der Citrix Workspace-App verfügbaren digitalen Workspace-Ressourcen werden vom Dienst für die Citrix Cloud Workspace-Benutzeroberfläche bereitgestellt.

Ein Workspace ist Teil einer digitalen Workspacelösung, mit der IT-Mitarbeiter von jedem Gerät aus den Zugriff auf Apps sicher bereitstellen können.

Der Screenshot ist ein Beispiel für die Workspace-Benutzeroberfläche Ihrer Abonnenten. Diese Benutzeroberfläche wird kontinuierlich weiterentwickelt und sieht möglicherweise anders aus als die, mit der Ihre Abonnenten heute arbeiten. Beispielsweise könnte oben auf der Seite "StoreFront" anstelle von "Workspace" angezeigt werden.



SaaS-Apps

Der sichere Zugriff auf SaaS-Anwendungen bietet eine einheitliche Benutzererfahrung bei der Bereitstellung veröffentlichter SaaS-Anwendungen. SaaS-Anwendungen sind mit Single Sign-On verfügbar. Administratoren können jetzt Netzwerk und Endbenutzergeräte eines Unternehmens vor Malware und Datenlecks schützen. Administratoren können dies erreichen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.

Die Citrix Workspace-App für Windows unterstützt die Verwendung von SaaS-Apps unter Einsatz des Citrix Secure Private Access. Über diesen Dienst können Administratoren eine geschlossene Erfahrung mit Single Sign-On und Inhaltsinspektion bereitstellen.

Die Bereitstellung von SaaS-Anwendungen über die Cloud hat folgende Vorteile:

- Einfache Konfiguration: einfach zu bedienen, zu aktualisieren und zu nutzen.
- Single Sign-On: mühelose Anmeldung.
- Standardvorlage für verschiedene Anwendungen: vorlagenbasierte Konfiguration beliebiger Anwendungen.

Die Citrix Workspace-App startet die SaaS-Anwendungen in Citrix Enterprise Browser (zuvor "Citrix Workspace Browser"). Informationen finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

Einschränkungen:

1. Wenn Sie eine veröffentlichte App mit aktivierter Druckoption und deaktivierter Downloadoption starten und einen Druckbefehl an eine gestartete App übergeben, können Sie die betreffende PDF-Datei möglicherweise trotzdem speichern. Sollen Downloads auf jeden Fall unterbunden werden, deaktivieren Sie auch die Druckoption.
2. In einer App eingebettete Videos funktionieren möglicherweise nicht.

Weitere Informationen zur Konfiguration von Workspace finden Sie unter [Workspacekonfiguration](#) in der Dokumentation zu Citrix Cloud.

PDF-Druck

Die Citrix Workspace-App für Windows unterstützt den PDF-Druck in einer Sitzung. Der universelle PDF-Druckertreiber von Citrix ermöglicht das Drucken von Dokumenten aus gehosteten Anwendungen und Desktops, die unter Citrix Virtual Apps and Desktops und Citrix DaaS ausgeführt werden.

Wenn Sie im Dialogfeld **Drucken** die Option **Citrix PDF-Drucker** auswählen, wird die Datei vom Treiber in das PDF-Format konvertiert und auf das lokale Gerät übertragen. Die PDF-Datei wird dann mit dem standardmäßigen PDF-Viewer zur Ansicht geöffnet und kann auf einem lokal angeschlossenen Drucker ausgedruckt werden.

Citrix empfiehlt den Google Chrome-Browser oder Adobe Acrobat Reader zur Anzeige von PDF-Dateien.

Sie können den PDF-Druck in Citrix mit Citrix Studio auf dem Delivery Controller aktivieren.

Voraussetzungen:

- Citrix Workspace-App Version 1808 oder höher
- Citrix Virtual Apps and Desktops Version 7 1808 oder höher
- Auf Ihrem Computer muss mindestens ein PDF-Viewer installiert sein.

Aktivieren der PDF-Druckfunktion:

1. Verwenden Sie auf dem Delivery Controller das Citrix Studio, und wählen Sie im linken Bereich den Knoten **Richtlinie**. Sie können entweder eine Richtlinie erstellen oder eine vorhandene Richtlinie bearbeiten.
2. Legen Sie die Richtlinie **Universellen PDF-Drucker automatisch erstellen** auf "Aktiviert" fest.

Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Einschränkung:

- Das Anzeigen und Drucken von PDF-Dateien wird im Microsoft Edge-Browser nicht unterstützt.

Erweiterter Tabletmodus in Windows 10 mit Windows Continuum

Windows Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Die Citrix Workspace-App für Windows Version 4.10 oder später unterstützt nun Windows Continuum, einschließlich der dynamischen Änderung von Modi.

Bei Geräten mit Touchscreen startet der Windows 10-VDA im Tabletmodus, wenn keine Tastatur oder Maus angeschlossen ist. Ist eine Tastatur und/oder Maus angeschlossen, startet er im Desktopmodus. Durch das Anschließen oder Trennen eines Eingabegeräts an beliebigen Clientgeräten oder am Bildschirm eines 2-in-1-Geräts (z. B. Surface Pro) wird zwischen Tablet- und Desktopmodus umgeschaltet. Weitere Informationen finden Sie unter [Tabletmodus für Geräte mit Touchscreen](#) in der Dokumentation von Citrix Virtual Apps and Desktops.

Auf Clientgeräten mit Touchscreen erkennt der Windows 10-VDA das Vorhandensein einer Tastatur oder einer Maus, wenn Sie eine Verbindung zu einer Sitzung herstellen oder wiederherstellen. Er erkennt auch, wenn Sie während der Sitzung eine Tastatur oder eine Maus anschließen oder entfernen. Dieses Feature ist standardmäßig auf dem VDA aktiviert. Um das Feature zu deaktivieren, ändern Sie mit Citrix Studio die Richtlinie **Tabletmodus ein/aus**.

Der Tabletmodus bietet eine für Touchscreens besser geeignete Benutzeroberfläche:

- Die Schaltflächen sind etwas größer.
- Die **Startseite** und alle gestarteten Apps werden im Vollbildmodus geöffnet.
- Die Taskleiste enthält eine Schaltfläche "Zurück".
- Die Taskleiste enthält keine Symbole.

Der Desktopmodus ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

Hinweis:

Workspace für Web unterstützt Windows Continuum nicht.

Citrix Analytics

Die Citrix Workspace-App ermöglicht die sichere Übertragung von Protokollen an Citrix Analytics. Wenn die Funktion aktiviert ist, werden die Protokolle auf Citrix Analytics-Servern analysiert und gespeichert. Weitere Informationen zu Citrix Analytics finden Sie unter [Citrix Analytics](#).

Relative Maus

Das Feature für die relative Mausfunktion bestimmt, wie weit sich die Maus seit dem letzten Frame innerhalb eines Fensters oder Bildschirms bewegt hat.

Die relative Maus verwendet das Pixeldelta zwischen den Mausbewegungen. Wenn Sie beispielsweise die Richtung der Kamera mit den Steuerelementen der Maus ändern, ist die Funktion effizient. Außerdem verbergen Apps den Mauszeiger häufig, da die Position des Cursors relativ zu den Bildschirmkoordinaten beim Bearbeiten eines 3D-Objekts oder einer Szene nicht relevant ist.

Durch die Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Interpretation ist für Anwendungen erforderlich, die relative Mausgabe statt absoluter Eingabe erfordern.

Sie können das Feature sowohl pro Benutzer als auch pro Sitzung konfigurieren, wodurch die Verfügbarkeit des Features genauer gesteuert werden kann.

Hinweis

Dieses Feature kann nur in einer veröffentlichten Desktopsitzung angewendet werden.

Wenn Sie das Feature mit dem Registrierungs-Editor oder der Datei default.ica konfigurieren, kann die Einstellung auch nach dem Beendigung der Sitzung fortbestehen.

Konfigurieren der relativen Mausfunktion mit dem Registrierungs-Editor

Um das Feature zu konfigurieren, aktivieren Sie die folgenden Registrierungsschlüssel und starten Sie dann die Sitzung neu, damit die Änderungen wirksam werden:

So stellen Sie das Feature pro Sitzung zur Verfügung:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

