Citrix Workspace-App für Linux

Contents

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Info zu diesem Release

September 12, 2023

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

> **Hinweis:**
>
> Suchen Sie nach Technical Previews? Wir führen eine Liste von Features unter Technical Preview, sodass Sie sie an einem Ort finden können. Erkunden Sie die Technical Preview-Features und teilen Sie uns Ihr Feedback mit dem Podio-Formular mit.

Was ist neu in 2308

HTTPS-Protokollunterstützung für Proxyserver

Bisher konnten Sie nur mithilfe des SOCKS-Protokolls eine Verbindung zu einem Proxyserver herstellen. Ab Version 2308 der Citrix Workspace-App für Linux können Sie auch über das HTTPS-Protokoll eine Verbindung zu einem Proxyserver herstellen.

Weitere Informationen zum Öffnen eines Desktops mithilfe eines HTTPS-Protokolls finden Sie unter HTTPS-Protokollunterstützung für Proxyserver.

Unterstützung für MJPEG-Webcams

Mit diesem Release werden MJPEG-Webcams im H264-Stream unterstützt. Eine interne MJEPG-Komprimierung in der Webcam verbessert die Bildqualität und erhöht die Bildrate. Dieses Feature ist standardmäßig aktiviert. Wenn die Webcam jedoch MJPEG nicht unterstützt, ist diese Funktion deaktiviert.

Unterstützte Systemzertifikatpfade für SSL-Verbindungen

Mit diesem Release unterstützt die Citrix Workspace-App Systemzertifikatpfade für SSL-Verbindungen. Dieses Feature vereinfacht die clientseitige Zertifikatsverwaltung und verbessert die Benutzererfahrung. Mit diesem Feature kann Citrix Workspace eine TLS-Verbindung mit dem Zertifikat im Systemzertifikatpfad herstellen. Dieses Feature ist standardmäßig aktiviert.

Verbessertes Virtual Channel SDK

Das Virtual Channel SDK für die Citrix Workspace-App für Linux wurde um neue APIs für E/A-Funktionen und Fensterpositionierung erweitert. Weitere Informationen:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Clientseitiger Mediaplayer (CSMP)
- Featureflag-Funktionen für virtuelle Treiber
- Viewport-Funktionen für virtuelle Treiber
- Programmierreferenz

Unterstützung von Tastenkombination zum Umschalten zwischen Vollbild- und Fenstermodus

Bisher konnten Sie im Desktop Viewer die Schaltfläche **Fenster** oder **Vollbild** verwenden, um zwischen **Vollbildmodus** und **Fenstermodus** zu wechseln.

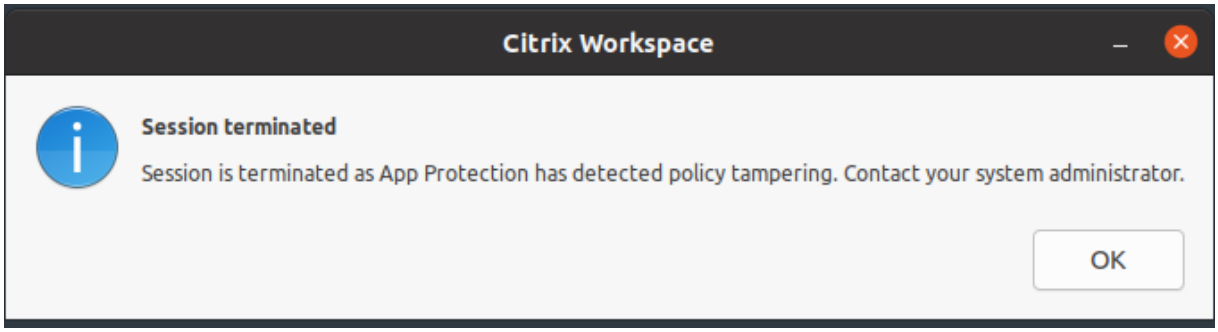
Ab diesem Release können Sie mit der Tastenkombination Strg+F2 zwischen **Vollbildmodus** und **Fenstermodus** wechseln. Wenn sich die Desktopsitzung beispielsweise im **Vollbildmodus** befindet und Sie Strg+F2 drücken, wird der **Vollbildmodus** der Desktopsitzung beendet.

Das Feature ist in der Standardeinstellung deaktiviert.

Weitere Informationen finden Sie unter Unterstützung von Tastenkombination zum Umschalten zwischen Vollbild- und Fenstermodus.

Erkennung von Richtlinienmanipulationen

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



Weitere Informationen zur Erkennung von Richtlinienmanipulationen finden Sie unter Erkennung von Richtlinienmanipulationen.

Technical Previews

- Unterstützung für Webcamumleitung und Servicekontinuität für ARM64-Geräte
- Maskierung von Datenpaketverlust zur Verbesserung der Audioleistung aktivieren
- Unterstützung für MultiTouch

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Behobene Probleme in 2308

- In einem Double-Hop-Szenario werden Sie möglicherweise von Anwendungen getrennt, die USB-Geräte wie das Topaz USB-Unterschriftenfeld verwenden. Das Problem tritt auf, wenn die generische USB-Umleitungsfunktion in beiden Hops verwendet wird. [CVADHELP-23053]
- Nach dem Upgrade der Citrix Workspace-App für Linux auf 2206 oder höher können Sie sich möglicherweise nicht bei der Citrix Workspace-App anmelden. Das Problem tritt nur im Freigabemodus auf, wenn Sie sich erneut anmelden. [CVADHELP-22775]
- Bei aktivierter Browserinhaltsumleitung (BCR) kann es auf Thin Clients zu Speicherplatzproblemen kommen. Das Problem tritt auf, weil der lokale Cache der umgeleiteten Webseite lokal gespeichert wird. [CVADHELP-21764]
- Es kann vorkommen, dass falsche HDMI-Audiogeräte in der Sitzung erkannt wurden. [CVADHELP-18849]
- Bei der Installation des 64-Bit-RPM-Pakets der Citrix Workspace-App für Linux werden Sie möglicherweise aufgefordert, ein Bibliothekspaket zu installieren, das für 32-Bit erforderlich ist. [CVADHELP-23347]
- Beim Zugriff auf umgeleitete Browserinhalte der YouTube-Website im Vollbildmodus können Sie möglicherweise keinen Text in das Suchfeld eingeben. Das Problem tritt bei der Citrix Workspace-App für Linux 2106 oder höher auf. [CVADHELP-20339]
- Wenn Sie mit dem Storebrowse-Befehl `-E` oder `-S` eine Verbindung zu einem PNA-Store herstellen, müssen Sie sich möglicherweise zweimal authentifizieren. Das Problem tritt bei der Citrix Workspace-App für Linux 2205 oder höher auf. [CVADHELP-22917]
- Bei Verwendung der Tastenkombination „Strg + Alt + Eingabe“ reagiert die Tastatur möglicherweise nicht mehr, wenn Sie die Eingabetaste drücken. Das Problem tritt nur in Linux VDA-Desktopsitzungen auf, die über die Citrix Workspace-App für Linux gestartet wurden. [CVADHELP-22930]
- Der weiße Cursor wird auf einem dunkelblauen oder schwarzen Hintergrund nicht deutlich angezeigt. Das Problem tritt in der Citrix Workspace-App für Linux Version 2307 auf. [HDX-52458]
- Sie können Sitzungen möglicherweise nicht auf beiden Monitoren im **Vollbildmodus** verwenden, wenn der sekundäre Bildschirm nach dem Sitzungsstart angeschlossen wurde. [HDX-52816]
- Sie können ein USB-Speichergerät in einer Double-Hop-Sitzung möglicherweise nicht zu einer App oder einem Desktop umleiten. [HDX-52155]
- Für mit der Browserinhaltsumleitung in Chrome umgeleitete Inhalte wird möglicherweise eine leere Seite angezeigt. Das Problem tritt auf, wenn Sie mit der Citrix Workspace-App für Linux 2305 auf eine zulässige Site zugreifen. [HDX-50561]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Bekannte Probleme in 2308

- Wenn Sie eine mit der Browserinhaltsumleitung umgeleitete Website besuchen und sich anschließend von der Benutzersitzung abmelden, kann eine Fehlermeldung angezeigt werden. Ignorieren Sie die Fehlermeldung als Workaround. [HDX-55087]

> **Hinweis:**
>
> Eine vollständige Liste der Probleme in früheren Versionen finden Sie unter Bekannte Probleme.

Frühere Releases

Dieser Abschnitt enthält Informationen zu den neuen Features und den behobenen Problemen in den vorherigen Versionen, die wir gemäß der Produktlebenszyklusmeilensteine für Citrix Workspace-App unterstützen.

2307

Was ist neu

Skript zur Überprüfung der Systemanforderungen für die Windows Media Player-Umleitung

Mit diesem Release wird ein neues Bash-Skript eingeführt, um die Konfiguration zu überprüfen, die für die Windows Media Player-Umleitungsfunktion in der Citrix Workspace-App für Linux erforderlich ist. Damit können Sie die Problembehandlung bei der Windows Media Player-Umleitungsfunktion beschleunigen. Zur Überprüfung der Konfiguration können Sie dieselbe Datei rave_troubleshooting.sh verwenden, die im Systemdiagnoseskript für RAVE verfügbar ist.

Unterstützung für die Wiedergabe kurzer Töne in optimiertem Microsoft Teams hinzugefügt

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

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

Voraussetzungen:

Installieren Sie die neueste Version von Microsoft Teams.

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfüg-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

Technical Previews

- HTTPS-Protokollunterstützung für Proxyserver
- Unterstützung für IPv6 UDT mit DTLS
- Unterstützung für App Protection auf ARM64-Geräten

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Möglicherweise können Sie in der Citrix Workspace-App Version 2303 keine Sitzung starten, wenn der Wert `AllowMultistream` unter Ubuntu 22.04 auf "True" gesetzt ist. [HDX-49916]
- Die DNS-Abfrage für die CAS-Datenerfassung kann bei einem direkten ICA-Start und bei für CAS deaktivierte Speicher auftreten. [CVADHELP-20018], [CVADHELP-12344]
- Wenn Sie Avaya WorkPlace öffnen, verbleibt ein schwarzer Rahmen auf dem Bildschirm der virtuellen Apps oder Desktops. [CVADHELP-21558]
- Wenn Sie Tools wie das Snipping-Tool verwenden, erscheint auf virtuellen Apps und Desktops möglicherweise ein Schatten des Cursors. [CVADHELP-22336]

2305

Was ist neu

Verbesserung zur Unterstützung der Tastaturlayoutsynchronisierung für GNOME 42

Ab diesem Release unterstützt die Citrix Workspace-App für Linux die Synchronisierung des Tastaturlayouts für Desktops wie Ubuntu 22.04, das die Desktopumgebung GNOME 42 und höher verwendet.

Weitere Informationen finden Sie unter Tastaturlayoutsynchronisierung.

Client-IME für ostasiatische Sprachen

Der Client-Eingabemethoden-Editor (Input Method Editor, IME) verbessert die Eingabe und Anzeige von chinesischen, japanischen und koreanischen (CJK) Schriftzeichen in der Citrix Workspace-App für Linux. In folgenden Fällen können Sie wahlweise den Client-IME verwenden:

- Sie haben einen bevorzugten IME im Linux-Client, oder
- der IME ist auf dem Remoteserver nicht verfügbar.

Weitere Informationen finden Sie unter Client-IME für ostasiatische Sprachen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Hinzufügen eines clientseitigen Jitter-Puffermechanismus

Dieses Feature sorgt für gute Audioqualität auch bei schwankender Netzwerklatenz. Standardmäßig ist dieses Feature aktiviert.
Um das Feature zu deaktivieren, navigieren Sie zur Konfigurationsdatei `/opt/Citrix/ICAClient/config/module.ini` und bearbeiten `JitterBufferEnabled=FALSE`.

Webcamumleitung für 64-Bit

Ab diesem Release wird die Webcamumleitung für 64-Bit-Anwendungen unterstützt. Weitere Informationen finden Sie unter Webcams.

Unterstützung für mehr als 200 Gruppen in Azure AD

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

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

Unterstützung für App-Schutz in Ubuntu 22.04

Ab Version 2305 der Citrix Workspace-App für Linux können Sie geschützte virtuelle Apps und Desktops über die Citrix Workspace-App unter Ubuntu 22.04 starten.

Verbesserter Energiesparmodus für optimierte Microsoft Teams-Anrufe

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

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

Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines Microsoft Teams-Updates verfügbar. Informationen zum voraussichtlichen Releasedatum finden Sie durch Suchen nach "Microsoft 365 roadmap" auf . Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

Technical Previews

- Dateien und Ordner zwischen zwei virtuellen Desktops kopieren und einfügen
- Unterstützung für die ARM64-Architektur
- Unterstützung für IPv6 TCP mit TLS
- Verbesserte Unterstützung für 32-Bit-Cursor
- Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit On-Premises-Stores
- Unterstützte Hardwarebeschleunigung für optimiertes Microsoft Teams

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Audioaufzeichnungen werden möglicherweise zu schnell abgespielt, wenn die Aufzeichnungs-App die Windows-API MME (Multimedia Extension) von Microsoft verwendet. Wenn Sie beispielsweise 20 Sekunden lang Audio aufnehmen, dauert die Wiedergabe unter Umständen nur 15 Sekunden. [CVADHELP-22162]
- Die Größe der Datei `.NSAP_Data` im Ordner `.ICAClient` kann die maximale Größe überschreiten und damit den Betrieb des Thin Clients beeinträchtigen. Dieses Problem tritt auf, wenn HDX Insight auf NetScaler aktiviert ist. [CVADHELP-22616]
- Das Öffnen geschützter Sitzungen in Mozilla Firefox schlägt bei der IGEL-Distribution fehl, wenn der Hybridstart verwendet wird. [CVADHELP-22436]
- Beim Öffnen einer App oder eines Desktops über die Citrix Workspace-App für Linux Version 2209 wird möglicherweise ein SSL-Fehler angezeigt. [HDX-49324]
- Die Citrix Workspace-App für Linux reagiert möglicherweise nicht mehr, wenn UWP-Apps (Universal Windows Platform) innerhalb der VDI versuchen, sich mit FIDO2 zu authentifizieren. [HDX-48942]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie im optimierten Microsoft Teams ein Bildsymbol auswählen, wird automatisch eine GZIP-Datei heruntergeladen. Möglicherweise können Sie dieses Bild im optimierten Microsoft Teams nicht als Hintergrundbild verwenden. [HDX-51694]
- Möglicherweise können Sie sich mit einer Smartcard nicht bei der Citrix Workspace-App für Linux Version 2303 authentifizieren. Dieses Problem tritt bei den Linux-Distributionen Red Hat, Ubuntu 22.04 und Debian 11 auf. [RFLNX-9620]
- Wenn Sie die Citrix Workspace-App über den App-Indikator beenden, reagiert die App möglicherweise nicht mehr und Sie erhalten folgende Fehlermeldung:

  "GLib (gthread-posix.c): Unexpected error from C library during 'pthread_setspecific': Invalid argument." [RFLNX-9445]
- Sie erhalten möglicherweise einen undefinierten Fehler mit `libAnalyticsInterface.so` und können Google Analytics-Daten nicht mit der Citrix Workspace-App teilen. [RFLNX-9705]

2303

Was ist neu

Persistente Anmeldung

Das Feature der persistenten Anmeldung ermöglicht es Ihnen, über den gesamten von Ihrem Administrator konfigurierten Zeitraum (2 bis 365 Tage) angemeldet zu bleiben. Wenn dieses Feature aktiviert ist, müssen Sie während des konfigurierten Zeitraums keine Anmeldeinformationen für die Citrix Workspace-App angeben.

Mit dieser Funktion wird das SSO an Citrix DaaS-Sitzungen auf einen Zeitraum von 365 Tagen verlängert. Diese Verlängerung basiert auf der Lebensdauer langlebiger Tokens. Ihre Anmeldeinformationen werden standardmäßig für 4 Tage oder für die Lebensdauer zwischengespeichert, je nachdem, welcher Wert niedriger ist. Die Verlängerung erfolgt, wenn Sie innerhalb dieser 4 Tage eine Verbindung zur Citrix Workspace-App herstellen.

Weitere Informationen finden Sie unter Persistente Anmeldung.

Unterstützung für die Authentifizierung mit FIDO2 in HDX-Sitzungen

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Sie die FIDO2-Geräteumleitung über USB verwenden, entfernen Sie die USB-Umleitungsregel des FIDO2-Geräts aus der Datei `usb.conf` im Ordner `$ICAROOT/`. Dieses Update hilft Ihnen beim Umschalten auf den virtuellen FIDO2-Kanal.

Standardmäßig ist die FIDO2-Authentifizierung deaktiviert.

Weitere Informationen finden Sie unter Unterstützung für FIDO2-Authentifizierung.

Verbesserte Unterstützung der Audioechounterdrückung

Ab diesem Release unterstützt die Citrix Workspace-App Echounterdrückung. Dieses Feature wurde für Echtzeitaudio entwickelt und verbessert die Benutzererfahrung. Die Echounterdrückung unterstützt Audio mit niedriger Qualität, mittlerer Qualität und adaptives Audio. Citrix empfiehlt, adaptives Audio für eine bessere Leistung zu verwenden.

Weitere Informationen finden Sie unter Verbesserte Unterstützung der Audioechounterdrückung

Inaktivitätstimeout für die Citrix Workspace-App

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

Der Wert für das Inaktivitätstimeout kann zwischen 10 und 1440 Minuten liegen. Das Intervall zur Änderung dieses Timeoutwerts muss ein Vielfaches von 5 sein. Beispiel: 10, 15, 20 oder 25 Minuten. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert.

> **Hinweis:**
>
> Das Feature ist nur in Cloud-Bereitstellungen verfügbar.

Weitere Informationen zur Konfiguration von InactivityTimeoutInMinutes finden Sie unter Inaktivitätstimeout für die Citrix Workspace-App.

Hintergrundunschärfe für Webcamumleitung

Die Citrix Workspace-App für Linux unterstützt jetzt Hintergrundunschärfe für die Webcamumleitung.

Weitere Informationen finden Sie unter Hintergrundunschärfe für Webcamumleitung.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren

Ab Version 2303 der Citrix Workspace-App müssen Sie den Pfad des Speichers für temporäre Daten für CEF-basierte Browser konfigurieren.

Weitere Informationen finden Sie unter Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren.

Unterstützung für neue PIV-Karten

Ab diesem Release unterstützt die Citrix Workspace-App die folgenden PIV-Karten (Personal Identification Verification):

- IDEMIA-Smartcard der nächsten Generation
- DELL TicTok-Smartcard

Leistungsoptimierung für Smartcardtreiber

Version 2303 der Citrix Workspace-App enthält leistungsbezogene Korrekturen und Optimierungen für den `VDSCARDV2.DLL`-Smartcardtreiber. Diese Verbesserungen erhöhen die Leistung gegenüber `VDSCARD.DLL` Version 1.

Verbesserungen bei Microsoft Teams

Schnittstelle für bevorzugtes Netzwerk konfigurieren

Ab Citrix Workspace-App 2303 können Sie für den Mediendatenverkehr eine Schnittstelle für das bevorzugte Netzwerk konfigurieren. Sie können dann zu einem anderen Netzwerk wechseln, wenn Sie mehrere Netzwerkverbindungen haben und die Leistung der Standardverbindung nicht gut ist.

Weitere Informationen finden Sie unter Schnittstelle für bevorzugtes Netzwerk konfigurieren.

Behobene Probleme

- Wenn Sie über Citrix Virtual Apps auf Hyperspace zugreifen, wird die Hyperspace-Anmeldeseite möglicherweise über den bereits gestarteten Apps angezeigt. [CVADHELP-20368]
- Wenn Sie auf eine zweite Anwendung zugreifen, wird die aktuelle Sitzung möglicherweise geschlossen und neu gestartet. Die Daten der vorherigen Sitzung sind dann ggf. nicht vorhanden, sondern werden so aktualisiert, als ob die Sitzung zum Zeitpunkt des Starts der zweiten Anwendung gestartet worden sei. Das Problem tritt nicht auf, wenn Sie die erste Anwendung in einer Sitzung starten. [CVADHELP-21914]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Möglicherweise können Sie das 24-Stunden-Zeitformat unter **Self-Service** > **Profil** > **Kontoeinstellungen** > **Regionale Einstellungen** > **Uhrzeitformat** nicht aktualisieren. Das Problem tritt nur in Cloudstores auf. [CVADHELP-20866]
- Eine Sitzung endet möglicherweise abrupt, wenn Sie ein USB-Gerät vom Stromnetz trennen, während Sie mehrere Dateien aus der VDA-Sitzung auf das USB-Gerät ziehen. Dieses Problem tritt nur unter Ubuntu auf. [HDX-30219]
- Möglicherweise treten Leistungsprobleme auf, wenn Sie sich mit einer Smartcard mit der Treiberversion VDSCARDV2.DLL bei der Citrix Workspace-App anmelden. Dieses Problem tritt nur bei eLux-Distributionen auf. [HDX-44314]

2302

Was ist neu

Inaktivitätstimeout für Citrix Workspace (Technical Preview)

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

Der Wert für das Inaktivitätstimeout kann zwischen 10 und 1440 Minuten liegen. Das Intervall zur Änderung dieses Timeoutwerts muss ein Vielfaches von 5 sein. Beispiel: 10, 15, 20 oder 25 Minuten. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert. Administratoren können die Eigenschaft “inactivityTimeoutInMinutes” mit einem PowerShell-Modul konfigurieren.

Weitere Informationen zur Konfiguration von InactivityTimeoutInMinutes finden Sie unter Inaktivitätstimeout für die Citrix Workspace-App.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Unterstützung für Koreanisch

Die Citrix Workspace-App für Linux ist jetzt auf Koreanisch verfügbar.

Leistungsoptimierung für die Citrix Workspace-App

Ab diesem Release ist die Leistung der Citrix Workspace-App für Linux bei der Authentifizierung mit AuthManLite besser.

Technical Previews

- Bildschirm anheften in benutzerdefinierten Webstores

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Es kann zu Konflikten zwischen ctxlogd.service in der Citrix Workspace-App für Linux und ctxlogd.service im Linux VDA kommen. [HDX-44569]
- Ein Hintergrundbild kann in einer Besprechung im optimierten Microsoft Teams möglicherweise nicht angewendet werden. Das Problem tritt bei bestimmten Betriebssystemen auf (darunter HP ThinPro OS). [HDX-47166]

2212

Was ist neu

Neuer clientseitiger Jitter-Puffer [Technical Preview]

Dieses Feature sorgt für flüssiges Audio auch bei schwankender Netzwerklatenz. Standardmäßig ist dieses Feature deaktiviert.

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

1. Gehen Sie zur Konfigurationsdatei `/opt/Citrix/ICAClient/config/module.ini` und bearbeiten Sie sie.
2. Deaktivieren Sie die Audiolatenzsteuerung wie folgt:

```
`AudioLatencyControlEnabled = FALSE`
```

3. Aktivieren Sie den Jitter-Puffer wie folgt:

```
`JitterBufferEnabled = TRUE`
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

Unterstützung für mehrere Audiogeräte

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

Das Feature zur Umleitung mehrerer Audiogeräte ist standardmäßig aktiviert. Um dieses Feature zu deaktivieren, legen Sie in der Datei module.ini den Wert für `AudioRedirectionV4` auf "False" fest.

Unterstützung der Audioaufzeichnung

Ab diesem Release ist das Feature zur Audioaufzeichnung standardmäßig aktiviert. Die Geräte zur Audioaufzeichnung werden angezeigt, wenn eine Sitzung beginnt.

Um dieses Feature zu deaktivieren, legen Sie in der Datei wfclient.ini den Wert für `AllowAudioInput` auf "False" fest.

Technical Previews

- Unterstützung für 32-Bit-Cursor
- Hintergrundunschärfe und Hintergrundersatz für Citrix Optimized Microsoft Teams

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Möglicherweise finden Sie kein gültiges Smartcardzertifikat, nachdem Sie die Smartcard entfernt und erneut eingeführt haben. [CVADHELP-20787]
- Sie können sich möglicherweise nicht mit einer TikTok-Smartcard bei der Citrix Workspace-App anmelden. [CVADHELP-20578]
- Sie können sich möglicherweise nicht mit einer Smartcard von IDEMIA bei der Citrix Workspace-App anmelden. [CVADHELP-20652]
- Die Citrix Workspace-App reagiert möglicherweise nicht mehr, wenn die Audioumleitung den Speex-Codec verwendet und mehrere Audiogeräte aktiviert sind. [CVADHELP-21212]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie sich von der Citrix Workspace-App abmelden und erneut anmelden, wird die Citrix Workspace-App gestartet, ohne Anmeldeinformationen einzugeben. Dieses Problem tritt nur in Cloud-Bereitstellungen auf und wenn der Wert des Parameters `longLivedTokenSupport` auf *True* festgelegt ist. [RFLNX-9160]
- Beim Starten einer Sitzung werden möglicherweise Transaktions-ID-Fehlermeldungen angezeigt. Beispiel: “Die Option “-transactionid” ist ungültig”. [HDX-45618]
- Wenn Sie die Citrix Workspace-App installieren und eine Sitzung mit Root-Privilegien starten, wird die Sitzung möglicherweise beendet. [HDX-46967]
- Wenn Sie die Citrix Workspace-App installieren und starten, wird möglicherweise die folgende Fehlermeldung angezeigt:

  “The X request 130.1 caused error:”10: BadAccess(Attempt to access private resource denied”. [HDX-44416]

2211

Was ist neu

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

Behobene Probleme

- Der VDA stürzt möglicherweise ab, nachdem die Audioschnittstelle des Geräts umgeleitet wurde. Das Problem tritt auf, wenn Sie die Richtlinie “Client-USB-Geräteumleitung” auf dem DDC aktivieren und USB-Verbundgeräte (z. B. ein USB-Headset) an den Endpunkt anschließen. [HDX-44117]
- Die QWERTY-Tastatur von Bloomberg 4 ist möglicherweise nach Verwendung der USB-Umleitung für die Sitzung gesperrt. [HDX-44555]
- Sie können Ihre YubiKey-Geräte möglicherweise nicht mit PIN-Code in der Citrix Workspace-App registrieren und verwenden. [HDX-44951]
- Wenn der Snap-Store-Prozess im Hintergrund ausgeführt wird, können Sie geschützte Apps und Desktops möglicherweise nicht starten. [APPP-110]

2209

Was ist neu

Unterstützung für Authentifizierung mit FIDO2 [Technical Preview]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

> **Hinweis:**
>
> Wenn Sie die FIDO2-Geräteumleitung über USB verwenden, entfernen Sie die USB-Umleitungsregel des FIDO2-Geräts aus der Datei `usb.conf` im Ordner `$ICAROOT/`. Dieses Update hilft Ihnen beim Umschalten auf den virtuellen FIDO2-Kanal.

Standardmäßig ist die FIDO2-Authentifizierung deaktiviert. Gehen Sie wie folgt vor, um die FIDO2-Authentifizierung zu aktivieren:

1. Navigieren Sie zur Datei `<ICAROOT>/config/module.ini`.
2. Gehen Sie zum Abschnitt ICA 3.0.
3. Legen Sie `FIDO2= On` fest.

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

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

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

Einschränkung:

Möglicherweise können Sie das zweite Gerät nicht mit der FIDO2-Authentifizierung bei demselben Konto registrieren.

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

Verbesserungen bei Microsoft Teams

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- App-Freigabe aktiviert: Ab Citrix Workspace-App 2209 für Linux bzw. Citrix Virtual Apps and Desktops 2109 können Sie Apps über die **Bildschirmfreigabe** in Microsoft Teams freigeben.
- **Verbesserungen der Unterstützung hoher DPI-Werte:** Wenn das Feature "Hoher DPI-Wert" aktiviert ist und Sie 4K-Bildschirme verwenden, werden Microsoft Teams-Videoüberlagerungen an der gewünschten Position und in der richtigen Größe angezeigt. Unabhängig von den Anzeigeeinstellungen (Einzel- oder Multimonitor-Anordnungen) erscheinen Überlagerungen immer korrekt und werden nicht vergrößert oder an einer unerwünschten Position angezeigt. Um diese Verbesserung zu aktivieren, stellen Sie sicher, dass der Parameter `DPIMatchingEnabled` in der Konfigurationsdatei `wfclient.ini` auf **True** festgelegt ist. Weitere Informationen finden Sie unter Unterstützung für DPI-Anpassung.
- **WebRTC SDK-Upgrade:** Die Version von WebRTC, die für optimiertes Microsoft Teams verwendet wird, wurde auf Version M98 aktualisiert.

Versionsupgrade der Kompatibilitätsbibliotheken

Ab diesem Release ist die Citrix Workspace-App für Linux mit den folgenden Bibliotheken kompatibel:

- `glibc` 2.27 oder höher
- `glibcxx` 3.4.25 oder höher

App-Schutzupdate

> **Hinweis:**
>
> App-Schutz wird unter Ubuntu 22.04 vor der Citrix Workspace-App Version 2305 nicht unterstützt. Daher können Sie virtuelle Apps und Desktops möglicherweise nicht in der Citrix Workspace-App starten, wenn Sie das App-Schutzmodul unter Ubuntu 22.04 installieren. Weitere Informationen zum App-Schutz finden Sie unter App-Schutz.

Technical Previews

- Verbesserungen des Tastatureingabemodus
- Unterstützung für erweiterte Tastaturlayouts

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Bei aktiviertem App Protection-Feature funktioniert der Keyloggingschutz möglicherweise nicht im Authentifizierungsmanager-Dienst, der die Webseite in einem eigenen Fenster lädt. [RFLNX-9004]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Nach dem Upgrade auf Citrix Workspace App 2007 für Linux kann das Hinzufügen eines Stores mit Storebrowse lange dauern. Das Problem tritt auf, weil der Store versucht, den nicht erreichbaren App-Konfigurationsdienst zu kontaktieren. [CVADHELP-20618]
- Wenn Sie über die Selfservice-Benutzeroberfläche eine Verbindung zu einem Cloudspeicher herstellen, ist auf der Anmeldeseite möglicherweise ein Wartesymbol zu sehen. [CVADHELP-20039]
- Wenn Sie zwei Apps aus zwei Bereitstellungsgruppen starten, kann es zu einer Verzögerung beim Starten der zweiten App kommen. [CVADHELP-18198]

2207

Was ist neu

Verbesserung der Audioqualität

Bisher betrug der maximale Ausgabepufferwert für die nahtlose Audiowiedergabe in der Citrix Workspace-App 200 ms, weshalb bei der Wiedergabe eine Latenz von 200 ms hinzukam. Dieser maximale Ausgabepufferwert wirkte sich auch auf interaktive Audioanwendungen aus.

Mit dieser Verbesserung wird der maximale Ausgabepufferwert in der Citrix Workspace-App auf 50 ms verringert, wodurch die Benutzererfahrung bei interaktiven Audioanwendungen verbessert wird. Außerdem wird die Roundtripzeit (RTT) um 150 ms verringert.

Ab dieser Version können Sie den entsprechenden Wiedergabeschwellenwert und den PulseAudio-Vorpuffer auswählen, um die Audioqualität zu verbessern. Für diese Verbesserung werden die folgenden Parameter im Abschnitt [ClientAudio] der Datei `module.ini` hinzugefügt:

- `PlaybackDelayThreshV4`: Anfänglicher Ausgabepufferwert in Millisekunden. Die Citrix Workspace-App versucht, diesen Pufferwert während der gesamten Dauer einer Sitzung aufrechtzuerhalten. Der Standardwert von `PlaybackDelayThreshV4` ist 50 ms. Dieser Parameter ist nur gültig, wenn `AudioRedirectionV4` auf **True** gesetzt ist.
- `AudioTempLatencyBoostV4`: Wenn der Audiodurchsatz plötzlich ansteigt oder für ein instabiles Netzwerk nicht ausreicht, erhöht dieser Wert den Ausgabepufferwert. Diese Erhöhung des Ausgangspufferwerts sorgt für ein gleichmäßiges Audio. Die Wiedergabe kann jedoch leicht verzögert sein. Der Standardwert von `AudioTempLatencyBoostV4` ist auf 100 ms festgelegt. Dieser Parameter ist nur gültig, wenn `AudioRedirectionV4` auf **True** und `AudioLatencyControlEnabled` auf **True** festgelegt sind. Standardmäßig ist der Wert von `AudioLatencyControlEnabled` auf "True" festgelegt.

Weitere Informationen zum Aktivieren dieser Verbesserung finden Sie im Abschnitt **Verbesserung der Audioqualität** in der Audiodokumentation.

Umleitung von USB-Verbundgeräten

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Ab diesem Release erlaubt die Citrix Workspace-App das Aufteilen (Splitting) von USB-Verbundgeräten. Ein USB-Verbundgerät kann mehrere Funktionen ausführen. Dies wird erreicht, indem jede Funktion über eine andere Schnittstelle verfügbar gemacht wird. Beispiele für USB-Verbundgeräte sind HID-Geräte, die Audio-/Videoeingang und -ausgang umfassen.

Derzeit ist die Umleitung von USB-Verbundgeräten nur in Desktopsitzungen verfügbar. Die aufgeteilten Geräte werden im Desktop Viewer angezeigt.

Früher wurde ein Gerät, das während einer Sitzung getrennt und wieder verbunden wurde, automatisch umgeleitet. Das Gerät wurde daher automatisch mit dem VDA verbunden. In diesem Release müssen Sie die automatische Umleitung manuell über die Konfigurationsdatei aktivieren. Die automatische Umleitung von USB-Verbundgeräten ist standardmäßig deaktiviert.

Weitere Informationen zum Konfigurieren von USB-Verbundgeräten finden Sie in der USB-Dokumentation unter **Umleitung von USB-Verbundgeräten**.

Verbesserte Unterstützung der Audioechounterdrückung [Technical Preview]

Ab diesem Release unterstützt die Citrix Workspace-App Echounterdrückung. Dieses Feature wurde für Echtzeitaudio entwickelt und verbessert die Benutzererfahrung. Die Echounterdrückung unterstützt Audio mit niedriger Qualität, mittlerer Qualität und adaptives Audio. Citrix empfiehlt, adaptives Audio für eine bessere Leistung zu verwenden.

Die Echounterdrückung ist standardmäßig deaktiviert. In Echtzeit-Fällen wird empfohlen, die Echounterdrückung einzuschalten, wenn der Lautsprecher anstelle des Headsets verwendet wird.

Einschränkung:

Die Echounterdrückung ist für hochwertige Audioqualität standardmäßig deaktiviert.

Weitere Informationen finden Sie im Abschnitt **Verbesserte Unterstützung der Audioechounterdrückung** in der Audiodokumentation.

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

Unterstützung für sekundären Klingelton

Sie können das Feature “Sekundärer Klingelton” verwenden, um ein zweites Gerät für die Benachrichtigung über eingehende Anrufe auszuwählen, wenn Microsoft Teams optimiert ist (Citrix HDX opti-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

miert in Info/Version). Angenommen, Sie haben einen Lautsprecher als sekundären Klingelton eingerichtet und Ihr Endpunkt ist mit einem Kopfhörer verbunden. In diesem Fall sendet Microsoft Teams das eingehende Rufsignal an den Lautsprecher, obwohl Ihre Kopfhörer das primäre Peripheriegerät für den Audioanruf sind. In den folgenden Fällen können Sie keinen sekundären Klingelton festlegen:

- Wenn Sie nicht mit mehreren Audiogeräten verbunden sind
- Wenn das Peripheriegerät nicht verfügbar ist (z. B. Bluetooth-Headset)

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Informationen zum Datum der Updateveröffentlichung finden Sie unter Microsoft 365-Roadmap. Die Revision der Dokumentation und die Ankündigung finden Sie außerdem unter CTX253754.

Technical Previews

- Unterstützung für DPI-Anpassung

Die vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Technical Preview.

Behobene Probleme

- Wenn Sie einen Desktop im Vollbildmodus mit Lightweight X11 Desktop Environment (LXDE) starten und die Verbindung zum Netzwerk trennen, wird die Fehlermeldung **Verbindung zu < XXX> wurde unterbrochen** mit der Option **Beenden** angezeigt. Die Meldung wird angezeigt, wenn die Richtlinie für die automatische Wiederverbindung von Clients oder für Sitzungszuverlässigkeit abgelaufen ist. Wenn Sie auf **Beenden** klicken, verschwindet der Benutzerdesktop. Wenn Sie jedoch auf eine andere Stelle auf dem Bildschirm klicken, wird die Schaltfläche **Beenden** möglicherweise nie im Dialogfeld angezeigt. Sie müssen den Benutzerdesktop manuell beenden, indem Sie die Taste **ESC** oder **EINGABE** drücken. [CVADHELP-17478]
- Die Citrix Workspace-App für Linux interpretiert URLs mit der Zeichenfolge **cloud** (z. B. <*xxx-yyy-cloud.com*>) möglicherweise als Clouddomänen-URLs, selbst wenn es sich um On-Premises-URLs handelt. [CVADHELP-19480]
- Die Sitzungsverbindung wird möglicherweise unterbrochen, wenn Sie versuchen, die HDX-Webcam zu verwenden. Das Problem tritt nur in VDA-Version 2203 auf. [CVADHELP-20223]
- Das Kopieren und Einfügen von Inhalten zwischen veröffentlichten Anwendungen, VDI-Sitzungen oder einer VDI-Sitzung und einer veröffentlichten Anwendung schlägt möglicherweise fehl. Die Sitzung oder Anwendung reagiert möglicherweise für einige Zeit nicht mehr. [CVADHELP-19899]
- Wenn Sie auf einem Endpunkt mit der Citrix Workspace-App für Linux 2205 eine Verbindung herstellen, wird die Sitzung möglicherweise unerwartet getrennt. Dieses Problem tritt auf, wenn

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Sie den Sperrbildschirm mit der Richtlinieneinstellung **Force a specific default lock screen image** für bestimmte Arten von JPEG-Dateitypen konfigurieren und auf den Citrix VDA 2203 anwenden. [CVADHELP-21572]

- Wenn Sie ein Video mit einer Webcam in Skype in der Vorschau anzeigen, wird möglicherweise ein schwarzer Bildschirm angezeigt. [HDX-37860]
- Die HDX RealTime-Webcamvideokomprimierung unterstützt keine Kamera mit MJPEG-Videoformat in der Citrix Workspace-App. [HDX-40352]
- Wenn Sie den Bildschirm oder eine App während des Microsoft Teams-Anrufs freigeben, sehen die Teilnehmer möglicherweise visuelle Artefakte. Dieses Problem tritt aufgrund instabiler Bildfrequenzen auf, wie z. B. falsche Videowiedergabe (eingefrorene oder vorübergehende schwarze Frames). Diese Version enthält verbesserte Bildfrequenzen oder Samplingraten, die dazu beitragen, visuelle Artefakte zu reduzieren. [HDX-38032]
- Das Video oder ein Bild in der Citrix Workspace-App wird möglicherweise nicht richtig gerendert. Dieses Problem tritt auf, wenn die Citrix Workspace-App zusammen mit VDA-Version 2109 oder höher verwendet wird. [HDX-40287]
- Wenn Sie wfica mit dem Befehl `-span o` starten, kann die Sitzung möglicherweise nicht gestartet und über alle verfügbaren Bildschirme verteilt werden. Wenn Sie wfica mit dem Befehl `-span h` starten, kann die Liste der derzeit mit dem Benutzergerät verbundenen Bildschirme möglicherweise nicht gedruckt werden. [HDX-32519]
- Wenn Sie wfica mit dem Befehl `-span o` starten, kann die Sitzung möglicherweise nicht gestartet und über alle verfügbaren Bildschirme verteilt werden. Wenn Sie wfica mit dem Befehl `-span h` starten, kann die Liste der derzeit mit dem Benutzergerät verbundenen Bildschirme möglicherweise nicht gedruckt werden. Weitere Informationen finden Sie in der Befehlsreferenz. [HDX-32519]
- Wenn in einem Protokoll während eines TCP- und EDT-/UDP-Verbindungsversuchs ein SSL-Fehler auftritt, können beide Verbindungen aufgrund der Racebedingung fehlschlagen. Dieser SSL-Fehler kann auftreten, wenn sich die TLS-Konfiguration der Protokolle unterscheidet und der Client keine Verbindung über ein Protokoll herstellen kann. [RFLNX-8747]
- Wenn Sie versuchen, eine Remoteverbindung mit einer Maschine herzustellen, auf der die Citrix Workspace-App mit App-Schutz installiert ist, stürzt der x11vnc-Server ab und die Verbindung schlägt fehl. Sie können dann möglicherweise keine Remoteverbindung mit der Maschine über den x11vnc-Server herstellen. [RFLNX-8933]
- Wenn Sie einen Store mit den Standardeinstellungen hinzufügen, schlägt die Storebrowse-Enumeration möglicherweise fehl. Dieses Problem tritt nur im Debian 32-Bit-Betriebssystem auf. [RFLNX-8743]
- Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie die Citrix Workspace-App mit aktiviertem App-Schutz auf 32-Bit-Linux-Maschinen installieren. [RFLNX-8809]
- Wenn Sie einen Store mit dem Befehl `storebrowse -a` hinzufügen und mit dem Befehl `storebrowse -E` auflisten, schlägt die Storebrowse-Auflistung möglicherweise fehl. Dieses

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Problem tritt nur im Raspberry Pi OS auf. [RFLNX-8803]

2205

Was ist neu

Verbesserung der Authentifizierung für Storebrowse

Ab diesem Release befindet sich das Authentifizierungsdialogfeld in der Citrix Workspace-App und die Storedetails werden im Anmeldebildschirm angezeigt. Dieses Feature bietet eine bessere Benutzererfahrung. Die Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht neu eingeben müssen.

Sie können die Verbesserung der Authentifizierung für Storebrowse auch mit dem Schlüssel `StorebrowseIPC` in der Datei `AuthmanConfig.xml` ein- oder ausschalten. Das Ein- und Ausschalten ist standardmäßig deaktiviert.

Die verbesserte Authentifizierung unterstützt Storebrowse für die folgenden Vorgänge:

- Storebrowse -E: Listet die verfügbaren Ressourcen auf.
- Storebrowse -L: Startet eine Verbindung zu einer veröffentlichten Ressource
- Storebrowse -S: Listet die abonnierten Ressourcen auf.
- Storebrowse -T: Beendet alle Sitzungen des angegebenen Stores.
- Storebrowse -Wr: Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [r] werden alle getrennten Sitzungen wieder verbunden.
- Storebrowse -WR: Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [R] werden alle aktiven und alle getrennten Sitzungen wieder verbunden.
- Storebrowse -s: Abonniert die angegebene Ressource aus dem jeweiligen Store.
- Storebrowse -u: Kündigt das Abonnement der angegebenen Ressource aus dem jeweiligen Store.
- Storebrowse -q: Startet eine Anwendung über die direkte URL. Dieser Befehl funktioniert nur bei StoreFront-Stores.

> **Hinweis:**
>
> - Sie können die verbleibenden Storebrowse-Befehle weiterhin wie zuvor verwenden (mit AuthMangerDaemon).
> - Die Verbesserung der Authentifizierung ist nur auf Cloud-Bereitstellungen anwendbar.
> - Mit dieser Verbesserung wird das Feature der persistenten Anmeldung unterstützt.

Weitere Informationen finden Sie unter Verbesserung der Authentifizierung.

Persistente Anmeldung [Technical Preview]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Das Feature der persistenten Anmeldung ermöglicht es Ihnen, über den gesamten von Ihrem Administrator konfigurierten Zeitraum (2 bis 365 Tage) angemeldet zu bleiben. Wenn dieses Feature aktiviert ist, müssen Sie während des konfigurierten Zeitraums keine Anmeldeinformationen für die Citrix Workspace-App angeben.

Mit dieser Funktion wird das SSO an Citrix DaaS-Sitzungen auf einen Zeitraum von 365 Tagen verlängert. Diese Verlängerung basiert auf der Lebensdauer langlebiger Tokens. Ihre Anmeldeinformationen werden standardmäßig für 4 Tage oder für die Lebensdauer zwischengespeichert, je nachdem, welcher Wert niedriger ist. Die Verlängerung erfolgt, wenn Sie innerhalb dieser 4 Tage eine Verbindung zur Citrix Workspace-App herstellen.

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

Weitere Informationen finden Sie unter Persistente Anmeldung.

Automatische Storesuche per E-Mail-Adresse

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

Weitere Informationen finden Sie im Abschnitt **Automatische Storesuche per E-Mail-Adresse** unter Store-URL zur Citrix Workspace-App hinzufügen.

Behobene Probleme

- Der DNS-Server in einer Kundenumgebung mit eingeschränktem Internetzugang löst die URL `clientstream.launchdarkly.com` möglicherweise nicht auf. Daher sendet die Citrix Workspace-App zahlreiche DNS-Abfragen (>1000 innerhalb von drei Sekunden pro Tag) an die URL. [CVADHELP-19559]
- Bei aktiviertem App-Schutzfeature funktioniert die Keyloggingschutzfunktion möglicherweise nicht für den Authentifizierungsmanager-Dienst, der die Bibliothek `UIDialogLibWebKit3.so` verwendet. Dieses Problem wurde in der GNOME- und KDE-Desktopumgebung behoben. [RFLNX-8027]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie versuchen, aus einer VDA-Sitzung zu drucken, die auf dem Raspberry Pi ARMHF-Client Version 3 oder 4 ausgeführt wird, reagiert die Sitzung möglicherweise nicht [CVADHELP-18506]
- Wenn Sie die Self-Service-Benutzeroberfläche mit den Standardeinstellungen starten, wird möglicherweise die folgende Fehlermeldung angezeigt:

  "Response for Secondary Token request is not 200/400/404 42"

  Dieses Problem tritt mit Fedora 35 auf. [RFLNX-8603]

2203

Was ist neu

Unterstützung für EDT IPv6

Ab diesem Release unterstützt die Citrix Workspace-App EDT IPv6.

Unterstützung für das TLS-Protokoll Version 1.3

Ab diesem Release unterstützt die Citrix Workspace-App das Transport Layer Security Protocol (TLS) Version 1.3.
Weitere Informationen finden Sie unter TLS.

Benutzerdefinierte Webstores

Ab Version 2203 können Sie auf den benutzerdefinierten Webstore Ihrer Organisation über die Citrix Workspace-App zugreifen.

> **Hinweis:**
>
> Das Feature zum Pinnen des Bildschirmlayouts im Multimonitormodus wird im benutzerdefinierten Webstore nicht unterstützt.

Weitere Informationen finden Sie unter Benutzerdefinierte Webstores.

Verbesserte Authentifizierung (experimentelles Feature)

Ab diesem Release unterstützt die verbesserte Authentifizierung Storebrowse für die folgenden Vorgänge:

- Storebrowse -E zum Auflisten der verfügbaren Ressourcen.
- Storebrowse -L zum Herstellen einer Verbindung zu einer veröffentlichten Ressource.
- Storebrowse -S zum Auflisten der abonnierten Ressourcen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Sie können die verbleibenden storebrowse-Befehle weiterhin im `AuthMangerDaemon` verwenden. Sie werden in der zukünftigen Version durch die verbesserte Authentifizierung unterstützt.

Weitere Informationen finden Sie unter Verbesserung der Authentifizierung für Storebrowse.

Verbesserte Synchronisierung des Tastaturlayouts

Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert. Wenn Sie dieses Feature aktivieren, wird das Clienttastaturlayout automatisch mit der Sitzung unter Citrix Virtual Apps and Desktops bzw. Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) synchronisiert.

Ab Version 2203 unterstützt die Citrix Workspace-App die folgenden drei Synchronisierungsmodi für das Tastaturlayout:

- **Nur einmal beim Sitzungsstart synchronisieren** - Basierend auf dem Wert `KeyboardLayout` in der Datei `wfclient.ini` wird das Clienttastaturlayout beim Start der Sitzung mit dem Server synchronisiert. Wenn der Wert `KeyboardLayout` auf `0` festgelegt ist, wird die Systemtastatur mit dem VDA synchronisiert. Wenn der Wert `KeyboardLayout` auf eine bestimmte Sprache festgelegt ist, wird die sprachspezifische Tastatur mit dem VDA synchronisiert. Änderungen, die Sie während der Sitzung am Clienttastaturlayout vornehmen, werden nicht sofort wirksam. Um die Änderungen zu übernehmen, melden Sie sich von der App ab und wieder an. Der Modus **Nur einmal beim Sitzungsstart synchronisieren** ist das Standardtastaturlayout, das für die Citrix Workspace-App ausgewählt wurde.
- **Dynamische Synchronisierung zulassen** - Diese Option synchronisiert das Clienttastaturlayout mit dem Server, wenn Sie das Clienttastaturlayout ändern.
- **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

Weitere Informationen finden Sie unter Tastaturlayoutsynchronisierung.

Chat und Besprechungen mit mehreren Fenstern für Microsoft Teams

Sie können mehrere Fenster für Chats und Besprechungen in Microsoft Teams benutzen, wenn die HDX-Optimierung in Citrix Virtual Apps and Desktops 2112 oder höher verwendet wird. Das Fenster-Pop-Out ist auf verschiedenerlei Art möglich. Einzelheiten zum Ausklappen von Fenstern finden Sie unter Microsoft Teams Pop-Out Windows for Chats and Meetings.

Benutzer älterer Versionen der Citrix Workspace-App oder des Virtual Delivery Agent (VDA) sollten bedenken, dass Microsoft den Einzelfenstercode künftig nicht mehr unterstützt. Sie können jedoch ein Upgrade auf eine VDA- bzw. Citrix Workspace-App-Version durchführen, die mehrere Fenster unterstützt (2203 und höher). Um auf eine höhere Version zu aktualisieren, haben Sie mindestens neun Monate Zeit, nachdem dieses Feature allgemein verfügbar ist.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

Verbesserung der automatischen Umleitung von USB-Geräten

Früher wurde ein Gerät, das während einer Sitzung getrennt und wieder verbunden wurde, automatisch umgeleitet. Das Gerät wurde daher automatisch mit dem VDA verbunden. In diesem Release müssen Sie die automatische Umleitung manuell über die Konfigurationsdatei aktivieren. Die automatische Umleitung von USB-Geräten ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter USB.

Behobene Probleme

- Wenn Sie einen Store hinzufügen und ihn bei der Citrix Workspace-App authentifizieren, wird das Authentifizierungsfenster auch nach erfolgreicher Authentifizierung ein zweites Mal geladen. Dieses Problem tritt auf, wenn Sie sich zum ersten Mal bei der Citrix Workspace-App anmelden, nachdem Sie `AuthManLiteEnabled` auf **True** festgelegt haben. [RFLNX-8694]
- Nach der Installation der Citrix Workspace-App mit aktiviertem App Protection-Feature auf einem Betriebssystem mit `glibc 2.34` oder höher kann der Betriebssystemstart beim Neustart des Systems fehlschlagen. [RFLNX-8358]
- Wenn Sie Microsoft Teams verwenden, um einen P2P-Anruf zu tätigen oder an einer Besprechung teilzunehmen, steigt möglicherweise nach einiger Zeit die Last eines CPU-Kerns aufgrund eines Socket-Fehlers auf 100 %. [HDX-38974]
- Die Citrix Workspace-App unterstützt nicht die neue Version von Raspberry Pi OS, die auf dem Debian-Bullseye basiert. [HDX-37000]
- Wenn Sie eine Sitzung mit der ICA-Datei starten und sich von der Sitzung abmelden, ist der erwartete Rückgabewert von der `wfica`-Befehlszeile 0. Anstelle des erwarteten Werts wird jedoch der Wert 2 zurückgegeben. Dieses Problem tritt in der Citrix Workspace-App Version 2106 oder höher auf. [HDX-38916]
- In der Citrix Workspace-App können gelegentlich Fehler auftreten, wenn Sie einen Microsoft Teams-Anruf beantworten oder tätigen. Die folgende Fehlermeldung wird angezeigt:

  Die Verbindung konnte nicht hergestellt werden.

  [HDX-38819]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Bekannte Probleme

Bekannte Probleme in Release 2307

- Wenn Sie die Citrix Workspace-App für Linux mit dem Debian-Paketmanager unter Ubuntu Version 22.04 installieren, wird der folgende Fehler angezeigt:

  A dependency job for AppProtectionService-install.service failed. See 'journalctl -xe' for details.

  Die Fehlermeldung wird angezeigt, obwohl App-Schutz erfolgreich installiert wurde. [RFLNX-9995]

Bekannte Probleme in Release 2305

- Wenn Sie Tools wie das Snipping-Tool verwenden, erscheint auf virtuellen Apps und Desktops möglicherweise ein Schatten des Cursors. [CVADHELP-22336]
- Wenn Sie Avaya WorkPlace öffnen, verbleibt ein schwarzer Rahmen auf dem Bildschirm der virtuellen Apps oder Desktops. [CVADHELP-21558]

Bekannte Probleme in Release 2303

- Wenn Sie die Citrix Workspace-App über die Benutzeroberfläche installieren, können Sie den App-Schutz möglicherweise nicht unter Ubuntu 20.04 und 22.04 installieren. Installieren Sie als Workaround die App über die Befehlszeilenschnittstelle. [APPP-1067]
- Möglicherweise können Sie in der Citrix Workspace-App Version 2303 keine Sitzung starten, wenn der Wert `AllowMultistream` unter Ubuntu 22.04 auf **True** gesetzt ist. [HDX-49916]
- Möglicherweise können Sie sich mit einer Smartcard nicht bei der Citrix Workspace-App für Linux Version 2303 authentifizieren. Dieses Problem tritt bei den Linux-Distributionen Red Hat, Ubuntu 22.04 und Debian 11 auf. [RFLNX-9620]
- Wenn Sie die Citrix Workspace-App über den App-Indikator beenden, reagiert die App möglicherweise nicht mehr und Sie erhalten folgende Fehlermeldung:

  "GLib (gthread-posix.c): Unexpected error from C library during 'pthread_setspecific': Invalid argument. "

  Stellen Sie als Workaround sicher, dass Sie die GLib-Version 2.76 oder höher verwenden. [RFLNX-9445]

Bekannte Probleme in Release 2211

- Beim Starten einer Sitzung werden möglicherweise Transaktions-ID-Fehlermeldungen angezeigt. Beispiel: "Die Option "-transactionid" ist ungültig". Klicken Sie als Workaround auf

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

OK, um die Meldung zu schließen und fortzufahren. [HDX-45618]

- Wenn Sie die Citrix Workspace-App installieren und starten, wird möglicherweise die folgende Fehlermeldung angezeigt:

  "The X request 130.1 caused error:"10: BadAccess(Attempt to access private resource denied"

  Klicken Sie auf **Abbrechen**, um die Sitzung fortzusetzen.

  Navigieren Sie als Workaround zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini` und ersetzen Sie `IgnoreErrors=9,15` durch `IgnoreErrors=9,15,32`. [HDX-44416]

- Wenn Sie sich von der Citrix Workspace-App abmelden und erneut anmelden, wird die Citrix Workspace-App gestartet, ohne Anmeldeinformationen einzugeben. Dieses Problem tritt nur in Cloud-Bereitstellungen auf und wenn der Wert des Parameters `longLivedTokenSupport` auf *True* festgelegt ist. Führen Sie als Workaround folgende Schritte aus:

  1. Navigieren Sie zur Datei `/config/AuthManConfig.xml`.
  2. Gehen Sie zum Abschnitt [AuthManLite] und aktualisieren Sie den folgenden Eintrag:

  ```
  <longLivedTokenSupport>false</longLivedTokenSupport>
  ```

  [RFLNX-9160]

Bekannte Probleme in Release 2209

- Wenn Sie eine Microsoft Edge App-Sitzung starten, wird das Microsoft Edge-Symbol in einer zufällig gewählten Skalierung angezeigt. Dieser Fehler tritt auf, wenn Sie die folgenden Einstellungen angewendet haben:

  - Wert `DPIMatchingEnabled` = **True**
  - Die Clientskalierung im Display ungleich 100 %

  [HDX-39764]

- Das Starten einer Server-VDA-Sitzung mit Smartcard-Authentifizierung kann bei einer Smartcard mit mehreren Benutzern fehlschlagen. Als Workaround führen Sie die Karte erneut ein. [HDX-44255]

- Der VDA stürzt möglicherweise ab, nachdem die Schnittstelle des Geräts umgeleitet wurde. Das Problem tritt auf, wenn Sie die Richtlinie "Client-USB-Geräteumleitung" auf dem DDC aktivieren und USB-Verbundgeräte (z. B. ein USB-Headset) an den Endpunkt anschließen. Geben Sie außerdem den Eingabewert `vid=** pid=** split=01 and intf=00,01` in der Datei usb.conf ein. Danach starten Sie die Sitzung über die Citrix Workspace-App und legen die Umleitung der Schnittstelle des Geräts fest. [HDX-44117]

- Der Sitzungsstart kann unter Raspberry Pi ARMHF auf Basis von Debian 11 fehlschlagen. Citrix empfiehlt die Verwendung von Raspberry Pi ARM64 auf Debian 11 oder eines älteren Raspberry Pi ARMHF-OS auf Debian 10. [HDX-41729]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie ein primäres Konto entfernen, werden die Anmeldeinformationen möglicherweise nicht aus dem Self-Service-Cache gelöscht. Sie können sich dann möglicherweise beim Store anmelden, ohne Anmeldeinformationen anzugeben. Beenden Sie als Workaround den Self-Service, um die Anmeldeinformationen zu löschen. [RFLNX-9051]
- Nachdem Sie die Anmeldeinformationen eingegeben und Self-Service gestartet haben, wird möglicherweise ein weißer Bildschirm angezeigt. Beenden Sie als Workaround den Self-Service und starten Sie ihn neu. [RFLNX–8951]
- Unter OpenSUSE SLES 15 wird möglicherweise ein Wartesymbol angezeigt, wenn Sie eine Verbindung zu einem Cloudspeicher herstellen. [RFLNX–9109]
- Möglicherweise können Sie den Self-Service unter RHEL9 und Fedora 36 nicht starten. Als Workaround muss der Wert von `AuthManLiteEnabled` in der Datei `$ICAROOT/config/AuthManConfig.xml` auf *False* festgelegt sein. [RFLNX-9128]

Bekannte Probleme in Release 2207

- Die DNS-Abfrage für die CAS-Datenerfassung kann bei einem direkten ICA-Start und bei für CAS deaktivierte Speicher auftreten. [CVADHELP-20018]
- Wenn Sie einen zweiten Store mit storebrowse-Befehlen hinzufügen und auflisten, können Sie die Apps oder Desktops möglicherweise nicht aus dem ersten Store starten. Um dieses Problem zu umgehen, müssen Sie den spezifischen Store erneut auflisten, bevor Sie Apps oder Desktops starten. [RFLNX-8953]
- Wenn Sie in einer Desktopsitzung ein Video mit Windows Media Player abspielen, wird der Mauszeiger im Rave-Video möglicherweise ausgeblendet. Das Problem tritt nur auf, wenn Sie die folgenden Richtlinien in DDC wie folgt festgelegt haben:
  - "Videocodec zur Komprimierung verwenden" auf "Für aktive Änderungsbereiche"
  - "Windows Media-Umleitung" auf "Zulässig" (Standardeinstellung)
  - "Browser-Inhaltsumleitung" auf "Zulässig" (Standardeinstellung)
  - "InvertCursorEnabled" auf "BOTH" und folgende Werte sind in der Datei ~/.ICAClient/wfclient.ini enthalten:
    - InvertCursorEnabled=True
    - InvertCursorRefreshRate=60
    - InvertCursorMode=1

[HDX-37259]

Bekannte Probleme in Release 2205

- Wenn Sie auf einem Endpunkt mit der Citrix Workspace-App für Linux 2205 eine Verbindung herstellen, wird die Sitzung möglicherweise unerwartet getrennt. Dieses Problem tritt auf, wenn

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Sie den Sperrbildschirm mit der Richtlinieneinstellung **Force a specific default lock screen image** für bestimmte Arten von JPEG-Dateitypen konfigurieren und auf den Citrix VDA 2203 anwenden. Um dieses Problem zu umgehen, führen Sie ein Upgrade auf die Version 2207 oder höher der Citrix Workspace-App durch. [CVADHELP-21572]

- Wenn in einem Protokoll während eines TCP- und EDT-/UDP-Verbindungsversuchs ein SSL-Fehler auftritt, können beide Verbindungen aufgrund der Racebedingung fehlschlagen. Dieser SSL-Fehler kann auftreten, wenn sich die TLS-Konfiguration der Protokolle unterscheidet und der Client keine Verbindung über ein Protokoll herstellen kann. Legen Sie als Workaround das HDXoverUDP-Attribut in der ICA-Datei auf "On" oder "Off" fest. [RFLNX-8747]
- Die HDX RealTime-Webcamvideokomprimierung unterstützt keine Kamera mit MJPEG-Videoformat in der Citrix Workspace-App. [HDX-40352]
- Das Video oder ein Bild in der Citrix Workspace-App wird möglicherweise nicht richtig gerendert. Dieses Problem tritt auf, wenn die Citrix Workspace-App zusammen mit VDA-Version 2109 oder höher verwendet wird. Führen Sie als Workaround folgende Schritte aus.

  1. Melden Sie sich bei Citrix Studio an.
  2. Bearbeiten Sie die Einstellungen für die Richtlinie "Videocodec zur Komprimierung verwenden".
  3. Wählen Sie in der Dropdownliste **Wert** die Option **Für den gesamten Bildschirm** aus. [HDX-40287]

- Wenn Sie einen Store mit dem Befehl `storebrowse -a` hinzufügen und mit dem Befehl `storebrowse -E` auflisten, schlägt die Storebrowse-Auflistung möglicherweise fehl. Dieses Problem tritt nur im Raspberry Pi OS auf. Führen Sie als Workaround folgende Schritte aus:

  1. Navigieren Sie zu /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Fügen Sie folgenden Eintrag hinzu:

```
<StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
<!--NeedCopy-->
```

  [RFLNX-8803]

- Wenn Sie einen Store mit den Standardeinstellungen hinzufügen, schlägt die Storebrowse-Enumeration möglicherweise fehl. Dieses Problem tritt nur im Debian 32-Bit-Betriebssystem auf. Führen Sie als Workaround folgende Schritte aus:

  1. Navigieren Sie zu /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Fügen Sie folgenden Eintrag hinzu:

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[RFLNX-8743]

- Möglicherweise können Sie das Debian-Paket der Citrix Workspace-App nicht auf Ubuntu 22.04 LTS installieren. Das liegt daran, dass das für `ICAClient` erforderliche `libidn11`-Paket auf Ubuntu 22.04 LTS nicht vorhanden ist. Installieren Sie als Workaround das `libidn11`-Paket unabhängig auf Ubuntu 22.04 LTS, bevor Sie das Debian-Paket der Citrix Workspace-App installieren. [RFLNX-8839]

Bekannte Probleme in Release 2203

- Beim Starten einer veröffentlichten Remote Desktop Protocol (RDP)-Anwendung mit mehreren Monitoren auf einem Ubuntu-Endpunkt zeigt nur ein Monitor den Inhalt an, obwohl die Clientmaschine über mehrere Monitore verfügt. Das Kontrollkästchen "Alle Monitore für Remotesitzung verwenden" in der Anzeigeoption der RDP-Anwendung wird ausgewählt, bevor über RDP eine Verbindung zu einem Remotedesktop hergestellt wird. Das Problem tritt im Seamlessmodus und bei einer Multimonitorkonfiguration auf. [CVADHELP-16768]
- Die Citrix Workspace-App übergibt die Parameter `Clientname` und `clientaddress` während der Ressourcenenumeration nicht an DDC. Daher funktioniert das Filtern von `Set-BrokerAccessPolicyRule` mit Clientname oder Client-IP möglicherweise nicht richtig. [CVADHELP-17667]
- Wenn Sie ein Video mit einer Webcam in Skype in der Vorschau anzeigen, wird möglicherweise ein schwarzer Bildschirm angezeigt. [HDX-37860]

Bekannte Probleme in Release 2112

- Wenn Sie versuchen, Text einzugeben, erscheint der Cursor weiß. Das Problem tritt in einem Double-Hop-Szenario auf, wenn die Verbindung von einer Linux-Endpunktmaschine erfolgt. [CVADHELP-16170]

Bekannte Probleme in Release 2111

- Wenn Sie sich bei einem Cloudstore anmelden, wird der Bildschirm möglicherweise weiß angezeigt. [RFLNX-8337]
- Wenn Sie versuchen, die Citrix Workspace-App zu starten, wird die Self-Service-Benutzeroberfläche möglicherweise nicht geöffnet und die folgende Fehlermeldung wird angezeigt:

  "User-defined signal 2"

  Das Problem tritt im Debug-Build und in Azure VM Debian 10 auf. [RFLNX-8336]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Bekannte Probleme in Release 2109

- Wenn Sie die Citrix Workspace-App deinstallieren, werden veraltete Cachedateien unter `$HOME/.local/share/webkitgtk` möglicherweise nicht automatisch entfernt. Entfernen Sie als Workaround die
  Cachedateien manuell. [HDX-28187]
- Das Starten von Desktops oder Anwendungen mit der Citrix Workspace-App kann fehlschlagen, wenn die Multiportrichtlinie auf dem DDC aktiviert ist. [HDX-31016]
- Versuche, eine Sitzung mit Smartcardauthentifizierung zu starten, schlagen möglicherweise fehl. Das Problem tritt bei der Citrix Workspace App-für Linux Version 2104 und höher auf. Als Workaround geben Sie die Smartcard-Anmeldeinformationen manuell ein. [CVADHELP-18402]
- Versuche, die Verbindung zur Sitzung wiederherzustellen, finden möglicherweise nur einmal während der automatischen Wiederverbindung von Clients statt. Daher funktioniert die Richtlinie **Automatische Wiederverbindung von Clients** möglicherweise nicht wie erwartet. [HDX-34114]
- Wenn Sie die Fortschrittsanzeige schließen, die den Fortschritt eines Anwendungsstarts anzeigt, schlägt der wfica-Prozess möglicherweise fehl. Dann wird die Anwendung möglicherweise gestartet und verschwindet von Ihrem Bildschirm. [HDX-34701]

Bekannte Probleme in Release 2108

- Wenn Sie Global Server Load Balancing (GSLB) verwenden, werden die DNS-Antworten (Domain Name System) möglicherweise für die Gültigkeitsdauer (Time-To-Live, TTL) nicht zwischengespeichert. Daher schlägt die Authentifizierung mit WebView möglicherweise fehl. [RFLNX-3673]

Bekannte Probleme in Release 2106

- In einer Desktopsitzung verschiebt sich der Tastaturfokus auf die aktuelle Mausposition, nachdem eine Seite mit CEF-Browserinhaltsumleitung umgeleitet wurde. Das Problem entsteht durch eine von einem Drittanbieter verursachte Einschränkung von Open Source CEF. [RFLNX-7724]
- Wenn Sie versuchen, auf das Browserinhaltsumleitungs-Overlay (z. B. YouTube-Suche) zu klicken, während eine andere Anwendung im Vordergrund ist, wird die Browserseite nicht im Vordergrund angezeigt. [RFLNX-7730]
- Wenn eine Seite mit CEF-Browserinhaltsumleitung umgeleitet wurde, wird beim Schließen der umgeleiteten Webseite ein Segmentierungsfehler in den Fehlerprotokollen erfasst. [RFLNX-7667]

Bekanntes Problem in Release 2103

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Während eines Videoanrufs oder der Bildschirmfreigabe reagiert Microsoft Teams möglicherweise nicht mehr und der Anruf kann abrupt enden. [CVADHELP-16918]

Bekannte Probleme in Release 2101

- Manchmal kann die Citrix Workspace-App die eingehenden Videos in Microsoft Teams nicht rendern. [RFLNX-6662]

Legacy-Dokumentation

Informationen zu Produktversionen, die das Ende der Lebensdauer erreicht haben, finden Sie in der Legacy-Dokumentation.

Hinweise zu Drittanbietern

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

Citrix Workspace-App für Linux – Hinweise zu Drittanbietern (PDF-Download)

Experimentelle Features

Gelegentlich veröffentlicht Citrix experimentelle Features, um Kundenfeedback zu neuen Technologien oder Features zu erhalten. Citrix akzeptiert keine Supportanfragen für experimentelle Features, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Citrix unterliegt keiner Verpflichtung, experimentelle Features in ein Produktrelease zu übernehmen und behält sich das Recht vor, diese Features jederzeit aus beliebigem Grund zurückziehen.

Technical Previews

September 12, 2023

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2308

Unterstützung für Webcamumleitung und Servicekontinuität für ARM64-Geräte [Technical Preview]

Ab diesem Release werden die folgenden Features auf Endpunktgeräten mit ARM64-Architektur unterstützt, auf denen die Citrix Workspace-App für Linux ausgeführt wird:

- Webcamumleitung
- Servicekontinuität

Weitere Informationen finden Sie unter Unterstützung für ARM64-Architektur.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Maskierung von Datenpaketverlust zur Verbesserung der Audioleistung aktivieren [Technical Preview]

Mit diesem Release wurde der Jitter-Puffermechanismus verbessert und die Maskierung von Datenpaketverlust (Packet Loss Concealment, PLC) für den Speex- und Opus-Codec hinzugefügt. Der verbesserte Jitter-Puffermechanismus erkennt fehlerhaft angeordnete Datenpakete und ordnet sie in der richtigen Reihenfolge. PLC unterstützt die Rekonstruktion der verlorenen Datenpakete. Diese Verbesserung verbessert die Paketverlust- und Jittertoleranz und erhöht somit die Audioleistung im Transportprotokoll EDT Lossy und in UDP. Diese Verbesserung ist standardmäßig deaktiviert.

Führen Sie folgende Schritte aus, um die Verbesserung zu aktivieren:

1. Navigieren Sie zur Konfigurationsdatei /opt/Citrix/ICAClient/config/module.ini und bearbeiten Sie sie.
2. Aktivieren Sie den Jitter-Puffer wie folgt:

```
JitterBufferEnabled = TRUE
<!--NeedCopy-->
```

3. Aktivieren Sie PLC wie folgt:

```
PacketLossConcealmentEnabled=TRUE
<!--NeedCopy-->
```

4. Aktivieren Sie das Feature zur Unterstützung des EDT Lossy-Protokolls (Technical Preview) oder das Feature UDP-Audio.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Unterstützung für MultiTouch [Technical Preview]

Ab diesem Release unterstützt die Citrix Workspace-App für Linux auch MultiTouch-Geräte. Mit diesem Feature können Geräte auch Touchscreeneingaben empfangen. Dazu gehören Berührungsgesten und Interaktionen mit einem Eingabestift oder Stylus. Dies ermöglicht die Interaktion mit MultiTouch-Bildschirmen, während Sie Apps oder Desktops in einer HDX-Sitzung verwenden.
Folgende Aktionen und entsprechende Gesten auf dem Touchscreen werden unterstützt:

- **Objekt auswählen**: Tippen Sie auf das Touchpad.
- **Scrollen**: Legen Sie zwei Finger auf das Touchpad und bewegen Sie sie horizontal oder vertikal.
- **Verkleinern oder vergrößern**: Legen Sie zwei Finger auf das Touchpad und ziehen Sie sie zusammen oder auseinander.
- **Weitere Befehle anzeigen (ähnlich dem Rechtsklick)**: Tippen Sie mit zwei Fingern auf das Touchpad oder drücken Sie in der unteren rechten Ecke.

Bekannte Einschränkung:

- Keine Unterstützung für Sitzungszuverlässigkeit, Touch-Ereignisse werden also nicht zwischengespeichert.
- Keine Unterstützung auf Linux VDA

Bekannte Probleme:

- MultiTouch wird nicht für Multimonitoranzeigen im Anzeigemodus **Join Displays** (erweiterter Modus) unterstützt. [HDX-52394]
- Auf dem ASUS-Touchscreen ist das längere Drücken mit einem Finger möglicherweise nicht verfügbar. [HDX-52521]

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

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

Ab diesem Release können sich Benutzer, die sich über die Citrix Workspace-App für Linux bei On-Premises Stores anmelden, mit kennwortlosen FIDO2-Sicherheitsschlüsseln authentifizieren. Die Sicherheitsschlüssel unterstützen verschiedene Arten von Sicherheitseingaben wie Sicherheits-PIN, Biometrie, Magnetstreifenkarte, Smartcard, Public-Key-Zertifikat und mehr. Weitere Informationen zu FIDO2 finden Sie unter FIDO2-Authentifizierung.

Die Citrix Workspace-App verwendet den Citrix Enterprise Browser als Standardbrowser für die FIDO2-Authentifizierung. Administratoren können den Browsertyp für die Authentifizierung bei der Citrix Workspace-App konfigurieren.

Um das Feature zu aktivieren, navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und geben folgende Einträge ein:

```
1      <key>FIDO2Enabled</key>
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
    <value>true</value>
<!--NeedCopy-->
```

Um den Standardbrowser zu ändern, navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und ändern die Browsereinstellungen nach Bedarf. Zulässige Werte sind `CEB`, `chromium`, `firefox` und `chromium-browser`.

```
    <FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>
<!--NeedCopy-->
```

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

2307

Unterstützung für IPv6 UDT mit DTLS

Bisher wurden DTLS-Verbindungen zwischen der Citrix Workspace-App für Linux und Virtual Delivery Agents (VDAs) nur über das IPv4-Netzwerk unterstützt.

Ab diesem Release unterstützt die Citrix Workspace-App DTLS-Verbindungen sowohl über IPv4 als auch über IPv6.

Dieses Feature ist standardmäßig aktiviert.

Zur Verwendung der IPv6-DTLS-Direktverbindung mit VDA in der Citrix Workspace-App für Linux ist keine zusätzliche Konfiguration erforderlich.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Unterstützung für App Protection auf ARM64-Geräten

Der App-Schutz wird auf Geräten mit ARM64-Architektur unterstützt, auf denen die Citrix Workspace-App für Linux ausgeführt wird. Weitere Informationen finden Sie unter Unterstützung für ARM64-Architektur.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

2305

Unterstützung für IPv6 TCP mit TLS

Bisher wurden TLS-Verbindungen zwischen der Citrix Workspace-App für Linux und Virtual Delivery Agents (VDAs) nur über das IPv4-Netzwerk unterstützt.

Ab diesem Release unterstützt die Citrix Workspace-App TLS-Verbindungen sowohl über IPv4 als auch über IPv6.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Dieses Feature ist standardmäßig aktiviert.

Zur Verwendung der IPv6-TLS-Direktverbindung mit VDA in der Citrix Workspace-App für Linux ist keine zusätzliche Konfiguration erforderlich.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Verbesserte Unterstützung für 32-Bit-Cursor

Seit Version 2212 der Citrix Workspace-App für Linux ist die Unterstützung für den 32-Bit-Cursor standardmäßig aktiviert.

Ab diesem Release können Sie die Unterstützung für den 32-Bit-Cursor deaktivieren. Für diese Verbesserung wurde in der Datei `wfclient.ini` der neue Parameter `Cursor32bitSupport` hinzugefügt.

Informationen zum Deaktivieren der Unterstützung für den 32-Bit-Cursor finden Sie unter Unterstützung für 32-Bit-Cursor.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

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

Ab diesem Release können sich Benutzer, die sich über die Citrix Workspace-App für Linux bei On-Premises Stores anmelden, mit kennwortlosen FIDO2-Sicherheitsschlüsseln authentifizieren. Die Sicherheitsschlüssel unterstützen verschiedene Arten von Sicherheitseingaben wie Sicherheits-PIN, Biometrie, Magnetstreifenkarte, Smartcard, Public-Key-Zertifikat und mehr. Weitere Informationen zu FIDO2 finden Sie unter FIDO2-Authentifizierung.

Die Citrix Workspace-App verwendet den Citrix Enterprise Browser als Standardbrowser für die FIDO2-Authentifizierung. Administratoren können den Browsertyp für die Authentifizierung bei der Citrix Workspace-App konfigurieren.

Um das Feature zu aktivieren, navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und geben folgende Einträge ein:

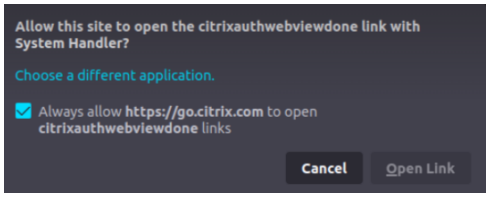
```
1 ```
2 <key>FIDO2Enabled</key>
3 <value>true</value>
4 <!--NeedCopy--> ```
```

Um den Standardbrowser zu ändern, navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und ändern die Browsereinstellungen nach Bedarf. Zulässige Werte sind `CEB`, `chromium`, `firefox` und `chromium-browser`.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
1 ```
2 <FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>
3 <!--NeedCopy--> ```
```

Für Benutzerberechtigungen wird beim ersten Öffnen des Browsers nach der FIDO2-Authentifizierung das folgende Dialogfeld angezeigt:



Aktivieren Sie das Kontrollkästchen **Always allow https://go.citrix.com to open citrixauthwebviewdone links** und klicken Sie auf **Open Link**.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Dateien und Ordner zwischen zwei virtuellen Desktops kopieren und einfügen

Bisher konnten Sie nur Text zwischen zwei virtuellen Desktops kopieren. Ab diesem Release können Sie auch Dateien und Ordner zwischen zwei virtuellen Desktops kopieren und einfügen. Die maximale Datenmenge, die im Linux Virtual Delivery Agent in einem einzelnen Vorgang kopiert bzw. eingefügt werden kann, ist 200 MB. Weitere Informationen finden Sie in der Dokumentation unter Kopieren und Einfügen von Dateien.

Dieses Feature ist standardmäßig aktiviert.

> **Hinweis:**
>
> Das Kopieren und Einfügen von Dateien und Ordnern zwischen zwei virtuellen Desktops wird nur auf der x64-Linux-Distribution und auf Geräten mit ARM64-Architektur unterstützt, auf denen die Citrix Workspace-App für Linux ausgeführt wird.

Weitere Informationen finden Sie unter Kopieren und Einfügen von Dateien und Ordnern zwischen zwei virtuellen Desktops.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Unterstützung für die ARM64-Architektur

Ab diesem Release unterstützt die Citrix Workspace-App für Linux auch Geräte, die auf der ARM64-Architektur basieren. Dafür wurden Binärdateien in das Installationspaket aufgenommen, mit denen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

die Citrix Workspace-App auf ARM64-basierten Geräten installiert werden kann. Dieses Installationspaket unterstützt nur die Ressourcenenumeration, den ICA-Start und die Audioumleitung. Voraussetzungen und Systemanforderungen sind dieselben wie bei der Installation der App auf anderen Architekturen.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Unterstützte Hardwarebeschleunigung für optimiertes Microsoft Teams

Die Citrix Workspace-App für Linux bietet eine verbesserte Leistung bei Videoanrufen mit Microsoft Teams.

Bisher wurde nur die CPU für Codierungszwecke verwendet. Ab diesem Release kann auch die GPU zum Codieren ausgehender Videoframes verwendet werden, um so die CPU-Auslastung zu reduzieren. Dieses Feature ist von Vorteil, wenn Sie einen Thin Client mit begrenzten CPU-Ressourcen und zusätzlicher GPU verwenden.

Voraussetzung:

Stellen Sie sicher, dass Sie den aktuellen GPU-Treiber verwenden. Installieren Sie gegebenenfalls den aktuellen GPU-Treiber über folgenden Befehl:

```
1 ```
2 sudo apt install va-driver-all
3 <!--NeedCopy--> ```
```

Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Navigieren Sie zur Datei `/var/.config/citrix/hdx_rtc_engine/config.json`.
2. Legen Sie die folgende Konfiguration fest:

```
1 ```
2 {
3   "VideoHwEncode": 1,  }
4
5 <!--NeedCopy--> ```
```

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

2302

Bildschirm anheften in benutzerdefinierten Webstores

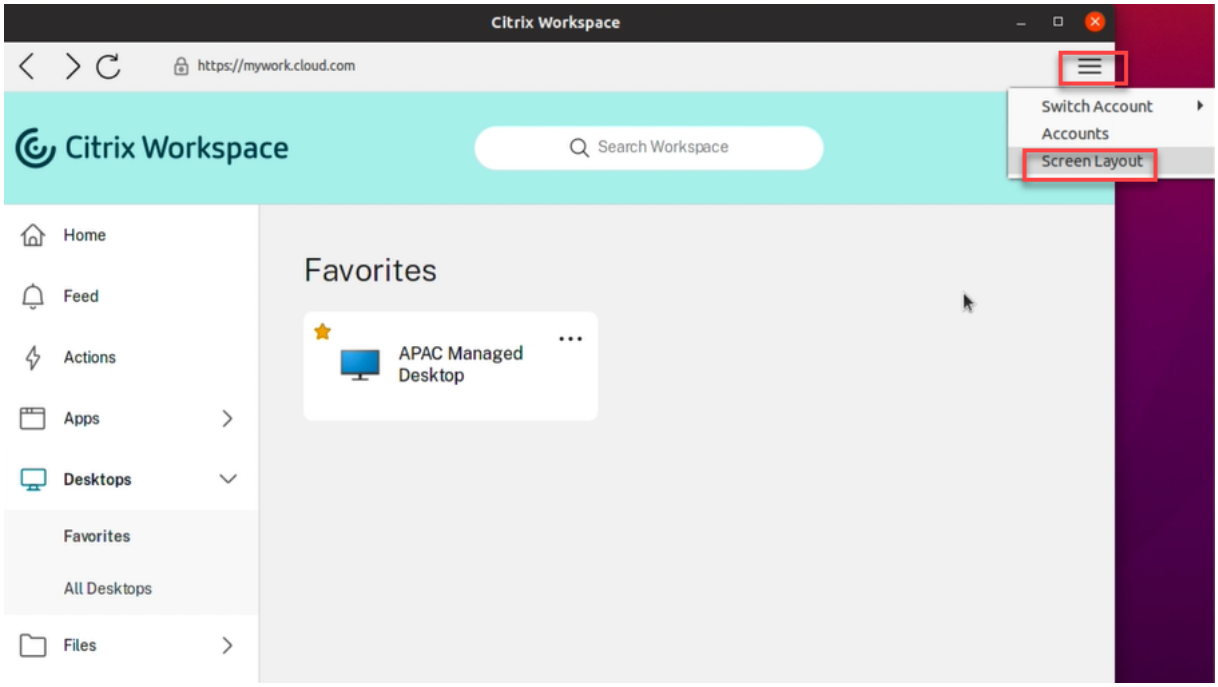
Ab Version 2302 können Sie die Auswahl für das Bildschirmlayout im Multimonitormodus in benutzerdefinierten Webstores speichern.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu:

```
<key>ScreenPinEnabled</key>
<value> true </value>
<!--NeedCopy-->
```

Erst nachdem Sie den vorhergehenden Schlüssel hinzugefügt haben, können Sie die Option **Bildschirmlayout** im Citrix Workspace-App-Menü sehen.



Um das Bildschirmlayout auszuwählen, wählen Sie im Menü der Citrix Workspace-App die Option **Bildschirmlayout** aus. Das Dialogfeld **Bildschirmlayout** wird angezeigt.

Wählen Sie einen virtuellen Desktop aus dem Dropdownmenü aus. Die Layoutauswahl wird nur auf den ausgewählten Desktop angewendet.

Wählen Sie eine oder mehrere Kacheln aus, um eine rechteckige Auswahl für das Layout zu bilden. Die Sitzung wird dann gemäß der Layoutauswahl angezeigt.

Einschränkungen:

- Durch Aktivieren des Pinnens wird die Funktion zum Speichern des Bildschirmlayouts in einer Sitzung deaktiviert.
- Dieses Feature gilt nur für Desktops, die als Favorit gekennzeichnet sind.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2212

Unterstützung für 32-Bit-Cursor

Bisher wurde der benutzerdefinierte 32-Bit-Cursor unter Umständen mit einem schwarzen Rahmen angezeigt.

Seit Version 2212 der Citrix Workspace-App für Linux ist die Unterstützung für den 32-Bit-Cursor standardmäßig aktiviert. Dadurch ist das Problem mit dem schwarzen Rahmen um den Cursor herum behoben.

Ab Version 2305 können Sie die Unterstützung für den 32-Bit-Cursor deaktivieren. Für diese Verbesserung wurde in der Datei `wfclient.ini` der neue Parameter `Cursor32bitSupport` hinzugefügt.

Führen Sie folgende Schritte aus, um die Unterstützung für den 32-Bit-Cursor zu deaktivieren:

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Gehen Sie zum Abschnitt [Thinwire3.0] und legen Sie folgenden Eintrag fest:

```
Cursor32bitSupport = False
<!--NeedCopy-->
```

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

Hintergrundunschärfe und Hintergrundersatz für Citrix Optimized Microsoft Teams

Voraussetzung:

Stellen Sie sicher, dass Sie wget installiert haben.

Ab Version 2212 der Citrix Workspace-App unterstützt Citrix Optimized Microsoft Teams in der Citrix Workspace-App für Linux die Hintergrundunschärfe und Hintergrundersetzung. Sie können das Feature verwenden, indem Sie in einer Besprechung oder einem Anruf **Mehr** > **Hintergrundeffekte anwenden** wählen.

2209

Verbesserungen des Tastatureingabemodus

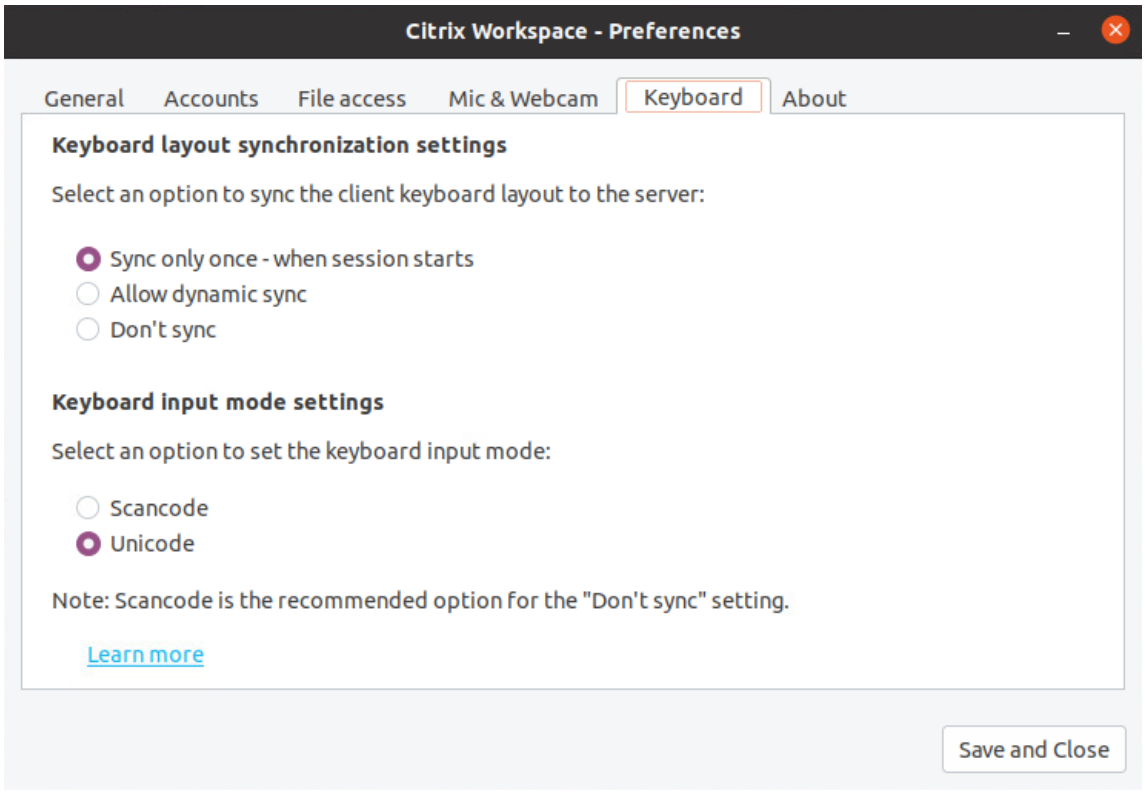
Bisher konnten Sie verschiedene Tastatureingabemodi nur aktivieren, indem Sie den Wert von `KeyboardEventMode` in der Konfigurationsdatei änderten. Es gab keine UI-Option zur Auswahl des Tastatureingabemodus.

Ab Citrix Workspace-App 2209 können Sie im neuen Bereich **Einstellungen für den Tastatureingabemodus** verschiedene Tastatureingabemodi konfigurieren. Sie können **Scancode** oder **Unicode** als Tastatureingabemodus auswählen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

1. Wählen Sie im Infobereich das Symbol der Citrix Workspace-App aus und dann die Option **Einstellungen**.
   Das Dialogfeld **Citrix Workspace - Einstellungen** wird angezeigt.
2. Klicken Sie auf “Tastatur”.
   Sie können den Bereich **Einstellungen für den Tastatureingabemodus** sehen.



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

   Standardmäßig ist der Tastatureingabemodus auf **Unicode** festgelegt. Weitere Informationen zum Tastatureingabemodus finden Sie im Abschnitt **Konfigurieren des Tastaturlayouts** in der Dokumentation zur Tastaturlayoutsynchronisierung .
4. Klicken Sie auf **Speichern und Schließen**.

> **Hinweis:**
>
> Änderungen an der Tastaturkonfiguration werden wirksam, sobald Sie die Verbindung zur An-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> wendung wieder herstellen. Wenn Sie den Tastatureingabemodus über die Benutzeroberfläche ändern, wird auch der Parameterwert von `KeyboardEventMode` in der Datei `wfclient.ini` automatisch aktualisiert.

Angenommen, Sie verwenden das Tastaturlayout USA international und der VDA das russische Tastaturlayout.

Wenn Sie **Scancode** auswählen und die Taste neben der Feststelltaste drücken, wird der Scancode `1E` an den VDA gesendet. Der VDA verwendet dann `1E`, um das Zeichen `ф` anzuzeigen.

Wenn Sie “Unicode” wählen und die Taste neben Feststelltaste drücken, wird das Zeichen `a` an den VDA gesendet. Obwohl der VDA das russische Tastaturlayout verwendet, erscheint das Zeichen `a` auf dem Bildschirm.

Unterstützung für erweiterte Tastaturlayouts

Ab Version 2209 der Citrix Workspace-App unterstützt der Scancode-Tastatureingabemodus die folgenden erweiterten Tastaturlayouts:

- Japanisch 106
- Portugiesisch ABNT/ABNT2
- Multimediatastaturen

Der Scancode-Tastatureingabemodus unterstützt die erweiterten Tastaturlayouts sowie alle Tastaturlayout-Synchronisierungsmodi.

Diese Unterstützung ist standardmäßig aktiviert.

2207

Unterstützung für DPI-Anpassung

Ab Version 2207 stimmen die in der Citrix Workspace-App festgelegten Werte für Bildschirmauflösung und DPI-Skalierung mit den entsprechenden Werten in der Sitzung für virtuelle Apps und Desktops überein. Sie können den erforderlichen Skalierungswert im Linux-Client festlegen, die Skalierung der VDA-Sitzung wird automatisch aktualisiert.

Die DPI-Skalierung wird hauptsächlich bei großen und hochauflösenden Bildschirmen verwendet. Mit diesem Feature ist die Anzeige folgender Elemente in einer gut sichtbaren Größe möglich:

- Anwendungen
- Text
- Bilder
- Andere grafische Elemente

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Das Feature "DPI-Anpassung" unterstützt nur die Desktop-Umgebungen GNOME, KDE und Xfce.

Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Gehen Sie zu der Konfigurationsdatei $HOME/.ICAClient/wfclient.ini.
2. Gehen Sie zum Abschnitt [WFClient] und legen Sie folgenden Eintrag fest:

   DPIMatchingEnabled=TRUE

Einschränkung:

Derzeit unterstützt das Feature zur DPI-Anpassung die clientseitige fraktionierte Skalierung nicht. Bei hohem DPI-Skalenwert funktioniert die Microsoft Teams-Optimierung möglicherweise nicht wie erwartet.

2211

Unterstützung für benutzerdefinierte Webstores

Ab diesem Release können Sie über die Citrix Workspace-App auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen.

Um dieses Feature verwenden zu können, muss der Administrator die Domäne oder den benutzerdefinierten Webstore der Liste der zulässigen URLs im Global App Configuration Service hinzufügen. Nachdem die URL hinzugefügt wurde, können Sie die URL des benutzerdefinierten Webstores im Bildschirm **Konto hinzufügen** in der Citrix Workspace-App angeben. Der benutzerdefinierte Webstore wird im nativen Workspace-App-Fenster geöffnet.

Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter Global App Configuration Service.

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**.

Als Voraussetzung müssen Sie den benutzerdefinierten Webstore in der Datei `AuthManConfig.xml` aktivieren. Weitere Informationen finden Sie unter Benutzerdefinierte Webstores.

> **Hinweis:**
>
> - Sie können nur die in der Datei `AuthManConfig.xml` aufgelisteten URLs für den benutzerdefinierten Webstore verwenden. Sie können der Datei `AuthManConfig.xml` mehrere URLs hinzufügen, die für den benutzerdefinierten Webstore gelten sollen.
> - Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

2109

Unterstützung von Servicekontinuität mit der Citrix Workspace-Weberweiterung für Google Chrome

Die Unterstützung der Servicekontinuität mit der Citrix Workspace-Weberweiterung für Google Chrome ist als öffentliche Technical Preview verfügbar. Sie können die Workspace-Weberweiterung für Google Chrome mit der Citrix Workspace-App für Linux 2109 verwenden. Diese Erweiterung ist im Google Chrome Web Store verfügbar. Die Workspace-App kommuniziert mit der Citrix Workspace-Weberweiterung unter Verwendung des nativen Messaging-Hostprotokolls zur Browsererweiterung. Die Workspace-App und die Workspace Web-Erweiterung verwenden gemeinsam Workspace-Verbindungsleases, um bei Ausfällen den Zugriff auf Apps und Desktops über einen Browser zu ermöglichen. Weitere Informationen finden Sie unter Servicekontinuität.

Global App Configuration Service

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

Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu:

```
1       <key>AppConfigEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Weitere Informationen über die Einstellungen für Workspace Service-URLs finden Sie in der Dokumentation zum Global App Configuration Service.

> **Hinweis:**
>
> - Die Citrix Workspace-App für Linux verwendet den Global App Configuration Service nur für die Bereitstellung von Workspace-Dienst-URLs.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Von Technical Preview zu allgemeiner Verfügbarkeit

|Übergangsdatum|Dienst oder Feature|Weitere Informationen
|—|—|—|

Systemanforderungen und Kompatibilität

September 12, 2023

Anforderungen

Hardwareanforderungen

Linux-Kernel:

- Version 2.6.29 oder höher

Speicherplatz:

- Mindestens 55 MB
- Zusätzliche 110 MB, wenn Sie das Installationspaket auf dem Datenträger erweitern/extrahieren
- Mindestens 1 GB RAM für SoC-Geräte (System on a Chip), die HDX MediaStream Flash-Umleitung verwenden.

Farbvideoanzeige:

- Farbvideoanzeige im 256-Farbenmodus oder höher.

Bibliotheken und Codec

Bibliotheken:

- `glibcxx` 3.4.25 oder höher
- `glibc` 2.27 oder höher
- gtk 2 (2.20.1 oder höher)
- libcap1 oder libcap2
- `libjson-c` (für Instrumentierung)
- X11 oder X.Org (Wayland wird nicht unterstützt)
- Unterstützung von `udev`
- Advanced Linux Sound Architecture (ALSA) libasound2
- PulseAudio

Self-Service-Benutzeroberfläche:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- webkit2gtk 2.16.6 oder höher
- libxml2 2.7.8
- `libxerces-c` 3.1

Codec-Bibliotheken:

- Speex
- Vorbis-Codec-Bibliotheken

Distributionsanforderungen basierend auf Red Hat Package Manager (RPM):

- `chkconfig`

Netzwerkanforderungen

Netzwerkprotokoll:

- TCP/IP

H.264-Anforderungen

Für x86-Geräte:

- Mindestprozessorgeschwindigkeit von 1,6 GHz

Für das HDX 3D Pro-Feature:

- Mindestprozessorgeschwindigkeit von 2 GHz
- Native Hardware mit beschleunigtem Grafiktreiber

Für ARM-Geräte:

- Ein Hardware-H.264-Decoder für die allgemeine H.264-Unterstützung und für HDX 3D Pro

HDX MediaStream Flash-Umleitung

Informationen zu allen Anforderungen für die HDX MediaStream Flash-Umleitung finden Sie im Knowledge Center-Artikel CTX134786.

Wir empfehlen, das aktuelle Plug-In zu testen, bevor Sie eine neue Version bereitstellen, um die Vorteile der neuesten Funktionen und Sicherheitsverbesserungen auszuschöpfen.

Anforderungen für die Authentifizierung

cURL 7.68 oder höher mit OpenSSL für Cloudauthentifizierung.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Anforderungen für die Integration des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

- `zlib` 1.2.3.3
- `libtar` 1.2 oder höher
- `libjson` 7.6.1 oder höher

Anforderungen für die HDX RealTime-Webcamvideokomprimierung

- Eine Video4Linux-kompatible Webcam
- `GStreamer` 0.10.25 (oder eine höhere 0.10.x-Version) einschließlich des “plugins-good”-Pakets für die Distribution.

  Oder

- `GStreamer` 1.0 (oder eine höhere 1.x-Version), einschließlich der Pakete “plugins-base”, “plugins-good”, “plugins-bad”, “plugins-ugly” und “gstreamer-libav” für die Distribution.

Anforderungen für die HDX MediaStream-Windows-Medienumleitung

- `GStreamer` 0.10.25 (oder eine höhere 0.10.x-Version) einschließlich des “plugins-good”-Pakets für die Distribution. In Allgemeinen ist Version 0.10.15 oder höher für die HDX MediaStream Windows Media-Umleitung ausreichend

  Oder

- `GStreamer` 1.0 (oder eine höhere 1.x-Version), einschließlich der Pakete “plugins-base”, “plugins-good”, “plugins-bad”, “plugins-ugly” und “gstreamer-libav” für die Distribution.

> **Hinweise:**
>
> - Wenn `GStreamer` in Ihrer Linux-Distribution nicht enthalten ist, können Sie es auch von der Seite GStreamer herunterladen.
> - Für bestimmte Codes (z. B. in “plugins-ugly”) ist u. U. eine Lizenz des Herstellers der jeweiligen Technologie erforderlich. Wenden Sie sich bei Fragen an den Systemadministrator.

Anforderungen für die Browserinhaltsumleitung

- webkit2gtk Version 2.16.6

Anforderungen für Philips SpeechMike

- Besuchen Sie die Philips-Website, um die relevanten Treiber zu installieren.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Anforderungen für den App-Schutz

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

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

> **Hinweis:**
>
> - Bei Verwendung einer älteren Version der Citrix Workspace-App als 2204 unterstützt das App-Schutz-Feature Betriebssysteme, die `glibc` 2.34 oder höher verwenden, nicht.
> - Wenn Sie in Ubuntu 20.04.5 oder höher auf die `.deb`-Paketdatei doppelklicken, wird das Snap Store-Installationsprogramm geöffnet. Dieses Installationsprogramm unterstützt keine Benutzereingaben. Sie müssen daher die Citrix Workspace-App über die Befehlszeile in einem Terminal oder mithilfe anderer Softwareinstallationsprogramme wie `gnome-software`, `gdebi` und `synaptics` installieren.

Anforderungen für die Microsoft Teams-Optimierung

Mindestversion:

- Citrix Workspace-App 2006

Software:

- `GStreamer` 1.0 oder höher und Cairo 2
- libc++-9.0 oder höher
- `libgdk` 3.22 oder höher
- OpenSSL 1.1.1d
- x64 Linux-Distribution

Hardware:

- Mindestens 1,8 GHz Dual-Core-CPU, die 720p HD-Auflösung während eines Peer-to-Peer-Videokonferenzanrufs unterstützen kann
- Dual- oder Quad-Core-CPU mit einer Basisgeschwindigkeit von 1,8 GHz und einer hohen Intel Turbo Boost Geschwindigkeit von mindestens 2,9 GHz

Verbesserung der Authentifizierung:

- `Libsecret`-Bibliothek
- libunwind-12-Bibliothek

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Anforderungen für die Servicekontinuität

Ab Version 2106 können Sie Servicekontinuität auf der Debian-Version der Citrix Workspace-App installieren.

Führen Sie die folgenden Befehle im Terminal aus, bevor Sie die Citrix Workspace-App installieren:

```
sudo apt-get update -y
```

Obligatorische vorinstallierte Bibliotheken:

- libwebkit2gtk-4.0-37 Version 2.30.1 oder höher
  - Wenn Sie Debian verwenden, führen Sie den folgenden Befehl aus:

    ```
    1 sudo apt-get install libwebkit2gtk-4.0-37
    2 <!--NeedCopy-->
    ```

  - Wenn Sie RPM verwenden, führen Sie den folgenden Befehl aus:

    ```
    1 sudo yum install libwebkit2gtk-4*
    2 <!--NeedCopy-->
    ```

  - Für Ubuntu, RHEL, SUSE, Fedora und Debian, empfiehlt Citrix, die neueste libwebkit2gtk-4.0-37 Version 2.30.1 oder höher zu installieren.
  - Für den Raspberry Pi mit Buster OS empfiehlt Citrix die Installation von libwebkit2gtk-4.0-37 Version 2.30.1.
- gnome-keyring Version 3.18.3 oder höher
  - Wenn Sie Debian verwenden, führen Sie den folgenden Befehl aus:

    ```
    1 sudo apt-get install gnome-keyring
    2 <!--NeedCopy-->
    ```

  - Wenn Sie RPM verwenden, führen Sie den folgenden Befehl aus:

    ```
    1 sudo yum install gnome-keyring
    2 <!--NeedCopy-->
    ```

- Libsecret
  - Wenn Sie Debian verwenden, führen Sie den folgenden Befehl aus:

    ```
    1 sudo apt-get install libsecret-1-0
    2 <!--NeedCopy-->
    ```

  - Wenn Sie RPM verwenden, führen Sie den folgenden Befehl aus:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
sudo yum install libsecret-1*
<!--NeedCopy-->
```

> **Hinweise:**
>
> Nach Version 1910 funktioniert die Citrix Workspace-App nur dann wie erwartet, wenn das Betriebssystem die folgenden GCC-Versionskriterien erfüllt:
>
> - GCC-Version für x64-Architektur: 4.8 oder höher
> - GCC-Version für ARMHF-Architektur: 4.9 oder höher
>
> Nach Version 2101 funktioniert die Citrix Workspace-App nur dann wie erwartet, wenn das Betriebssystem die folgenden Anforderungen erfüllt:
>
> - GCC Version 4.9 oder höher
> - `glibcxx` 3.4.20 oder höher
>
> Nach Version 2209 funktioniert die Citrix Workspace-App nur dann wie erwartet, wenn das Betriebssystem folgende Anforderung erfüllt:
>
> `glibcxx` 3.4.25 oder höher

Kompatibilitätsmatrix

Die Citrix Workspace-App ist mit allen derzeit unterstützten Versionen der folgenden Citrix-Produkte kompatibel.

Weitere Informationen zum Citrix Produktlebenszyklus und wann Citrix die Unterstützung bestimmter Produktversionen beendet, finden Sie unter Citrix Product Lifecycle Matrix.

Serveranforderungen

StoreFront

- Sie können alle derzeit unterstützten Versionen der Citrix Workspace-App für den Zugriff auf StoreFront-Stores über interne Netzwerkverbindungen und über Citrix Gateway verwenden:
  - StoreFront 1811 und höher.
  - StoreFront 3.12.
- Sie können StoreFront verwenden, das mit Workspace für Web konfiguriert wurde. Workspace für Web ermöglicht den Zugriff auf StoreFront-Stores über einen Webbrowser. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie unter Wichtige Überlegungen in der StoreFront-Dokumentation.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Verbindungen und Zertifikate

Verbindungen

Die Citrix Workspace-App für Linux unterstützt HTTPS- und ICA-über-TLS-Verbindungen über folgende Konfigurationen.

- LAN-Verbindungen:
  - StoreFront mit StoreFront Services oder Workspace für Web
- Für sichere Remote- oder lokale Verbindungen:
  - Citrix Gateway 12.0 und höher
  - NetScaler Gateway 10.1 und höher
  - NetScaler Access Gateway Enterprise Edition 10
  - NetScaler Access Gateway Enterprise Edition 9.x
  - NetScaler Access Gateway VPX

  Weitere Informationen zu den von StoreFront unterstützten Citrix Gateway-Versionen finden Sie unter den Systemanforderungen von StoreFront.

Zertifikate

Verwenden Sie die folgenden Zertifikate, um sichere Transaktionen zwischen Server und Client sicherzustellen:

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, muss das Stammzertifikat für die Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installiert sein. Diese Installation hilft beim Zugriff auf Citrix Ressourcen mit der Citrix Workspace-App.

> **Hinweis:**
>
> Eine Warnung über ein nicht vertrauenswürdiges Zertifikat wird angezeigt, wenn das Zertifikat des Remote-Gateways sich beim Herstellen der Verbindung nicht überprüfen lässt. Diese Überprüfung schlägt möglicherweise fehl, da das Stammzertifikat nicht im lokalen Schlüsselspeicher enthalten ist. Wenn Sie trotz Warnung fortfahren, werden die Apps zwar angezeigt, können jedoch nicht gestartet werden. Das Stammzertifikat muss im Zertifikatspeicher des Clients installiert werden.

Stammzertifikate

Für in Domänen eingebundene Maschinen verwenden Sie die administrative Gruppenrichtlinienobjektvorlage, um ZS-Zertifikate zu verteilen und als vertrauenswürdig einzustufen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Für nicht in Domänen eingebundene Maschinen erstellen Sie ein benutzerdefiniertes Installationspaket, um das ZS-Zertifikat zu verteilen und zu installieren. Wenden Sie sich bei Fragen an den Systemadministrator.

Installieren von Stammzertifikaten auf Benutzergeräten

Zur Verwendung von TLS benötigen Sie ein Stammzertifikat auf dem Benutzergerät, das die Signatur der Zertifizierungsstelle auf dem Serverzertifikat überprüfen kann. Standardmäßig unterstützt die Citrix Workspace-App die folgenden Zertifikate.

Zertifikat	Zertifizierungsstelle
Class4PCA_G2_v2.pem	Verisign Trust Network
Class3PCA_G2_v2.pem	Verisign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App unterstützt Zertifikate mit Platzhalterzeichen. Diese dürfen jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden.

Die Verwendung von Alternativen, z. B. von Zertifikaten mit einer Liste der Servernamen in der SAN-Erweiterung (Subject Alternative Name), kann in Betracht gezogen werden. Solche Zertifikate können von privaten und öffentlichen Zertifizierungsstellen ausgestellt werden.

Zwischenzertifikate und Citrix Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter Configuring Intermediate Certificates in der Citrix Gateway-Dokumentation.

Wenn der StoreFront-Server keine Zwischenzertifikate bereitstellen kann, die dem verwendeten Zertifikat entsprechen, oder wenn Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren, führen Sie diese Schritte aus, bevor Sie einen StoreFront-Store hinzufügen:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Rufen Sie separat ein oder mehr Zwischenzertifikate im PEM-Format ab.

   > **Tipp:**
   >
   > Wenn Sie kein Zertifikat mit der Dateierweiterung .pem finden können, verwenden Sie das Dienstprogramm `openssl`, um ein Zertifikat in eine Datei mit der Dateierweiterung .pem zu konvertieren.

2. Bei der Installation des Pakets (normalerweise root):

   a) Kopieren Sie eine oder mehrere Dateien zu $ICAROOT/keystore/intcerts.

   b) Führen Sie nach der Installation des Pakets den folgenden Befehl aus:

   ```
   $ICAROOT/util/ctx_rehash
   ```

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

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

> **Wichtig:**
>
> Bestätigen Sie vor der Installation der Citrix Workspace-App, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:
>
> - Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
> - Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
> - Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
> - Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet die Citrix Workspace-App alle Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie schon in früheren Versionen der Citrix Workspace-App wird überprüft, ob die Zertifikate vertrauenswürdig sind. Wenn eines der Zertifikate nicht vertrauenswürdig ist, schlägt die Verbindung fehl.

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

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

Wenn ein Gateway mit diesen gültigen Zertifikaten konfiguriert ist, erreichen Sie mit der folgenden Konfiguration eine strengere Validierung. Diese Konfiguration bestimmt genau, welches Stammzertifikat von der Citrix Workspace-App verwendet wird:

- Beispielserverzertifikat

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Beispielzwischenzertifikat
- Beispielstammzertifikat

Die Citrix Workspace-App stellt sicher, dass alle Zertifikate gültig sind. Citrix Workspace-App überprüft ebenfalls, dass dem Beispielstammzertifikat bereits vertraut wird. Wenn die Citrix Workspace-App dem Beispielstammzertifikat nicht vertraut, schlägt die Verbindung fehl.

> **Wichtig:**
>
> - Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet. Beispielsweise gibt es derzeit zwei Zertifikate (DigiCert/GTE CyberTrust Global Root und DigiCert Baltimore Root/Baltimore CyberTrust Root), mit denen die gleichen Serverzertifikate validiert werden können. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar (DigiCert Baltimore Root/Baltimore CyberTrust Root).
> - Wenn Sie "GTE CyberTrust Global Root" auf dem Gateway konfigurieren, schlagen die Citrix Workspace-App-Verbindungen auf diesen Benutzergeräten fehl. Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist. Beachten Sie außerdem, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.
> - Einige Server und Gateways senden nie das Stammzertifikat, selbst wenn es konfiguriert ist. Ein strengere Validierung ist dann nicht möglich.

Wenn ein Gateway mit diesen gültigen Zertifikaten konfiguriert ist, können wir die folgende Konfiguration ohne Stammzertifikat verwenden:

- Beispielserverzertifikat
- Beispielzwischenzertifikat

Citrix Workspace-App verwendet diese beiden Zertifikate. Die App sucht nach einem Stammzertifikat auf dem Benutzergerät. Wenn die Citrix Workspace-App ein Stammzertifikat findet, das korrekt validiert und dem vertraut wird (z. B. Beispielstammzertifikat), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt das von der Citrix Workspace-App benötigte Zwischenzertifikat zur Verfügung, ermöglicht der Citrix Workspace-App aber auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

Wenn ein Gateway ist mit den folgenden Zertifikaten konfiguriert wurde:

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Falsches Stammzertifikat

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

- Beispielserverzertifikat
- Beispielzwischenzertifikat 1
- Beispielzwischenzertifikat 2

> **Wichtig:**
>
> - Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat. Dieses Zertifikat wird verwendet, wenn mehrere Stammzertifikate vorhanden sind, die zu unterschiedlichen Zeiten ausgestellt und gleichzeitig verwendet werden. In diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden. Beispielsweise hat das früher ausgestellte Stammzertifikat *Class 3 Public Primary Certification Authority* das entsprechende übergreifende Zwischenzertifikat *Verisign Class 3 Public Primary Certification Authority - G5*. Ein entsprechendes später ausgestelltes Stammzertifikat *Verisign Class 3 Public Primary Certification Authority - G5* ist ebenfalls verfügbar und es ersetzt *Class 3 Public Primary Certification Authority*. Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.
> - Das übergreifende Zwischenzertifikat und das Stammzertifikat haben den gleichen Antragstellernamen (Ausgestellt an). Das übergreifende Zwischenzertifikat hat jedoch einen anderen Ausstellernamen (Ausgestellt durch). Dadurch unterscheidet sich das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat (wie Beispielzwischenzertifikat 2).

Diese Konfiguration, ohne das Stammzertifikat und das übergreifende Zwischenzertifikat, wird empfohlen:

- Beispielserverzertifikat
- Beispielzwischenzertifikat

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

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Übergreifendes Beispielzwischenzertifikat [nicht empfohlen]

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

- Beispielserverzertifikat

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Unterstützte Systemzertifikatpfade für SSL-Verbindungen

Version 2308 der Citrix Workspace-App unterstützt Systemzertifikatpfade für SSL-Verbindungen. Dieses Feature vereinfacht die clientseitige Zertifikatsverwaltung und verbessert die Benutzererfahrung. Mit diesem Feature kann Citrix Workspace eine TLS-Verbindung mit dem Zertifikat im Systemzertifikatpfad herstellen. Dieses Feature ist standardmäßig aktiviert.

Workspacecheck

Wir stellen das Skript workspacecheck.sh als Teil des Citrix Workspace-App-Installationspakets bereit. Das Skript überprüft, ob das Gerät alle Systemanforderungen erfüllt, um die gesamte Funktionalität der Citrix Workspace-App zu unterstützen. Das Skript ist im Verzeichnis `Utilities` im Installationspaket.

Ausführen des Skripts workspacecheck.sh

1. Öffnen Sie das Terminal auf Ihrer Linux-Maschine.
2. Geben Sie `cd $ICAROOT/util` ein und drücken Sie die **EINGABETASTE**, um zum Verzeichnis `Utilities` des Installationspakets zu navigieren.
3. Geben Sie `./workspacecheck.sh` ein, um das Skript auszuführen.

Anwendungen und Betriebssysteme, für die kein Support mehr angeboten wird

Citrix bietet keinen Support für Anwendungen und Betriebssysteme, die von ihren Anbietern nicht mehr unterstützt werden.

Aus diesem Grund bewertet Citrix bei jedem gemeldeten Problem, ob es sich direkt auf nicht unterstützte Anwendungen oder Betriebssysteme bezieht. Hierfür werden Sie unter Umständen von Citrix gebeten, ein Problem mit der unterstützten Version der Anwendung oder des Betriebssystems zu reproduzieren. Wenn das Problem mit nicht unterstützten Anwendungen oder Betriebssystemen verbunden zu sein scheint, untersucht Citrix das Problem nicht weiter.

Installieren, Deinstallieren und Aktualisieren

September 12, 2023

Sie können die Citrix Workspace-App installieren, wenn Sie die Datei von der Citrix-Website unter Downloads herunterladen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Version der Citrix Workspace-App verifizieren

Führen Sie die folgenden Schritte aus, um die aktuelle Version der auf Ihrem System installierten Citrix Workspace-App zu verifizieren:

1. Öffnen Sie ein Terminal-Fenster.
2. Führen Sie den folgenden Befehl aus:

   Für Debian-Pakete:

   ```
   dpkg --list | grep -i icaclient
   <!--NeedCopy-->
   ```

   ODER

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

   Für Red Hat-Pakete:

   ```
   rpm -qa | grep -i icaclient

   <!--NeedCopy-->
   ```

   ODER

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

   Für Tarball-Pakete:

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

Manuelle Installation

Laden Sie die folgenden Pakete von der Seite Citrix Downloads herunter.

Debian-Pakete

Installieren Sie das Paket `Icaclient` basierend auf Ihrer Betriebssystemarchitektur.

Um die generische USB-Umleitung zu verwenden, installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `ctxusb`-Pakete.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Um das Kompatibilitätsproblem zu vermeiden, installieren Sie dieselbe Version der Pakete `Icaclient` und `ctxusb`.

Paketname	Inhalt
Debian-Pakete (Ubuntu, Debian, Linux Mint usw.)	
`icaclient_<version>_amd64.deb`	Self-Service-Support, 64 Bit, x86_64
`icaclient_<version>_i386.deb`	Self-Service-Support, 32 Bit, x86
`icaclient_<version>_armhf.deb`	Self-Service-Support, ARM HF
`ctxusb_<version>_amd64.deb`	USB-Paket, 64 Bit, x86_64
`ctxusb_<version>_i386.deb`	USB-Paket, 32 Bit, x86
`ctxusb_<version>_armhf.deb`	USB-Paket, ARM HF

Installation mit einem Debian-Paket

> **Voraussetzungen:**
>
> Stellen Sie sicher, dass Sie alle erforderlichen Systemanforderungen installiert haben, wie im Abschnitt Systemanforderungen beschrieben.

Wenn Sie die Citrix Workspace-App mit dem Debian-Paket unter Ubuntu installieren, öffnen Sie die Pakete im Ubuntu Software Center.

Ersetzen Sie in den folgenden Anweisungen
packagename durch den Namen des Pakets, das Sie installieren möchten.

Für diese Vorgehensweise werden eine Befehlszeile und der native Paketmanager für Ubuntu, Debian oder Mint verwendet. Sie können das Paket auch durch Doppelklicken auf das heruntergeladene DEB-Paket in einem Dateibrowser installieren. Dadurch wird in der Regel ein Paketmanager gestartet, der fehlende erforderliche Software herunterlädt. Falls kein Paketmanager verfügbar ist, empfiehlt Citrix das Befehlszeilentool **gdebi**.

> **Hinweis:**
>
> Wenn Sie in Ubuntu 20.04.5 oder höher auf die `.deb`-Paketdatei doppelklicken, wird das Snap Store-Installationsprogramm geöffnet. Dieses Installationsprogramm unterstützt keine Benutzereingaben. Sie müssen daher die Citrix Workspace-App über die Befehlszeile in einem Terminal oder mithilfe anderer Softwareinstallationsprogramme wie `gnome-software`, `gdebi`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> und `synaptics` installieren.

Installieren des Pakets an der Befehlszeile:

1. Melden Sie sich als privilegierter Benutzer (root) an.
2. Öffnen Sie ein Terminal-Fenster.
3. Führen Sie die Installation mit einem der folgenden Befehle aus:

   - `apt` — Verwenden Sie den folgenden Befehl, um die Citrix Workspace-App mit Abhängigkeiten zu installieren:

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

     Führen Sie den folgenden Befehl aus, um das USB-Paket zu installieren:

     ```
     sudo apt install -f ctxusb_<version>._amd64.deb
     <!--NeedCopy-->
     ```

   - `dpkg -i` — Verwenden Sie den folgenden Befehl, um die Citrix Workspace-App zu installieren:

     ```
     sudo dpkg -i icaclient_<version>_amd64.deb
     sudo apt-get -f install
     <!--NeedCopy-->
     ```

     Führen Sie den folgenden Befehl aus, um das USB-Paket zu installieren:

     ```
     sudo dpkg -i ctxusb_<version>_amd64.deb
     sudo apt-get -f install
     <!--NeedCopy-->
     ```

   - `gdebi` — Verwenden Sie den folgenden Befehl, um die Citrix Workspace-App zu installieren:

     ```
     gdebi icaclient_<version>_amd64.deb
     <!--NeedCopy-->
     ```

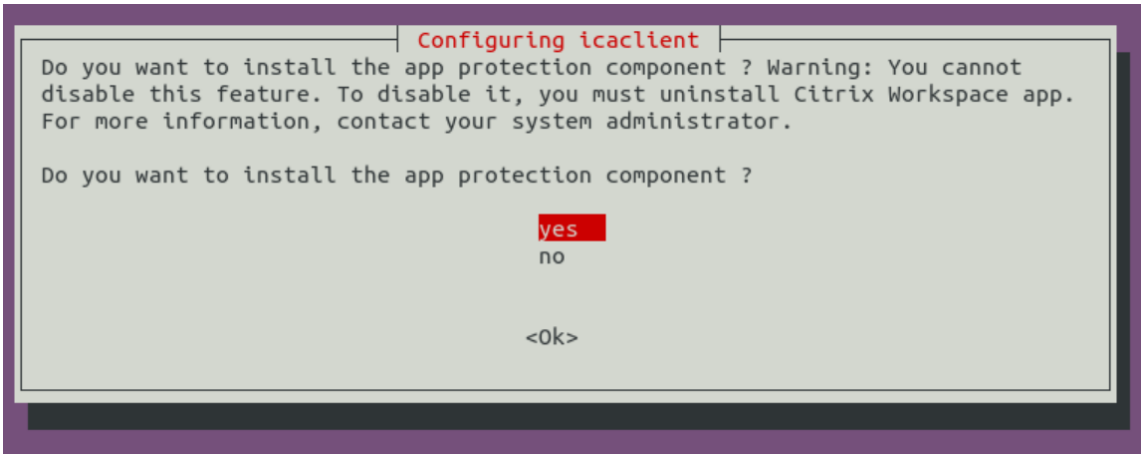
     Führen Sie den folgenden Befehl aus, um das USB-Paket zu installieren:

     ```
     gdebi ctxusb_<version>_amd64.deb
     <!--NeedCopy-->
     ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Das `ctxusb`-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.

4. Ab Version 2101 werden Sie über folgende interaktive Meldung aufgefordert, App Protection zu installieren:



5. Wählen Sie **Ja**, um mit der Installation der App Protection-Komponente fortzufahren.

Automatische Installation der App Protection-Komponente bei Debian-Paketen

Ab Version 2102 wird der App-Schutz von der Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie für die unbeaufsichtigte Installation der App-Schutzkomponente den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

```
export DEBIAN_FRONTEND="noninteractive"
<!--NeedCopy-->
```

```
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
<!--NeedCopy-->
```

```
sudo debconf-show icaclient
<!--NeedCopy-->
```

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

<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Red Hat-Pakete

Installieren Sie das Paket `ICAClient` basierend auf Ihrer Betriebssystemarchitektur.

Um die generische USB-Umleitung zu verwenden, installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der `ctxusb`-Pakete.

> **Hinweis:**
>
> Um das Kompatibilitätsproblem zu vermeiden, installieren Sie dieselbe Version der Pakete `Icaclient` und `ctxusb`.

Paketname	Inhalt
Redhat-Pakete (Redhat, SUSE, Fedora usw.)	
`ICAClient-rhel-<version>.x86_64.rpm`	Self-Service-Support, basierend auf Red Hat (einschl. Linux VDA), 64 Bit, x86_64
`ICAClient-rhel-<version>.i386.rpm`	Self-Service-Support, basierend auf Red Hat, 32 Bit, x86
`ICAClient-suse-<version>.x86_64.rpm`	Self-Service-Support, basierend auf SUSE, 64 Bit, x86_64
`ICAClient-suse-<version>.i386.rpm`	Self-Service-Support, basierend auf SUSE, 32-Bit, x86
`ctxusb-<version>.x86_64.rpm`	USB-Paket, 64 Bit, x86_64
`ctxusb-<version>.i386.rpm`	USB-Paket, 32 Bit, x86

> **Hinweis:**
>
> Das RPM-Paket `SuSE 11 SP3 Full Package (Self-Service Support)` ist veraltet.

Installation mit einem RPM-Paket

Wenn Sie die Citrix Workspace-App vom RPM-Paket auf SUSE installieren, verwenden Sie das Hilfsprogramm YaST oder Zypper. Das RPM-Dienstprogramm installiert das `.rpm`-Paket. Ein Fehler tritt auf, wenn die erforderlichen Abhängigkeiten fehlen.

> **Tipp:**
>
> RPM Package Manager installiert keine fehlende erforderliche Software.
>
> - Kunden, die SUSE verwenden, können die Software über die Befehlszeile in OpenSUSE mit `zypper install <file name>` herunterladen und installieren.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> - Kunden, die Red Hat verwenden, laden die Software mit `yum localinstall <filename>` in Fedora/Red Hat herunter und installieren sie.

Installation von einem RPM-Paket

> **Voraussetzungen:**
>
> Stellen Sie sicher, dass Sie alle erforderlichen Systemanforderungen installiert haben, wie im Abschnitt Systemanforderungen beschrieben.