So stellen Sie das Feature pro Benutzer zur Verfügung:

```
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

- Name: Maus
- Typ: REG_SZ
- Wert: True

Hinweis:

- Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.
- Die in HKEY_LOCAL_MACHINE und HKEY_CURRENT_USER festgelegten Werte müssen identisch sein. Unterschiedliche Werte können Konflikte verursachen.

Konfigurieren der relativen Mausfunktion mit der Datei default.ica

1. Öffnen Sie die Datei default.ica, die normalerweise in `C:\inetpub\wwwroot\Citrix\
site name>\conf\default.ica` ist, wobei "sitename" der Name der Site ist, der bei der Erstellung angegeben wurde. Bei StoreFront-Kunden ist die Datei default.ica normalerweise unter `C:\inetpub\wwwroot\Citrix\
<Storename>\App_Data\default.ica`, wobei `storename` der Name des Stores ist, der bei der Erstellung angegeben wurde.
2. Fügen Sie im Abschnitt WFClient den Schlüssel RelativeMouse hinzu. Legen Sie als Wert dieselbe Konfiguration wie für das JSON-Objekt fest.
3. Legen Sie den Wert wie gewünscht fest:
 - true –Aktivieren der relativen Maus
 - false –Deaktivieren der relativen Maus
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Hinweis:

Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.

Aktivieren der relativen Mausfunktion über den Desktop Viewer

1. Melden Sie sich bei der Citrix Workspace-App an.
2. Starten Sie eine veröffentlichte Desktopsitzung.
3. Klicken Sie auf der Desktop Viewer-Symbolleiste auf **Einstellungen**.
Das Fenster "Citrix Workspace-Einstellungen" wird angezeigt.
4. Wählen Sie **Verbindungen**.
5. Aktivieren Sie unter **Relative Mauseinstellungen** die Option **Relative Maus verwenden**.
6. Klicken Sie auf **Anwenden** und auf **OK**.

Hinweis:

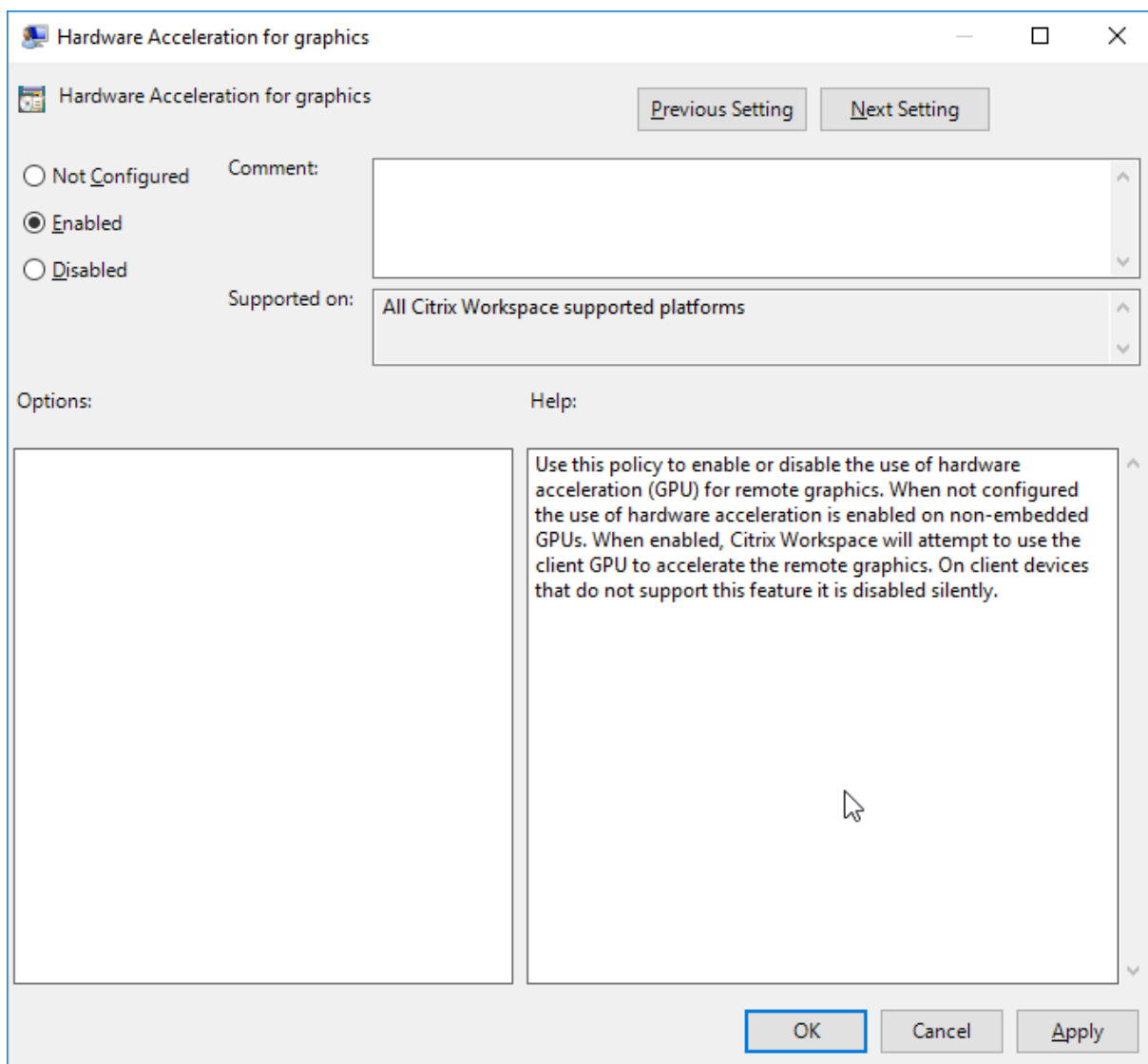
Beim Konfigurieren der relativen Maus mit dem Desktop Viewer wird das Feature nur pro Sitzung angewendet.

Hardwaredecodierung

Wenn Sie die Citrix Workspace-App (mit HDX Engine 14.4) verwenden, kann die GPU für H.264-Decodierung verwendet werden, wenn sie auf dem Client verfügbar ist. Die für GPU-Decodierung verwendete API-Ebene ist DirectX Video Acceleration.

Aktivieren der Hardwaredecodierung mit der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie **Hardwarebeschleunigung für Grafiken**.
4. Wählen Sie **Aktiviert** und klicken Sie auf **Übernehmen** und anschließend auf **OK**.



Anhand der folgenden Registrierungseinträge prüfen Sie, ob die Richtlinie eingerichtet ist und die Hardwarebeschleunigung in einer aktiven ICA-Sitzung verwendet wird:

Registrierungspfad: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

Tipp

Der Wert für **Graphics_GfxRender_Decoder** und **Graphics_GfxRender_Renderer** muss 2 sein. Wenn der Wert 1 ist, wird auf der CPU basierende Decodierung verwendet.

Wenn Sie das Hardwaredecodierungsfeature verwenden, berücksichtigen Sie folgende Einschränkungen:

- Wenn der Client zwei GPUs hat und wenn einer der Bildschirme auf der zweiten GPU aktiv ist, wird CPU-Decodierung verwendet.
- Verwenden Sie keine Hardwaredecodierung auf dem Windows-Gerät des Benutzers, wenn Sie eine Verbindung mit einem Citrix Virtual Apps-Server herstellen, der unter Windows Server 2008 R2 ausgeführt wird. Ist die Hardwaredecodierung aktiviert, treten Probleme auf, wie geringe Leistung beim Markieren von Text und Flackern.

Mikrofoneingabe

Die Citrix Workspace-App unterstützt die mehrfache clientseitige Mikrofoneingabe. Sie können lokal installierte Mikrofone für Folgendes verwenden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Benutzer der Citrix Workspace-App können in Connection Center auswählen, ob am Gerät angeschlossene Mikrofone verwendet werden sollen. Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS können außerdem ihre Mikrofone und Webcams im Citrix Virtual Apps and Desktops-Viewer unter "Einstellungen" deaktivieren.

Clientlaufwerkzuordnung

Die Clientlaufwerkzuordnung unterstützt die Datenübertragung zwischen Host und Client als Stream. Die Dateiübertragung passt sich an veränderliche Netzwerkdurchsatzbedingungen an. Dabei wird außerdem jede verfügbare zusätzliche Bandbreite genutzt, um die Datenübertragungsrate zu erhöhen.

Standardmäßig ist dieses Feature aktiviert.

Um das Feature zu deaktivieren, legen Sie den folgenden Registrierungsschlüssel fest und starten Sie den Server neu:

Pfad: `HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`

Name: `DisableFullStreamWrite`

Typ: REG_DWORD

Wert:

`0x01` = deaktiviert,

0 oder Wert löschen = aktiviert

Multimonitorunterstützung

Sie können maximal acht Monitore mit der Citrix Workspace-App für Windows verwenden.

Jeder Monitor in einer Multimonitorumgebung hat eine eigene, vom Hersteller festgelegte Auflösung. Monitore können in Sitzungen verschiedene Auflösungen und Ausrichtungen haben.

Sitzungen können auf zwei Arten auf mehrere Monitore übergreifend ausgeführt werden:

- Vollbildmodus: Mehrere Monitore werden in der Sitzung angezeigt; Anwendungen werden genauso wie beim lokalen Desktop an Monitore angedockt.

Citrix Virtual Apps and Desktops und Citrix DaaS: Sie können das Desktop Viewer-Fenster über eine beliebige rechteckige Untergruppe von Monitoren ausdehnen, wenn Sie die Größe des Fensters über einen Monitorbereich hinweg ändern und auf **Maximieren** klicken.

- Im Fenstermodus mit nur einem Monitorbild für die Sitzung werden Anwendungen nicht an einzelne Monitore angedockt.

Citrix Virtual Apps and Desktops und Citrix DaaS: Wenn ein Desktop in derselben Zuordnung (früher Desktopgruppe) dann gestartet wird, wird die Fenstereinstellung gespeichert, und der Desktop wird auf denselben Monitoren angezeigt. Mehrere virtuelle Desktops können auf einem Gerät angezeigt werden, wenn die Monitoranordnung rechteckig ist. Wenn der primäre Monitor auf dem Gerät von der Sitzung mit virtuellen Apps und Desktops verwendet wird, wird er zum primären Monitor in der Sitzung. Sonst wird der zahlenmäßig niedrigste Monitor in der Sitzung zum primären Monitor.

Für die Multimonitorunterstützung müssen Sie Folgendes sicherstellen:

- Das Benutzergerät ist für die Unterstützung von mehreren Monitoren konfiguriert.
- Das Betriebssystem kann jeden Monitor erkennen. Um auf Windows-Plattformen zu überprüfen, ob diese Erkennung erfolgt, gehen Sie zu **Einstellungen > System**, klicken Sie auf **Anzeige** und bestätigen Sie, dass jeder Monitor separat angezeigt wird.
- Nach dem Erkennen der Monitore:
 - **Citrix Virtual Desktops:** Konfigurieren Sie das Grafikspeicherlimit mit der Citrix Maschinenrichtlinieneinstellung **Anzeigespeicherlimit**.
 - **Citrix Virtual Apps:** Je nach installierter Citrix Virtual Apps-Serverversion:
 - * Konfigurieren Sie das Limit für den Grafikspeicher mit der Citrix Computerrichtlinieneinstellung **Anzeigespeicherlimit**.

- * Wählen Sie die Farm in der Citrix Verwaltungskonsole für den Citrix Virtual Apps-Server aus und wählen Sie im Aufgabenbereich Folgendes:
 - **Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > HDX Broadcast > Anzeige** oder
 - **Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > ICA > Anzeige.**
- * Legen Sie dann den maximalen Grafikspeicher pro Sitzung fest.

Prüfen Sie, ob die Einstellung (in Kilobyte) hoch genug ist, damit ausreichend Grafikspeicher bereitgestellt wird. Ist der Wert zu niedrig, wird die veröffentlichte Ressource auf einen Teilbereich der Monitore beschränkt, der in die angegebene Größe passt.

Verwenden von Citrix Virtual Desktops auf zwei Monitoren:

1. Wählen Sie den Desktop Viewer aus und klicken Sie auf den Pfeil nach unten.
2. Wählen Sie **Fenster**.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die beiden Monitore. Stellen Sie sicher, dass etwa die Hälfte des Bildschirms in jedem Monitor angezeigt wird.
4. Wählen Sie auf der Symbolleiste des Citrix Virtual Desktops die Option **Vollbild** aus.

Der Bildschirm ist nun auf beide Monitore erweitert.

Informationen zum Berechnen der Größe des Grafikspeichers in Sitzungen für Citrix Virtual Apps and Desktops und Citrix DaaS finden Sie im Knowledge Center-Artikel [CTX115637](#).

Drucker

Überschreiben der Druckereinstellungen auf dem Benutzergerät

1. Klicken Sie im Menü **Drucken**, das in einer Anwendung auf dem Benutzergerät zur Verfügung steht, auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Clienteneinstellungen** auf “Erweiterte Optimierungen” und ändern Sie die Optionen “Bildkomprimierung” und “Bild- und Schriftartcaching”.

Steuerung der Bildschirmtastatur

Damit über Windows-Tablets der Touchzugriff auf virtuelle Anwendungen und Desktops möglich ist, zeigt die Citrix Workspace-App in folgenden Situationen automatisch die Bildschirmtastatur an:

- wenn Sie ein Texteingabefeld aktivieren und
- wenn das Gerät im Zelt- oder Tabletmodus ist.

Auf einigen Geräten und unter bestimmten Umständen kann die Citrix Workspace-App den Geräte-
modus nicht präzise erkennen. Die Bildschirmtastatur wird möglicherweise auch angezeigt, wenn sie
nicht benötigt wird.

Um auf einem konvertierbaren Gerät keine Bildschirmtastatur anzuzeigen:

- Erstellen Sie in `HKEY\LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` den REG_DWORD-Wert `DisableKeyboardPopup`.
- Legen Sie den Wert auf 1 fest.

Hinweis:

Erstellen Sie den Wert auf einer 64-Bit-Maschine in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver`.

Die Tasten können auf folgende 3 Modi festgelegt werden:

- **Automatisch:** `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0`
- **Immer anzeigen** (Bildschirmtastatur): `AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0`
- **Nie anzeigen** (Bildschirmtastatur): `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1`

Tastenkombinationen

Sie können Tastenkombinationen konfigurieren, die die Citrix Workspace-App als Sonderfunktionen interpretiert. Wenn die Richtlinie für Tastenkombinationen aktiviert ist, können Sie Zuordnungen von Citrix Tastenkombinationen, das Verhalten von Windows-Tastenkombinationen und das Tastaturlayout für Sitzungen festlegen.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie Tastenkombinationen.
4. Wählen Sie **Aktiviert** und die gewünschten Optionen.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Citrix Workspace-App-Unterstützung für Symbole in 32-Bit-Farben:

Die Citrix Workspace-App unterstützt Symbole in 32-Bit-High Color. Um Anwendungen im Seamlessmodus darzustellen, wird die Farbtiefe automatisch ausgewählt für:

- Anwendungen im Dialogfeld **Connection Center**,

- das Startmenü und
- die Taskleiste.

Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Um eine bevorzugte Farbtiefe zu definieren, können Sie unter `HKEY\LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` als Registrierungsschlüssel die Zeichenfolge `TWIDesiredIconColor` hinzufügen und den gewünschten Wert festlegen. Die möglichen Werte für die Farbtiefe von Symbolen sind 4, 8, 16, 24 und 32 Bits pro Pixel. Benutzer können eine geringere Farbtiefe für die Symbole wählen, wenn die Netzwerkverbindung langsam ist.

Desktop Viewer

Jedes Unternehmen kann andere Anforderungen haben. Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern. Wie Benutzer das Verbinden mit virtuellen Desktops erleben und inwiefern sie Verbindungen selbst konfigurieren können, wird beim Einrichten der Citrix Workspace-App für Windows festgelegt.

Verwenden Sie **Desktop Viewer**, wenn Benutzer mit dem virtuellen Desktop interagieren müssen. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario kann der Benutzer über die **Desktop Viewer**-Symbolleiste einen virtuellen Desktop in einem Fenster öffnen und den Desktop im lokalen Desktop ziehen und skalieren. Benutzer können Einstellungen festlegen und mit mehreren Desktops über mehrere Citrix Virtual Apps and Desktops- und Citrix DaaS-Verbindungen auf demselben Benutzergerät arbeiten.

Hinweis:

Verwenden Sie die Citrix Workspace-App, um die Bildschirmauflösung auf virtuellen Desktops zu ändern. Die Bildschirmauflösung kann nicht in der Windows-Systemsteuerung geändert werden.

Tastatureingabe in Desktop Viewer

In Desktop Viewer-Sitzungen wird die **Windows-Logo-Taste+L** an den lokalen Computer gesendet.

Strg+Alt+Entf wird an den lokalen Computer gesendet.

Tastatureingaben, die Microsoft-Eingabehilfen wie die Einrastfunktion, die Anschlagverzögerung und Umschalttasten aktivieren, werden normalerweise an den lokalen Computer gesendet.

Als Eingabehilfe von Desktop Viewer werden die Schaltflächen der **Desktop Viewer**-Symbolleiste in einem Pop-upfenster angezeigt, wenn Sie Strg+Alt+Entf drücken.

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

Hinweis:

Wenn Desktop Viewer maximiert ist, können Sie mit Alt+Tab standardmäßig zwischen Fenstern in der Sitzung wechseln. Wenn Desktop Viewer in einem Fenster angezeigt wird, wechseln Sie mit Alt+Tab zwischen Fenstern außerhalb der Sitzung.

Citrix hat bestimmte Tastenkombinationen entwickelt. Beispiele für Tastenkombinationen: Mit Strg+F1 reproduzieren Sie Strg+Alt+Entf und mit Umschalt+F2 wechseln Sie Anwendungen vom Vollbild- in den Fenstermodus und umgekehrt.

Hinweis:

Sie können Tastenkombinationen nicht mit virtuellen Desktops verwenden, die in Desktop Viewer angezeigt werden (d. h. in Sitzungen mit virtuellen Apps und Desktops). Sie können sie aber mit veröffentlichten Anwendungen verwenden (d. h. in Sitzungen mit virtuellen Apps).

Virtuelle Desktops

In einer Desktopsitzung können Benutzer keine Verbindung zu demselben Desktop herstellen. Wenn ein Benutzer dies versucht, wird die vorhandene Desktopsitzung getrennt. Citrix empfiehlt daher:

- Administratoren dürfen die Clients auf dem Desktop nicht so konfigurieren, dass sie auf eine Site verweisen, die denselben Desktop veröffentlicht.
- Benutzer dürfen keine Site besuchen, die denselben Desktop hostet, wenn die Site für die automatische Wiederverbindung der Benutzer mit vorhandenen Sitzungen konfiguriert ist.
- Benutzer dürfen keine Site besuchen, die denselben Desktop hostet, und versuchen, ihn zu starten.

Wenn ein Benutzer sich lokal an einem Computer anmeldet, der als virtueller Desktop fungiert, blockiert er Verbindungen zu diesem Desktop.

Citrix empfiehlt ein gemeinsames Definieren der Gerätezuordnung:

- wenn Benutzer sich über einen virtuellen Desktop mit virtuellen Anwendungen verbinden, die mit Citrix Virtual Apps veröffentlicht wurden, und
- wenn es im Unternehmen einen separaten Citrix Virtual Apps-Administrator gibt.

Durch die Gerätezuordnung wird überprüft, ob Desktopgeräte konsistent in Desktop- und Anwendungssitzungen zugeordnet werden. Da lokale Laufwerke in Desktopsitzungen als Netzwerklaufwerke angezeigt werden, muss der Citrix Virtual Apps-Administrator die Richtlinie für die Laufwerkzuordnung ändern und Netzwerklaufwerke einschließen.

Timeout der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird.

Sie ändern den Timeoutzeitraum mit den folgenden Schritten:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu folgendem Pfad:
 - Auf 64-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
 - Auf 32-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`
3. Erstellen Sie einen Registrierungsschlüssel wie im Folgenden beschrieben:
 - Typ: `REG_DWORD`
 - Name: `SI_INACTIVE_MS`
 - Wert: 4, wenn die Statusanzeige früher ausgeblendet werden soll.

Wenn Sie diesen Schlüssel konfigurieren, wird der Statusindikator möglicherweise häufig angezeigt und ausgeblendet. Dieses Verhalten entspricht dem Design. Sie können den Statusindikator wie folgt unterdrücken:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu folgendem Pfad:
 - Auf 64-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
 - Auf 32-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`
3. Erstellen Sie einen Registrierungsschlüssel wie im Folgenden beschrieben:
 - Typ: `REG_DWORD`
 - Name: `NotificationDelay`
 - Wert: Beliebiger Wert in Millisekunden (zum Beispiel 120000)

Inaktivitätstimeout für Workspace-Sitzungen

Mit dem Inaktivitätstimeout können Administratoren festlegen, nach wie viel Zeit inaktive Benutzer automatisch von der Citrix Workspace-Sitzung abgemeldet werden. Sie werden automatisch von Workspace abgemeldet, wenn Maus, Tastatur oder Toucheingabe im angegebenen Zeitintervall inaktiv sind. Das Inaktivitätstimeout hat keine Auswirkungen auf aktive Sitzungen mit virtuellen Apps oder Desktops oder auf Citrix StoreFront-Stores.

Der Wert für das Inaktivitätstimeout kann zwischen einer Minute und 1440 Minuten liegen. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert. Administratoren können die Eigenschaft “inactivityTimeoutInMinutes” mit einem PowerShell-Modul konfigurieren. Klicken Sie [hier](#), um die PowerShell-Module für die Citrix Workspace-Konfiguration herunterzuladen.

Für die Endbenutzererfahrung gilt Folgendes:

- Drei Minuten vor der Abmeldung wird eine Benachrichtigung in Ihrem Sitzungsfenster angezeigt. Sie können angemeldet bleiben oder sich abmelden.
- Die Benachrichtigung wird nur angezeigt, wenn der konfigurierte Wert für das Inaktivitätstimeout größer oder gleich fünf Minuten ist.
- Benutzer können auf **Angemeldet bleiben** klicken, um die Benachrichtigung zu schließen und die App weiter zu verwenden. In diesem Fall wird der Inaktivitätstimer auf den konfigurierten Wert zurückgesetzt. Sie können auch auf **Abmelden** klicken, um die Sitzung für den aktuellen Store zu beenden.

Hinweis:

Administratoren können das Inaktivitätstimeout nur für Workspace-Sitzungen (Cloud) konfigurieren.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Citrix Workspace-App für Windows und sendet die Daten automatisch an Citrix und Google Analytics.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Citrix Workspace-App zu verbessern.

Hinweis:

Ab Version 2203.1 LTSR CU4 sammelt die Citrix Workspace-App keine CEIP-Daten von Benutzern in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR), in der Schweiz und im Vereinigten Königreich (UK). Aktualisieren Sie die Citrix Workspace-App, wenn Sie diese Funktion nutzen möchten.

Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix und schützt sie, wie im [Citrix Services Security Exhibit](#) festgelegt. Das Citrix Services Security Exhibit ist im [Citrix Trust Center](#) verfügbar.

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.

Sie können das Senden von CEIP-Daten an Citrix und Google Analytics deaktivieren.

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen**.
Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
3. Wählen Sie **Datensammlung**.
4. Wählen Sie **Nein, danke**, um CEIP zu deaktivieren und die Teilnahme abzulehnen.
5. Klicken Sie auf **Speichern**.

Hinweis:

Sie können das Senden von CEIP-Daten beenden, mit Ausnahme der für Google Analytics erfassten Betriebssystem- und Citrix Workspace-App-Version, die in der zweiten Tabelle durch ein * gekennzeichnet sind.

Sie können auch zum folgenden Registrierungseintrag navigieren und den Wert wie vorgeschlagen festlegen:

Pfad: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

Schlüssel: `Enable_CEIP`

Wert: `False`

Hinweis:

Wenn Sie **Nein, danke** auswählen oder den Schlüssel `Enable_CEIP` auf `False` festlegen, um auch die letzten beiden CEIP-Datenelemente (Betriebssystemversion und Version der Citrix

Workspace-App) nicht zu senden, navigieren Sie zum folgenden Registrierungseintrag und legen Sie den Wert fest:

Pfad: HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP

Schlüssel: DisableHeartbeat

Wert: True

Folgende CEIP-Datenelemente werden von Citrix gesammelt:

Betriebssystemversion	Citrix Workspace-App	Angeschlossene externe Geräte	Bildschirmauflösung
Flash-Version	Desktop Lock-Konfiguration	Toucheingabe aktiviert	Authentifizierungskonfiguration
Sitzungsstartmethode	Grafikkonfiguration	Desktop Viewer-Konfiguration	Drucken
Verbindungsfehler	Dauer des Starts	Sprache der Citrix Workspace-App	VDA-Informationen
SSON-Status	Status des Installers	Dauer der Installation	Verbindungsprotokoll
Internet Explorer-Version			

Folgende CEIP-Datenelemente werden von Google Analytics erfasst:

Betriebssystemversion*	Citrix Workspace-App-Version*	Authentifizierungskonfiguration	Sprache der Citrix Workspace-App
Sitzungsstartmethode	Verbindungsfehler	Verbindungsprotokoll	VDA-Informationen
Installerkonfiguration	Status des Installers	Clienttastaturlayout	Storekonfiguration
Einstellung für automatische Aktualisierung	Nutzung des Connection Centers	Konfiguration von App Protection	Grund für das Offline-Banner

Regionale Einstellungen

Die Citrix Workspace-App zeigt Datum, Uhrzeit und Zahlen basierend auf dem Gebietsschema des Browsers oder Endpunktgeräts an.

Ab Citrix Workspace-App 2106 können Sie die Formate für Datum, Uhrzeit und Zahlen unter “Regionale Einstellungen” regional anpassen. Die in diesen Einstellungen vorgenommenen Änderungen werden für einen einzelnen Benutzer gespeichert und auf alle Geräte angewendet.

Hinweis:

Diese Option ist nur auf Cloudbereitstellungen verfügbar.

Weitere Informationen finden Sie unter [Regionale Einstellungen](#).

Single Sign-On für die Citrix Workspace-App konfigurieren

October 26, 2023

Single Sign-On mit Azure Active Directory

In diesem Abschnitt wird erläutert, wie Sie Single Sign-On (SSO) mithilfe von Azure Active Directory (AAD) als Identitätsanbieter mit domänenverbundenen Workloads in Hybrid- oder AAD-registrierten Endpunkten implementieren. Bei dieser Konfiguration ist die Authentifizierung bei Workspace mit Windows Hello oder FIDO2 auf bei AAD registrierten Endpunkten möglich.

Hinweis:

Wenn Sie Windows Hello als eigenständige Authentifizierung verwenden, ist Single Sign-On bei der Citrix Workspace-App möglich. Beim Zugriff auf veröffentlichte virtuelle Apps oder Desktops werden Ihr Benutzername und das Kennwort jedoch angefordert. Dieses Problem können Sie umgehen, indem Sie den Verbundauthentifizierungsdienst (FAS) implementieren.

Voraussetzungen

- Aktive Verbindung von Azure Active Directory mit Citrix Cloud. Weitere Informationen finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).
- Azure Active Directory-Authentifizierung für Workspace Weitere Informationen finden Sie unter [Aktivieren der Azure AD-Authentifizierung für Workspaces](#).
- Stellen Sie sicher, dass Sie Azure AD Connect konfiguriert haben. Weitere Informationen finden Sie unter [Erste Schritte mit Azure AD Connect mit Expresseinstellungen](#).
- Aktivieren Sie die Passthrough-Authentifizierung auf Azure AD Connect. Überprüfen Sie außerdem, ob die Optionen für Single Sign-On und Passthrough auf dem Azure-Portal funktionieren.

Weitere Informationen finden Sie unter [Azure Active Directory-Passthrough-Authentifizierung: Schnellstart](#).

Konfiguration

Führen Sie die folgenden Schritte aus, um SSO auf Ihrem Gerät zu konfigurieren:

1. Installieren der Citrix Workspace-App über die Windows-Befehlszeile mit der Option `includeSSON`:

```
CitrixWorkspaceApp.exe /includeSSON
```

1. Starten Sie das Gerät neu.
2. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
3. Wählen Sie **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort**.
4. Wählen Sie **Passthrough-Authentifizierung aktivieren**. Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen** aktivieren, damit die Passthrough-Authentifizierung funktioniert.
5. Ändern Sie im Internet Explorer die Einstellungen unter Benutzerauthentifizierung. Schrittfolge zum Anpassen der Einstellungen:
 - Öffnen Sie in der Systemsteuerung die Option **Interneteigenschaften**.
 - Navigieren Sie zu **Allgemeine Eigenschaften > Lokales Intranet** und klicken Sie auf **Sites**.
 - Klicken Sie im Fenster **Lokales Intranet** auf **Erweitert, vertrauenswürdige Sites hinzufügen** fügen Sie die folgenden vertrauenswürdigen Sites hinzu und klicken Sie auf **Schließen**:
 - `https://aadg.windows.net.nsatc.net`
 - `https://autologon.microsoftazuread-sso.com`
 - The name of your tenant, **for** example: `https://xxxtenantxxx.cloud.com`
6. Deaktivieren Sie zusätzliche Authentifizierungsaufforderungen, indem Sie das Attribut `prompt=login` im Mandanten deaktivieren. Weitere Informationen finden Sie unter [User Prompted for Additional Credentials on Workspace URLs When Using Federated Authentication Providers](#). Sie können den technischen Support von Citrix bitten, das Attribut `prompt=login` in Ihrem Mandanten für die Konfiguration von Single Sign-On zu deaktivieren.

7. Aktivieren Sie die Domänen-Passthrough-Authentifizierung auf dem Citrix Workspace-App-Client. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).
8. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

Single Sign-On mit Okta und Verbundauthentifizierungsdienst

In diesem Abschnitt wird erläutert, wie Sie Single Sign-On (SSO) mit Okta als Identitätsanbieter mit domänenverbundenem Gerät und Verbundauthentifizierungsdienst implementieren können. Bei dieser Konfiguration können Sie sich mit Okta bei Workspace per Single Sign-On authentifizieren und eine zweite Anmeldeaufforderung vermeiden. Dieser Authentifizierungsmechanismus erfordert den Citrix Verbundauthentifizierungsdienst in Citrix Cloud. Weitere Informationen finden Sie unter [Verbinden des Citrix Verbundauthentifizierungsdiensts \(FAS\) mit Citrix Cloud](#).

Voraussetzungen

- Cloud Connector. Weitere Informationen zur Installation des Cloud Connectors finden Sie unter [Cloud Connector-Installation](#).
- Ein Okta-Agent. Weitere Informationen zum Installieren eines Okta-Agents finden Sie unter [Install the Okta Active Directory agent](#). Sie können außerdem den Okta IWA Web-Agent für die Anmeldung von einem mit der Windows-Domäne verbundenen Gerät konfigurieren. Weitere Informationen finden Sie unter [Install and configure the Okta IWA Web agent for Desktop single sign-on](#)
- Aktive Verbindung von Azure Active Directory mit Citrix Cloud. Weitere Informationen finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).
- Verbundauthentifizierungsdienst. Weitere Informationen finden Sie unter [Installieren des Verbundauthentifizierungsdiensts](#).

Konfiguration

Führen Sie die folgenden Schritte aus, um SSO auf Ihrem Gerät zu konfigurieren:

Verbinden von Citrix Cloud mit Ihrer Okta-Organisation:

1. Laden Sie den Okta Active Directory-Agent herunter und installieren Sie ihn. Weitere Informationen finden Sie unter [Install the Okta Active Directory agent](#).
2. Melden Sie sich bei Citrix Cloud auf <https://citrix.cloud.com> an.
3. Klicken Sie im Menü "Citrix Cloud" auf **Identitäts- und Zugriffsverwaltung**.

4. Suchen Sie Okta, klicken Sie auf die Auslassungspunkte (...) und wählen Sie im Menü **Verbinden** aus.
5. Geben Sie unter **Okta-URL** Ihre Okta-Domäne ein.
6. Geben Sie unter **Okta-API-Token** den API-Token für Ihre Okta-Organisation ein.
7. Geben Sie für **Client-ID** und **Geheimer Clientschlüssel** die Client-ID und den geheimen Clientschlüssel der zuvor erstellten OIDC-Webanwendungsintegration ein. Um diese Werte aus der Okta-Konsole zu kopieren, wählen Sie **Anwendungen** und suchen die Okta-Anwendung. Klicken Sie unter **Client-Anmeldeinformationen** auf die Schaltfläche **In Zwischenablage kopieren** für jeden Wert.
8. Klicken Sie auf **Testen und schließen**. Citrix Cloud überprüft Ihre Okta-Details und testet die Verbindung.

Aktivieren der Okta-Authentifizierung für Workspaces:

1. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Authentifizierung**.
2. Wählen Sie **Okta**. Wählen Sie **Ich verstehe die Auswirkungen auf Abonnenten**, wenn Sie dazu aufgefordert werden.
3. Klicken Sie auf **Akzeptieren**, um die Berechtigungsanforderung zu akzeptieren.

Aktivieren des Verbundauthentifizierungsdiensts:

1. Wählen Sie im Citrix Cloud-Menü zunächst **Workspacekonfiguration** und dann **Authentifizierung**.
2. Klicken Sie auf **FAS aktivieren**. Es kann bis zu fünf Minuten dauern, bis die Änderung auf Teilnehmersitzungen angewendet wird.

Anschließend ist der Verbundauthentifizierungsdienst für alle Starts virtueller Apps und Desktops in Citrix Workspace aktiv.

Wenn sich Abonnenten bei ihrem Workspace anmelden und eine virtuelle App oder einen virtuellen Desktop am Ressourcenstandort des FAS-Servers starten, erfolgt der Start ohne Aufforderung zur Eingabe von Anmeldeinformationen.

Hinweis:

Wenn alle FAS-Server an einem Ressourcenstandort ausgefallen sind oder sich im Wartungsmodus befinden, wird die Anwendung erfolgreich gestartet, aber Single Sign-On ist nicht aktiv. Abonnenten müssen dann bei jedem Zugriff auf eine App oder einen Desktop ihre AD-Anmeldeinformationen eingeben.

Authentifizieren

April 22, 2024

Zur maximalen Sicherung der Umgebung müssen Sie die Verbindungen zwischen der Citrix Workspace-App und den veröffentlichten Ressourcen sichern. Sie können verschiedene Authentifizierungsmethoden für die Citrix Workspace-App konfigurieren, u. a. Domänen-Passthrough-Authentifizierung, Smartcardauthentifizierung und Kerberos-Passthrough-Authentifizierung.

Domänen-Passthrough-Authentifizierung

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) verwenden, ohne sich erneut authentifizieren zu müssen.

Wenn Sie sich bei der Citrix Workspace-App anmelden, werden Ihre Anmeldeinformationen zusammen mit den Apps und Desktops sowie Startmenüeinstellungen an StoreFront übergeben. Nach der Konfiguration von Single Sign-On können Sie sich bei der Citrix Workspace-App anmelden und Sitzungen mit virtuellen Apps und Desktops starten, ohne Ihre Anmeldeinformationen erneut eingeben zu müssen.

Sie müssen bei allen Webbrowsern Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren. Weitere Informationen zum Konfigurieren von Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage finden Sie unter [Konfigurieren von Single Sign-On mit Citrix Gateway](#).

Sie können Single Sign-On sowohl bei der Neuinstallation als auch bei einem Upgrade konfigurieren, indem Sie eine der folgenden Optionen verwenden:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

Single Sign-On während der Neuinstallation konfigurieren

Konfigurieren Sie Single Sign-On während einer Neuinstallation mit folgenden Schritten:

1. Konfiguration in StoreFront.
2. Konfigurieren Sie XML-Vertrauensdienste auf dem Delivery Controller.
3. Ändern der Internet Explorer-Einstellungen.
4. Installieren der Citrix Workspace-App mit Single Sign-On.

Single Sign-On in StoreFront konfigurieren

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und das von dieser Domäne bereitgestellte Citrix Virtual Apps and Desktops und Citrix DaaS verwenden, ohne sich für jede App oder jeden Desktop neu authentifizieren zu müssen.

Wenn Sie mit dem **Storebrowse**-Hilfsprogramm einen Store hinzufügen, werden Ihre Anmeldeinformationen zusammen mit den für Sie enumerierten Apps und Desktops (einschließlich Startmenü-einstellungen) an den Citrix Gateway-Server übergeben. Nach dem Konfigurieren von Single Sign-On können Sie den Store hinzufügen, Ihre Apps und Desktops enumerieren und erforderliche Ressourcen starten, ohne Ihre Anmeldeinformationen mehrmals eingeben zu müssen.

Abhängig von der Citrix Virtual Apps and Desktops-Bereitstellung kann die Single Sign-On-Authentifizierung über die Verwaltungskonsole in StoreFront konfiguriert werden.

In der folgenden Tabelle finden Sie verschiedene Anwendungsfälle und die entsprechende Konfiguration:

Anwendungsfall	Konfigurationsdetails	Weitere Informationen
SSON ist in StoreFront konfiguriert	Starten Sie Citrix Studio, navigieren Sie zu Store > Authentifizierungsmethoden verwalten - Store und aktivieren Sie Domänen-Passthrough-Authentifizierung .	Wenn die Citrix Workspace-App nicht mit Single Sign-On konfiguriert ist, ändert sich die Authentifizierungsmethode automatisch von Domänen-Passthrough-Authentifizierung in Benutzername und Kennwort , sofern verfügbar.
Wenn Workspace für Web erforderlich ist	Starten Sie Stores > Workspace für Websites > Authentifizierungsmethoden verwalten und aktivieren Sie Domänen-Passthrough-Authentifizierung .	Wenn die Citrix Workspace-App nicht mit Single Sign-On konfiguriert ist, ändert sich die Authentifizierungsmethode automatisch von Domänen-Passthrough-Authentifizierung in Benutzername und Kennwort , sofern verfügbar.

Single Sign-On mit Citrix Gateway konfigurieren

Sie aktivieren Single Sign-On mit Citrix Gateway über die administrative Gruppenrichtlinienobjektvorlage.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**. Wählen Sie dann die Richtlinie **Single Sign-On für Citrix Gateway**.
3. Wählen Sie **Aktiviert**.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

XML-Vertrauensdienste auf dem Delivery Controller konfigurieren

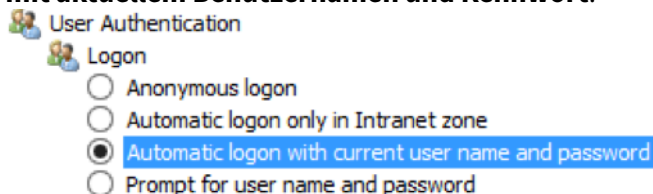
Führen Sie in Citrix Virtual Apps and Desktops und Citrix DaaS als Administrator den folgenden PowerShell-Befehl auf dem Delivery Controller aus:

```
asnpx Citrix* ; Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

Ändern der Internet Explorer-Einstellungen

1. Fügen Sie den StoreFront-Server der Liste der vertrauenswürdigen Sites im Internet Explorer hinzu. Schrittfolge zum Hinzufügen:
 - a) Starten Sie **Internetoptionen** über die Systemsteuerung.
 - b) Klicken Sie auf **Sicherheit** > **Lokales Internet** und dann auf **Sites**.
Das Fenster **Lokales Intranet** wird angezeigt.
 - c) Wählen Sie **Erweitert**.
 - d) Fügen Sie die URL des StoreFront-FQDN mit den entsprechenden HTTP- oder HTTPS-Protokollen hinzu.
 - e) Klicken Sie auf **Anwenden** und auf **OK**.
2. Ändern Sie im **Internet Explorer** die Einstellungen unter **Benutzerauthentifizierung**. Schrittfolge zum Modifizieren:
 - a) Starten Sie **Internetoptionen** über die Systemsteuerung.
 - b) Klicken Sie auf **Sicherheit** > **Vertrauenswürdige Sites**.

- c) Klicken Sie auf **Stufe anpassen**. Das Fenster **Sicherheitseinstellungen - Zone vertrauenswürdiger Sites** wird angezeigt.
- d) Wählen Sie im Bereich **Benutzerauthentifizierung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**.



- e) Klicken Sie auf **Anwenden** und auf **OK**.

Single Sign-On über die Befehlszeilenschnittstelle konfigurieren

Installieren Sie die Citrix Workspace-App mit dem Switch `/includeSSON` und starten Sie die Citrix Workspace-App neu, damit die Änderungen wirksam werden.

Hinweis:

Wenn Sie die Citrix Workspace-App für Windows ohne die Single Sign-On-Komponente installieren, wird das Upgrade auf die neueste Version der Citrix Workspace-App mit dem Switch `/includeSSON` nicht unterstützt.

Single Sign-On mit der GUI konfigurieren

1. Suchen Sie die Installationsdatei der Citrix Workspace-App (`CitrixWorkspaceApp.exe`).
2. Doppelklicken Sie auf `CitrixWorkspaceApp.exe`, um das Installationsprogramm zu starten.
3. Wählen Sie im **Installationsassistenten zum Aktivieren von Single Sign-On** die Option **Single Sign-On aktivieren**.
4. Klicken Sie auf **Weiter** und folgen Sie den Anweisungen, um die Installation abzuschließen.

Sie können sich jetzt ohne Eingabe von Benutzeranmeldeinformationen mit der Citrix Workspace-App bei einem vorhandenen Store anmelden (oder einen neuen Store konfigurieren).

Single Sign-On in Workspace für Web konfigurieren

Sie können Single Sign-On in Workspace für Web mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren.

1. Öffnen Sie die administrative GPO-Vorlage von Workspace für Web, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**.
3. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Passthrough-Authentifizierung aktivieren**. Mit dieser Option kann Workspace für Web Ihre Anmeldeinformationen für die Authentifizierung auf dem Remoteserver verwenden.
5. Klicken Sie auf **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen**. Mit dieser Option werden alle Authentifizierungseinschränkungen umgangen und das Passthrough von Anmeldeinformationen für alle Verbindungen ermöglicht.
6. Klicken Sie auf **Anwenden** und auf **OK**.
7. Starten Sie Workspace für Web neu, um die Änderungen zu übernehmen.

Stellen Sie sicher, dass Single Sign-On aktiviert ist, indem Sie den **Task-Manager** starten und prüfen, ob der Prozess `ssonsvr.exe` ausgeführt wird.

Single Sign-On mit Active Directory konfigurieren

Führen Sie die folgenden Schritte aus, um die Citrix Workspace-App für die Passthrough-Authentifizierung mit der Active Directory-Gruppenrichtlinie zu konfigurieren. In diesem Szenario können Sie die Authentifizierung per Single Sign-On auch ohne Enterprise-Software-Bereitstellungstools wie Microsoft System Center Configuration Manager erzielen.