1. Richten Sie das EPEL-Repository ein.

   > **Hinweis:**
   >
   > Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA erfolgreich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen.

2. Melden Sie sich als privilegierter Benutzer (root) an.
3. Öffnen Sie ein Terminal-Fenster.
4. Führen Sie die Installation der folgenden drei Pakete aus, indem Sie “Zypper” in eingeben.

   > **Hinweis:**
   >
   > - `ctxusb` ist ein optionales Paket. Installieren Sie das Paket zur Unterstützung der generischen USB-Umleitung.
   > - `ctxappprotection` ist ein optionales Paket. Installieren Sie das Paket nur, wenn Sie die App-Schutzkomponente installieren möchten.

   Für SUSE-Installationen:

   - `zypper in ICAClient-suse-<version>.x86_64.rpm`
   - `zypper in ctxusb-<version>.x86_64.rpm`
   - `zypper in ctxappprotection-<version>.x86_64.rpm`

   Für Red Hat-Installationen:

   - `yum localinstall ICAClient-rhel-<version>.x86_64.rpm`
   - `yum localinstall ctxusb-<version>.x86_64.rpm`
   - `yum localinstall ctxappprotection-<version>.x86_64.rpm`

Installieren eines fehlenden Pakets

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Fügen Sie ein EPEL-Repository hinzu (Details unter https://docs.fedoraproject.org/en-US/epel/), wenn bei einer auf Red Hat basierenden Distribution (RHEL, CentOS, Fedora usw.) die folgende Fehlermeldung angezeigt wird:

```
1  "… requires libwebkitgtk-1.0.so.0"
```

Tarball-Pakete

Installieren Sie entsprechend Ihrer Betriebssystemarchitektur eines der folgenden Pakete.

Paketname	Inhalt
Tarballs (Skriptinstallation für jede Distribution)	
`linuxx64-<version>.tar.gz`	64 Bit Intel
`linuxx86-<version>.tar.gz`	32 Bit Intel
`linuxarmhf-<version>.tar.gz`	ARM HF

> **Hinweis:**
>
> - Wenn Sie den Installationsort anpassen möchten, installieren Sie die Citrix Workspace-App vom Tarball-Paket. Wenn Sie erforderliche Pakete automatisch installieren möchten, installieren Sie die Citrix Workspace-App aus dem Debian-Paket oder dem RPM-Paket.
> - Verwenden Sie nicht zwei unterschiedliche Installationsmethoden auf derselben Maschine. Andernfalls kann es zu Fehlermeldungen und unerwünschtem Verhalten kommen.

Installation mit einem Tarball-Paket

> **Hinweis:**
>
> Das Tarball-Paket führt keine Abhängigkeitenprüfung durch und installiert auch keine Abhängigkeiten. Alle Systemabhängigkeiten müssen separat gelöst werden.

1. Öffnen Sie ein Terminal-Fenster.
2. Extrahieren Sie den Inhalt der `.tar.gz`-Datei in ein leeres Verzeichnis. Geben Sie beispielsweise Folgendes ein: `tar xvfz packagename.tar.gz`.
3. Geben Sie `./setupwfc` ein und drücken Sie die Eingabetaste, um das Setupprogramm auszuführen.
4. Akzeptieren Sie den Standardwert `1` (Citrix Workspace-App installieren) und drücken Sie die **Eingabetaste**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. Geben Sie den Pfad und den Namen des gewünschten Installationsverzeichnisses ein und drücken Sie die Eingabetaste. Oder drücken Sie die Eingabetaste, um die Citrix Workspace-App im Standardverzeichnis zu installieren.

   Das Standardverzeichnis für Installationen durch privilegierte Benutzer (root) ist `/opt/Citrix/ICAClient`.

   Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist `$HOME/ICAClient/platform`. "platform" ist ein systemgenerierter Bezeichner des installierten Betriebssystems, z. B. `$HOME/ICAClient/linuxx86` für die Linux/x86-Plattform.

   > **Hinweis:**
   >
   > Wenn Sie einen anderen Speicherort als den Standardspeicherort verwenden, legen Sie ihn in $ICAROOT in `$HOME/.profile` oder `$HOME/.bash\\_profile` fest.

6. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie `y` ein und drücken Sie die Eingabetaste.

7. Wählen Sie, ob die Citrix Workspace-App in die Desktopumgebung integriert werden soll. Die Installation erstellt eine Menüoption, über die Benutzer die Citrix Workspace-App starten können. Geben Sie an der Eingabeaufforderung `y` ein, um die Integration zu aktivieren.

8. Wenn Sie `GStreamer` bereits installiert haben, können Sie entscheiden, ob Sie `GStreamer` in die Citrix Workspace-App integrieren und damit die HDX MediaStream-Multimediabeschleunigung bereitstellen. Zur Integration von `GStreamer` in die Citrix Workspace-App geben Sie an der Eingabeaufforderung `y` ein.

   > **Hinweis:**
   >
   > Auf einigen Plattformen kann die Installation des Clients mit einem Tarball-Paket dazu führen, dass das System nicht mehr reagiert, nachdem Sie zur Integration mit KDE und GNOME aufgefordert wurden. Das Problem tritt bei der ersten Initialisierung von gstreamer-0.10 auf. Wenn dieses Problem auftritt, brechen Sie den Installationsvorgang mit Strg+C ab und führen Sie den folgenden Befehl aus: `gst-inspect-0.10 -- gst-disable-registry-fork --version`. Nach dem Ausführen des Befehls können Sie das Tarball-Paket erneut ausführen, ohne dass das Problem auftritt.

9. Wenn Sie sich als privilegierter Benutzer (root) anmelden, können Sie entscheiden, ob Sie die USB-Unterstützung für mit Citrix Virtual Apps and Desktops bzw. Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) veröffentlichte VDI-Anwendungen aktivieren möchten. Geben Sie an der Eingabeaufforderung `y` ein, um die USB-Unterstützung zu installieren.

   > **Hinweis:**
   >
   > Wenn Sie nicht als privilegierter Benutzer (root) angemeldet sind, wird die folgende War-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> nung angezeigt:
>
> "USB-Unterstützung kann nur von Root-Benutzern installiert werden. Führen Sie den Installer als root aus, um diese Option installieren zu können."

10. Nach Abschluss der Installation wird das Hauptinstallationsmenü wieder angezeigt. Geben Sie zum Beenden des Setups 3 ein und drücken Sie die Eingabetaste.

Deinstallieren

Die Umgebungsvariable ICAROOT muss für das Installationsverzeichnis des Clients festgelegt sein. Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist `$HOME/ICAClient/platform`. Die Variable "platform" ist ein systemgenerierter Bezeichner des installierten Betriebssystems, z. B. `$HOME/ICAClient/linuxx86` für die Linux/x86-Plattform. Das Standardverzeichnis für Installationen durch privilegierte Benutzer ist `/opt/Citrix/ICAClient`.

> **Hinweise:**
>
> - Um die Citrix Workspace-App zu deinstallieren, müssen Sie als der Benutzer angemeldet sein, der die Installation durchgeführt hat.
> - Wenn Sie die Citrix Workspace-App deinstallieren, werden veraltete Cachedateien unter `$HOME/.local/share/webkitgtk` möglicherweise nicht automatisch entfernt. Entfernen Sie als Workaround die Cachedateien manuell.

Deinstallieren der Citrix Workspace-App von dem Tarball-Paket

1. Führen Sie das Setupprogramm aus. Geben Sie hierfür `$ICAROOT/setupwfc` ein und drücken Sie die Eingabetaste.
2. Geben Sie zum Entfernen des Clients 2 ein und drücken Sie die **Eingabetaste**.

Deinstallieren der Citrix Workspace-App von Debian-/Ubuntu-Betriebssystemen

1. Öffnen Sie ein Terminal-Fenster.
2. Führen Sie die Installation mit einem der folgenden Befehle aus:

```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt autoremove -y
<!--NeedCopy-->
```

ODER

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt purge icaclient -y
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können das Debian-Paket auch mit den Standardwerkzeugen Ihres Betriebssystems entfernen.

Deinstallieren der Citrix Workspace-App von Fedora-/RHEL-/CentOS-Betriebssystemen

1. Öffnen Sie ein Terminal-Fenster.
2. Führen Sie die Installation mit dem folgenden Befehl aus:

```
yum remove icaclient -y
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können das RPM-Paket auch mit den Standardtools Ihres Betriebssystems entfernen.

Überprüfen Sie, ob die Deinstallation der Citrix Workspace-App erfolgreich war. Weitere Informationen finden Sie im Abschnitt Version der Citrix Workspace-App verifizieren.

Aktualisieren

Überprüfen Sie vor dem Aktualisieren der Citrix Workspace-App die aktuelle Version der Citrix Workspace-App, die auf Ihrem System installiert ist. Weitere Informationen finden Sie im Abschnitt Version der Citrix Workspace-App verifizieren.

Zum Aktualisieren auf eine neuere Version der Citrix Workspace-App laden Sie die aktuelle Version der Citrix Workspace-App von Citrix Downloads herunter und installieren Sie sie. Führen Sie zur Installation die im folgenden Installationsabschnitt beschriebenen Schritte aus:

- Debian-Pakete
- Red Hat-Pakete
- Tarball-Pakete

Wenn die Citrix Workspace-App in Ihrem System installiert ist, erkennt das System die vorhandene App und aktualisiert sie auf eine neuere Version. Bei Tarball-Paketen kann es jedoch vorkommen, dass Sie eine frühere Version der App in einem Ordner und die neuere Version der App in einem anderen Ordner

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

installiert haben. In diesem Szenario sind möglicherweise beide Versionen der App in Ihrem System vorhanden.

Die **Citrix Workspace**-Bildschirmüberlagerung wird beim ersten Start der App, beim Aktualisieren sowie bei der Deinstallation und Neuinstallation der App angezeigt. Klicken Sie auf **Verstanden**, um die Citrix Workspace-App weiter zu verwenden, oder klicken Sie auf **Weitere Informationen**, um weitere Informationen zu erhalten.

Erste Schritte

September 12, 2023

Dieser Artikel ist ein Referenzdokument, das Ihnen den Einstieg in die Citrix Workspace-App für Linux erleichtert.

Überprüfen Sie die aktuelle Version der Citrix Workspace-App, die auf Ihrem System installiert ist. Weitere Informationen finden Sie im Abschnitt “Version der Citrix Workspace-App verifizieren”.](/en-us/citrix-workspace-app-for-linux/install.html#verify-the-version-of-the-citrix-workspace-app).

Store

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

Weitere Informationen zu Stores finden Sie in der StoreFront-Dokumentation.

Arten von Stores

Sie können die folgenden Arten von Stores in der Citrix Workspace-App hinzufügen:

- Workspace
- StoreFront
- Citrix Gateway Store
- Benutzerdefinierter Webstore

Workspace

Citrix Workspace ist ein cloudbasierter Unternehmensappstore, der sicheren und einheitlichen Zugriff auf Apps, Desktops und Ressourcen bzw. Inhalte von überall und auf jedem Gerät bietet. Ressourcen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

können Citrix DaaS, Inhalts-Apps, lokale und mobile Apps, SaaS- und Web-Apps sowie Browser-Apps sein. Weitere Informationen finden Sie unter Citrix Workspace.

StoreFront

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

Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Citrix Gateway Store

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

Benutzerdefinierte Webstores

Ab Version 2203 können Sie auf den benutzerdefinierten Webstore Ihrer Organisation über die Citrix Workspace-App zugreifen.

Verwendung des Features, wenn der Global App Configuration Service verfügbar ist:

Der Administrator muss die Domäne oder den benutzerdefinierten Webstore der Liste der zulässigen URLs im Global App Configuration Service hinzufügen. Nachdem Sie die Domäne oder den benutzerdefinierten Webstore hinzugefügt haben, geben Sie die URL des benutzerdefinierten Webstores oder die E-Mail-Adresse im Bildschirm **Konto hinzufügen** in der Citrix Workspace-App an. Der benutzerdefinierte Webstore wird im nativen Workspace-App-Fenster geöffnet.

Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter Global App Configuration Service.

> **Hinweis:**
>
> Das Feature zum Pinnen des Bildschirmlayouts im Multimonitormodus wird im benutzerdefinierten Webstore nicht unterstützt.

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**.

Als Voraussetzung müssen Sie den benutzerdefinierten Webstore in der Datei `AuthManConfig.xml` aktivieren. Aktivieren der Option

1. Navigieren Sie zur Konfigurationsdatei `$ICAROOT/config/AuthManConfig.xml`.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. Fügen Sie die folgenden Einträge hinzu:

```
<key>AppConfigEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

Verwendung des Features, wenn der Global App Configuration Service nicht verfügbar ist:

Führen Sie die folgenden Konfigurationsänderungen durch:

1. Navigieren Sie zur Konfigurationsdatei `$ICAROOT/config/AuthManConfig.xml`.
2. Fügen Sie die folgenden Einträge hinzu:

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

3. Fügen Sie die Liste der URLs, die für den benutzerdefinierten Webstore berücksichtigt werden müssen, wie folgt hinzu.

```
<AllowedWebStoreCache>
<value><URL1></value>
<value><URL2></value>
..
<value>....</value>
</AllowedWebStoreCache>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können nur die in der Datei `AuthManConfig.xml` aufgelisteten URLs für den benutzerdefinierten Webstore verwenden. Sie können der Datei `AuthManConfig.xml` weitere URLs hinzufügen, die für den benutzerdefinierten Webstore gelten sollen.

Store-URL zur Citrix Workspace-App hinzufügen

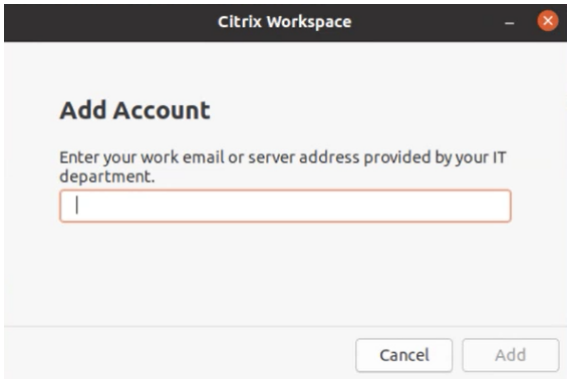
Sie können Benutzern wie folgt die Kontoinformationen mitteilen, die sie zum Zugriff auf die virtuellen Anwendungen und Desktops benötigen:

- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen
- Konfigurieren der e-mail-basierten autmatischen Discovery
- Hinzufügen von Stores über die Befehlszeilenschnittstelle

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

Nach erfolgreicher Installation der Citrix Workspace-App und wenn Sie die App zum ersten Mal starten, 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`.
- Um eine Verbindung über Citrix Gateway herzustellen, teilen Sie Benutzern den vollqualifizierten Domänennamen von Citrix Gateway mit.

Automatische Storesuche per E-Mail-Adresse

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

Um das Feature zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zur Datei `$ICAROOT/config/AuthManConfig.xml`.
2. Legen Sie für den folgenden Eintrag “false” fest.

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Hinzufügen von Stores über die Befehlszeilenschnittstelle

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

Weitere Informationen finden Sie unter Storebrowse.

Einrichten

Sie können das Installationspaket herunterladen, die Konfiguration anpassen und dann die Citrix Workspace-App installieren.

Sie können den Inhalt des Citrix Workspace-App-Pakets ändern und die Dateien anschließend neu verpacken.

Anpassen der Installation

1. Entpacken Sie das Citrix Workspace-App-Paket in einem leeren Verzeichnis. Die Paketdatei heißt platform.major.minor.release.build.tar.gz (z. B. `linuxx86-<version>.tar.gz` für die Plattform Linux/x86).
2. Nehmen Sie die erforderlichen Änderungen am Citrix Workspace-App-Paket vor. Sie können dem Paket beispielsweise ein TLS-Stammzertifikat hinzufügen, um ein Zertifikat einer Zertifizierungsstelle zu verwenden, die nicht Teil der Standardinstallation der Citrix Workspace-App ist.
3. Öffnen Sie die Datei `PkgID`.
4. Fügen Sie folgende Zeile hinzu, um anzuzeigen, dass das Paket bearbeitet worden ist:

   MODIFIED=traceinfo

   wobei `traceinfo` Informationen darüber enthält, wer die Änderung vorgenommen hat und wann.
5. Speichern und schließen Sie die Datei.
6. Öffnen Sie die Dateiliste des Pakets Plattform/Plattform.psf (z. B. linuxx86/linuxx86.psf für die Plattform Linux/x86).
7. Aktualisieren Sie die Dateiliste des Pakets, um Ihre Änderungen aufzunehmen. Ohne Aktualisierung kann bei der Installation des neuen Pakets en Fehler auftreten. Beispielsweise können Sie die Größe der geänderten Dateien aktualisieren oder neue Zeilen hinzufügen für Dateien, die Sie dem Paket hinzugefügt haben. Im Folgenden werden die Spaltentitel der Dateiliste des Pakets aufgeführt:

   - Dateityp
   - Relativer Pfad

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Unterpaket (immer auf `cor` einzustellen)
- Berechtigungen
- Besitzer
- Gruppe
- Größe

8. Speichern und schließen Sie die Datei.
9. Verwenden Sie den Befehl tar, um die Paketdatei der Citrix Workspace-App neu zu erstellen. Zum Beispiel `tar czf ../newpackage.tar.gz *`, wobei `newpackagez` der Name der neuen Paketdatei der Citrix Workspace-App ist.

Aktuelle Webkitunterstützung

Die Citrix Workspace-App für Linux erfordert libwebkit2gtk (2.16.6+).

libwebkit2gtk hat folgende Vorteile:

- Verbesserte Benutzeroberfläche. webkit2gtk ist mit der Funktion für die Browserinhaltsumleitung kompatibel. Verwenden Sie webkit2gtk Version 2.24 und höher für ein besseres YouTube-Erlebnis.
- webkit2gtk Version 2.16.6 und höher verbessert und beschleunigt die Anmeldeerfahrung.
- Die App funktioniert besser mit den neueren Linux-Distributionen und umfasst die neuesten Webkit-Sicherheitsupdates.

> **Hinweis:**
>
> Auf einigen Linux-Distributionen ist webkit2gtk nicht verfügbar. Als Workaround gibt es die folgenden Optionen:
>
> - Erstellen Sie das webkit2gtk aus der Quelle, bevor Sie die Citrix Workspace-App Version 1906 installieren.
> - Wechseln Sie zu einer neueren Linux-Distribution, die webkit2gtk 2.16.6 oder höher unterstützt.

Start

Sie können die Citrix Workspace-App entweder an einer Terminal-Eingabeaufforderung oder von einer der unterstützten Desktopumgebungen aus starten.

Die Umgebungsvariable `ICAROOT` muss auf das richtige Installationsverzeichnis verweisen.

> **Tipp:**

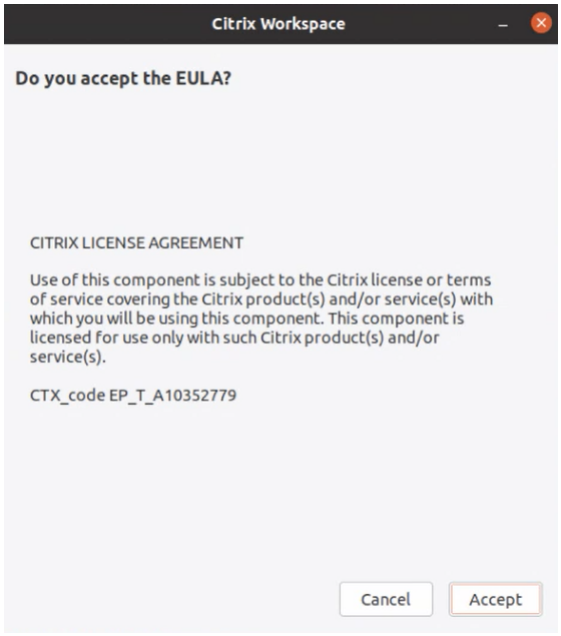
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Die folgenden Anweisungen gelten nicht für mit Webpaketen und Tarball ausgeführte Installationen. Die Anweisung gilt, wenn die Anforderungen für den Self-Service nicht erfüllt sind.

Terminal-Eingabeaufforderung

Starten der Citrix Workspace-App an der Terminal-Eingabeaufforderung:

1. Geben Sie ein: `/opt/Citrix/ICAClient/selfservice`
2. Drücken Sie dann die Eingabetaste. Hierbei ist /opt/Citrix/ICAClient das Verzeichnis, in dem Sie die Citrix Workspace-App installiert haben.
   Das Dialogfeld **Akzeptieren Sie die EULA?** wird angezeigt.



3. Klicken Sie auf **Akzeptieren**, um mit dem Hinzufügen des Stores fortzufahren.

> **Hinweis:**
>
> **Akzeptieren Sie die EULA?** wird nur angezeigt, wenn Sie nach der Installation zum ersten Mal auf die Citrix Workspace-App für Linux zugreifen.

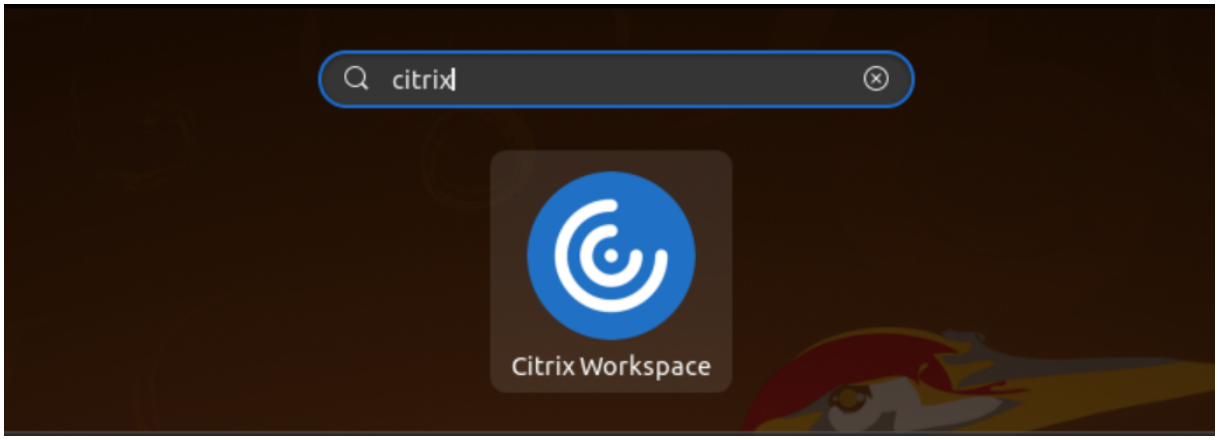
Linux-Desktop

Mit einem Dateimanager können Sie die Citrix Workspace-App von einer Desktopumgebung für Linux aus starten.

Auf einigen Desktops können Sie die Citrix Workspace-App auch über ein Menü starten. Die Citrix Workspace-App ist, je nach Linux-Distribution, in unterschiedlichen Menüs verfügbar.

Unter Ubuntu wird das Citrix Workspace-App-Symbol wie folgt angezeigt:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Einstellungen

Sie legen Einstellungen fest, indem Sie im Citrix Workspace-App-Menü auf **Einstellungen** klicken. Folgendes lässt sich hier steuern:

- Anzeige von Desktops
- Verbindung zu verschiedenen Anwendungen und Desktops
- Verwalten des Datei- und Gerätezugriffs

Verwalten eines Kontos

Für den Zugriff auf Desktops und Anwendungen benötigen Sie ein Konto bei Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Sites (ehemals Citrix Virtual Apps and Desktops Service). Ihr IT-Helpdesk fordert Sie u. U. auf, zu diesem Zweck ein Konto zu Citrix Workspace hinzuzufügen. Oder Sie werden aufgefordert, einen anderen Citrix Gateway- oder Access Gateway-Server für ein vorhandenes Konto zu verwenden. Sie können Konten auch aus Citrix Workspace entfernen.

1. Führen Sie auf der Seite **Konten** im Dialogfeld **Einstellungen** einen der folgenden Schritte aus:
   - Klicken Sie auf **Hinzufügen**, um ein Konto hinzuzufügen. Wenden Sie sich an Ihren Systemadministrator, um weitere Informationen zu erhalten.
   - Zum Ändern der Details eines von dem Konto verwendeten Stores, z. B. des Standardgateways, klicken Sie auf **Bearbeiten**.
   - Zum Entfernen eines Kontos klicken Sie auf **Entfernen**.
2. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen. Wenn Sie dazu aufgefordert werden, authentifizieren Sie sich beim Server.

Desktopanzeige

Sie können Desktops über den ganzen Bildschirm hinweg auf dem Benutzergerät anzeigen (Vollbildmodus, Standardeinstellung) oder im Fenstermodus, d. h. in einem separaten Fenster.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wählen Sie im Dialogfeld **Einstellungen** auf der Seite **Allgemein** einen Modus mit der Option **Anzeige für Desktops**.

Verwenden Sie die Symbolleistenfunktion zum **Aktivieren des Desktop Viewer**, um die Fensterkonfiguration Ihrer Remotesitzung dynamisch zu ändern.

Desktop Viewer

Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern.

Verwenden Sie Desktop Viewer für die Interaktion der Benutzer mit dem virtuellen Desktop. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario können Benutzer mit der Symbolleistenfunktionalität von **Desktop Viewer** in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore. Benutzer können zwischen Desktopsitzungen wechseln und auf einem Benutzergerät mehrere Desktops über mehrere Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Verbindungen verwenden. Zur bequemen Verwaltung einer Benutzersitzung gibt es Schaltflächen zum Minimieren aller Desktopsitzungen, zum Übermitteln der Tastenkombination Strg+Alt+Entf, zum Trennen der Sitzung und zum Abmelden.

Durch Drücken von **Strg+Alt+Untbr** werden die Schaltflächen der **Desktop Viewer**-Symbolleiste in einem Popup-Fenster angezeigt.

Automatische Sitzungswiederverbindung

Die Citrix Workspace-App kann Desktops und Anwendungen, deren Verbindung getrennt wurde, wiederverbinden. Dies kann beispielsweise bei einem Problem mit der Netzwerkinfrastruktur erforderlich sein.

- Wählen Sie auf der Seite **Allgemein** im Dialogfeld **Einstellungen** eine Option unter **Apps und Desktops wieder verbinden** aus.

Zugriff auf lokale Dateien

Virtuelle Desktops bzw. Anwendungen benötigen ggf. Zugriff auf Dateien auf dem Gerät. Sie können diesen Zugriff steuern.

1. Wählen Sie auf der Seite **Dateizugriff** im Dialogfeld **Einstellungen** ein zugeordnetes Laufwerk und dann eine der folgenden Optionen:
    - **Lesen/Schreiben**: Ermöglicht dem Desktop bzw. der Anwendung das Lesen bzw. Ändern der lokalen Dateien.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Leserechte**: Ermöglicht dem Desktop bzw. der Anwendung das Lesen, jedoch nicht das Ändern der lokalen Dateien.
- **Kein Zugriff**: Der Desktop bzw. die Anwendung hat keinen Zugriff auf lokale Dateien.
- **Immer fragen**: Zeigt jedes Mal eine Aufforderung an, wenn der Desktop oder die Anwendung auf lokale Dateien zugreifen.

2. Klicken Sie auf **Hinzufügen**, geben Sie den Speicherort an und wählen Sie ein Laufwerk für die Zuordnung.

Mikrofon und Webcam

Zum Einrichten eines Mikrofons oder einer Webcam können Sie die Art und Weise ändern, wie ein virtueller Desktop oder eine Anwendung auf Ihr lokales Mikrofon oder Ihre Webcam zugreift:

Wählen Sie im Dialogfeld **Einstellungen** auf der Seite **Mikrofon & Webcam** eine der folgenden Optionen aus:

- **Mikrofon und Webcam verwenden**: Ermöglicht das Verwenden von Mikrofon und Webcam durch den Desktop bzw. die Anwendung.
- **Mikrofon und Webcam nicht verwenden**: Unterbindet das Verwenden von Mikrofon und Webcam durch den Desktop bzw. die Anwendung.

Flash Player

Sie können wählen, wie Flash-Inhalt angezeigt wird. Solcher Inhalt wird normalerweise in **Flash Player** angezeigt und enthält Animationen, Videos und Anwendungen:

Wählen Sie auf der Seite **Flash** im Dialogfeld **Einstellungen** eine der folgenden Optionen:

- **Inhalt optimieren**: Steigert die Wiedergabequalität, wobei die Sicherheit vermindert werden kann.
- **Inhalt nicht optimieren**: Liefert eine einfache Wiedergabequalität ohne Minderung der Sicherheit.
- **Immer fragen**: Bei jeder Anzeige von Flash-Inhalt wird eine Aufforderung angezeigt.

Verbinden

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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Herstellen einer Verbindung zu Ressourcen mit der Citrix Workspace-Benutzeroberfläche

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

> **Tipp:**
>
> Wenn Sie denselben Namen für mehrere Stores auf dem StoreFront-Server verwenden, vermeiden Sie Duplikationen, indem Sie Nummern hinzufügen. Die Namen dieser Stores hängen von der Reihenfolge ab, in der sie hinzugefügt werden. Für die Citrix Workspace-App wird die Store-URL angezeigt und identifiziert den Store eindeutig.

Wenn Sie die Verbindung zu einem Store hergestellt haben, zeigt Self-Service folgende Registerkarten an: **FAVORITEN**, **DESKTOPS** und **APPS**. Um eine Sitzung zu starten, klicken Sie auf das entsprechende Symbol. Um ein Symbol zu **FAVORITEN** hinzuzufügen, klicken Sie auf den Link **Details** neben dem Symbol, und wählen Sie **Zu Favoriten hinzufügen**.

Konfigurieren von Verbindungseinstellungen

Sie können einige Standardeinstellungen für Verbindungen zwischen der Citrix Workspace-App und Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Servern konfigurieren. Sie können diese Einstellungen ggf. für einzelne Verbindungen ändern.

Aufgaben und Verantwortungsbereiche von Administratoren und Benutzern können sich gelegentlich überschneiden. Der Ausdruck “Benutzer” wird verwendet, um die von Benutzern ausgeführten Aufgaben von den Aufgaben eines Administrators abzugrenzen.

Verbinden mit Ressourcen per Eingabeaufforderung oder Browser

Verbindungen mit Servern werden hergestellt, wenn Sie auf der Citrix Workspace-App-Homepage auf ein Desktop- oder Anwendungssymbol klicken. Sie können Verbindungen auch über eine Eingabeaufforderung oder über einen Webbrowser herstellen.

Herstellen einer Verbindung zu einem Program Neighborhood- oder StoreFront-Server mit einer Befehlszeile

Voraussetzung:

Stellen Sie sicher, dass der Store der Citrix Workspace-App bekannt ist. Falls erforderlich, fügen Sie ihn mit dem folgenden Befehl hinzu:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
```
./util/storebrowse --addstore \<store URL\>
<!--NeedCopy--> ```
```

1. Rufen Sie die eindeutige ID des Desktops oder der Anwendung ab, mit dem bzw. der Sie eine Verbindung herstellen möchten. Diese ID ist die erste Zeichenfolge in Anführungszeichen auf einer Zeile, die über einen der folgenden Befehle aufgerufen wird:

   - Auflisten aller Desktops und Anwendungen auf dem Server:

     ```
     ./util/storebrowse -E <store URL>
     <!--NeedCopy-->
     ```

   - Auflisten der Desktops und Anwendungen, die Sie abonniert haben:

     ```
     ./util/storebrowse -S <store URL>
     <!--NeedCopy-->
     ```

2. Führen Sie den folgenden Befehl aus, um den Desktop oder die Anwendung zu starten:

   ```
   ./util/storebrowse - L <desktop or application ID> <store URL>
   <!--NeedCopy-->
   ```

Wenn Sie keine Verbindung zum Server herstellen können, muss Ihr Administrator möglicherweise die Angaben zum Serverstandort oder SOCKS-Proxyserver prüfen. Weitere Informationen finden Sie unter
Proxyserver.

Herstellen einer Verbindung mit einem Webbrowser

Die Konfiguration zum Starten von Sitzungen über einen Webbrowser erfolgt normalerweise während der Installation automatisch. Aufgrund der Vielzahl von Browsern und Betriebssystemen ist möglicherweise etwas manuelle Konfiguration erforderlich.

Wenn Sie die `.mailcap`- und `MIME`-Dateien für Firefox, Mozilla oder Chrome manuell einrichten, führen Sie die nachfolgend aufgeführten Dateiänderungen durch. Mit diesen Änderungen starten die `.ICA`-Dateien die ausführbare Datei `wfica` der Citrix Workspace-App. Um andere Browser zu verwenden, müssen Sie die Browserkonfiguration entsprechend konfigurieren.

1. Führen Sie die folgenden Befehle aus, wenn die Citrix Workspace-App von einem Benutzer ohne Administratorrechte installiert wird. Die Einstellungen von ICAROOT werden möglicherweise geändert, wenn sie nicht in einem Standardspeicherort installiert werden. Sie können das Ergebnis mit dem Befehl

© 1999–2023 Cloud Software Group, Inc. All rights reserved.
   ```

`xdg-mime query default application/x-ica` testen, der “wfica.desktop” zurückgeben muss.

```
export ICAROOT=/opt/Citrix/ICAClient

xdg-icon-resource install --size 64 $ICAROOT/icons/000_Receiver_64.png
Citrix Workspace app

xdg-mime default wfica.desktop application/x-ica

xdg-mime default new_store.desktop application/vnd.citrix.receiver.
configure
```

2. Erstellen oder erweitern Sie die Datei /etc/xdg/mimeapps.list (bei Installation durch einen Administrator) oder `$HOME/.local/share/applications/mimeapps.list (mimeapps.list)`. Die Datei muss mit [Default Applications] beginnen, dann folgt:

   ```
   application/x-ica=wfica.desktop;

   application/vnd.citrix.receiver.configure=new_store.desktop;
   ```

   Möglicherweise müssen Sie in Firefox unter “Einstellungen > Anwendungen” Konfigurationen vornehmen.