1. Laden Sie die Installationsdatei für die Citrix Workspace-App ([CitrixWorkspaceApp.exe](#)) auf eine geeignete Netzwerkfreigabe herunter. Die Maschinen, auf denen die Citrix Workspace-App installiert werden soll, müssen darauf Zugriff haben.
2. Laden Sie die Vorlage [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) von der [Downloadseite für die Citrix Workspace-App für Windows](#) herunter.
3. Bearbeiten Sie den Inhalt, damit der Speicherort und die Version von `CitrixWorkspaceApp.exe` korrekt sind.
4. Geben Sie in der **Active Directory-Gruppenrichtlinienverwaltungskonsolle** als Startskript [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) ein. Weitere Informationen zum Bereitstellen der Startskripts finden Sie im Abschnitt [Active Directory](#).
5. Navigieren Sie im Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Vorlagen hinzufügen/entfernen**, um die Datei `receiver.adml` hinzuzufügen.
6. Nachdem Sie die Vorlage `receiver.adml` hinzugefügt haben, navigieren Sie zu **Computerkonfiguration** > **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Be-**

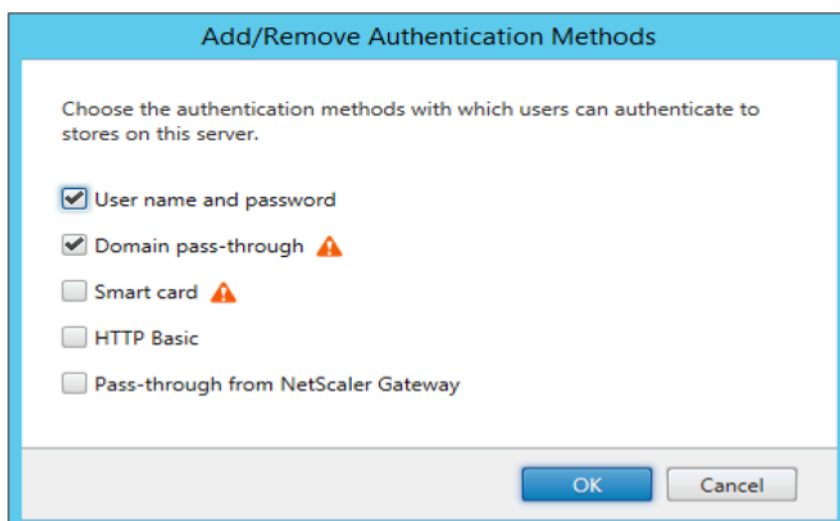
nutzerauthentifizierung. Weitere Informationen über das Hinzufügen von Vorlagendateien finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#).

7. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** und legen Sie sie auf **Aktiviert** fest.
8. Wählen Sie **Passthrough-Authentifizierung aktivieren** und klicken Sie auf **Übernehmen**.
9. Starten Sie die Maschine neu, damit die Änderungen wirksam werden.

Single Sign-On in StoreFront konfigurieren

Konfigurieren in StoreFront

1. Starten Sie **Citrix Studio** auf dem StoreFront-Server und wählen Sie **Stores > Authentifizierungsmethoden verwalten –Store**.
2. Wählen Sie dann **Domänen-Passthrough**.



Authentifizierungstoken

Authentifizierungstoken werden verschlüsselt und auf dem lokalen Datenträger gespeichert, sodass Sie Ihre Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht erneut eingeben müssen. Die Citrix Workspace-App bietet eine Option, mit der das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktiviert werden kann.

Mit einer neuen Richtlinie für ein Gruppenrichtlinienobjekt (GPO) kann das Speichern von Authentifizierungstoken konfiguriert und so die Sicherheit erhöht werden.

Hinweis:

Diese Konfiguration ist nur in Cloud-Bereitstellungen anwendbar.

Speicherung von Authentifizierungstoken über die GPO-Richtlinie deaktivieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Self-Service**.
3. Wählen Sie in der Richtlinie **Authentifizierungstoken speichern** eine der folgenden Optionen aus:
 - **Aktiviert:** Gibt an, dass die Authentifizierungstoken auf dem Datenträger gespeichert werden. Die Standardeinstellung ist "Aktiviert".
 - **Deaktiviert:** Gibt an, dass die Authentifizierungstoken nicht auf dem Datenträger gespeichert sind. Geben Sie Ihre Anmeldeinformationen erneut ein, wenn Ihr System oder Ihre Sitzung neu gestartet wird.
4. Klicken Sie auf **Anwenden** und auf **OK**.

Ab Version 2106 bietet die Citrix Workspace-App eine weitere Option, mit der das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktiviert werden kann. Mit dem Global App Configuration Service können Sie die vorhandene GPO-Konfiguration und das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktivieren.

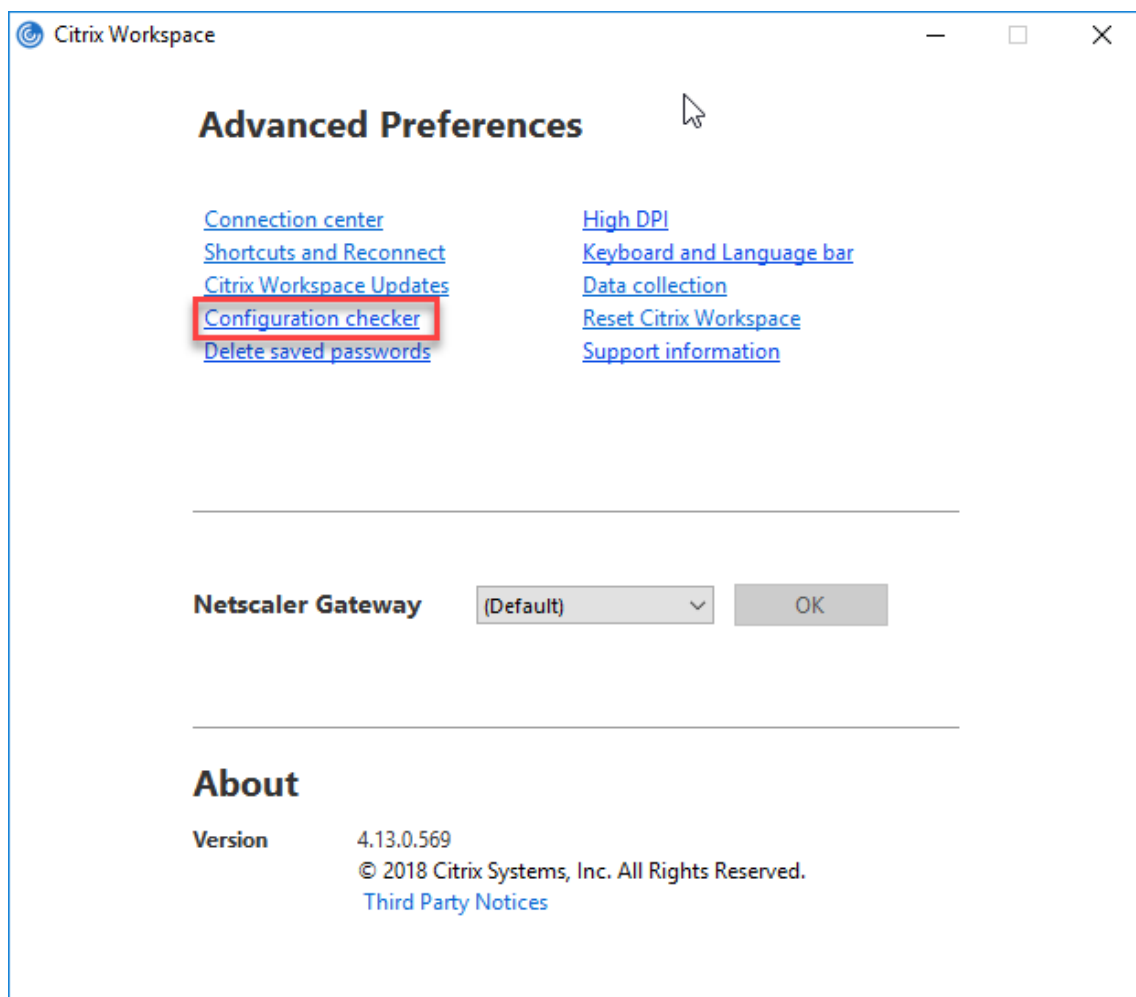
Legen Sie im Global App Configuration Service das Attribut `Store Authentication Tokens` auf `False` fest.

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

Konfigurationsprüfung

Mit der Konfigurationsprüfung können Sie testen, ob Single Sign-On ordnungsgemäß konfiguriert ist. Der Test wird für verschiedene Prüfpunkte der Single Sign-On-Konfiguration ausgeführt und die Konfigurationsergebnisse werden angezeigt.

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol der Citrix Workspace-App und dann auf **Erweiterte Einstellungen**.
Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
2. Klicken Sie auf **Konfigurationsprüfung**.
Das Fenster **Citrix Konfigurationsprüfung** wird angezeigt.



3. Wählen Sie **SSONChecker** im Bereich **Auswählen** aus.
4. Klicken Sie auf **Ausführen**. Eine Fortschrittsanzeige mit dem Status des Tests wird angezeigt.

Das Fenster der **Konfigurationsprüfung** enthält die folgenden Spalten:

1. **Status:** zeigt das Ergebnis eines Tests auf einem bestimmten Prüfpunkt an.
 - Ein grünes Häkchen bedeutet, dass der Prüfpunkt ordnungsgemäß konfiguriert ist.
 - Ein blaues I bedeutet, dass zu dem Prüfpunkt Informationen vorhanden sind.
 - Ein rotes X bedeutet, dass der Prüfpunkt nicht ordnungsgemäß konfiguriert ist.
2. **Anbieter:** zeigt den Namen des Moduls an, auf dem der Test ausgeführt wird. In diesem Fall Single Sign-On.
3. **Suite:** die Kategorie des Tests. Beispiel: Installation.
4. **Test:** der Name des Tests, der ausgeführt wird.
5. **Details:** zusätzliche Informationen zum Test (für bestandene und für fehlgeschlagene Tests).

Der Benutzer erhält weitere Informationen zu den einzelnen Prüfpunkten und den entsprechenden Ergebnissen.

Die folgenden Tests werden durchgeführt:

1. Installation mit Single Sign-On.
2. Erfassen der Anmeldeinformationen.
3. Registrierung von Netzwerkanbieter: Das Testergebnis für “Registrierung von Netzwerkanbieter” hat nur dann ein grünes Häkchen, wenn “Citrix Single Sign-On” als erster Netzwerkanbieter festgelegt ist. Wenn “Citrix Single Sign-On” an einer weiteren Stelle in der Liste steht, werden neben dem Testergebnis für “Registrierung von Netzwerkanbieter” ein blaues I und zusätzliche Informationen angezeigt.
4. Single Sign-On-Prozess wird ausgeführt.
5. Gruppenrichtlinie: Diese Richtlinie ist standardmäßig auf dem Client konfiguriert.
6. Interneteinstellungen für Sicherheitszonen: Sie müssen die Store-/XenApp-Dienst-URL der Liste der Sicherheitszonen in den Internetoptionen hinzufügen.
Wenn die Sicherheitszonen per Gruppenrichtlinie konfiguriert sind, erfordern Änderungen in der Richtlinie das erneute Öffnen des Fensters **Erweiterte Einstellungen**, damit die Änderungen wirksam werden und der richtige Teststatus angezeigt wird.
7. Authentifizierungsmethode für StoreFront.

Hinweis:

- Wenn Sie auf Workspace für Web zugreifen, gelten die Testergebnisse nicht.
- Wenn die Citrix Workspace-App mit mehreren Stores konfiguriert ist, wird der Test für die Authentifizierungsmethode für alle konfigurierten Stores ausgeführt.
- Sie können die Testergebnisse als Berichte speichern. Das Standardberichtformat ist TXT.

Ausblenden der Konfigurationsprüfung im Fenster “Erweiterte Einstellungen”

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie zu **Citrix Komponenten > Citrix Workspace > Self-Service > DisableConfigChecker**.
3. Klicken Sie auf **Aktiviert**, um die Option **Konfigurationsprüfung** im Fenster **Erweiterte Einstellungen** auszublenden.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Führen Sie den Befehl `gpupdate /force` aus.

Einschränkung:

Die Konfigurationsprüfung enthält nicht den Prüfpunkt für die Konfiguration von “An XML-Dienst gesendeten Anfragen vertrauen” auf Citrix Virtual Apps and Desktops-Servern.

Beacontest Mit der Citrix Workspace-App können Sie einen Beacontest durchführen. Hierfür verwenden Sie den in der **Konfigurationsprüfung** enthaltenen Beacon Checker. Über den Beacontest können Sie prüfen, ob der Beacon (ping.citrix.com) erreichbar ist. Mit dem Test können Sie eine der vielen möglichen Ursachen für eine langsame Ressourcenenumeration (Beacon nicht verfügbar) eliminieren. Um den Test auszuführen, klicken Sie mit der rechten Maustaste auf die Citrix Workspace-App im Infobereich und wählen Sie **Erweiterte Einstellungen > Konfigurationsprüfung**. Wählen Sie in der Liste der vorhandenen Tests die Option **Beacon checker** und klicken Sie auf **Ausführen**.

Der Test kann folgende Ergebnisse haben:

- Erreichbar: Die Citrix Workspace-App kann den Beacon erfolgreich kontaktieren.
- Nicht erreichbar: Die Citrix Workspace-App kann den Beacon nicht kontaktieren.
- Teilweise erreichbar: Die Citrix Workspace-App kann den Beacon sporadisch kontaktieren.

Hinweis:

- Die Testergebnisse gelten nicht für Workspace für Web.
- Sie können die Testergebnisse als Bericht speichern. Das Standardberichtformat ist TXT.

Domänen-Passthrough-Authentifizierung mit Kerberos

Dieser Abschnitt gilt nur für Verbindungen zwischen der Citrix Workspace-App für Windows und StoreFront, Citrix Virtual Apps and Desktops und Citrix DaaS.

Die Citrix Workspace-App für Windows unterstützt Kerberos für Domänen-Passthrough-Authentifizierung in Bereitstellungen mit Smartcardverwendung. Kerberos ist eine der in der **integrierten Windows-Authentifizierung (IWA)** enthaltenen Authentifizierungsmethoden.

Bei Aktivierung handhabt Kerberos die Authentifizierung ohne Kennwörter für die Citrix Workspace-App und verhindert so trojanerartige Angriffe auf Benutzergeräte, die den Zugriff auf Kennwörter zum Ziel haben. Benutzer nutzen eine beliebige Authentifizierungsmethode (z. B. biometrische Authentifizierungsmethoden wie ein Fingerabdrucklesegerät), um sich anzumelden und auf veröffentlichte Ressourcen zuzugreifen.

Sind die Citrix Workspace-App, StoreFront sowie Citrix Virtual Apps and Desktops und Citrix DaaS für die Smartcard-Authentifizierung konfiguriert, geschieht bei der Anmeldung bei der Citrix Workspace-App mit einer Smartcard Folgendes:

1. Die App erfasst die Smartcard-PIN beim Single Sign-On.
2. Die App authentifiziert den Benutzer mit IWA (Kerberos) bei StoreFront. StoreFront stellt der Citrix Workspace-App dann Informationen zum verfügbaren Citrix Virtual Apps and Desktops und Citrix DaaS bereit.

Hinweis

Aktivieren Sie Kerberos, um eine zusätzliche PIN-Eingabeaufforderung zu vermeiden. Wird die Kerberos-Authentifizierung nicht verwendet, führt die Citrix Workspace-App mit den Smartcard-Anmeldeinformationen eine Authentifizierung bei StoreFront durch.

3. Die HDX Engine (zuvor "ICA-Client") übergibt die Smartcard-PIN an den VDA, um den Benutzer an der Citrix Workspace-App-Sitzung anzumelden. Citrix Virtual Apps and Desktops und Citrix DaaS stellen dann die angeforderten Ressourcen bereit.

Zur Verwendung der Kerberos-Authentifizierung mit der Citrix Workspace-App prüfen Sie, ob die Kerberos-Konfiguration folgenden Punkten entspricht.

- Kerberos funktioniert nur zwischen Citrix Workspace-App und Servern, die zu denselben oder vertrauenswürdigen Windows Server-Domänen gehören. Den Servern wird zudem für Delegierungszwecke vertraut. Dies können Sie über das Verwaltungstool für Active Directory-Benutzer und -Computer konfigurieren.
- Kerberos muss sowohl in der Domäne als auch in Citrix Virtual Apps and Desktops und Citrix DaaS aktiviert sein. Um hohe Sicherheitsstandards und die Verwendung von Kerberos zu gewährleisten, deaktivieren Sie in der Domäne alle IWA-Optionen außer Kerberos.
- Die Kerberos-Anmeldung ist nicht verfügbar für Remotedesktopdienste-Verbindungen, die eine Standardauthentifizierung nutzen, stets vorgegebene Anmeldeinformationen verwenden oder immer zur Eingabe des Kennworts auffordern.

Warnung

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

Domänen-Passthrough-Authentifizierung mit Kerberos für die Verwendung mit Smartcards

Lesen Sie zuerst die Informationen im Abschnitt [Sichern der Bereitstellung](#) in der Citrix Virtual Apps and Desktops-Dokumentation, bevor Sie fortfahren.