   Wählen Sie für “Citrix ICA settings file content” Folgendes aus:

   - “Citrix Workspace app Engine (default)” im Dropdownmenü

     oder

   - “Use other …” und dann die Datei /usr/share/applications/wfica.desktop (für die Administratorinstallation der Citrix Workspace-App)

     oder

   - $HOME/.local/share/applications/wfica.desktop (für eine Installation ohne Administratorrechte).

Connection Center

Benutzer können aktive Verbindungen mit dem Connection Center verwalten. Dieses Feature ist ein nützliches Tool, mit dem Benutzer und Administratoren Probleme mit langsamen oder fehlerhaften Verbindungen beheben können. Mit Connection Center, können Benutzer folgende Verbindungsverwaltungsaufgaben durchführen:

- Schließen einer Anwendung
- Abmelden von einer Sitzung. Dabei wird die Sitzung beendet und alle geöffneten Anwendungen werden geschlossen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Trennen der Verbindung mit einer Sitzung. Mit diesem Schritt wird die ausgewählte Verbindung mit dem Server getrennt, ohne offene Anwendungen zu schließen (außer wenn der Server zum Schließen von Anwendungen bei Verbindungstrennung konfiguriert ist).
- Anzeigen der Verbindungsübertragungsstatistik

Verwalten einer Verbindung

Verwalten einer Verbindung mit dem **Connection Center**:

1. Klicken Sie im Citrix Workspace-App-Menü auf **Connection Center**.

   Die verwendeten Server und die jeweils aktiven Sitzungen werden aufgelistet.

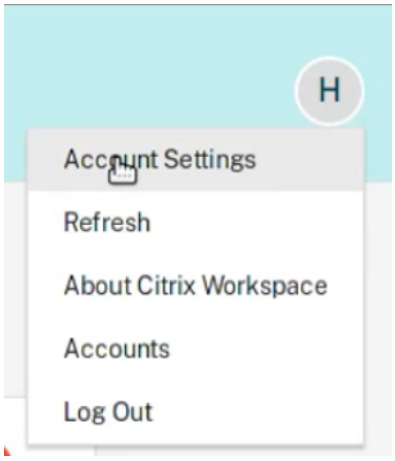
2. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie einen Server, trennen Sie die Verbindung oder melden Sie sich ab, oder zeigen Sie seine Eigenschaften an.
   - Wählen Sie eine Anwendung aus und schließen Sie das Fenster.

Verbesserung der Benutzeroberfläche

In früheren Versionen war das Menü “Einstellungen” über die Option **Einstellungen** im Desktop Viewer verfügbar.

Ab Version 2106 wird das Menü “Einstellungen” im Einklang mit dem Self-Service-Plug-In angezeigt. Die Menüoptionen wurden jetzt verbessert, sodass sie dem Erscheinungsbild des nativen Citrix Workspace entsprechen. Dies führt zu einer nahtlosen und besseren Benutzererfahrung.



> **Hinweis:**
>
> Diese Verbesserung ist in Cloudbereitstellungen standardmäßig in der Citrix Workspace-App Version 2106 verfügbar.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Gehen Sie wie folgt vor, um zum alten nativen Darstellungsstil zu wechseln:

Gehen Sie zu `$ICAROOT/config/AuthManConfig.xml` und legen Sie den Wert von `WebUISettings` auf **False** fest.

Konfigurieren

September 12, 2023

Wenn Sie die Citrix Workspace-App für Linux verwenden, führen Sie die folgenden Konfigurationsschritte aus, damit die Benutzer auf ihre gehosteten Anwendungen und Desktops zugreifen können.

Einstellungen

Konfigurationsdateien

Zum Ändern erweiterter oder selten verwendeter Einstellungen können Sie die Konfigurationsdateien der Citrix Workspace-App bearbeiten. Die Konfigurationsdateien werden jedes Mal gelesen, wenn `wfica` gestartet wird. Sie können mehrere Dateien bearbeiten, je nachdem welche Wirkung Sie mit Ihren Änderungen erzielen möchten.

Ist die Sitzungsfreigabe aktiviert, wird möglicherweise eine vorhandene Sitzung anstelle einer neu konfigurierten verwendet. Diese Einstellung kann dazu führen, dass in einer Konfigurationsdatei vorgenommene Änderungen ignoriert werden.

Standardeinstellungen

Wenn Sie Standardwerte für alle Citrix Workspace-App-Benutzer ändern möchten, bearbeiten Sie die Konfigurationsdatei `module.ini` im Verzeichnis `$ICAROOT/config`.

> **Hinweis:**
>
> Wenn ein Eintrag in `All\\_Regions.ini` auf einen bestimmten Wert festlegt ist, wird der Wert in `module.ini` für diesen Eintrag nicht verwendet. Die Werte in `All\\_Regions.ini` haben Vorrang vor dem Wert in `module.ini`.

Vorlagendatei

Wenn die Datei `$HOME/.ICAClient/wfclient.ini` nicht vorhanden ist, erstellt `wfica` sie durch Kopieren von `$ICAROOT/config/wfclient.template`. Wenn Sie diese Vorlagendatei ändern, werden die Änderungen auf alle Citrix Workspace-App-Benutzer angewendet.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Benutzereinstellungen

Um Konfigurationsänderungen für einen Benutzer anzuwenden, ändern Sie die Datei `wfclient.ini` im Benutzerverzeichnis `$HOME/.ICAClient`. Die Einstellungen in dieser Datei gelten für zukünftige Verbindungen für diesen Benutzer.

Überprüfen von Einträgen in Konfigurationsdateien

Um die Werte für Einträge in `wfclient.ini` zu beschränken, müssen Sie die zulässigen Optionen oder Optionsbereiche in der Datei `All\\_Regions.ini` festlegen.

Wenn Sie nur einen Wert angeben, wird dieser Wert verwendet. Die Datei `$HOME/.ICAClient/All\\_Regions.ini` kann mit den in der Datei `$ICAROOT/config/All\\_Regions.ini` festgelegten möglichen Werten übereinstimmen oder diese reduzieren, Einschränkungen können nicht aufgehoben werden.

> **Hinweis:**
>
> Der in `wfclient.ini` festgelegte Wert hat Vorrang vor dem Wert in `module.ini`.

Parameter

Die Parameter in jeder Datei sind in Abschnitte zusammengefasst. Jeder Abschnitt beginnt mit einem Namen in Klammern, der auf zusammengehörige Parameter hinweist. `\[ClientDrive\]` steht beispielsweise für die Parameter der Clientlaufwerkzuordnung (CDM).

Standardwerte werden, sofern nicht anders angegeben, automatisch für alle fehlenden Parameter eingesetzt. Wenn ein Parameter keinen Wert besitzt, wird automatisch der Standardwert angewendet. Stellen Sie sich zum Beispiel vor, auf den Parameter `InitialProgram` folgt ein Gleichheitszeichen (=), aber es ist kein Wert angegeben. In diesem Beispiel wird der Standardwert (nach dem Anmelden kein Programm ausführen) angewendet.

Rangfolge

Die Datei `All\\_Regions.ini` definiert Parameter, die durch andere Dateien festgelegt werden können. In dieser Datei können Werte für Parameter eingeschränkt oder genau festgelegt werden.

Für jede einzelne Verbindung werden die Dateien normalerweise in der in der folgenden Reihenfolge geprüft:

1. `All\\_Regions.ini` - Die Werte in dieser Datei überschreiben die Werte in:
    - Die `.ICA`-Datei der Verbindungen
    - `wfclient.ini`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. `module.ini` - Die Werte in dieser Datei werden verwendet, wenn sie nicht in `All\\_Regions.ini`, der `.ICA`-Datei der Verbindungen oder in `wfclient.ini` festgelegt wurden. Diese Werte werden jedoch nicht durch die Einträge in `All\\_Regions.ini` eingeschränkt.

Wird in keiner dieser Dateien ein Wert gefunden, dann wird der Standardwert im Citrix Workspace-App-Code verwendet.

> **Hinweis:**
>
> Es gibt Ausnahmen bei dieser Rangfolge. Beispielsweise werden vom Code aus Sicherheitsgründen gezielt einige Werte aus `wfclient.ini` gelesen.

Inaktivitätstimeout für die Citrix Workspace-App

Die Inaktivitätstimeout-Funktion meldet Sie basierend auf einem vom Administrator festgelegten Wert von der Citrix Workspace-App ab. Ab Version 2303 können Administratoren die zulässige Leerlaufzeit angeben, bevor ein Benutzer automatisch von der Citrix Workspace-App abgemeldet wird. Wenn innerhalb des angegebenen Zeitintervalls im Fenster der Citrix Workspace-App keine Aktivität über Maus, Tastatur oder Berührung erfolgt, werden Sie automatisch abgemeldet. Das Inaktivitätstimeout hat keine Auswirkungen auf die bereits ausgeführten Citrix Virtual Apps and Desktops- und Citrix DaaS-Sitzungen oder die StoreFront-Stores.

Der Wert für das Inaktivitätstimeout kann zwischen 10 und 1440 Minuten liegen. Das Intervall zur Änderung dieses Timeoutwerts muss ein Vielfaches von 5 sein. Beispiel: 10, 15, 20 oder 25 Minuten. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert.

> **Hinweis:**
>
> Das Feature ist nur in Cloud-Bereitstellungen verfügbar.

Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu:

```
<key>ITOEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

Administratoren können die Eigenschaft “inactivityTimeoutInMinutes” mit einem PowerShell-Modul konfigurieren.

Schritte zum Konfigurieren von “InactivityTimeoutInMinutes” auf der Clientmaschine:

1. Laden Sie Configuring Citrix Workspace using PowerShell module herunter.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. Um das Modul verwenden zu können, müssen Sie eine API-Client-ID und ein Geheimnis generieren. Weitere Informationen zum Erhalt von Anmeldeinformationen und eine Einführung in die Citrix Cloud-APIs finden Sie unter Erste Schritte mit Citrix Cloud-APIs.
3. Um dieses Modul zu importieren, übergeben Sie den Pfad zum Verzeichnis Citrix.Workspace.StoreConfigs an das Cmdlet Import-Module, d. h. führen Sie `Import-Module ./Citrix.Workspace.StoreConfigs` vom Verzeichnis aus, das diese Datei enthält.
4. Führen Sie nach dem Import des Moduls `Get-Help -Full` aus, um Hilfe zu spezifischen Cmdlets zu erhalten. Beispiel: `Get-Help Set-WorkspaceCustomConfigurations -Full`
5. Führen Sie den folgenden Befehl aus, um `inactivityTimeoutInMinutes` beispielsweise auf 1 Stunde einzustellen:

   ```
   Set-WorkspaceCustomConfigurations -WorkspaceUrl -ClientId -
       ClientSecret -InactivityTimeoutInMinutes "60"
   <!--NeedCopy-->
   ```

   Sie müssen den genannten Befehl nicht auf allen Clients ausführen. Sie müssen ihn nur einmal ausführen und testen.

Für die Endbenutzererfahrung gilt Folgendes:

- Drei Minuten vor der Abmeldung wird eine Benachrichtigung angezeigt. Sie können angemeldet bleiben oder sich abmelden.
- 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:**
>
> Die Timeout bei Inaktivität unterstützt keine Distributionen mit dem Standardgrafikprotokoll Wayland. Für Distributionen, die Wayland verwenden, heben Sie die Auskommentierung für einen der folgenden Einträge auf: `WaylandEnable=false` in `/etc/gdm/custom.conf` oder `/etc/gdm3/custom.conf`.

Persistente Anmeldung

Ab Version 2303 ermöglicht Ihnen das Feature der persistenten Anmeldung, über den gesamten von Ihrem Administrator konfigurierten Zeitraum (2 bis 365 Tage) angemeldet zu bleiben. Wenn dieses Feature aktiviert ist, müssen Sie während des konfigurierten Zeitraums keine Anmeldeinformationen für die Citrix Workspace-App angeben.

Mit dieser Funktion wird das SSO an Citrix DaaS-Sitzungen auf einen Zeitraum von 365 Tagen verlängert. Diese Verlängerung basiert auf der Lebensdauer langlebiger Tokens. Ihre Anmeldeinforma-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

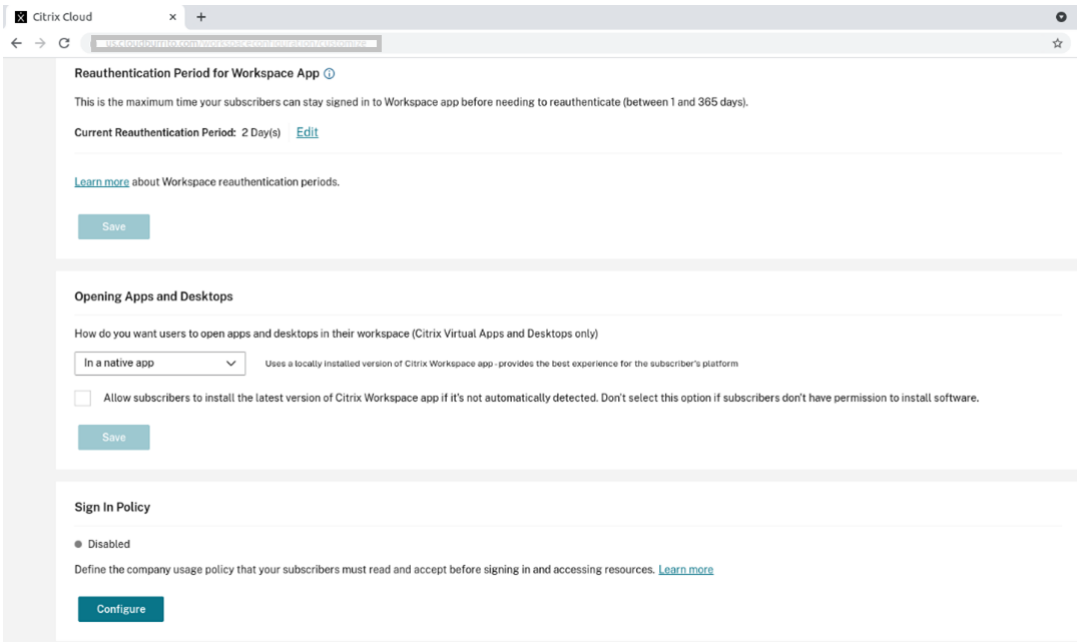
tionen werden standardmäßig für 4 Tage oder für die Lebensdauer zwischengespeichert, je nachdem, welcher Wert niedriger ist. Die Verlängerung erfolgt, wenn Sie innerhalb dieser 4 Tage eine Verbindung zur Citrix Workspace-App herstellen.

Konfigurieren der persistenten Anmeldung

Ein Administrator muss die persistente Anmeldung in der Workspaceumgebung mit dem folgenden Verfahren konfigurieren:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie in der Citrix Cloud-Konsole auf das Menü in der oberen linken Ecke des Bildschirms.
3. Wählen Sie die Option **Workspacekonfiguration** > **Anpassen** > **Einstellungen** aus.
4. Scrollen Sie nach unten zu **Neuauthentifizierungszeitraum für die Workspace-App**.
5. Klicken Sie neben dem Feld **Aktueller Zeitraum für die erneute Authentifizierung** auf **Bearbeiten**.
6. Geben Sie die erforderlichen Tage in das Feld **Aktueller Zeitraum für die erneute Authentifizierung** ein.
7. Sie müssen mindestens zwei Tage in das Feld **Aktueller Zeitraum für die erneute Authentifizierung** eingeben.

Weitere Informationen finden Sie in den Anweisungen im Abschnitt **Neuauthentifizierungszeitraum für die Workspace-App** in der folgenden Abbildung:

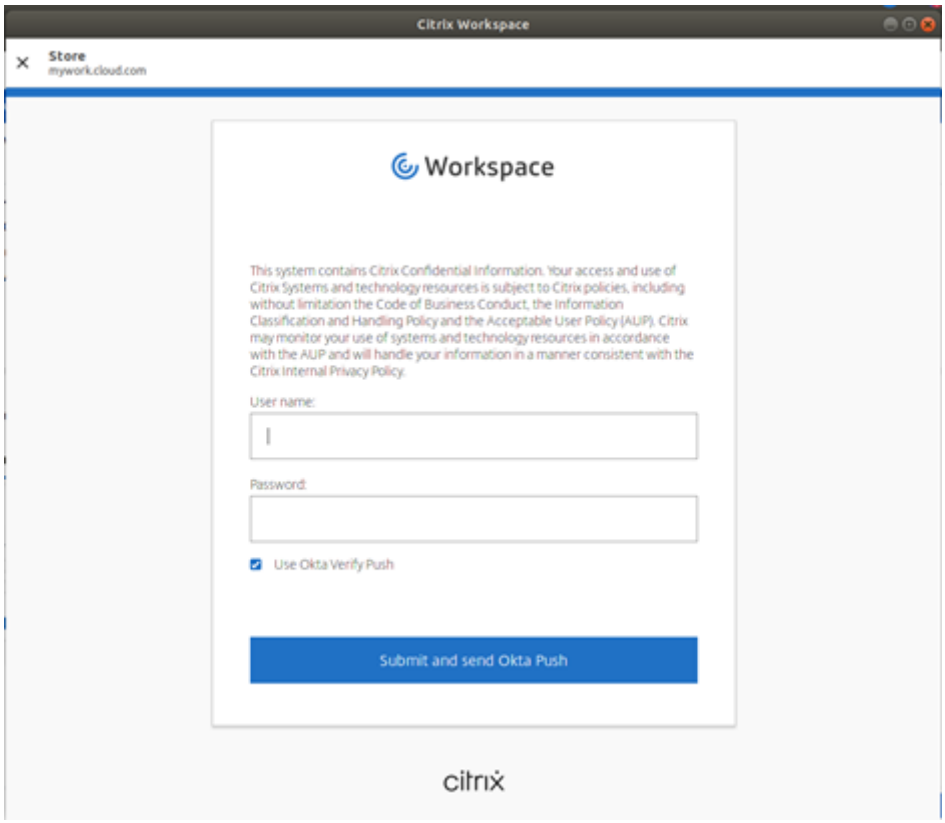


Erfahrung mit verbesserter Authentifizierung

Das Fenster für die persistente Anmeldung ist in das Self-Service-Fenster integriert.

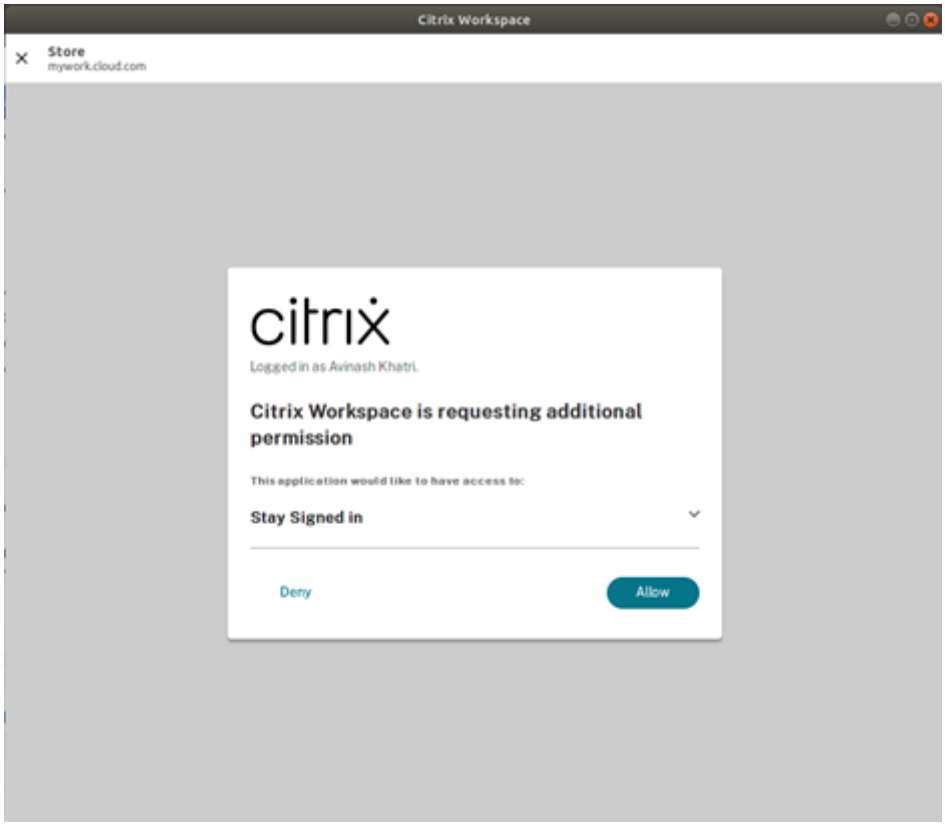
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Rufen Sie die Citrix Workspace-App auf.
   Das Authentifizierungsfenster wird angezeigt.



2. Melden Sie sich mit Ihren Anmeldeinformationen an.
   Sie werden zwecks Bestätigung zur Berechtigungsaufforderung weitergeleitet.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. Klicken Sie auf **Zulassen**.

> **Hinweis:**
>
> Wenn Sie **Deny** auswählen, wird eine zweite Anmeldeaufforderung angezeigt, und Sie müssen sich alle 24 Stunden bei der Citrix Workspace-App anmelden.

Deaktivieren der persistenten Anmeldung

Ein Administrator kann das Feature der persistenten Anmeldung in der Citrix Cloud-Benutzeroberfläche oder in der Datei `AuthManConfig.xml` deaktivieren. Der in der Datei `AuthManConfig.xml` festgelegte Wert überschreibt jedoch den in der Citrix Cloud-Benutzeroberfläche festgelegten Wert.

Verwenden der Citrix Cloud-Benutzeroberfläche

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie in der Citrix Cloud-Konsole auf das Menü in der oberen linken Ecke des Bildschirms.
3. Wählen Sie die Option **Workspacekonfiguration** > **Anpassen** > **Einstellungen** aus.
4. Scrollen Sie nach unten zu **Neuauthentifizierungszeitraum für die Workspace-App**.
5. Klicken Sie neben dem Feld **Aktueller Zeitraum für die erneute Authentifizierung** auf **Bearbeiten**.
6. Geben Sie in das Feld **Aktueller Zeitraum für die erneute Authentifizierung** einen Tag ein.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Verwenden der Datei AuthManConfig.xml

Gehen Sie wie folgt vor, um das Feature der persistenten Anmeldung zu deaktivieren.

1. Navigieren Sie zur Datei <ICAROOT>/config/AuthManConfig.xml.
2. Legen Sie die Werte wie folgt fest:

```
<AuthManLite>

<primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>

<secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>

<longLivedTokenSupport>false</longLivedTokenSupport>

<nativeLoggingEnabled>true</nativeLoggingEnabled>

<platform>linux</platform>

<saveTokens>true</saveTokens>

</AuthManLite>
<!--NeedCopy-->
```

Erstellen benutzerdefinierter UserAgent-Zeichenfolgen in Netzwerkanforderungen

Ab Version 2109 bietet die Citrix Workspace-App eine Option zum Anfügen der UserAgent-Zeichenfolgen in der Netzwerkanforderung und zum Identifizieren der Quelle einer Netzwerkanforderung. Basierend auf dieser UserAgent-Zeichenfolgeanforderung können Sie entscheiden, wie Sie Ihre Netzwerkanforderung verwalten. Mit diesem Feature können Sie Netzwerkanforderungen nur von vertrauenswürdigen Geräten annehmen.

> **Hinweis:**
>
> - Dieses Feature wird für Cloudbereitstellungen der Citrix Workspace-App unterstützt. Darüber hinaus werden die folgenden Pakete unterstützt: x86, x64 und ARMHF.

Zum Anpassen der UserAgent-Zeichenfolgen gehen Sie folgendermaßen vor:

1. Suchen Sie die Konfigurationsdatei: $ICAROOT/config/AuthManConfig.xml.
2. Fügen Sie dem folgenden Eintrag einen Wert hinzu:

```
<UserAgentSuffix> </UserAgentSuffix>
```

Beispiel, das App und Version im benutzerdefinierten Text einschließt:

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Wenn Sie App und AppVersion hinzufügen, trennen Sie sie durch einen Schrägstrich (/).

- Wenn die Netzwerkanforderung von der Benutzeroberfläche der Citrix Workspace-App stammt, wird in den Netzwerkanforderungen der folgende UserAgent angezeigt:

  `CWAWEBVIEW/CWAVersion App/AppVersion`

- Wenn die Netzwerkanforderung nicht von der Benutzeroberfläche der Citrix Workspace-App stammt, wird in den Netzwerkanforderungen der folgende UserAgent angezeigt:

  `CWA/CWAVersion App/AppVersion`

> **Hinweise:**
>
> - Wenn Sie AppVersion am Ende der Zeichenfolge "UserAgentSuffix" nicht hinzufügen, wird die Version der Citrix Workspace-App in den Netzwerkanforderungen angehängt.
> - Starten Sie `AuthManagerDaemon` und `ServiceRecord` neu, damit die Änderungen wirksam werden.

Servicekontinuität

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Die Benutzer können so Citrix Virtual Apps and Desktops bzw. Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) unabhängig vom Integritätsstatus der Clouddienste starten.

Informationen zu Anforderungen für die Unterstützung von Servicekontinuität in der Citrix Workspace-App finden Sie unter Systemanforderungen.

Weitere Informationen finden Sie unter Servicekontinuität in der Dokumentation zu Citrix Workspace.

Pinnen des Bildschirmlayouts im Multimonitormodus

Ab Version 2103 können Sie die Auswahl für das Bildschirmlayout im Multimonitormodus speichern. Das Layout bestimmt, wie eine Desktopsitzung angezeigt wird. Durch Pinnen wird das ausgewählte Layout beim Neustarten einer Sitzung beibehalten, was die Benutzererfahrung optimiert.

Als Voraussetzung müssen Sie dieses Feature in der Datei `AuthManConfig.xml` aktivieren. Navigieren Sie zu `$ICAROOT/config/AuthManConfig.xml` und fügen Sie die folgenden Einträge hinzu:

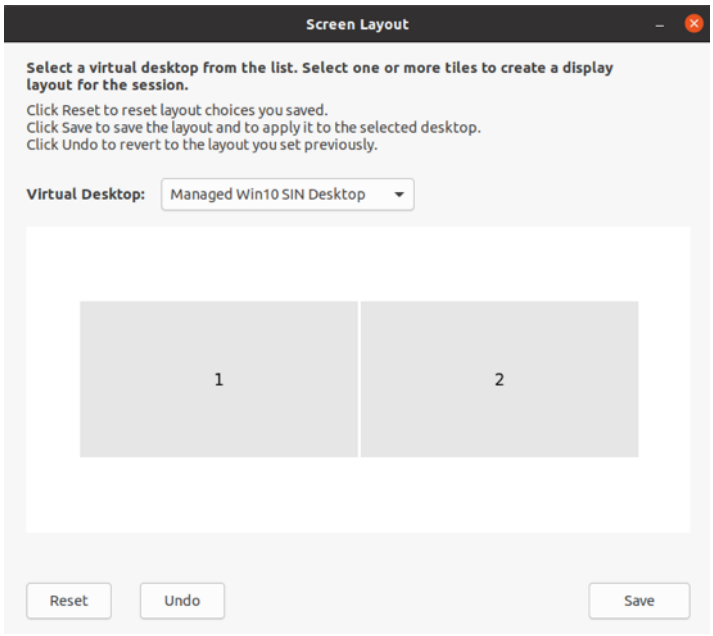
```
1       <key>ScreenPinEnabled</key>
2       <value> true </value>
3 <!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Erst nachdem Sie den vorhergehenden Schlüssel hinzugefügt haben, können Sie die Option **Bildschirmlayout** im **App-Indikatorsymbol** sehen. Weitere Informationen zum App-Indikator finden Sie unter App-Indikatorsymbol.