Wenn Sie die Citrix Workspace-App für Windows installieren, fügen Sie die folgende Befehlszeilenoption hinzu:

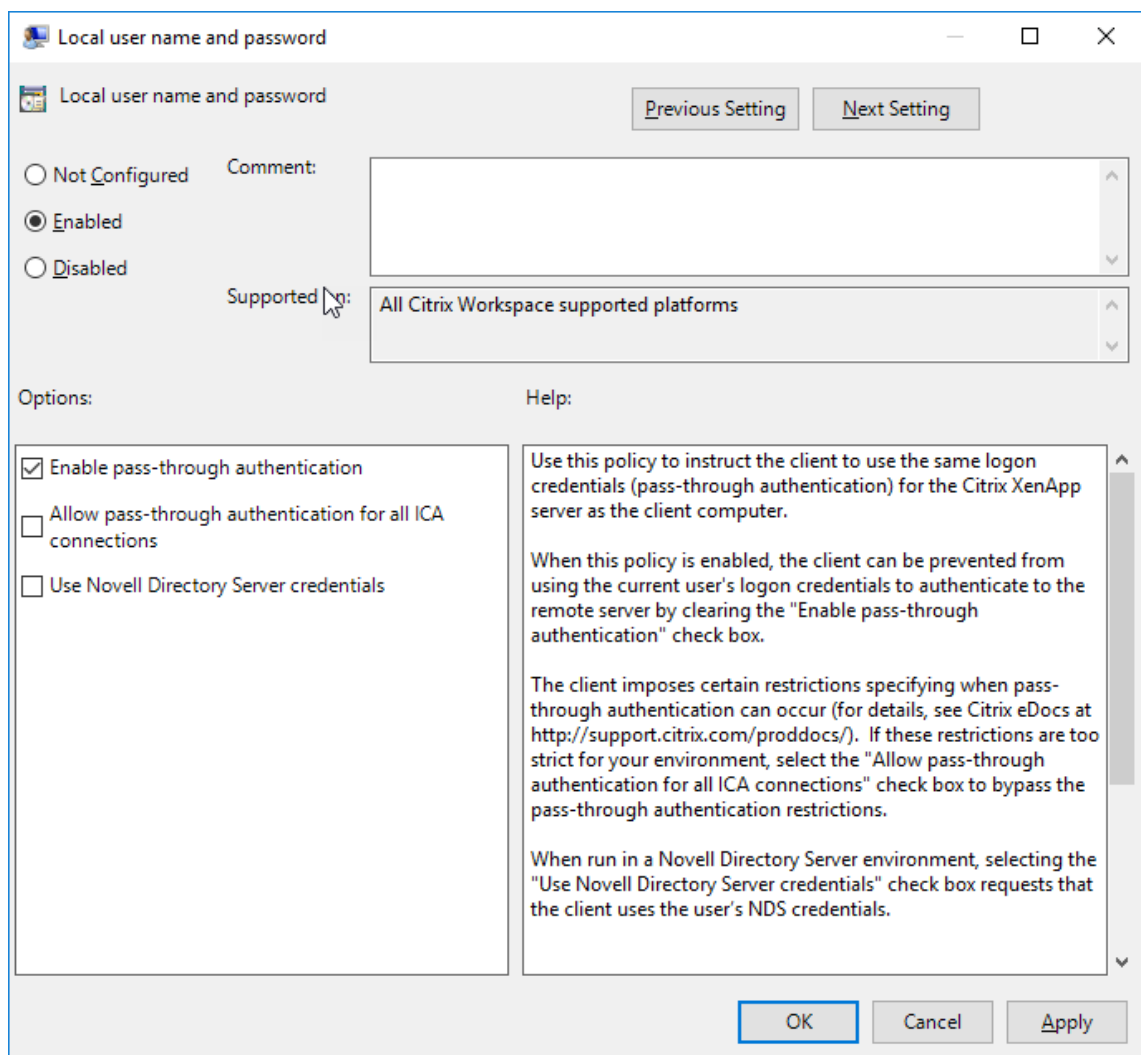
- `/includeSSON`

Mit dieser Option wird die Single Sign-On-Komponente auf dem in die Domäne eingebundenen Computer installiert, sodass der Workspace mit IWA (Kerberos) die Authentifizierung bei StoreFront durchführen kann. Die Single Sign-On-Komponente speichert die Smartcard-PIN, mit der die HDX Engine eine Remoteverbindung zwischen Smartcard-Hardware und -Anmeldeinformationen und Citrix Virtual Apps and Desktops und Citrix DaaS herstellt. Citrix Virtual Apps and Desktops und Citrix DaaS wählen automatisch ein Zertifikat von der Smartcard aus und rufen die PIN von der HDX Engine ab.

Die verwandte Option `ENABLE_SSON` ist standardmäßig aktiviert.

Wenn Sie Single Sign-On aufgrund einer Sicherheitsrichtlinie auf einem Gerät nicht aktivieren können, konfigurieren Sie die Citrix Workspace-App mit der administrativen Gruppenrichtlinienobjektvorlage.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Wählen Sie **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort**.
3. Wählen Sie **Passthrough-Authentifizierung aktivieren**.
4. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.



StoreFront konfigurieren:

Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie die Option Domänen-Passthrough. Mit dieser Einstellung wird die integrierte Windows-Authentifizierung aktiviert. Die Option "Smartcard" muss nur aktiviert werden, wenn Sie auch Clients haben, die nicht in Domänen eingebunden sind und mit Smartcards eine Verbindung mit StoreFront herstellen.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter [Konfigurieren des Authentifizierungsdiensts](#) in der StoreFront-Dokumentation.

Unterstützung für bedingten Zugriff mit Azure Active Directory

Der bedingte Zugriff ist ein Tool, mit dem Azure Active Directory Organisationsrichtlinien durchsetzt. Workspace-Administratoren können Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei der Citrix Workspace-App authentifizieren. Auf

der Windows-Maschine, auf der die Citrix Workspace-App ausgeführt wird, muss Microsoft Edge WebView2 Runtime-Version 92 oder höher installiert sein.

Ausführliche Informationen und Anweisungen zum Konfigurieren von Richtlinien für den bedingten Zugriff mit Azure Active Directory finden Sie in der **Dokumentation zum bedingten Azure AD-Zugriff** unter [Docs.microsoft.com/de-de/azure/active-directory/conditional-access/](https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/).

Hinweis:

Dieses Feature wird nur für Workspace (Cloud)-Bereitstellungen unterstützt.

Weitere Methoden der Authentifizierung bei Citrix Workspace

Sie können die folgenden Authentifizierungsmethoden mit der Citrix Workspace-App konfigurieren. Damit die folgenden Authentifizierungsmethoden wie erwartet funktionieren, muss auf der Windows-Maschine, auf der die Citrix Workspace-App ausgeführt wird, Microsoft Edge WebView2 Runtime-Version 92 oder höher installiert sein.

1. Windows Hello-basierte Authentifizierung: Anweisungen zum Konfigurieren der Windows Hello-basierten Authentifizierung finden Sie im Artikel **Configure Windows Hello for Business Policy settings - Certificate Trust** unter “[Docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings)”.

Hinweis:

Windows Hello-basierte Authentifizierung mit Domänen-Passthrough wird nicht unterstützt.

1. Authentifizierung mit FIDO2-Sicherheitsschlüsseln: FIDO2-Sicherheitsschlüssel ermöglichen Unternehmensmitarbeitern eine nahtlose Authentifizierung ohne Eingabe von Benutzernamen oder Kennwort. Sie können die Authentifizierung mit FIDO2-Sicherheitsschlüsseln für Citrix Workspace konfigurieren. Wenn sich Benutzer bei Citrix Workspace mit ihrem Azure AD-Konto mit einem FIDO2-Sicherheitsschlüssel authentifizieren sollen, lesen Sie den Artikel **Enable passwordless security key sign-in** unter [Docs.microsoft.com/de-de/azure/active-directory/authentication/howto-authentication-passwordless-security-key](https://docs.microsoft.com/de-de/azure/active-directory/authentication/howto-authentication-passwordless-security-key).
2. Sie können Single Sign-On (SSO) für Citrix Workspace-App auch von in Microsoft Azure Active Directory (AAD) eingebundenen Maschinen mit AAD als Identitätsanbieter konfigurieren. Weitere Informationen zum Konfigurieren von Azure Active Directory-Domänendiensten finden Sie im Artikel **Configuring Azure Active Directory Domain services** unter [Docs.microsoft.com/de-de/azure/active-directory-domain-services/overview](https://docs.microsoft.com/de-de/azure/active-directory-domain-services/overview). Weitere Informationen zum Verbinden von Azure Active Directory mit Citrix Cloud finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).

Smartcard

Citrix Workspace-App für Windows unterstützt folgende Smartcardauthentifizierung.

- **Passthrough-Authentifizierung (Single Sign-On):** Die Passthrough-Authentifizierung erfasst die Smartcard-Anmeldeinformationen, wenn Benutzer sich bei der Citrix Workspace-App anmelden. Die Citrix Workspace-App verwendet die erfassten Anmeldeinformationen wie folgt:
 - Benutzer von in Domänen eingebundenen Geräten, die sich mit einer Smartcard bei der Citrix Workspace-App anmelden, können virtuelle Desktops und Anwendungen ohne erneute Authentifizierung starten.
 - Ist die Citrix Workspace-App auf nicht in Domänen eingebundenen Geräten, die die Smartcard-Anmeldeinformationen verwenden, müssen die Benutzer zum Starten eines virtuellen Desktops oder einer virtuellen Anwendung die Anmeldeinformationen erneut eingeben.

StoreFront und die Citrix Workspace-App müssen beide für die Passthrough-Authentifizierung konfiguriert werden.

- **Bimodale Authentifizierung:** Bei der bimodalen Authentifizierung können die Benutzer zwischen einer Smartcard und der Eingabe des Benutzernamens und des Kennworts wählen. Das Feature eignet sich für Fälle, wenn keine Smartcard verwendet werden kann. Beispielsweise wenn das Anmeldezertifikat abgelaufen ist. Für die bimodale Authentifizierung müssen dedizierte Stores pro Site eingerichtet werden, damit die Methode **DisableCtrlAltDel** zur Smartcardverwendung auf **False** festgelegt werden kann. Die bimodale Authentifizierung erfordert eine StoreFront-Konfiguration.

Mit der bimodalen Authentifizierung kann der StoreFront-Administrator die Authentifizierung über Benutzernamen/Kennwort und per Smartcard bei dem gleichen Store durch Auswahl in der StoreFront-Konsole zulassen. Weitere Informationen finden Sie in der [StoreFront-Dokumentation](#).

- **Mehrere Zertifikate:** Mehrere Zertifikate können für eine Smartcard genutzt werden und wenn mehrere Smartcards verwendet werden. Wird eine Smartcard in einen Kartenleser eingeführt, gelten die Zertifikate für alle Anwendungen, die auf dem Gerät ausgeführt werden, einschließlich der Citrix Workspace-App.
- **Clientzertifikatauthentifizierung:** Citrix Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
 - Für den Zugriff auf StoreFront über Citrix Gateway ist nach dem Entfernen der Smartcard eine erneute Authentifizierung erforderlich.
 - Wenn die SSL-Konfiguration von Citrix Gateway auf **Mandatory client certificate authentication** (Verbindliche Clientzertifikatauthentifizierung) festgelegt ist, ist der Betrieb

sicherer. Die verbindliche Clientzertifikatauthentifizierung ist jedoch nicht mit der bimodalen Authentifizierung kompatibel.

- **Double-Hop-Sitzungen:** Wenn ein Double Hop benötigt wird, wird eine Verbindung zwischen Citrix Workspace-App und dem virtuellen Desktop des Benutzers hergestellt.
- **Smartcard-aktivierte Anwendungen:** In smartcard-aktivierten Anwendungen, wie Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in Sitzungen mit virtuellen Apps und Desktops verfügbar sind, digital signieren oder verschlüsseln.

Einschränkungen:

- Zertifikate müssen auf der Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Zertifikatauswahl wird in der Citrix Workspace-App nicht gespeichert, es wird jedoch bei entsprechender Konfiguration die PIN gespeichert. Die PIN wird im nicht ausgelagerten Speicher für die Dauer der Benutzersitzung zwischengespeichert. Sie wird nicht auf der Festplatte gespeichert.
- Die Citrix Workspace-App stellt die Verbindung mit einer Sitzung nicht wieder her, wenn eine Smartcard eingesteckt wird.
- Wenn die Citrix Workspace-App für die Smartcardauthentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung eines VPN mit der Smartcardauthentifizierung installieren Sie das Citrix Gateway Plug-In. Melden Sie sich über eine Webseite an und authentifizieren Sie sich bei jedem Schritt mit den Smartcards und PINs. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Die Kommunikation des Updater-Tools der Citrix Workspace-App mit citrix.com und Merchandising Server ist nicht kompatibel mit der Smartcardauthentifizierung auf Citrix Gateway.

Warnung

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

Single Sign-On für die Smartcardauthentifizierung aktivieren:

Fügen Sie zum Konfigurieren der Citrix Workspace-App für Windows bei der Installation die folgende Befehlszeilenoption hinzu:

- `ENABLE_SSON=Yes`

Single Sign-On ist ein anderer Begriff für Passthrough-Authentifizierung. Wenn diese Einstellung aktiviert ist, zeigt die Citrix Workspace-App keine zweite PIN-Eingabeaufforderung an.

- Navigieren Sie im Registrierungseditor zum folgenden Pfad und legen Sie die Zeichenfolge `SSONCheckEnabled` auf `False` fest, wenn die Single Sign-On-Komponente nicht installiert ist.

```
HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols  
\integratedwindows\
```

```
HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\  
protocols\integratedwindows\
```

Der Schlüssel verhindert, dass der Authentifizierungsmanager der Citrix Workspace-App nach der Single Sign-On-Komponente sucht, sodass die Citrix Workspace-App die Authentifizierung bei StoreFront durchführen kann.

Zum Aktivieren der Smartcardauthentifizierung bei StoreFront anstelle von Kerberos installieren Sie die Citrix Workspace-App für Windows mit folgenden Befehlszeilenoptionen:

- `/includeSSON` installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Aktiviert das Zwischenspeichern der Anmeldeinformationen und die Verwendung der domänenbasierten Passthrough-Authentifizierung.
- Meldet der Benutzer sich beim Endpunkt mit einer anderen Authentifizierungsmethode an (z. B. über Benutzernamen und Kennwort), verwenden Sie folgende Befehlszeile:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Diese Art der Authentifizierung verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden. Gleichzeitig kann die Citrix Workspace-App die PIN bei der Anmeldung an der Citrix Workspace-App speichern.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Wählen Sie **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort**.
3. Wählen Sie **Passthrough-Authentifizierung aktivieren**. Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise die Option **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen** aktivieren, damit die Passthrough-Authentifizierung funktioniert.

StoreFront konfigurieren:

- Wenn Sie den Authentifizierungsdienst konfigurieren, aktivieren Sie das Kontrollkästchen **Smartcard**.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter [Konfigurieren des Authentifizierungsdiensts](#) in der StoreFront-Dokumentation.

Aktivieren der Benutzergeräte für die Smartcardverwendung:

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
2. Installieren Sie die kryptografische Middleware.
3. Installieren und konfigurieren Sie die Citrix Workspace-App.

Ändern der Zertifikatauswahl:

Wenn mehrere Zertifikate gültig sind, fordert die Citrix Workspace-App den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können die Citrix Workspace-App jedoch auch so konfigurieren, dass das Standardzertifikat (gemäß Smartcardanbieter) oder das Zertifikat mit dem spätesten Ablaufdatum verwendet wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden.

Ein gültiges Zertifikat muss die drei folgenden Merkmale haben:

- Die aktuelle Uhrzeit auf dem lokalen Computer liegt im Gültigkeitszeitraum des Zertifikats.
- Der **öffentliche Schlüssel des Subjekts** muss den RSA-Algorithmus verwenden und eine Schlüssellänge von 1024, 2048 oder 4096 Bit haben.
- Die Schlüsselverwendung muss die digitale Signatur enthalten.
- Der alternative Antragstellername muss den Benutzerprinzipalnamen (UPN) enthalten.
- Die erweiterte Schlüsselverwendung muss Smartcard-Anmeldung und Clientauthentifizierung oder alle Schlüsselverwendungen enthalten.
- Eine der Zertifizierungsstellen in der Ausstellerkette des Zertifikats muss mit einem der zulässigen Distinguished Names übereinstimmen, den der Server im TLS-Handshake sendet.

Ändern Sie mit einer der folgenden Methoden, wie Zertifikate ausgewählt werden:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` an.

Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Citrix Workspace für `SmartCardDefault` oder `LatestExpiry` den Benutzer zur Auswahl eines Zertifikats auf.

Fügen Sie dem `SmartCardDefault` `LatestExpiry` }.
Registrierungsschlüssel
`HKEY_CURRENT_USER` OR
`HKEY_LOCAL_MACHINE\`
`Software\[Wow6432Node`
`\Citrix\AuthManager`
den folgenden Schlüsselwert
hinzu:
`CertificateSelectionMode={`
`Prompt`

•

In `HKEY_CURRENT_USER` definierte Werte haben Priorität über Werte in `HKEY_LOCAL_MACHINE`, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

CSP-PIN-Aufforderungen verwenden:

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von der Citrix Workspace-App für Windows und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Die Citrix Workspace-App fordert die Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN an den Smartcard-Kryptografiedienstanbieter. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung zulässt, können Sie in der Citrix Workspace-App konfigurieren, dass die PIN-Eingabe, einschließlich der Aufforderung für eine PIN, von den Komponenten des Kryptografiedienstanbieters verwaltet wird.

Ändern Sie mit einer der folgenden Methoden, wie die PIN-Eingabe gehandhabt wird:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM_SMARTCARDPINENTRY=CSP` an.
- Fügen Sie dem Registrierungsschlüssel `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager` den folgenden Schlüsselwert hinzu: `SmartCardPINEntry=CSP`.

Änderungen bei der Unterstützung und Entfernung von Smartcards

Eine Citrix Virtual Apps-Sitzung wird abgemeldet, wenn Sie die Smartcard entfernen. Wenn Smartcard als Authentifizierungsmethode für die Citrix Workspace-App konfiguriert ist, müssen Sie die entsprechende Richtlinie in der Citrix Workspace-App für Windows konfigurieren, damit das Abmelden der Citrix Virtual Apps-Sitzung erzwungen werden kann. Der Benutzer bleibt an der Citrix Workspace-App-Sitzung angemeldet.