Um das Bildschirmlayout auszuwählen, klicken Sie auf das App-Indikatorsymbol in der Taskleiste und wählen Sie **Bildschirmlayout**. Das Dialogfeld **Bildschirmlayout** wird angezeigt.

Alternativ können Sie das Dialogfeld **Bildschirmlayout** im Self-Service-Fenster durch Drücken der Tastenkombination **Ctrl+M** öffnen.



Wählen Sie einen virtuellen Desktop aus dem Dropdownmenü aus. Die Layoutauswahl wird nur auf den ausgewählten Desktop angewendet.

Wählen Sie eine oder mehrere Kacheln aus, um eine rechteckige Auswahl für das Layout zu bilden. Die Sitzung wird dann gemäß der Layoutauswahl angezeigt.

Einschränkungen:

- Durch Aktivieren des Pinnens wird die Funktion zum Speichern des Bildschirmlayouts in einer Sitzung deaktiviert.
- Dieses Feature gilt nur für Desktops, die als Favorit gekennzeichnet sind.

Anwendungskategorien

Mithilfe von Anwendungskategorien können Benutzer Anwendungssammlungen in der Citrix Workspace-App verwalten. Sie können Anwendungsgruppen für Folgendes erstellen:

- Anwendungen, die in verschiedenen Bereitstellungsgruppen verwendet werden
- Anwendungen, die von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Erstellen von Anwendungsgruppen in der Citrix Virtual Apps and Desktops-Dokumentation.

App Protection

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

Der App-Schutz ist eine Zusatzfunktion, die erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops bietet. Sie verringert das Risiko, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. Der App-Schutz verhindert das Exfiltrieren vertraulicher Informationen, wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

> **Hinweise:**
>
> - Diese Funktion wird nur unterstützt, wenn die Citrix Workspace-App mit einem der folgenden Pakete installiert wird: Tarball, Debian, Red Hat Package Manager (RPM). x64 und ARMHF sind zudem die einzigen unterstützten Architekturen.
> - Dieses Feature wird für On-Premises-Bereitstellungen von Citrix Virtual Apps and Desktops unterstützt. Und für Bereitstellungen mit Citrix Virtual Apps and Desktops Service mit StoreFront.

Für den App-Schutz müssen Sie eine Add-On-Lizenz auf dem Lizenzserver installieren. Eine Citrix Virtual Desktops-Lizenz muss ebenfalls vorhanden sein. Weitere Informationen finden Sie unter Konfigurieren in der Dokumentation zu **Citrix Virtual Apps and Desktops**.

Ab Version 2108 ist das App-Schutzfeature voll funktionsfähig. Das App-Schutzfeature unterstützt App- und Desktopsitzungen und ist standardmäßig aktiviert. Sie müssen das App-Schutzfeature jedoch in der Datei `AuthManConfig.xml` konfigurieren, um es für den Authentifizierungsmanager und das Self-Service-Plug-In zu aktivieren.

Ab dieser Version können Sie geschützte Ressourcen aus der Citrix Workspace-App starten, während Mozilla Firefox ausgeführt wird.

Ab Version 2012 ist der App-Schutz ein experimentelles Feature.

Voraussetzung:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

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

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

Installieren der App-Schutzkomponente:

Wenn Sie die Citrix Workspace-App mit dem Tarball-Paket installieren, wird die folgende Meldung angezeigt.

“Möchten Sie die App-Schutzkomponente installieren? Warnung: Sie können dieses Feature nicht deaktivieren. Zum Deaktivieren müssen Sie die Citrix Workspace-App deinstallieren. Weitere Informationen erhalten Sie von Ihrem Systemadministrator. [default $INSTALLER_N]:”

Geben Sie **Y** ein, um die App-Schutzkomponente zu installieren.

Die App-Schutzkomponente ist standardmäßig nicht installiert.

Starten Sie die Maschine neu, damit die Änderungen wirksam werden. Damit der App-Schutz wie erwartet funktioniert, müssen Sie Ihre Maschine neu starten.

Installieren der App-Schutzkomponente auf RPM-Paketen:

Ab Version 2104 wird der App-Schutz von der RPM-Version der Citrix Workspace-App unterstützt.

Mit den folgenden Schritten installieren Sie den App-Schutz:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

Installieren der App-Schutzkomponente auf Debian-Paketen:

Ab Version 2101 wird der App-Schutz von der Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie für die unbeaufsichtigte Installation der App-Schutzkomponente den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

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

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

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

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

Konfigurieren des App-Schutzes für den Authentifizierungsmanager:

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

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

<!--NeedCopy-->
```

Konfigurieren des App-Schutzes für das Self-Service-Plug-In:

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

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    protection -A 4
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>

<!--NeedCopy-->
```

Bekannte Probleme:

- Wenn Sie einen geschützten Bildschirm minimieren, läuft der App-Schutz weiterhin im Hintergrund.

Einschränkung:

- In einigen Fällen können Sie geschützte Ressourcen nicht starten, wenn eine aus dem Snap-Store installierte Anwendung ausgeführt wird. Prüfen Sie als Workaround in der Protokolldatei der Citrix Workspace-App, welche Anwendung das Problem verursacht. Schließen Sie dann die Anwendung.
- Beim Versuch, den Screenshot eines geschützten Fensters zu erstellen, wird der gesamte Bildschirm abgeblendet, einschließlich der nicht geschützten Apps im Hintergrund.

Akkustatusanzeige

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

> **Hinweis:**
>
> Ab Version 2111 wird die Akkustatusanzeige auch für Server-VDAs angezeigt.

Die Akkustatusanzeige ist standardmäßig aktiviert.

Deaktivieren der Batteriestatusanzeige:

1. Navigieren Sie zum Ordner `<ICAROOT>/config/module.ini`.
2. Navigieren Sie zum Abschnitt `ICA 3.0`.
3. Legen Sie Folgendes fest: `MobileReceiver= Off`.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Erfasste Daten	Beschreibung	Wofür verwenden wir es?
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Citrix Workspace-App für Linux und sendet die Daten automatisch an Google Analytics.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Citrix Workspace-App zu verbessern.

Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix. Citrix schützt die Daten gemäß der Anlage zur Sicherheit von Citrix Diensten, die im Citrix Trust Center verfügbar ist.

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.

Deaktivieren des Sendens von CEIP-Daten an Citrix und Google Analytics. Bei dieser Aktivität gibt es eine Ausnahme bei den für Google Analytics gesammelten Daten (in der zweiten Tabelle im folgenden Abschnitt mit * gekennzeichnet). Gehen Sie wie folgt vor, um das Senden von CEIP-Daten an Citrix und Google Analytics zu deaktivieren:

1. Navigieren Sie zum Ordner `<ICAROOT>/config/module.ini` und dann zum Abschnitt `CEIP`.
2. Wählen Sie den Eintrag `EnableCeip` aus und legen Sie ihn auf `Disable` fest.

> **Hinweis:**
>
> Nachdem Sie den Schlüssel `EnableCeip` auf `Disable` gesetzt haben, können Sie das Senden der letzten beiden CEIP-Datenelemente an Google Analytics deaktivieren. Diese Datenelemente sind die Betriebssystemversion und die Version der Workspace-App. Navigieren Sie für diese Aktion zum folgenden Abschnitt und legen Sie den Wert wie vorgeschlagen fest:

Speicherort: `<ICAROOT>/config/module.ini`

Abschnitt: `GoogleAnalytics`

Eintrag: `DisableHeartBeat`

Wert: True

> **Hinweis:**
>
> Es werden keine Daten für Benutzer in der Europäischen Union (EU), dem Europäischen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK) gesammelt.

Folgende CEIP-Datenelemente werden von Google Analytics erfasst:

Betriebssystemversion'	Version der Workspace-App*	App-Name	Sprache der Workspace-App
Sitzungsstartmethode	Compiler-Version	Hardwareplattform	Storekonfiguration
Citrix Virtual Apps and Desktops-Sitzungsstartstatus	Authentifizierungskonfi	Verbindungsprotokoll	Verwendung der Browserinhaltsum-leitung
Verbindungsleasedetails	Konfiguration von App Protection		

App-Indikatorsymbol

Der App-Indikator wird beim Start der Citrix Workspace-App gestartet und ist ein Symbol im Infobereich. Die Einführung des App-Indikators verbessert die Anmeldeleistung der Citrix Workspace-App für Linux.

Sie können Leistungsverbesserungen in folgenden Situationen bemerken:

- Erster Start der Citrix Workspace-App
- Schließen und Neustarten der App
- Beenden und Neustarten der App

> **Hinweis:**
>
> Das Paket `libappindicator` ist erforderlich, damit der App-Indikator angezeigt wird. Installieren Sie das für Ihre Linux-Distribution geeignete Paket `libappindicator` aus dem Internet.

ICA-zu-X-Proxy

Sie können eine Workstation, auf der die Citrix Workspace-App ausgeführt wird, als Server verwenden und die Ausgabe auf ein anderes X11-fähiges Gerät umleiten. So können Sie Microsoft Windows-Anwendungen auch auf X-Terminals oder auf UNIX-Workstations bereitstellen, für die es die Citrix Workspace-App nicht gibt.

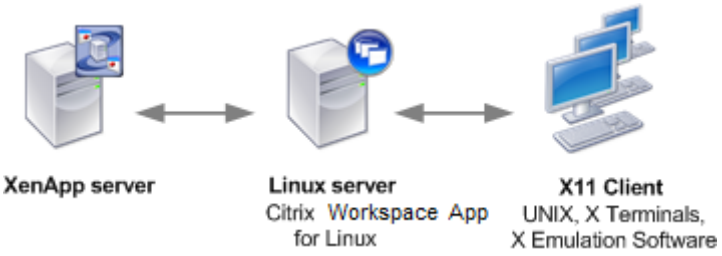
> **Hinweis:**
>
> Die Citrix Workspace-App-Software ist für zahlreiche X-Geräte verfügbar und in diesen Fällen ist

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> das Installieren der Software auf diesen Geräten die bevorzugte Lösung. Das Ausführen der Citrix Workspace-App in dieser Weise, als ICA-zu-X-Proxy, wird auch serverseitiges ICA genannt.

Die Citrix Workspace-App kann als ICA-X11-Konverter angesehen werden, der die X11-Ausgabe auf den lokalen Linux-Desktop leitet. Natürlich können Sie die Ausgabe auch auf ein anderes X11-Display umleiten. Sie können weitere Kopien der Citrix Workspace-App gleichzeitig auf einem System ausführen. Jede Citrix Workspace-App sendet ihre Ausgabe dann an ein anderes Gerät.

Diese Grafik zeigt ein System, in dem die Citrix Workspace-App für Linux als ICA-zu-X-Proxy eingerichtet ist:



Für solche Systeme benötigen Sie einen Linux-Server als ICA-zu-X11-Proxy:

- Wenn Sie bereits X-Terminals verwenden, können Sie die Citrix Workspace-App auf dem Linux-Server ausführen, der normalerweise die X-Anwendungen für die X-Terminals bereitstellt.
- Um UNIX-Workstations bereitzustellen, für die es die Citrix Workspace-App nicht gibt, benötigen Sie einen eigenen Server, der als Proxy dient. Dieser Server kann ein PC sein, auf dem Linux ausgeführt wird.

Anwendungen werden dem Endgerät mit X11 und den Funktionen des ICA-Protokolls bereitgestellt. Standardmäßig können Sie mit der Laufwerkszuordnung nur auf Laufwerke auf dem Proxy zugreifen. Diese Einstellung ist bei X-Terminals kein Problem, da diese in der Regel keine lokalen Laufwerke haben. Wenn Sie Anwendungen für andere UNIX-Workstations bereitstellen, können Sie Folgendes tun:

- Bereitstellen der lokalen UNIX-Workstation über NFS auf der als Proxy dienenden Workstation und Zuordnen eines Clientlaufwerks am NFS-Bereitstellungspunkt auf dem Proxy.
- Verwenden eines NFS-SMB-Proxys (z. B. SAMBA) oder eines NFS-Clients auf dem Server (z. B. Microsoft Services for UNIX).

Einige Leistungsmerkmale werden nicht an das Endgerät weitergeleitet:

- USB-Umleitung
- Smartcard-Umleitung
- COM-Portumleitung
- Dem X11-Gerät wird kein Audio übermittelt, selbst wenn der als Proxy dienende Server Audio unterstützt.
- Clientdrucker werden nicht an das X11-Gerät weitergeleitet. Sie müssen mit LPD-Druck manuell auf den UNIX-Drucker vom Server zugreifen oder einen Netzwerkdrucker verwenden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Die Umleitung von Multimediaeingaben wird nicht unterstützt. Hierfür ist auf der Maschine, die die Citrix Workspace-App ausführt, eine Webcam erforderlich. Diese Maschine ist jedoch der Server, der als Proxy fungiert. Die Umleitung von Multimedia-Ausgaben funktioniert jedoch, wenn `GStreamer` auf dem Server, der als Proxy fungiert, installiert ist (nicht getestet).

Starten der Citrix Workspace-App mit serverseitigem ICA von einem X-Terminal oder einer UNIX-Workstation:

1. Stellen Sie über ssh oder Telnet eine Verbindung zum Computer her, der als Proxy dient.
2. Setzen Sie in einer Shell auf dem Proxygerät die Umgebungsvariable **DISPLAY** auf den lokalen Computer. Geben Sie z. B. in einer C-Shell Folgendes ein:

   ```
   setenv DISPLAY <local:0>
   ```

   > **Hinweis:**
   >
   > Wenn Sie mit dem Befehl `ssh -X` eine Verbindung zu dem Gerät, das als Proxy fungiert, herstellen, müssen Sie die Umgebungsvariable **DISPLAY** nicht einrichten.

3. Geben Sie an der Befehlszeile des lokalen Geräts Folgendes ein: xhost <Proxyservername>
4. Überprüfen Sie, ob die Citrix Workspace-App im Standardverzeichnis installiert ist. Falls nicht, muss die Umgebungsvariable ICAROOT auf das tatsächliche Installationsverzeichnis verweisen.
5. Suchen Sie das Verzeichnis, in dem die Citrix Workspace-App installiert ist. Geben Sie an der Eingabeaufforderung Folgendes ein: `selfservice &`

Server-zu-Client-Inhaltsumleitung

Mit der Server-zu-Client-Inhaltsumleitung können Administratoren festlegen, dass URLs in einer veröffentlichten Anwendung mit einer lokalen Anwendung geöffnet werden. Wenn Sie beispielsweise einen Link zu einer Webseite öffnen, während Sie Microsoft Outlook in einer Sitzung verwenden, wird die erforderliche Datei mit dem Browser auf dem Benutzergerät geöffnet.

Die Server-zu-Client-Inhaltsumleitung ermöglicht Administratoren eine effizientere Vergabe von Citrix Ressourcen und damit eine bessere Leistung für Benutzer. Folgende URL-Typen können umgeleitet werden:

- HTTP
- HTTPS
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Ältere Real Player)

In folgenden Situationen wird die URL mit der Serveranwendung geöffnet:

- Die Citrix Workspace-App hat keine geeignete Anwendung.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Die Citrix Workspace-App kann nicht direkt auf den Inhalt zugreifen.

Die Server-zu-Client-Inhaltsumleitung ist auf dem Server konfiguriert. Dieses Feature ist in der Citrix Workspace-App standardmäßig aktiviert, wenn der Pfad Folgendes enthält:

- RealPlayer
- Firefox, Mozilla oder Netscape.

Aktivieren der Server-zu-Client-Inhaltsumleitung, wenn der Pfad weder RealPlayer noch einen Browser enthält:

1. Öffnen Sie die Konfigurationsdatei `wfclient.ini`.
2. Bearbeiten Sie im Abschnitt [Browser] die folgenden Einstellungen:

   Path=path

   Command=command

   "path" ist das Verzeichnis, in dem sich die ausführbare Browserdatei befindet. "command" ist der Name der ausführbaren Datei, die verwendet wird, um umgeleitete Browser-URLs zu verarbeiten, die mit der vom Server gesendeten URL angehängt werden. Beispiel:

   `$ICAROOT/nslaunch` Netscape, Firefox, Mozilla

   Mit dieser Einstellung wird Folgendes festgelegt:

   - Das Hilfsprogramm `nslaunch` wird ausgeführt, um die URL in ein vorhandenes Browserfenster zu verschieben.
   - Jeder Browser in der Liste wird der Reihe nach ausprobiert, bis der Inhalt richtig angezeigt wird.
3. Bearbeiten Sie im Abschnitt [Player] die folgenden Einstellungen:

   Path=path

   Command=command

   "path" ist das Verzeichnis, in dem sich die ausführbare RealPlayer-Datei befindet. "command" ist der Name der ausführbaren Datei, die zur Verarbeitung der umgeleiteten Multimedia-URLs verwendet wird, welche mit der vom Server gesendeten URL angehängt werden.
4. Speichern und schließen Sie die Datei.

> **Hinweis:**
>
> Für beide Pfadeinstellungen müssen Sie das Verzeichnis angeben, in dem sich die ausführbaren Dateien für den Browser und für RealPlayer befinden. Sie brauchen nicht dem vollständigen Pfad zu den ausführbaren Dateien anzugeben. Beispiel: Im Abschnitt [Browser] kann als Pfad /usr/X11R6/bin statt /usr/X11R6/bin/netscape angegeben sein. Sie können auch mehrere Verzeichnisnamen in einer durch Doppelpunkte getrennten Liste angeben. Wenn diese Einstellungen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> nicht angegeben sind, wird die aktuelle Variable $PATH des Benutzers verwendet.

Deaktivieren der Server-zu-Client-Inhaltsumleitung in Citrix Workspace:

1. Öffnen Sie die Konfigurationsdatei `module.ini`.
2. Ändern Sie die Einstellung für `CREnabled` in `Off`.
3. Speichern und schließen Sie die Datei.

Verbindung

Konfigurieren von Verbindungen

Auf Geräten mit beschränkter Rechenleistung oder geringer Bandbreite kommt es zu Einbußen bei der Leistung oder der Funktionalität. Benutzer und Administratoren können eine akzeptable Mischung aus umfassender Funktionalität und interaktiver Leistung wählen. Wenn Sie eine oder mehrere der folgenden Änderungen – häufig auf dem Server anstatt auf dem Benutzergerät – vornehmen, kann dies die von der Verbindung benötigte Bandbreite verringern und die Leistung verbessern:

- **Aktivieren Sie die SpeedScreen-Latenzreduktion**: Die SpeedScreen-Latenzreduktion steigert die Leistung bei Verbindungen mit hoher Latenz. Der Benutzer erhält schnell Feedback für eingegebene Daten und Mausklicks. Aktivieren Sie dieses Feature auf dem Server mit dem SpeedScreen-Latenzreduktionsmanager. Dieses Feature ist in der Citrix Workspace-App für Windows standardmäßig für die Tastatur deaktiviert. Dieses Feature ist nur für die Maus bei Verbindungen mit hoher Latenz aktiviert. Weitere Informationen finden Sie in der Dokumentation Citrix Workspace app for Linux OEM's Reference Guide.
- **Aktivieren Sie die Datenkomprimierung**: Mit der Datenkomprimierung wird die in der Verbindung übertragene Datenmenge reduziert. Für das Komprimieren und Dekomprimieren werden zusätzliche Prozessorressourcen benötigt. Diese Konfiguration kann jedoch die Leistung bei Verbindungen mit eingeschränkter Bandbreite erhöhen. Verwenden Sie die Citrix-Richtlinieneinstellungen **Audioqualität und Bildkomprimierung**, um dieses Feature zu aktivieren.
- **Reduzieren Sie die Fenstergröße**: Ändern Sie die Fenstergröße auf die kleinste Größe, mit der Sie noch gut arbeiten können. Legen Sie in der Farm die Sitzungsoptionen fest.
- **Reduzieren Sie die Farbanzahl**: Reduzieren Sie die Anzahl der Farben auf 256. Legen Sie auf der Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Site die Sitzungsoptionen fest.
- **Verringern Sie die Audioqualität**: Wenn die Audiozuordnung aktiviert ist, verringern Sie die Audioqualität mit der Citrix Richtlinieneinstellung "Audioqualität" auf die niedrigste Einstellung.

Informationen zur Problembehandlung finden Sie unter Verbindungen im Abschnitt zur Problembehandlung.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Schriftart

ClearType-Schriftartenglättung

Mit ClearType-Schriftartenglättung wird eine höhere Qualität der Schriftartenanzeige erzielt als bei:

- traditioneller Schriftartenglättung oder
- Anti-Aliasing.

Die ClearType-Schriftartenglättung wird auch als “Subpixel-Rendering von Schriftarten” bezeichnet. Sie können dieses Feature ein- und ausschalten.

Sie können die Art der Glättung auch wie folgt festlegen:

1. Gehen Sie in der entsprechenden Konfigurationsdatei zum Abschnitt [WFClient].
2. Bearbeiten Sie die folgende Einstellung:

   FontSmoothingType = Zahl

   “Zahl” kann einer der folgenden Werte sein:

Wert	Ergebnis
0	Die lokale Einstellung auf dem Gerät wird verwendet. Dieser Wert wird über die Einstellung **FontSmoothingTypePref** festgelegt.
1	Keine Glättung
2	Standardglättung
3	ClearType-Glättung (horizontale Subpixel-Technologie)

Sowohl Standardglättung als auch ClearType-Glättung können die Bandbreitenanforderungen der Citrix Workspace-App erhöhen.

> **Wichtig:**
>
> Der Server kann `FontSmoothingType` über die `ICA`-Datei konfigurieren. Dieser Wert hat Vorrang vor dem Wert unter [WFClient].

Wenn vom Server der Wert 0 festgelegt ist, wird die lokale Einstellung im [WFClient] durch folgende Einstellung bestimmt:
FontSmoothingTypePref = Zahl

“Zahl” kann einer der folgenden Werte sein:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Wert	Ergebnis
0	Keine Glättung
1	Keine Glättung
2	Standardglättung
3	ClearType-Glättung (horizontale Subpixel-Technologie, Standard)

Ordner

Konfigurieren der Umleitung spezieller Ordner

Jeder Benutzer hat zwei spezielle Ordner:

- Ordner “Desktop”
- Ordner “Dokumente” (“Eigene Dateien” unter Windows XP)

Mit der Funktion “Umleitung spezieller Ordner” können Sie den Speicherort der speziellen Ordner eines Benutzers angeben. Diese Ordner bleiben dann auch bei Verwendung verschiedener Servertypen und Serverfarmkonfigurationen bestehen. Dies ist wichtig, wenn Benutzer, die häufig den Standort wechseln, sich an Servern in unterschiedlichen Serverfarmen anmelden. Bei Benutzern, die einen festen Schreibtisch haben und sich an Servern anmelden, die sich in derselben Serverfarm befinden, ist die Umleitung spezieller Ordner selten notwendig.

Konfigurieren der Umleitung spezieller Ordner:

Aktivieren Sie die Umleitung spezieller Ordner, indem Sie der Datei module.ini einen Eintrag hinzufügen und die Ordnerspeicherorte wie folgt angeben:

1. Fügen Sie module.ini (z. B. $ICAROOT/config/module.ini) folgenden Text hinzu:

   [ClientDrive]

   SFRAllowed = True

   DocumentsFolder = Dokumente

   DesktopFolder = Desktop

   Dabei sind Dokumente und Desktop die UNIX-Dateinamen, einschließlich vollständiger Pfade, der Verzeichnisse, die für die Benutzerordner “Dokumente” und “Desktop” verwendet werden sollen. Beispiel:

   DesktopFolder = $HOME/.ICAClient/desktop

   - Sie können alle Komponenten in dem Pfad als Umgebungsvariablen angeben, z. B. $HOME.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Geben Sie für beide Parameter Werte an.
- Die angegebenen Verzeichnisse müssen über die Clientgerätzuordnung verfügbar sein. Das heißt, das Verzeichnis muss sich in der Struktur eines verknüpften Clientgeräts befinden.
- Verwenden Sie die Laufwerksbuchstaben C oder höher.

Clientlaufwerkzuordnung

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf dem Citrix Virtual Apps and Desktops-Server bzw. dem Citrix DaaS-Server auf Verzeichnisse, die auf dem lokalen Benutzergerät vorhanden sind. In einer Citrix-Benutzersitzung kann beispielsweise das Laufwerk H einem Verzeichnis auf dem lokalen Computer, auf dem die Workspace-App ausgeführt wird, zugeordnet werden.

Mit der Clientlaufwerkszuordnung kann jedes Verzeichnis auf dem lokalen Benutzergerät bereitgestellt werden. Das lokale Benutzergerät schließt CD-ROMs, DVDs oder USB-Sticks ein, die dem Benutzer während einer Sitzung zur Verfügung stehen. Der lokale Benutzer ist zudem berechtigt, auf das lokale Benutzergerät zuzugreifen. Wenn ein Server für die Clientlaufwerkszuordnung konfiguriert ist, können Benutzer:

- auf lokal gespeicherte Dateien zugreifen
- diese Dateien in der Sitzung verwenden
- und die Dateien dann neu speichern – entweder auf einem lokalen Laufwerk oder auf dem Server.

Die Citrix Workspace-App unterstützt Clientgerätzuordnung für Verbindungen zu Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Servern. Mit diesem Feature kann eine auf dem Server ausgeführte Remoteanwendung auf Geräte zugreifen, die an das lokale Benutzergerät angeschlossen sind. Dem Benutzer des Benutzergeräts erscheinen die Anwendungen und Systemressourcen, als würden sie lokal ausgeführt. Stellen Sie sicher, dass der Server die Clientgerätzuordnung unterstützt, bevor Sie diese Funktionen verwenden.

> **Hinweis:**
>
> Das Sicherheitsmodul Security-Enhanced Linux (SELinux) kann sich auf die Clientlaufwerkzuordnung und die USB-Umleitung auswirken. Dieses Modell gilt sowohl für Citrix Virtual Apps and Desktops als auch auf Citrix DaaS. Wenn Sie eines dieser Features (oder beide) benötigen, deaktivieren Sie SELinux, bevor Sie es auf dem Server konfigurieren.

Es gibt zwei Arten von Laufwerkzuordnung:

- Statische Clientlaufwerkzuordnung: Hiermit können Administratoren einen beliebigen Teil des Dateisystems auf dem Benutzergerät bei der Anmeldung einem bestimmten Laufwerk auf dem Server zuordnen. Beispielsweise können das Basisverzeichnis eines Benutzers oder der tem-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

poräre Ordner (/tmp) ganz oder teilweise zugeordnet werden. Auch die Bereitstellungspunkte von Massenspeichergeräten wie CD-ROMs, DVDs oder USB-Sticks lassen sich zuordnen.

- Dynamische Clientlaufwerkzuordnung: Dient zum Überwachen der Verzeichnisse, in denen Massenspeichergeräte wie CD-ROMs, DVDs und USB-Sticks üblicherweise auf dem Benutzergerät bereitgestellt werden. Geräte, die der Sitzung neu hinzugefügt werden, werden automatisch dem nächsten verfügbaren Laufwerksbuchstaben auf dem Server zugeordnet.

Wenn eine Verbindung zwischen der Citrix Workspace-App und Citrix Virtual Apps and Desktops bzw. Citrix DaaS hergestellt wird, werden die Clientlaufwerkzuordnungen wiederhergestellt, es sei denn, die Clientgerätzuordnung ist deaktiviert. Sie können mit Richtlinien genauer steuern, wie die Clientgerätzuordnung angewendet wird. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

Benutzer können Laufwerke im Dialogfeld **Einstellungen** zuordnen.

> **Hinweis:**
>
> Standardmäßig wird durch das Aktivieren der statischen Clientlaufwerkszuordnung auch die dynamische Clientlaufwerkszuordnung aktiviert. Um nur die statische Clientlaufwerkzuordnung und nicht die dynamische Clientlaufwerkzuordnung zu aktivieren, legen Sie `DynamicCDM` in `wfclient.ini` auf **False** fest.

Ab Version 2101 gibt es für den Zugriff auf zugeordnete Laufwerke ein zusätzliches Sicherheitsfeature.

Sie können jetzt die Zugriffsebene für das zugeordnete Laufwerk für jeden Store in einer Sitzung auswählen.

Um zu verhindern, dass das Dialogfeld für die Zugriffsebene jedes Mal angezeigt wird, wählen Sie die Option **Nicht wieder fragen** aus. Die Einstellung wird auf diesen bestimmten Store angewendet.

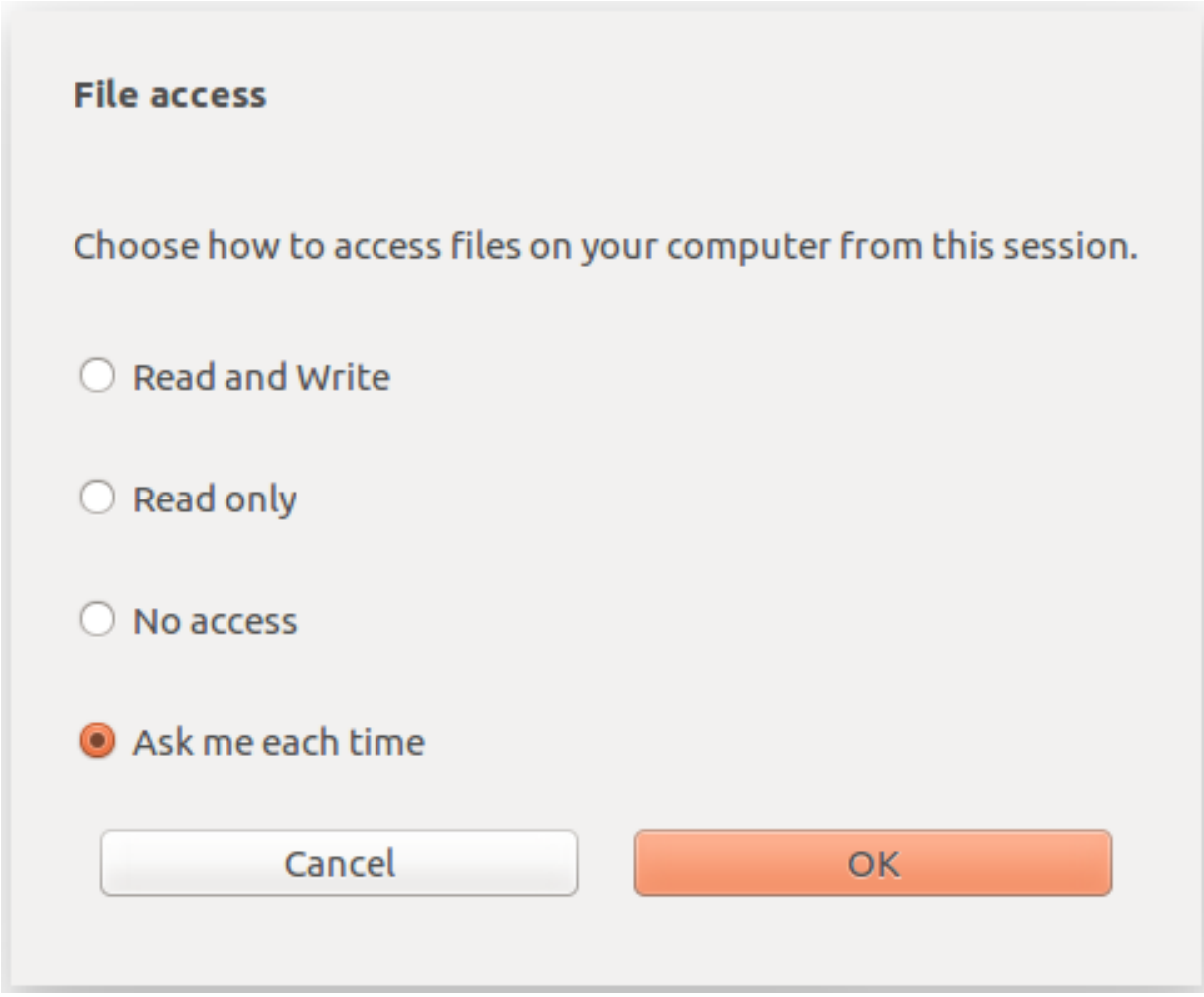
Andernfalls können Sie die Zugriffsebenen bei jedem Sitzungsstart festlegen.