Einschränkung:

Wenn Sie sich an der Citrix Workspace-App per Smartcardauthentifizierung anmelden, wird der Benutzername als **Angemeldet** angezeigt.

Schnelle-Smartcard-Feature Das Schnelle-Smartcard-Feature ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden.

Schnelle Smartcards werden nur unter Windows VDA unterstützt.

Aktivieren der schnellen Smartcardanmeldung in der Citrix Workspace-App:

Die schnelle Smartcardanmeldung ist standardmäßig auf dem VDA aktiviert und in der Citrix Workspace-App standardmäßig deaktiviert. Um die schnelle Smartcardanmeldung zu aktivieren, fügen Sie den folgenden Parameter in die Datei `default.ica` der zugeordneten StoreFront-Site ein:

```
1 copy[WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

Deaktivieren der schnellen Smartcardanmeldung in der Citrix Workspace-App:

Um die schnelle Smartcardanmeldung in der Citrix Workspace-App zu deaktivieren, entfernen Sie den Parameter `SmartCardCryptographicRedirection` aus der Datei `default.ica` der zugeordneten StoreFront-Site.

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

Automatische Authentifizierung für Citrix Workspace

Die Citrix Workspace-App führt eine Richtlinie für ein Gruppenrichtlinienobjekt (GPO) ein, um die automatische Authentifizierung für Citrix Workspace zu aktivieren. Diese Richtlinie ermöglicht es der Citrix Workspace-App, sich beim Systemstart automatisch bei Citrix Workspace anzumelden. Verwenden Sie diese Richtlinie nur, wenn Domänen-Passthrough (Single Sign-On) für Citrix Workspace auf in Domänen eingebundenen Geräten konfiguriert ist.

Damit diese Richtlinie funktioniert, müssen die folgenden Kriterien erfüllt sein:

- Single Sign-On muss aktiviert sein.
- Der Schlüssel `SelfServiceMode` muss im Registrierungseditor auf `Off` festgelegt sein.

Aktivieren der automatischen Authentifizierung:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Self-Service**.
3. Klicken Sie auf die Richtlinie **Automatische Authentifizierung für Citrix Workspace** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Anwenden** und auf **OK**.

Sichere Kommunikation

April 22, 2024

Zum Sichern der Kommunikation zwischen dem Citrix Virtual Apps and Desktops-Server und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen mit verschiedenen sicheren Technologien wie den Folgenden integrieren:

- Citrix Gateway: Weitere Informationen finden Sie im vorliegenden Abschnitt und in der Dokumentation zu Citrix Gateway und StoreFront.
- Eine Firewall: Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden.
- Transport Layer Security (TLS) Versionen 1.0 bis 1.2 werden unterstützt.
- Vertrauenswürdige Server zum Herstellen von Vertrauensbeziehungen in Citrix Workspace-App-Verbindungen.
- ICA-Dateisignierung
- Schutz durch lokale Sicherheitsautorität
- Proxyserver nur für Citrix Virtual Apps-Bereitstellungen: Ein SOCKS-Proxyserver oder ein sicherer Proxyserver. Proxyserver helfen, den Zugriff auf und vom Netzwerk zu beschränken. Sie verarbeiten außerdem die Verbindungen zwischen der Citrix Workspace-App und dem Server. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.
- Ausgehender Proxy

Citrix Gateway

Citrix Gateway (ehemals Access Gateway) sichert Verbindungen mit StoreFront-Stores. Administratoren können hiermit zudem präzise den Benutzerzugriff auf Desktops und Anwendungen steuern.

Herstellen einer Verbindung mit Desktops und Anwendungen über Citrix Gateway:

1. Nutzen Sie eine der folgenden Methoden, um die vom Administrator erhaltene Citrix Gateway-URL einzugeben:

- Bei der ersten Verwendung der Self-Service-Benutzeroberfläche werden Sie aufgefordert, die URL im Dialogfeld **Konto hinzufügen** einzugeben.
- Wenn Sie die Self-Service-Benutzeroberfläche später verwenden, geben Sie die URL ein, indem Sie auf **Einstellungen > Konten > Hinzufügen** klicken.
- Beim Herstellen einer Verbindung mit dem Befehl “storebrowse” geben Sie die URL in der Befehlszeile ein.

Über die URL wird das Gateway und optional ein bestimmter Store angegeben:

- Zum Herstellen einer Verbindung mit dem ersten Store, den die Citrix Workspace-App findet, verwenden Sie eine URL im folgenden Format:
 - <https://gateway.company.com>
 - Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im folgenden Format: <https://gateway.company.com?<storename>>. Diese dynamische URL besitzt kein standardmäßiges Format, verwenden Sie kein Gleichheitszeichen (=) in der URL. Beim Herstellen einer Verbindung mit einem bestimmten Store mit storebrowse müssen Sie die URL im storebrowse-Befehl eventuell in Anführungszeichen setzen.
1. Wenn Sie dazu aufgefordert werden, stellen Sie eine Verbindung mit dem Store (über das Gateway) unter Verwendung Ihres Benutzernamens, Kennworts und Sicherheitstokens her. Weitere Informationen zu diesem Schritt finden Sie in der Citrix Gateway-Dokumentation.

Wenn die Authentifizierung abgeschlossen ist, werden Ihre Desktops und Anwendungen angezeigt.

Herstellen einer Verbindung durch eine Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall verwenden, kann die Citrix Workspace-App für Windows über die Firewall mit dem Webserver und dem Citrix Server kommunizieren.

Allgemeine Citrix Kommunikationsports

Quelle	Typ	Port	Details
Citrix Workspace-App	TCP	80/443	Kommunikation mit StoreFront
ICA oder HDX	TCP/UDP	1494	Zugriff auf Anwendungen und virtuelle Desktops

Quelle	Typ	Port	Details
ICA oder HDX mit Sitzungszuverlässigkeit	TCP/UDP	2598	Zugriff auf Anwendungen und virtuelle Desktops
ICA oder HDX über TLS	TCP/UDP	443	Zugriff auf Anwendungen und virtuelle Desktops

Weitere Informationen zu den Ports finden Sie im Knowledge Center-Artikel [CTX101810](#).

TLS (Transport Layer Security)

Transport Layer Security (TLS) ersetzt das SSL-Protokoll (Secure Sockets Layer). Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von TLS als offenem Standard übernahm.

TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie FIPS 140. FIPS 140 ist ein Standard für die Kryptografie.

Um die TLS-Verschlüsselung als Kommunikationsmedium zu verwenden, müssen Sie das Benutzergerät und die Citrix Workspace-App konfigurieren. Weitere Informationen zum Sichern der StoreFront-Kommunikation finden Sie unter [Sicherheit](#) in der StoreFront-Dokumentation. Informationen zum Sichern des VDA finden Sie unter [Transport Layer Security \(TLS\)](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Sie können die folgenden Richtlinien zu folgenden Zwecken verwenden:

- Erzwingen der Verwendung von TLS: Es wird empfohlen, TLS für Verbindungen über nicht vertrauenswürdige Netzwerke zu verwenden, einschließlich des Internets.
- Erzwingen der Verwendung von FIPS (Federal Information Processing Standards): genehmigte Kryptografie gemäß den Empfehlungen im Dokument NIST SP 800-52. Diese Optionen sind standardmäßig deaktiviert.
- Erzwingen der Verwendung einer bestimmten Version von TLS und bestimmter TLS-Verschlüsselungssammlungen: Citrix unterstützt die Protokolle TLS 1.0, TLS 1.1 und TLS 1.2.
- Herstellen von Verbindungen mit bestimmten Servern.
- Überprüfen, ob das Serverzertifikat widerrufen wurde.

- Überprüfen auf eine bestimmte Serverzertifikatsausstellungsrichtlinie.
- Auswählen eines bestimmten Clientzertifikats, wenn der Server für die Anforderung konfiguriert ist.

Die Citrix Workspace-App für Windows unterstützt die folgenden Verschlüsselungssammlungen für das TLS 1.2-Protokoll:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Informationen zu den unterstützten Verschlüsselungssammlungen finden Sie im Knowledge Center-Artikel [CTX250104](#).

Wichtig:

Die folgenden Verschlüsselungssammlungen sind aus Sicherheitsgründen veraltet:

- Verschlüsselungssammlungen RC4 und 3DES
- Verschlüsselungssammlungen mit dem Präfix "TLS_RSA_**"
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Unterstützung für TLS

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Netzwerkrouting**. Wählen Sie dann die Richtlinie **Konfiguration von TLS und Konformitätsmodus**.

TLS and Compliance Mode Configuration

Previous Setting Next Setting

Not Configured Comment:
 Enabled
 Disabled

Supported on: All Citrix Workspace supported platforms

Options:

Require TLS for all connections

Security Compliance Mode: FIPS

Allowed TLS servers:

TLS version: TLS1.0 | TLS1.1 | TLS1.2

TLS cipher set: Commercial

Certificate Revocation Check Policy: Check with no network access

Policy Extension OID:

Client Authentication: Not Configured

Client Certificate:

Help:

This option enables Citrix Workspace to identify secure connections and encrypt communication within the server.

Following are the type of TLS secure connection between Citrix Workspace and XenApp and XenDesktop that Citrix supports:

1. TLS 1.0
2. TLS 1.1
3. TLS 1.2

The Security Compliance Mode values are:

- FIPS - Enabling FIPS mode forces Windows operating system and its sub-systems to use only FIPS-validated cryptographic algorithms.
- None - No compliance mode is enforced.
- SP800-52 - NIST SP800-52r1 compliance is enforced. When you select SP800-52 from the Security Compliance Mode drop down, the following Certificate Revocation Check Policy (CRCP) is allowed:
 - Full Access Check And CRL Required. This is the default option.
 - Full Access Check And CRL Required All

OK Cancel Apply

3. Wählen Sie **Aktiviert**, um sichere Verbindungen zu aktivieren und die Kommunikation auf dem Server zu verschlüsseln. Legen Sie folgende Optionen fest:

Hinweis:

Citrix empfiehlt TLS für sichere Verbindungen.

- aktivieren Sie **TLS für alle Verbindungen verwenden**. Damit erzwingen Sie, dass die Citrix Workspace-App TLS für alle Verbindungen mit veröffentlichten Anwendungen und Desktops verwendet.
- Wählen Sie im Menü **Sicherheitskonformitätsmodus** die geeignete Option aus:

 - Ohne:** Es wird kein Konformitätsmodus erzwungen.
 - SP800-52:** Wählen Sie **SP800-52** für Konformität mit NIST SP 800-52. Wählen Sie diese Option nur, wenn Server oder Gateway gemäß den Empfehlungen in NIST SP 800-52 konfiguriert sind.

Hinweis:

Bei Auswahl von **SP800-52** wird automatisch FIPS-validierte Kryptografie verwendet, selbst wenn **FIPS aktivieren** nicht ausgewählt ist. Aktivieren Sie auch die Windows-Sicherheitsoption **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu den veröffentlichten Anwendungen und Desktops herstellen.

Wenn Sie **SP800-52** auswählen, legen Sie die Einstellung für **Richtlinie ‘Zertifikatsprüfung’** auf **Volle Zugriffsprüfung und CRL erforderlich** fest.

Wenn Sie **SP800-52** auswählen, überprüft die Citrix Workspace-App, ob das Serverzertifikat den Empfehlungen in NIST SP 800-52 entspricht. Wenn dies nicht der Fall ist, kann die Citrix Workspace-App möglicherweise keine Verbindung herstellen.

- i. **FIPS aktivieren:** Wählen Sie diese Option, um die Verwendung von FIPS-validierter Kryptografie zu erzwingen. Aktivieren Sie auch die Windows-Sicherheitsoption aus der Gruppenrichtlinie des Betriebssystems **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu veröffentlichten Anwendungen und Desktops herstellen.
- c) Wählen Sie im Dropdownmenü neben **Zulässige TLS-Server** die Portnummer aus. Verwenden Sie eine durch Trennzeichen getrennte Liste, um sicherzustellen, dass die Citrix Workspace-App Verbindungen nur zu angegebenen Servern herstellt. Sie können Platzhalter und Portnummern angeben. Beispielsweise ermöglicht *.citrix.com: 4433 die Verbindung mit allen Servern auf Port 4433, deren allgemeiner Name mit .citrix.com endet. Die Genauigkeit der Informationen in einem Sicherheitszertifikat wird durch den Aussteller des Zertifikats bestätigt. Wenn Citrix Workspace den Aussteller nicht erkennt oder ihm nicht traut, wird die Verbindung abgelehnt.
- d) Wählen Sie im Menü **TLS-Version** eine der folgenden Optionen:
 - **TLS 1.0, TLS 1.1 oder TLS 1.2:** Dies ist die Standardeinstellung. Diese Option wird nur empfohlen, wenn die Kompatibilität mit TLS 1.0 eine Geschäftsanforderung ist.
 - **TLS 1.1, TLS 1.2:** Mit dieser Option stellen Sie sicher, dass TLS 1.1 oder TLS 1.2 für Verbindungen verwendet wird.
 - **TLS 1.2:** Diese Option wird empfohlen, wenn TLS 1.2 eine Geschäftsanforderung ist.
- a) **TLS-Verschlüsselungssatz:** Um die Verwendung von bestimmten TLS-Verschlüsselungssätzen zu erzwingen, wählen Sie “Behörden”(GOV), “Kommerziell”(COM) oder “Alle”(ALL). Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX250104](#).

- b) Wählen Sie im Menü **Richtlinie ‘Zertifikatssperrüberprüfung’** eine der folgenden Optionen aus:
- **Prüfung ohne Netzwerkzugriff:** Es wird eine Überprüfung der Zertifikatssperrliste durchgeführt. Es werden nur lokale Zertifikatssperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Eine Überprüfung der Zertifikatssperrliste zum Verifizieren des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Citrix Secure Web Gateway-Server bereitgestellt ist, ist nicht obligatorisch.
 - **Volle Zugriffsprüfung:** Es wird eine Überprüfung der Zertifikatssperrliste durchgeführt. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Eine Überprüfung der Zertifikatssperrliste zum Verifizieren des Serverzertifikats, das vom Zielservers bereitgestellt wird, ist nicht kritisch.
 - **Volle Zugriffsprüfung und CRL erforderlich:** Die Zertifikatssperrliste wird ohne Stamm-Zertifizierungsstelle überprüft. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatssperrlisten ist für die Überprüfung wichtig.
 - **Volle Zugriffsprüfung und alle CRL erforderlich:** Die Zertifikatssperrliste und die Stamm-Zertifizierungsstelle werden überprüft. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatssperrlisten ist für die Überprüfung wichtig.
 - **Keine Prüfung:** Es wird keine Überprüfung der Zertifikatssperrliste durchgeführt.
- a) Mit der **Richtlinienerweiterungs-OID** können Sie die Citrix Workspace-App auf Verbindungen mit Servern beschränken, auf denen eine bestimmte Zertifikatausstellungsrichtlinie festgelegt ist. Wenn Sie **Richtlinienerweiterungs-OID** auswählen, akzeptiert die Citrix Workspace-App nur Serverzertifikate mit dieser Richtlinienerweiterungs-OID.
- b) Wählen Sie im Menü zur **Clientauthentifizierung** eine der folgenden Optionen aus:
- **Deaktiviert:** Die Clientauthentifizierung ist deaktiviert.
 - **Zertifikatauswähler anzeigen:** Der Benutzer wird immer aufgefordert, ein Zertifikat auszuwählen.
 - **Wenn möglich automatisch auswählen:** Die Aufforderung wird nur angezeigt, wenn mehrere Zertifikate zur Identifizierung ausgewählt werden können.
 - **Nicht konfiguriert:** Gibt an, dass die Clientauthentifizierung nicht konfiguriert ist.

- **Angegebenes Zertifikat verwenden:** Verwenden Sie das unter “Clientzertifikat” festgelegte Clientzertifikat.
- a) Geben Sie mit der Einstellung **Clientzertifikat** den Fingerabdruck des identifizierenden Zertifikats an, damit Benutzer nicht unnötig aufgefordert werden.
- b) Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

Informationen zur Matrix der internen und externen Netzwerkverbindungen finden Sie im Knowledge Center-Artikel [CTX250104](#).

Vertrauenswürdige Server

Die Konfiguration von vertrauenswürdigen Servern dient dazu, Vertrauensstellungen bei Verbindungen der Citrix Workspace-App zu identifizieren und durchzusetzen.

Wenn Sie die Option für vertrauenswürdige Server aktivieren, legt die Citrix Workspace-App die Anforderungen für vertrauenswürdige Server fest und entscheidet, ob die Verbindung zum Server als vertrauenswürdig angesehen werden kann. Beispiel: Wenn die Citrix Workspace-App eine Verbindung mit einer bestimmten Adresse herstellt (wie https://*.citrix.com) und dabei einen bestimmten Verbindungstyp verwendet (wie TLS), wird sie an eine vertrauenswürdige Zone auf dem Server weitergeleitet.

Wenn Sie dieses Feature aktivieren, befindet sich der verbundene Server in der **Zone vertrauenswürdiger Sites** von Windows. Eine Anleitung, wie Sie Server der **Zone vertrauenswürdiger Sites** von Windows hinzufügen, finden Sie in der Onlinehilfe von Internet Explorer.

Aktivieren der vertrauenswürdigen Serverkonfiguration über die administrative Gruppenrichtlinienobjektvorlage

Voraussetzung:

Beenden Sie alle Citrix Workspace-App-Komponenten, einschließlich Connection Center.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Erweitern Sie den Knoten **Computerkonfiguration** und navigieren Sie zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Netzwerkrouting > Vertrauenswürdige Serverkonfiguration konfigurieren**.
3. Wählen Sie **Aktiviert**, um die Regionsidentifizierung in der Citrix Workspace-App durchzusetzen.
4. Wählen Sie **Vertrauenswürdige Serverkonfiguration erzwingen**. Der Client muss dann die Identifizierung mit einem vertrauenswürdigen Server durchführen.
5. Wählen Sie im Dropdownmenü zu **Windows-Internetzone** die Client-Serveradresse aus. Diese Einstellung gilt nur für die Zone vertrauenswürdiger Sites von Windows.

6. Legen Sie im Feld **Adresse** die Client-Serveradresse für die Zone vertrauenswürdiger Sites außer Windows fest. Sie können eine durch Trennzeichen getrennte Liste verwenden.
7. Klicken Sie auf **OK** und **Übernehmen**.

ICA-Dateisignierung

Die ICA-Dateisignierung schützt vor unautorisierten Anwendungs- oder Desktopstarts. Die Citrix Workspace-App prüft, ob eine vertrauenswürdige Quelle die Anwendung oder den Desktop gestartet hat und verhindert basierend auf administrativen Richtlinien das Starten von Ressourcen auf nicht vertrauenswürdigen Servern. Sie können die ICA-Dateisignierung über die administrative Vorlage für Gruppenrichtlinienobjekte oder StoreFront konfigurieren. Das Feature der ICA-Dateisignierung ist in der Standardeinstellung nicht aktiviert.

Informationen zum Aktivieren der ICA-Dateisignierung für StoreFront finden Sie unter [Aktivieren der ICA-Dateisignierung](#) in der StoreFront-Dokumentation.

Konfigurieren der ICA-Dateisignatur

Hinweis:

Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, ist die **Richtlinie zum Aktivieren der ICA-Dateisignierung** evtl. nicht vorhanden.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten**.
3. Wählen Sie die Richtlinie **ICA-Dateisignierung aktivieren** und dann nach Bedarf eine der folgenden Optionen:
 - a) Aktiviert: gibt an, dass Sie den Fingerabdruck des Signaturzertifikats der Positivliste der vertrauenswürdigen Zertifikatfingerabdrücke hinzufügen können.
 - b) Vertrauenswürdige Zertifikate: Klicken Sie auf **Anzeigen**, um den Fingerabdruck des Signaturzertifikats aus der Positivliste zu entfernen. Sie können die Fingerabdrücke von Signaturzertifikaten von den Eigenschaften des Signaturzertifikats kopieren und einfügen.
 - c) Sicherheitsrichtlinie: Folgende Optionen sind im Menü verfügbar.
 - i. Nur signierte Starts zulassen (sicherer): lässt nur richtig signierte Anwendungs- und Desktopstarts von einem vertrauenswürdigen Server zu. Im Falle einer ungültigen Signatur wird eine Sicherheitswarnung angezeigt. Die Sitzung wird dann wegen fehlender Autorisierung nicht gestartet.

- ii. Benutzer bei nicht signierten Starts auffordern (weniger sicher): Eine Nachricht wird angezeigt, wenn eine nicht signierte oder ungültig signierte Sitzung gestartet wird. Sie können den Start fortsetzen oder abbrechen (Standard).
4. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Auswählen und Verteilen eines digitalen Signaturzertifikats:

Bei der Auswahl eines digitalen Signaturzertifikats empfehlen wir eine Auswahl aus der folgenden Prioritätsliste:

1. Erwerben Sie ein codesigniertes Zertifikat oder ein SSL-Signaturzertifikat einer öffentlichen Zertifizierungsstelle.
2. Wenn Ihr Unternehmen eine private Zertifizierungsstelle hat, erstellen Sie ein codesigniertes oder SSL-Signaturzertifikat mit der privaten Zertifizierungsstelle.
3. Verwenden Sie ein vorhandenes SSL-Zertifikat.
4. Erstellen Sie ein Stammzertifikat der Zertifizierungsstelle und verteilen es mit einem Gruppenrichtlinienobjekt oder einer manuellen Installation auf die Benutzergeräte.

Schutz durch lokale Sicherheitsautorität

Die lokale Sicherheitsautorität von Windows, die Informationen zu allen Aspekten der lokalen Sicherheit auf einem System enthält, wird von der Citrix Workspace-App unterstützt. Diese Unterstützung ermöglicht einen Systemschutz durch die lokale Sicherheitsautorität für gehostete Desktops.

Herstellen von Verbindungen über Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und die Verbindung zwischen der Citrix Workspace-App für Windows und Servern gehandhabt. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Server verwendet die Citrix Workspace-App die Proxyservereinstellungen, die remote auf dem Server konfiguriert sind, auf dem Workspace für Web ausgeführt wird.

Bei der Kommunikation mit dem Webserver verwendet die Citrix Workspace-App die Einstellungen für den Proxyserver, die über die **Internetoptionen** des Standardwebrowsers auf dem Benutzergerät konfiguriert wurden. Konfigurieren Sie die **Internetoptionen** des Standardwebrowsers auf dem Benutzergerät entsprechend.

Informationen zum Erzwingen von Proxyeinstellungen mit der ICA-Datei in StoreFront finden Sie im Citrix Knowledge Center-Artikel [CTX136516](#).

Unterstützung für den ausgehenden Proxy

SmartControl ermöglicht Administratoren das Konfigurieren und Durchsetzen von Richtlinien, die sich auf die Umgebung auswirken. Beispielsweise können Sie verhindern, dass Benutzer ihren Remotedesktops weitere Laufwerke zuordnen. Sie können diese Granularität mit dem SmartControl-Feature auf dem Citrix Gateway erreichen.

Das Szenario ändert sich jedoch, wenn die Citrix Workspace-App und Citrix Gateway zu separaten Unternehmenskonten gehören. In diesem Fall kann die Clientdomäne das SmartControl-Feature nicht anwenden, da das Gateway in der Domäne fehlt. Sie können den ausgehenden ICA-Proxy verwenden. Mit dem ausgehenden ICA-Proxy können Sie das SmartControl-Feature auch dann verwenden, wenn die Citrix Workspace-App und Citrix Gateway in verschiedenen Organisationen bereitgestellt sind.

Die Citrix Workspace-App unterstützt Sitzungsstarts mit dem NetScaler LAN-Proxy. Verwenden Sie das ausgehende Proxy-Plug-In, um einen einzelnen statischen Proxy zu konfigurieren, oder wählen Sie zur Laufzeit einen Proxyserver aus.

Es gibt folgende Konfigurationsmethoden für ausgehende Proxys:

- **Statischer Proxy:** Der Proxyserver wird durch Angabe eines Proxy-Hostnamen und der Portnummer konfiguriert.
- **Dynamischer Proxy:** Ein einzelner Proxyserver wird mit der Proxy-Plug-In-DLL unter einem oder mehreren Proxyservern ausgewählt.

Sie können den ausgehenden Proxy mit der administrativen Gruppenrichtlinienobjektvorlage oder dem Registrierungs-Editor konfigurieren.

Weitere Informationen zum ausgehenden Proxy finden Sie unter [Unterstützung für den ausgehenden ICA-Proxy](#) in der Citrix Gateway-Dokumentation.

Unterstützung für den ausgehenden Proxy - Konfiguration

Hinweis:

Wenn statische und dynamische Proxys konfiguriert sind, hat die Konfiguration des dynamischen Proxys Vorrang.

Konfigurieren des ausgehenden Proxys mit der administrativen GPO-Vorlage:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Netzwerkrouting**.
3. Wählen Sie eine der folgenden Optionen:

- Statischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy manuell konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den Hostnamen und die Portnummer ein.
- Dynamischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy mit DLL konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den vollständigen Pfad zur DLL-Datei ein. Beispiel: `C:\Workspace\Proxy\ProxyChooser.dll`.

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

Konfigurieren des ausgehenden Proxys mit dem Registrierungs-Editor:

- **Statischer Proxy:**

- Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.

- Erstellen Sie folgende DWORD-Wertschlüssel:

```
"StaticProxyEnabled"=dword:00000001
```

```
"ProxyHost"="testproxy1.testdomain.com"
```

```
"ProxyPort"=dword:000001bb
```

- **Dynamischer Proxy:**

- Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.

- Erstellen Sie folgende DWORD-Wertschlüssel:

```
"DynamicProxyEnabled"=dword:00000001
```

```
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

Storebrowse

June 14, 2023

Storebrowse ist ein Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Es wird zur Authentifizierung aller Operationen innerhalb von StoreFront und mit Citrix Gateway verwendet.

Mit **Storebrowse** können Administratoren folgende Vorgänge automatisieren:

- Hinzufügen von Stores
- Auflisten der veröffentlichten Apps und Desktops eines konfigurierten Stores

- Manuelles Erstellen einer ICA-Datei unter Auswahl von beliebigen virtuellen Apps und Desktops
- Generieren einer ICA-Datei mit der **Storebrowse**-Befehlszeile
- Starten der veröffentlichten Anwendung

Das **Storebrowse**-Hilfsprogramm ist Teil der **Authmanager**-Komponente. Nach abgeschlossener Installation der Citrix Workspace-App ist das **Storebrowse**-Hilfsprogramm im **AuthManager**-Installationsordner.

Um sicherzustellen, dass **Storebrowse** gemeinsam mit der **Authmanager**-Komponente installiert wurde, überprüfen Sie den folgenden Registrierungspfad:

Bei Installation der Citrix Workspace-App durch Administratoren:

Auf 32-Bit-Maschinen [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Insta

Auf 64-Bit-Maschinen [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

Bei Installation der Citrix Workspace-App durch Benutzer (Nicht-Administratoren):

Auf 32-Bit-Maschinen [HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta

Auf 64-Bit-Maschinen [HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\A

Anforderungen

- Citrix Workspace-App Version 1808 für Windows oder höher
- Mindestens 530 MB freier Festplattenspeicher
- 2 GB RAM

Compatibility Matrix

Das **Storebrowse**-Hilfsprogramm ist mit folgenden Betriebssystemen kompatibel:

Betriebssystem

Windows 10 (32-Bit- und 64-Bit-Edition)

Windows 8.1 (32- und 64-Bit-Edition)

Betriebssystem

Windows 7 SP1 (32- und 64-Bit-Edition)

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2, Standard und Datacenter Edition

Windows Server 2012, Standard und Datacenter Edition

Windows Server 2008 R2, 64-Bit-Edition

Windows Server 2008 R2, 64-Bit-Edition

Verbindungen

Das **Storebrowse**-Hilfsprogramm unterstützt folgende Verbindungsarten:

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 11.0 und höher

Hinweis:

In einem HTTP-Store akzeptiert das **Storebrowse**-Hilfsprogramm nicht die Eingabe der Anmeldeinformationen über die Befehlszeile.

Authentifizierungsmethoden

StoreFront-Server StoreFront unterstützt verschiedene Authentifizierungsmethoden für den Zugriff auf Stores, es werden jedoch nicht alle empfohlen. Aus Sicherheitsgründen sind einige Authentifizierungsmethoden standardmäßig deaktiviert, wenn Sie einen Store erstellen.

- **Benutzername und Kennwort:** Geben Sie die Anmeldeinformationen zur Authentifizierung des Zugriffs auf Stores ein. Die explizite Authentifizierung ist standardmäßig aktiviert, wenn Sie den ersten Store erstellen.
- **Domänen-Passthrough:** Nach der Authentifizierung bei den Windows-Computern, die der Domäne angehören, werden Sie automatisch an Stores angemeldet. Um diese Option zu verwenden, aktivieren Sie die Passthrough-Authentifizierung bei der Installation der Citrix Workspace-App. Weitere Informationen zu Domänen-Passthrough finden Sie unter [Konfigurieren von Passthrough-Authentifizierung](#).

- **HTTP-Basic:** Aktivieren Sie die HTTP Basic-Authentifizierung, damit das **Storebrowse**-Hilfsprogramm mit StoreFront-Servern kommunizieren kann. Diese Option ist standardmäßig auf dem StoreFront-Server deaktiviert. Aktivieren Sie die **HTTP Basic-Authentifizierungsmethode**.

Das **Storebrowse**-Hilfsprogramm unterstützt folgende Authentifizierungsmethoden:

- Verwendung des **AuthManager**, der in das **Storebrowse**-Hilfsprogramm integriert ist. Hinweis: Aktivieren Sie die HTTP Basic-Authentifizierungsmethode in StoreFront, während Sie mit **Storebrowse** arbeiten. Dies gilt, wenn der Benutzer die Anmeldeinformationen über die **Storebrowse**-Befehle bereitstellt.
- Externer **Authmanager**, der in die Citrix Workspace-App für Windows integriert werden kann.

Single Sign-On mit Citrix Gateway

Zusätzlich zur neuen Unterstützung für Citrix Gateway können Sie jetzt auch Single Sign-On verwenden. Sie können einen Store hinzufügen und die veröffentlichten Ressourcen auflisten, ohne Ihre Benutzeranmeldeinformationen angeben zu müssen.

Weitere Informationen zur Unterstützung von Single Sign-On mit Citrix Gateway finden Sie unter [Unterstützung von Single Sign-On mit Citrix Gateway](#).

Hinweis:

Dieses Feature wird nur auf in Domänen eingebundenen Maschinen unterstützt, auf denen Citrix Gateway mit Authentifizierung per Single Sign-On konfiguriert ist.

Starten eines veröffentlichten Desktops oder einer veröffentlichten Anwendung

Sie können Ressourcen jetzt direkt aus dem Store starten, ohne eine ICA-Datei verwenden zu müssen.

Verwendung von Befehlen

Der folgende Abschnitt enthält detaillierte Informationen zu den Befehlen, die Sie im **Storebrowse**-Hilfsprogramm verwenden können.

-a, --addstore

Beschreibung:

Fügt einen neuen Store hinzu. Gibt die vollständige URL des Stores zurück. Wenn die Rückgabe fehlschlägt, wird ein Fehler gemeldet.

Hinweis:

Das **Storebrowse**-Hilfsprogramm unterstützt Konfigurationen mit mehreren Stores.

Befehlsbeispiel in StoreFront:

Befehl:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*
```

Beispiel:

```
.\storebrowse.exe -U {Username} -P {Password} -D {Domain} -a https://my.firstexamplestore.net
```

Befehlsbeispiel in Citrix Gateway:

Befehl:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Beispiel:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <  
https://mysecondexample.com>
```

/?

Beschreibung:

Bietet Details zur Verwendung des **Storebrowse**-Hilfsprogramms.

(-l), --liststore

Beschreibung:

Listet die Stores auf, die vom Benutzer hinzugefügt wurden.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -l
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -l
```


(-M 0x2000 -E)

Beschreibung:

Enumeriert die Ressourcen.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.secondexample.net>
```

-q, --quicklaunch

Beschreibung:

Erstellt die ICA-Datei für veröffentlichte Apps und Desktops mit dem **Storebrowse**-Hilfsprogramm. Die `quicklaunch`-Option erfordert die Eingabe einer Start-URL und der Store-URL. Die Start-URL kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Sie können die Start-URL für alle veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Eine typische Start-URL lautet wie folgt:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.secondexamplestore.com>
```

-L, --launch

Beschreibung:

Erstellt die erforderliche ICA-Datei für veröffentlichte Apps und Desktops mit dem **Storebrowse**-Hilfsprogramm. Die Startoption erfordert die Eingabe des Ressourcennamens und der Store-URL. Der Name kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Mit dem folgenden Befehl rufen Sie den Anzeigenamen der veröffentlichten Apps und Desktops ab:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Der in der vorherigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Startoption verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L
"{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L {
Resource_Name } https://my.secondexamplestore.com>
```

-S, --sessionlaunch

Beschreibung:

Mit diesem Befehl können Sie einen Store hinzufügen sowie die veröffentlichten Ressourcen überprüfen und starten. Diese Option übernimmt die folgenden Parameter:

- Benutzername
- Kennwort
- Domäne
- Name der zu startenden Ressource
- Store-URL

Wenn Benutzer keine Anmeldeinformationen angeben, werden sie von **AuthManager** zur Eingabe der Anmeldeinformationen aufgefordert. Anschließend wird die Ressource gestartet.

Sie können den Namen der Ressource von veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Der in der vorherigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Option `-S` verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S "{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery >
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S { Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

-f, --filefolder

Beschreibung:

Generiert die ICA-Datei im benutzerdefinierten Pfad für die veröffentlichten Apps und Desktops.

Die Startoption erfordert die Eingabe eines Ordernamens und des Ressourcennamens sowie der Store-URL. Die Store-URL kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```

-t, --traceauthentication

Beschreibung:

Generiert Protokolle für die [AuthManager](#)-Komponente. Protokolle werden nur erstellt, wenn **Storebrowse** einen integrierten [AuthManager](#) verwendet. Protokolle werden im Verzeichnis `localappdata%\Citrix\Storebrowse\logs` erstellt.

Hinweis:

Diese Option darf nicht der letzte Parameter in der Befehlszeile des Benutzers sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { StoreURL }
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { NSG_URL }
```

-d, --deletestore

Beschreibung:

Löscht den vorhandenen StoreFront- oder Citrix Gateway-Store.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -d https://my.secondexamplestore.com
```

Unterstützung von Single Sign-On mit Citrix Gateway

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und das von dieser Domäne bereitgestellte Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) verwenden. Sie können sich anmelden, ohne sich für jede App oder jeden Desktop neu authentifizieren zu müssen. Wenn Sie einen Store hinzufügen, werden Ihre Anmeldeinformationen zusammen mit den Citrix Virtual Apps and Desktops und Citrix DaaS und den Startmenüeinstellungen an den Citrix Gateway-Server übergeben.

Dieses Feature wird ab Citrix Gateway Version 11 unterstützt.

Voraussetzungen:

Informationen zu den Voraussetzungen für die Konfiguration von Single Sign-On für Citrix Gateway finden Sie unter [Konfigurieren von Domänen-Passthrough-Authentifizierung](#).

Das Single Sign-On-Feature mit Citrix Gateway kann über die administrative Gruppenrichtlinienobjektvorlage aktiviert werden.

1. Öffnen Sie die administrative GPO-Vorlage von Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Single Sign-On für Citrix Gateway**.
3. Verwenden Sie die Umschaltoptionen, um Single Sign-On ein- oder auszuschalten.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

Einschränkungen:

- Zur Eingabe von Anmeldedaten mit dem **Storebrowse**-Hilfsprogramm muss auf dem StoreFront-Server die **HTTP Basic-Authentifizierung** aktiviert sein.
- Wenn Sie mit dem Hilfsprogramm eine Verbindung zum HTTP-Store herstellen, um die veröffentlichten virtuellen Apps und Desktops zu prüfen oder zu starten, wird die Eingabe der Anmeldeinformationen über die Befehlszeilenoption nicht unterstützt. Verwenden Sie als Workaround das externe **AuthManager**-Modul, wenn Sie keine Anmeldeinformationen über die Befehlszeile bereitstellen.
- Das **Storebrowse**-Hilfsprogramm unterstützt derzeit nur ein einzelnes, Store-konfiguriertes Citrix Gateway auf dem StoreFront-Server.
- Die Funktion "Credential Injection" im **Storebrowse**-Hilfsprogramm funktioniert nur, wenn Citrix Gateway mit einstufiger Authentifizierung konfiguriert ist.
- Für die Befehlszeilenoptionen **Username** (-U), **Password** (-P) und **Domain** (-D) im **Storebrowse**-Hilfsprogramm wird die Groß- und Kleinschreibung beachtet und es dürfen nur Großbuchstaben verwendet werden.

Um Single Sign-On für Anwendungen von Drittanbietern zu aktivieren, die ICOSDK verwenden, erstellen Sie die folgende Registrierung:

- Registrierungsschlüssel: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registrierungswert: vollständiger Pfad der Drittanbieteranwendungen
- Registrierungstyp: `reg_multi_sz`

Beispiel:

- Registrierungsschlüssel: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registrierungswert: `C:\temp1\abc.exe;C:\temp2\xyz.exe`
- Registrierungstyp: `reg_multi_sz`

Hinweis:

- Sie können mehrere Anwendungen von Drittanbietern bereitstellen, indem Sie sie durch Semikolons trennen.

Citrix Workspace-App Desktop Lock

January 18, 2024

Sie können Citrix Workspace-App Desktop Lock verwenden, wenn Sie nicht mit dem lokalen Desktop arbeiten müssen. Sie können den Desktop Viewer verwenden (wenn aktiviert), jedoch sind auf der Symbolleiste nur die folgenden Optionen verfügbar:

- Strg+Alt+Entf
- Einstellungen
- Geräte
- Trennen:

Die Citrix Workspace-App für Windows mit Desktop Lock funktioniert auf in Domänen eingebundenen Maschinen mit aktiviertem Single Sign-On und konfigurierbarem Store. PNA-Sites werden nicht unterstützt. Vorherige Versionen von Desktop Lock werden beim Upgrade auf Citrix Receiver für Windows 4.2 oder höher nicht unterstützt.

Installieren Sie die Citrix Workspace-App für Windows mit dem Flag `/includeSSON`. Konfigurieren Sie Single Sign-On und den Store mit der ADM/ADMX-Datei oder über die Befehlszeilenoption. Weitere Informationen finden Sie unter [Installation](#).

Installieren Sie dann Citrix Workspace-App Desktop Lock als Administrator mit dem Installationspaket `CitrixWorkspaceDesktopLock.msi`, das auf der [Citrix Downloadseite](#) verfügbar ist.

Systemanforderungen

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Weitere Informationen finden Sie auf der [Microsoft-Downloadseite](#).
- Unterstützung für Windows 8, Windows 8.1, Windows 10 (einschließlich Anniversary Update) und Windows 11.
- Verbindung mit StoreFront nur über native Protokolle.
- In Domänen eingebundene Endpunkte:
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

Lokaler App-Zugriff

Wichtig!

Das Aktivieren des lokalen App-Zugriffs kann den lokalen Desktopzugriff zulassen, es sei denn, es wurde eine vollständige Sperrung über die Gruppenrichtlinienobjektvorlage oder eine ähnliche Richtlinie angewendet. Weitere Informationen finden Sie unter [Konfigurieren von lokalem App-Zugriff und URL-Umleitung](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Arbeiten mit Citrix Workspace-App Desktop Lock

- Citrix Workspace-App Desktop Lock kann mit den folgenden Features der Citrix Workspace-App verwendet werden:
 - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013-Plug-In und lokaler App-Zugriff.
 - Nur Domänen-, Smartcard- oder zweistufige Authentifizierung.
- Trennen der Citrix Workspace-App Desktop Lock-Sitzung führt zur Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Citrix Workspace-App Desktop Lock ohne die Eigenschaften “Home”, “Restore”, “Maximize” und “Display” optimiert.
- Strg+Alt+Entf ist auf der Desktop Viewer-Symbolleiste verfügbar.
- Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. Eine Ausnahme bildet Windows+L.
- Strg+F1 löst Strg+Alt+Entf aus, wenn Sie die Verbindung oder Desktop Viewer für Desktopverbindungen deaktivieren.

Hinweis:

Wenn Desktop Lock installiert ist und `LiveInDesktopDisconnectOnLock` am Registrierungspfad `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` oder `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` auf **False** festgelegt ist, wird die aktive Sitzung getrennt, wenn der Endpunkt aus dem Ruhezustand oder Standbymodus reaktiviert wird.

Installieren von Citrix Workspace-App Desktop Lock

Mit diesen Schritten installieren Sie die Citrix Workspace-App für Windows so, dass virtuelle Desktops mit Citrix Workspace-App Desktop Lock angezeigt werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter [Smartcard](#).

1. Melden Sie sich mit einem lokalen Administratorkonto an.

2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus:

Beispiel:

```
1 CitrixWorkspaceApp.exe
2     /includeSSON
3 STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
4     discovery;on;Desktop Store"
5 <!--NeedCopy-->
```

Der Befehl ist in der Citrix Workspace-App und im Ordner **Plug-Ins > Windows > Citrix Workspace-App** auf dem Installationsmedium verfügbar. Weitere Informationen zu den Befehlen finden Sie in der Installationsdokumentation zur Citrix Workspace-App unter [Installation](#).

3. Doppelklicken Sie im selben Ordner auf dem Installationsmedium auf [CitrixWorkspaceDesktopLock.msi](#). Der Assistent "Desktop Lock" wird angezeigt. Folgen Sie den Anweisungen.
4. Wenn die Installation abgeschlossen ist, starten Sie das Benutzergerät neu. Wenn Sie Zugriffsrechte für einen Desktop haben und sich als Domänenbenutzer anmelden, wird das neu gestartete Gerät mit Citrix Workspace-App Desktop Lock angezeigt.

Sie können die Verwaltung des Benutzergeräts nach der Installation ermöglichen. Das für die Installation von [CitrixWorkspaceDesktopLock.msi](#) verwendete Konto wird dazu bei der Ersatz-Shell ausgeschlossen. Wenn das Konto später gelöscht wird, können Sie sich nicht bei dem Gerät anmelden und es verwalten.

Verwenden Sie zum Installieren von Citrix Workspace Desktop Lock **ohne Benutzereingriff** folgenden Befehl:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

Konfigurieren von Citrix Workspace-App Desktop Lock

Wenn Sie sich als Nicht-Administrator angemeldet haben, startet Desktop Lock automatisch eine zugewiesene Desktopsitzung.

Verhindern Sie mit Active Directory-Richtlinien, dass Benutzer virtuelle Desktops in den Ruhezustand versetzen.

Verwenden Sie das Administratorkonto zum Konfigurieren von Citrix Workspace-App Desktop Lock, das Sie für die Installation verwendet haben.

- Überprüfen Sie, ob die Dateien receiver.admx (oder receiver.adml) und receiver_usb.admx (.adml) in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter "Computerkonfiguration" bzw. **Benutzerkonfiguration > Administrative Vorlagen > Klassische administrative**

Vorlagen (ADMX) > Citrix Komponenten angezeigt werden). Die ADMX-Dateien sind in %Programme%\Citrix\ICA Client\Configuration\.

- USB-Einstellungen: Wenn ein Benutzer ein USB-Gerät anschließt, erfolgt ein automatisches Remoting des Geräts zum virtuellen Desktop. Es ist kein Benutzereingriff erforderlich. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.
 - Aktivieren Sie die USB-Richtlinienregel.
 - Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten > Generisches USB-Remoting** die Richtlinien “Vorhandene USB-Geräte” und “Neue USB-Geräte”.
- Laufwerkzuordnung: Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten** die Richtlinie “Clientlaufwerkzuordnung”.
- Mikrofon: Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten** die Richtlinie “Clientmikrofon”.

Konfigurieren von Smartcards für die Verwendung mit Windows Desktop Lock

1. Konfigurieren Sie StoreFront.
 - a) Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
 - b) Konfigurieren Sie StoreFront-Sites für HTTPS-Zugriff, erstellen Sie ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde und fügen Sie HTTPS-Bindung zur Standardwebsite hinzu.
 - c) Stellen Sie sicher, dass Passthrough-Authentifizierung mit Smartcard aktiviert ist (standardmäßig aktiviert).
 - d) Aktivieren Sie Kerberos.
 - e) Aktivieren Sie Kerberos und Passthrough-Authentifizierung mit Smartcard.
 - f) Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
 - g) Stellen Sie sicher, dass für die IIS-Standardwebsite kein SSL erforderlich ist, und dass Clientzertifikate ignoriert werden.
2. Verwenden Sie die Gruppenrichtlinien-Verwaltungskonsolle zum Konfigurieren lokaler Computerrichtlinien auf dem Benutzergerät.
 - a) Importieren Sie die Vorlage Receiver.admx aus %Programme%\Citrix\ICA Client\Configuration\.
 - b) Erweitern Sie **Administrative Vorlagen > Klassische administrative Vorlagen (ADMX) > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung**.
 - c) Aktivieren Sie “Smartcardauthentifizierung”.
 - d) Aktivieren Sie “Lokaler Benutzername und Kennwort”.

3. Konfigurieren Sie das Benutzergerät vor der Installation von Citrix Workspace-App Desktop Lock.
 - a) Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu.
 - b) Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu. Fügen Sie die URL im Format "desktop://delivery-group-name" hinzu.
 - c) Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Citrix Workspace-App Desktop Lock auf dem Benutzergerät installiert ist, wird eine konsistente Richtlinie für das Entfernen der Smartcard zwingend angewendet. Wird die Richtlinie für das Entfernen der Smartcard beispielsweise für den Desktop auf "Abmelden erzwingen" festgelegt, muss der Benutzer sich vom Benutzergerät abmelden, unabhängig davon, wie die Richtlinie dort eingestellt ist. Desktop Lock stellt sicher, dass das Benutzergerät sich nicht in einem inkonsistenten Zustand befindet. Dies gilt nur für Benutzergeräte mit Citrix Workspace-App Desktop Lock.

Entfernen von Desktop Lock

Stellen Sie sicher, dass beide der folgenden Komponenten entfernt werden:

1. Melden Sie sich mit demselben lokalen Administratorkonto an, das bei der Installation und Konfiguration von Citrix Workspace-App Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:
 - Entfernen Sie Citrix Workspace-App Desktop Lock.
 - Entfernen Sie die Citrix Workspace-App für Windows.

Weitergeben von Windows-Tastenkombinationen an die Remotesitzung

Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. In diesem Abschnitt finden Sie einige der gebräuchlichsten Tastenkombinationen.

Windows

- Win+D - Minimieren aller Fenster auf dem Desktop.
- Alt+Tab - Wechseln des aktiven Fensters.
- Strg+Alt+Entf - über Strg+F1 und die Desktop Viewer-Symbolleiste.
- Alt+Umschalt+Tab

- Windows+Tab
- Windows+Umschalt+Tab
- Windows+Alle Zeichentasten

Windows 8

- Win+C - Charms öffnen.
- Win+Q - Charm "Suche".
- Win+H - Charm "Teilen".
- Win+K - Charm "Geräte".
- Win+I - Charm "Einstellungen".
- Win+Q - Apps durchsuchen.
- Win+W - Einstellungen durchsuchen.
- Win+F - Dateien durchsuchen.

Windows 8 Apps

- Win+Z - App-Optionen anzeigen.
- Win+, - App links andocken.
- Win+Umschalt+. - App rechts andocken.
- Strg+Tab - Zum App-Verlauf wechseln.
- Alt+F4 - App schließen.

Desktop

- Win+D - Desktop öffnen.
- Win+, - Desktop kurz anzeigen.
- Win+B - Zurück zum Desktop.

Sonstiges

- Win+U - Center für erleichterte Bedienung öffnen.
- Strg+Esc - Startbildschirm.
- Win+Eingabetaste - Windows Sprachausgabe öffnen.
- Win+X - Menü für Systemprogrammeinstellungen öffnen.
- Win+Druck - Bildschirmfoto erstellen und unter "Bilder" speichern.
- Win+Tab - Liste zum Wechseln öffnen.
- Win+T - Vorschau offener Fenster in Taskleiste anzeigen.

Software Development Kit (SDK) und API

October 26, 2023

Certificate Identity Declaration SDK

Mit dem Certificate Identity Declaration (CID) SDK können Entwickler ein Plug-In erstellen. Mit diesem Plug-In kann die Citrix Workspace-App sich mithilfe des auf der Clientmaschine installierten Zertifikats beim StoreFront-Server authentifizieren. CID deklariert die Smartcard-Identität des Benutzers an einem StoreFront-Server, ohne anhand der Smartcard eine Authentifizierung durchzuführen.

Weitere Informationen finden Sie unter [Certificate Identity Declaration SDK for Citrix Workspace app for Windows](#).

Citrix Common Connection Manager SDK

Das Common Connection Manager (CCM) SDK stellt eine Reihe nativer APIs bereit, mit denen Sie programmgesteuert interagieren und grundlegende Vorgänge ausführen können. Das SDK erfordert keinen separaten Download, da es Teil des Installationspakets der Citrix Workspace-App für Windows ist.

Hinweis:

Bei einigen APIs, die mit dem Start in Zusammenhang stehen, muss die ICA-Datei den Startvorgang für Sitzungen mit virtuellen Apps und Desktops initiieren.

Die CCM SDK-Funktionen umfassen Folgende:

- Sitzungsstart
 - Ermöglicht das Starten von Anwendungen und Desktops mit der generierten ICA-Datei.
- Session disconnect
 - Ähnlich wie das Trennen der Verbindung über Connection Center. Die Trennung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Session logoff
 - Ähnlich wie die Abmeldung über Connection Center. Die Abmeldung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Sitzungsinformationen

- Bietet verschiedene Methoden zum Abrufen von Verbindungsinformationen zu den gestarteten Sitzungen. Dazu gehören Desktopsitzung, Anwendungssitzung und invertierte Seamless-Anwendungssitzung.

Weitere Informationen über die Dokumentation zum SDK finden Sie unter [Programmers guide to Citrix CCM SDK](#).

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für weitere virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalapplikationen 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.

Weitere Informationen finden Sie unter [Citrix Virtual Channel SDK for Citrix Workspace app for Windows](#).

Fast Connect 3 Credential Insertion API

Die Fast Connect 3 Credential Insertion API bietet eine Schnittstelle zum Bereitstellen von Benutzeranmeldeinformationen für das Single Sign-On (SSO)-Feature. Dieses Feature ist in der Citrix Workspace-App für Windows Version 4.2 und höher verfügbar. Mit dieser API können Citrix Partner Authentifizierungs- und SSO-Produkte bereitstellen, die StoreFront verwenden, um Benutzer an virtuellen Anwendungen oder Desktops anzumelden und die Verbindungen zu diesen Sitzungen auch wieder zu trennen.

Weitere Informationen finden Sie unter [Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#).

Referenz für ICA-Einstellungen

June 14, 2023

Die Referenzdatei für ICA-Einstellungen enthält Registrierungseinstellungen und Listen der ICA-Dateieinstellungen, mit denen Administratoren das Verhalten der Citrix Workspace-App anpassen können. Sie können die Referenz für ICA-Einstellungen auch zur Problembehandlung bei unerwartetem Verhalten der App verwenden.

[Referenz für ICA-Einstellungen \(PDF-Download\)](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).