Bisher wurde Ihre Einstellung für den Dateizugriff über CDM auf alle konfigurierten Stores angewendet.

Ab Version 2012 ermöglicht die Citrix Workspace-App die Konfiguration des CDM-Dateizugriffs pro Store.

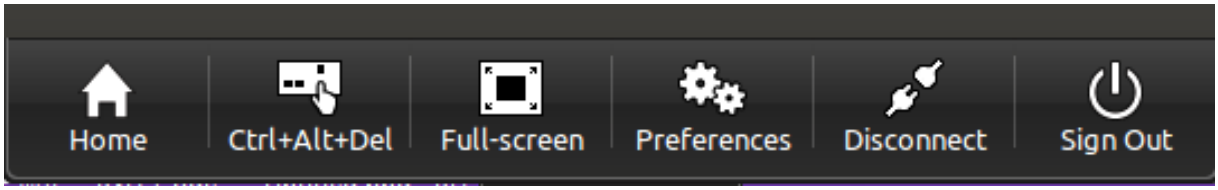
> **Hinweis:**
>
> Die Einstellung für den Dateizugriff ist nicht in allen Sitzungen persistent, wenn Workspace für Web verwendet wird. Es wird standardmäßig die Option **Jedes Mal fragen** verwendet.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



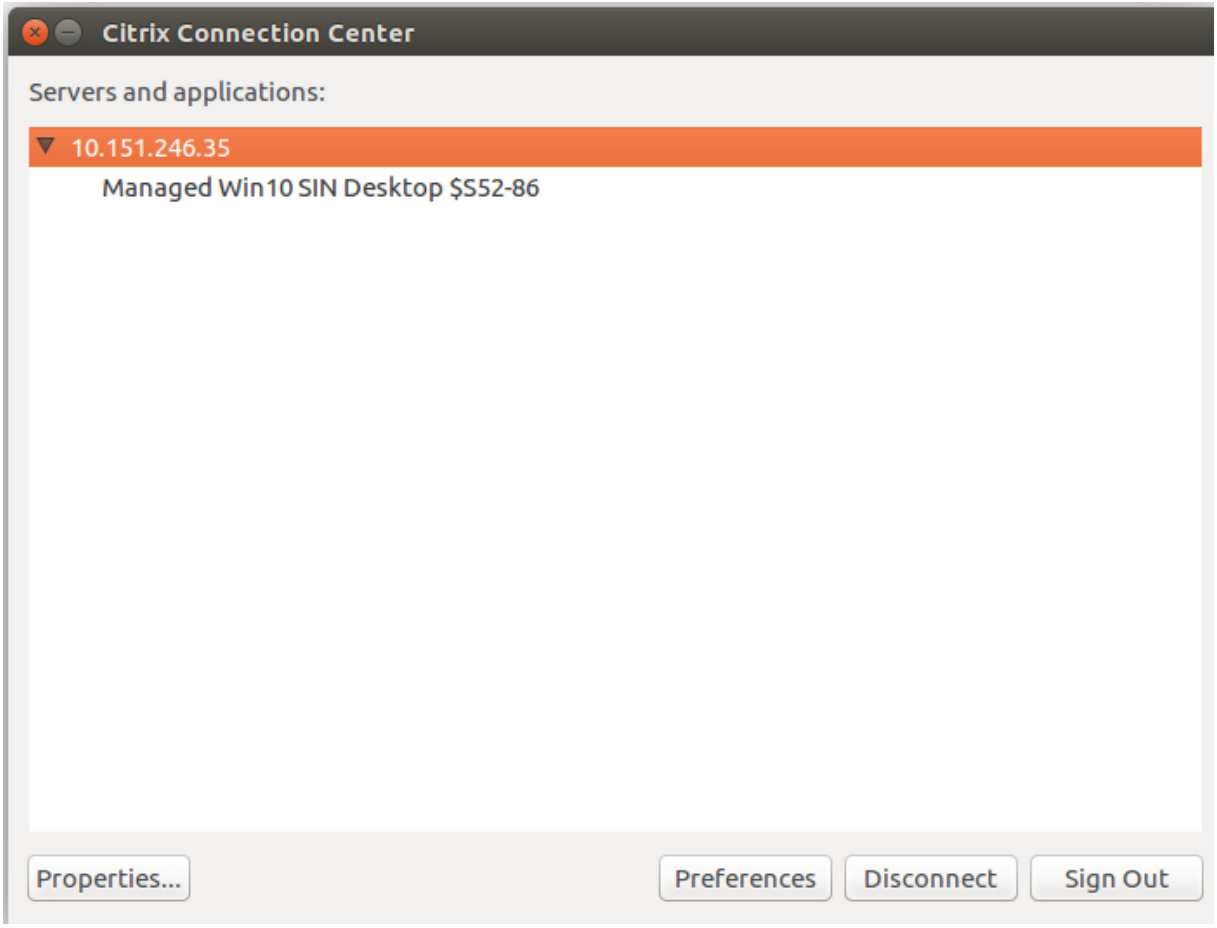
Mit der Datei `wfclient.ini` können Sie den zugeordneten Pfad und die Dateinamenattribute konfigurieren. Verwenden Sie die GUI, um eine Dateizugriffsebene festzulegen, wie im obigen Screenshot angezeigt.

In einer Desktopsitzung können Sie eine Dateizugriffsebene festlegen, indem Sie im Desktop Viewer zum Dialogfeld **Einstellungen** > **Dateizugriff** navigieren.



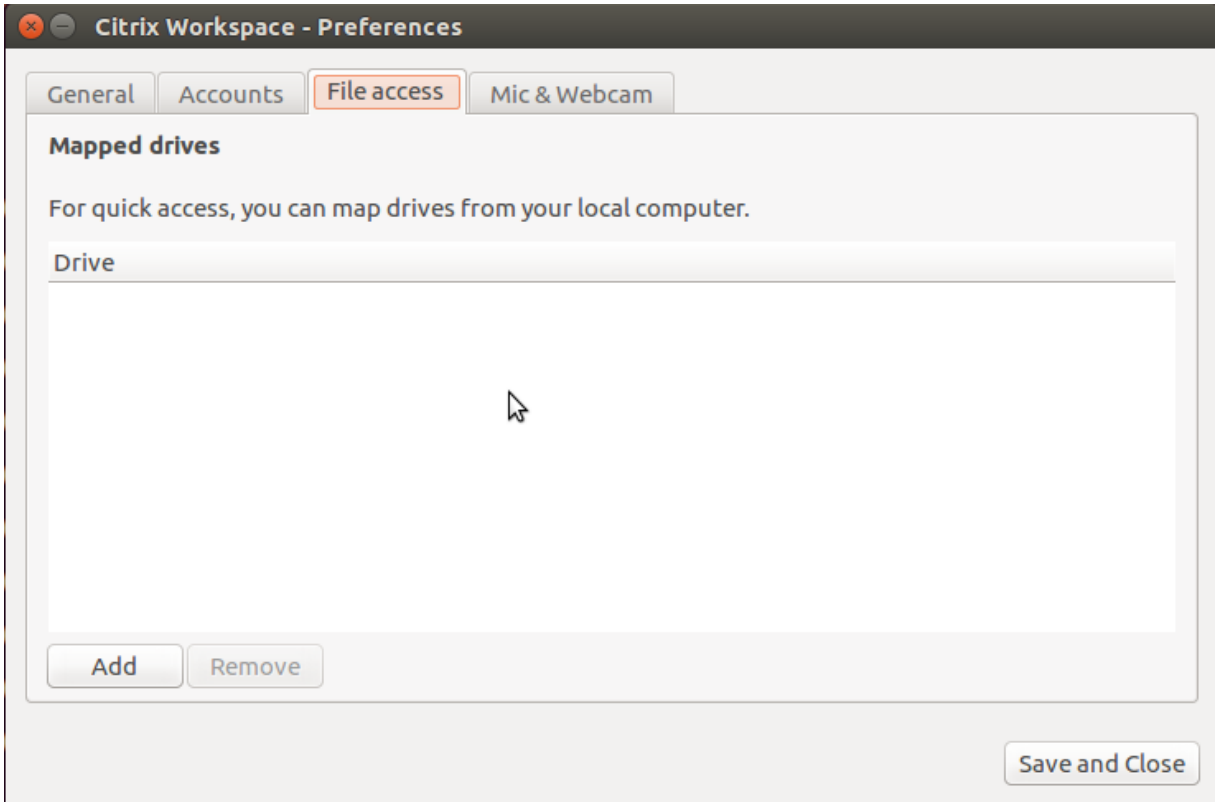
In einer App-Sitzung können Sie eine Dateizugriffsebene festlegen, indem Sie im **Citrix Connection Center** das Dialogfeld **Dateizugriff** öffnen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Das Dialogfeld **Dateizugriff** enthält Namen und Pfad des zugeordneten Ordners.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Das Flag für die Zugriffsebene wird in der Datei `wfclient.ini` nicht mehr unterstützt.

Zuordnen von Clientdruckern

Die Citrix Workspace-App unterstützt das Drucken auf Netzwerkdruckern und auf lokal an Benutzergeräte angeschlossenen Druckern. Citrix Virtual Apps and Desktops bzw. Citrix DaaS ermöglicht Benutzern Folgendes, außer wenn Sie dies durch Richtlinien verhindern:

- Drucken auf allen Druckgeräten, die vom Benutzergerät aus verfügbar sind
- Hinzufügen von Druckern

Diese Einstellungen sind jedoch möglicherweise nicht für alle Umgebungen optimal. Beispielsweise ist die Standardeinstellung, bei der Benutzer alle Drucker verwenden können, auf die sie über das Benutzergerät zugreifen können, anfänglich die am einfachsten zu verwaltende Lösung. Die Standardeinstellung kann jedoch in manchen Umgebungen zu langen Anmeldezeiten führen. In solchen Situationen sollten Sie die Liste der auf dem Benutzergerät konfigurierten Drucker einschränken.

Die Sicherheitsrichtlinien des Unternehmens könnten es zudem erforderlich machen, dass Sie das benutzerseitige Zuordnen lokaler Druckerports nicht zulassen. Hierfür wählen Sie für die ICA-Richtlinie **Client-COM-Ports automatisch verbinden** auf dem Server die Einstellung “Deaktiviert”.

Einschränken der Liste der auf dem Benutzergerät konfigurierten Drucker:

1. Öffnen Sie die Konfigurationsdatei wfclient.ini in einem der folgenden Verzeichnisse:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Im Verzeichnis $HOME/.ICAClient, um die automatisch erstellten Drucker für einen einzelnen Benutzer einzuschränken.
- Im Verzeichnis $ICAROOT/config, um die Drucker für alle Workspace-App-Benutzer einzuschränken. In diesem Fall sind “alle Benutzer” diejenigen, die das Self-Service-Programm nach der Änderung zuerst verwenden.

2. Geben Sie im Abschnitt [WFClient] der Datei Folgendes ein:

   ClientPrinterList=printer1:printer2:printer3

   Dabei sind Drucker1, Drucker2 usw. die Namen der ausgewählten Drucker. Trennen Sie die Einträge für die Druckernamen mit einem Doppelpunkt (:).

3. Speichern und schließen Sie die Datei.

Zuordnen eines lokalen Druckers

Die Citrix Workspace-App für Linux unterstützt den universellen Citrix PS Druckertreiber. Daher ist normalerweise keine lokale Konfiguration erforderlich, damit Benutzer mit Netzwerkdruckern oder Druckern, die an die lokalen Benutzergeräte angeschlossen sind, drucken können. Sie müssen Clientdrucker unter Citrix Virtual Apps and Desktops bzw. Citrix DaaS für Windows u. U. manuell zuordnen, wenn z. B. die Drucksoftware des Benutzergeräts nicht den universellen Druckertreiber unterstützt.

Zuordnen eines lokalen Druckers auf einem Server:

1. Starten Sie eine Serververbindung von der Citrix Workspace-App und melden Sie sich an einem Server an, auf dem Citrix Virtual Apps and Desktops bzw. Citrix DaaS ausgeführt wird.
2. Wählen Sie im Startmenü **Einstellungen > Drucker**.
3. Wählen Sie im Menü “Datei” die Option **Drucker hinzufügen**.

   Der Druckerinstallationsassistent wird angezeigt.

4. Fügen Sie mit dem Assistenten einen Netzwerkdrucker aus dem Clientnetzwerk und der Clientdomäne hinzu. Hierbei handelt es sich normalerweise um einen Standarddruckernamen, vergleichbar mit Werten, die durch native Remotedesktopdienste erstellt werden, z. B. “HP LaserJet 4 von Clientname in Sitzung 3”.

   Weitere Informationen zum Hinzufügen von Druckern finden Sie in der Dokumentation zum Windows-Betriebssystem.

Audio

Ab Version 2112 ist das Attribut `VdcamVersion4Support` in der Datei `module.ini` umbenannt in `AudioRedirectionV4`. Ab Version 2212 lautet der Standardwert von `AudioRedirectionV4` **True**. Dies bewirkt Folgendes:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Die PulseAudio-Bibliothek wird für den Zugriff auf die Audiogeräte verwendet und es werden zusätzliche Geräte unterstützt.
- Mehrere Apps können gleichzeitig die Audiogeräte verwenden.
- Die Citrix Workspace-App für Linux zeigt alle lokalen Audiogeräte an, die in einer Sitzung verfügbar sind. Anstelle von Citrix HDX Audio werden die Audiogeräte mit den entsprechenden Gerätenamen aufgeführt. In einer Sitzung können Sie dynamisch zu jedem der verfügbaren Geräte wechseln.
- Sitzungen werden dynamisch aktualisiert, wenn Sie Audiogeräte anschließen oder entfernen.

Wenn Sie `AudioRedirectionV4` auf **False** setzen, hat dies folgende Auswirkungen:

- Die ALSA-Bibliothek wird für den Zugriff auf die Audiogeräte verwendet und es wird nur ein einziges Gerät unterstützt.
- Es wird nur das Standardaudiogerät "Citrix HDX Audio" in der Sitzung angezeigt.
- Es kann immer nur eine App das Citrix HDX Audio-Gerät verwenden.

Gehen Sie wie folgt vor, um `AudioRedirectionV4` auf **False** zu setzen:

1. Navigieren Sie zum Ordner `<ICAROOT>/config` und öffnen Sie die Datei `module.ini`.
2. Gehen Sie zum Abschnitt [ClientAudio] und fügen Sie folgenden Eintrag hinzu:

   AudioRedirectionV4=False
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Unterstützung der Audioaufzeichnung

Ab Version 2212 ist das Feature zur Audioaufzeichnung standardmäßig aktiviert. Die Geräte zur Audioaufzeichnung werden angezeigt, wenn eine Sitzung beginnt.

Um dieses Feature zu deaktivieren, legen Sie in der Datei `wfclient.ini` den Wert für `AllowAudioInput` auf *False* fest.

> **Hinweise:**
>
> - Die Option **Mikrofon und Webcam** im Dialogfeld **Einstellungen** ist standardmäßig deaktiviert. Informationen zum Aktivieren von Mikrofon und Webcam finden Sie unter Einstellungen.
> - In der Citrix Workspace-App Version 2010 wurden Probleme behoben, um das Multistream-ICA-Feature zu verbessern.

Bekannte Einschränkungen:

Standardmäßig ist `AudioRedirectionV4` auf **True** festgelegt. Wenn der Wert von `AudioRedirectionV4` auf **True** gesetzt wird gilt folgende bekannte Einschränkung:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie eine Sitzung über die Befehlszeilenschnittstelle mit Root-Privileg starten, lehnt der PulseAudio-Server möglicherweise den Verbindungsversuch ab. In diesem Fall verwenden die Audiogeräte möglicherweise die ALSA-Bibliothek, die nur einzelne Geräte unterstützt.

Wenn Sie `AudioRedirectionV4` auf **False** festlegen, gelten die folgenden bekannten Einschränkungen:

- Auf VDAs mit Windows Server 2016 können Sie die Audiogerätauswahl in einer Sitzung nicht ändern. Die Auswahl ist auf den Standardaudioeingang und -ausgang beschränkt. Diese Einschränkung gilt nicht, wenn Sie den Wert `AudioRedirectionV4` auf **True** setzen.
- Die Audiogerätumleitung wird für Bluetooth-Audiogeräte nicht unterstützt. Diese Einschränkung gilt nicht, wenn Sie den Wert `AudioRedirectionV4` auf **True** setzen.
- Sie können das Standardaudiogerät nur unter Windows 10, Windows 7 und Windows 8 ändern. Unter Windows Server-Betriebssystemen wie Windows Server 2012, 2016 und 2019 können Sie das Standardaudiogerät nicht ändern. Dies gilt aufgrund einer Einschränkung in der Microsoft-Remotedesktopsitzung.
- Die Audiogerätumleitung wird für HDMI-Audiogeräte nicht unterstützt. Diese Einschränkung gilt nicht, wenn Sie den Wert `AudioRedirectionV4` auf **True** setzen. Die Citrix Workspace-App zeigt jedoch möglicherweise HDMI-Audiogeräte an, die nicht in einer Sitzung verbunden sind.

Wenn der Wert `AudioRedirectionV4` auf **False** gesetzt wird, ist das Standardaudiogerät normalerweise das Standard-ALSA-Gerät, das für Ihr System konfiguriert ist. Mit der folgenden Methode können Sie ein anderes Gerät festlegen:

1. Wählen Sie je nachdem, für welche Benutzer die Änderungen gelten sollen, die entsprechende Konfigurationsdatei aus und öffnen Sie sie. Informationen dazu, wie sich Änderungen in bestimmten Konfigurationsdateien auf bestimmte Benutzer auswirken, finden Sie unter Standardeinstellungen.
2. Fügen Sie die folgende Option hinzu. Wenn dieser Abschnitt nicht vorhanden ist, erstellen Sie ihn.

```
[ClientAudio]

AudioDevice = \<device\>
<!--NeedCopy-->
```

In diesem Abschnitt befinden sich die Geräteinformationen in der ALSA-Konfigurationsdatei auf Ihrem Betriebssystem.

> **Hinweis:**
>
> Der Speicherort für diese Informationen ist nicht auf allen Linux-Betriebssystemen einheitlich.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Citrix empfiehlt, in der Dokumentation Ihres Betriebssystems nachzulesen, wo Sie diese Informationen finden können.

Verbesserung der Audioqualität

Bisher betrug der maximale Ausgabepufferwert für die nahtlose Audiowiedergabe in der Citrix Workspace-App 200 ms, weshalb bei der Wiedergabe eine Latenz von 200 ms hinzukam. Dieser maximale Ausgabepufferwert wirkte sich auch auf interaktive Audioanwendungen aus.

Mit dieser Verbesserung wird der maximale Ausgabepufferwert in der Citrix Workspace-App auf 50 ms verringert, wodurch die Benutzererfahrung bei interaktiven Audioanwendungen verbessert wird. Außerdem wird die Roundtripzeit (RTT) um 150 ms verringert.

Ab Version 2207 können Sie den entsprechenden Wiedergabeschwellenwert und den PulseAudio-Vorpuffer auswählen, um die Audioqualität zu verbessern. Für diese Verbesserung werden die folgenden Parameter im Abschnitt [ClientAudio] der Datei `module.ini` hinzugefügt:

- `PlaybackDelayThreshV4`: Anfänglicher Ausgabepufferwert in Millisekunden. Die Citrix Workspace-App versucht, diesen Pufferwert während der gesamten Dauer einer Sitzung aufrechtzuerhalten. Der Standardwert von `PlaybackDelayThreshV4` ist 50 ms. Dieser Parameter ist nur gültig, wenn `AudioRedirectionV4` auf **True** gesetzt ist.
- `AudioTempLatencyBoostV4`: Wenn der Audiodurchsatz plötzlich ansteigt oder für ein instabiles Netzwerk nicht ausreicht, erhöht dieser Wert den Ausgabepufferwert. Diese Erhöhung des Ausgangspufferwerts sorgt für ein gleichmäßiges Audio. Die Wiedergabe kann jedoch leicht verzögert sein. Der Standardwert von `AudioTempLatencyBoostV4` ist auf 100 ms festgelegt. Dieser Parameter ist nur gültig, wenn `AudioRedirectionV4` auf **True** und `AudioLatencyControlEnabled` auf **True** festgelegt sind. Standardmäßig ist der Wert von `AudioLatencyControlEnabled` auf “True” festgelegt.

Standardmäßig ist der Wert von `AudioRedirectionV4` auf “True” festgelegt. Um das Feature zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zum Ordner <`ICAROOT`>/`config` und öffnen Sie die Datei module.ini.
2. Gehen Sie zum Abschnitt [ClientAudio] und fügen Sie folgenden Eintrag hinzu:

   AudioRedirectionV4=False
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Verbesserte Unterstützung der Audioechounterdrückung

Ab Version 2303 unterstützt die Citrix Workspace-App die Echounterdrückung. Dieses Feature wurde für Echtzeitaudio entwickelt und verbessert die Benutzererfahrung. Die Echounterdrückung unterstützt Audio mit niedriger Qualität, mittlerer Qualität und adaptives Audio. Citrix empfiehlt, adaptives Audio für eine bessere Leistung zu verwenden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die Echounterdrückung ist standardmäßig deaktiviert. In Echtzeit-Fällen wird empfohlen, die Echounterdrückung einzuschalten, wenn der Lautsprecher anstelle des Headsets verwendet wird.

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

1. Navigieren Sie zum Ordner <ICAROOT>/config und öffnen Sie die Datei module.ini.
2. Aktualisieren Sie im Abschnitt [ClientAudio] den Wert des Parameters EnableEchoCancellation wie folgt:

   ```
   EnableEchoCancellation =TRUE
   ```

Einschränkung:

Die Echounterdrückung ist für hochwertige Audioqualität standardmäßig deaktiviert.

Hinzufügen eines clientseitigen Jitter-Puffermechanismus

Ab Version 2305 sorgt die Citrix Workspace-App auch bei schwankender Netzwerklatenz für gute Audioqualität. Standardmäßig ist dieses Feature aktiviert.

Um das Feature zu deaktivieren, navigieren Sie zur Konfigurationsdatei /opt/Citrix/ICAClient/config/module.ini und bearbeiten JitterBufferEnabled=FALSE.

Zuordnen von Clientaudio

Die Clientaudiozuordnung ermöglicht es, dass auf Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Servern ausgeführte Anwendungen Audiodaten über ein auf dem Benutzergerät installiertes Audiogerät abspielen. Sie können die Audioqualität auf dem Server auf Verbindungsbasis festlegen und Benutzer können sie auf dem Benutzergerät einstellen. Bei unterschiedlichen Einstellungen wird die niedrigere Einstellung verwendet.

Die Clientaudiozuordnung kann zu einer Überlastung der Server und des Netzwerks führen. Je höher die Audioqualität, desto größer die erforderliche Bandbreite für die Übertragung der Audiodaten. Bei der höheren Audioqualität wird außerdem auch mehr Server-CPU in Anspruch genommen.

Sie können die Clientaudiozuordnung mithilfe von Richtlinien konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

Adaptives Audio

Ab Version 2109 wird adaptives Audio von der Citrix Workspace-App unterstützt. Bei adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht manuell konfigurieren. Adaptives Audio optimiert die Einstellungen für Ihre Umgebung und ersetzt veraltete Audiokomprimierungsformate für eine hervorragende Benutzererfahrung. Adaptives Audio ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Adaptives Audio.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Ab Version 2112 funktioniert adaptives Audio bei der Bereitstellung von Audio über UDP (User Datagram Protocol).

Bekannte Einschränkung:

- Adaptives Audio erfordert CPU-Prozessoren, die Streaming SIMD Extensions (SSE) 4.x unterstützen. Die Citrix Workspace-App wird möglicherweise geschlossen, wenn adaptives Audio mit einem CPU-Prozessor verwendet wird, der SSE 4.x nicht unterstützt.

Aktivieren von UDP-Audio

UDP-Audio kann die Qualität von Telefonanrufen über das Internet verbessern. Es verwendet UDP statt TCP.

Ab Version 2112 funktioniert adaptives Audio bei der Bereitstellung von Audio über UDP. Ab dieser Version wird außerdem das DTLS-Protokoll (Datagram Transport Layer Security) für UDP-Audio von der Citrix Workspace-App unterstützt. Sie können daher über Citrix Gateway auf das UDP-Audio zugreifen. Standardmäßig ist dieses Feature deaktiviert.

Ab Version 2202 unterstützt die Citrix Workspace-App UDP-Audio über Citrix Gateway.

Aktivieren von UDP-Audio:

1. Stellen Sie die folgenden Optionen in module.ini im Abschnitt [ClientAudio] ein:
   - `EnableUDPAudio` auf **True**. Der Standardwert ist **False**, wodurch UDP-Audio deaktiviert wird.
   - Geben Sie mit `UDPAudioPortLow` und `UDPAudioPortHigh` Minimum und Maximum für die Portnummern von UDP-Audiodatenverkehr an. Standardmäßig werden die Ports 16500 - 16509 verwendet.
2. Adaptives Audio ist standardmäßig auf dem VDA aktiviert und unterstützt UDP-Audio. Wenn adaptives Audio deaktiviert ist, wählen Sie zur Unterstützung von UDP-Audio folgende Client- und Serveraudioeinstellungen. Dies führt dann zu einer mittleren Audioqualität (also weder hoch noch niedrig).

		Audioqualität auf dem Client	Audioqualität auf dem Client	Audioqualität auf dem Client
		Hoch	Medium	Niedrig
Audioqualität auf dem Server	Hoch	Hoch	Medium	Niedrig
Audioqualität auf dem Server	Medium	Medium	Medium	Niedrig
Audioqualität auf dem Server	Niedrig	Niedrig	Niedrig	Niedrig

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Aktivieren von UDP-Audio über Citrix Gateway:

1. Navigieren Sie zum Ordner <ICAROOT>/config und öffnen Sie die Datei module.ini.
2. Gehen Sie zum Abschnitt [WFClient] und legen Sie folgenden Eintrag fest:

   EnableUDPThroughGateway=True
3. Gehen Sie zum Abschnitt [ClientAudio] und legen Sie folgenden Eintrag fest:

   EnableUDPAudio=True

> **Hinweis:**
>
> Wenn Sie die StoreFront-Konfiguration von default.ica verwenden, hat der im Abschnitt [Application] festgelegte Wert für EnableUDPThroughGateway Vorrang vor dem Wert in der Datei module.ini. Sie können den Wert EnableUDPAudio im Abschnitt [ClientAudio] jedoch nur mit der Datei module.ini festlegen. Er hat auch keinen Vorrang vor dem Wert, der in default.ica in der StoreFront-Konfiguration festgelegt ist.

Einschränkungen:

- UDP-Audio ist nicht für verschlüsselte Sitzungen verfügbar (solche, die TLS- oder ICA-Verschlüsselung verwenden). In solchen Sitzungen verwenden Audioübertragungen TCP.
- Die ICA-Kanalpriorität kann UDP-Audio beeinflussen.

UDP auf dem Client

1. Navigieren Sie zur Datei $ICAROOT/config/module.ini.
2. Stellen Sie im Abschnitt [ClientAudio] Folgendes ein:

   EnableUDPAudio=True

   UDPAudioPortLow=int

   UDPAudioPortHigh=int
3. Stellen Sie im Abschnitt [WFClient] Folgendes ein:

   EnableUDPThroughGateway=True
4. Navigieren Sie zur Datei $HOME/.ICAClient/wfclient.ini.
5. Stellen Sie im Abschnitt [WFClient] Folgendes ein:

   AllowAudioInput=True

   EnableAudioInput=true

   AudioBandWidthLimit=1

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweise:**
>
> - Die für die Attribute `AllowAudioInput`, `EnableAudioInput` und `AudioBandWidthLimit` im Abschnitt [WFClient] festgelegten Werte gelten sowohl für UDP-Audio als auch für TCP-Audio.
> - Wenn der Ordner `.ICAClient` nicht vorhanden ist (nur beim Starten nach Erstinstallation), starten Sie die Citrix Workspace-App und schließen Sie die App. Mit dieser Aktion wird der Ordner `.ICAClient` erstellt.
> - Wenn das `AudioBandWidthLimit` auf 1 eingestellt ist, ist die Audioqualität auf dem Client mittel.

6. Legen Sie folgende Richtlinien auf dem Domain Delivery Controller (DDC) fest:
    - Wählen Sie für “Windows Media-Umleitung” die Einstellung “Nicht zugelassen”.
    - Wählen Sie für “Audio über UDP” die Einstellung “Zugelassen”.
    - Wählen Sie für “Audio über UDP - Real-time Transport” die Einstellung “Aktiviert”.
    - Wählen Sie für “Audioqualität” die Einstellung “Mittel”.

Ändern der Verwendungsweise der Citrix Workspace-App

Die ICA-Technologie ist äußerst optimiert und stellt normalerweise keine hohen Anforderungen an CPU und Bandbreite. Wenn Sie jedoch eine Verbindung mit sehr geringer Bandbreite verwenden, beachten Sie zur Aufrechterhaltung der Leistung Folgendes:

- **Vermeiden Sie den Zugriff auf große Dateien unter Verwendung der Clientlaufwerkszuordnung**: Wenn Sie über die Clientlaufwerkzuordnung auf eine große Datei zugreifen, wird diese über die Serververbindung übertragen. Bei langsamen Verbindungen kann diese Dateiübertragung sehr lange dauern.
- **Vermeiden Sie das Drucken von großen Dokumenten auf lokalen Druckern**: Wenn Sie ein Dokument auf einem lokalen Drucker drucken, wird die zu druckende Datei über die Serververbindung übertragen. Bei langsamen Verbindungen kann diese Dateiübertragung sehr lange dauern.
- **Vermeiden Sie das Abspielen von Multimediainhalten**. Die Wiedergabe von Multimediainhalten benötigt viel Bandbreite und kann die Leistung reduzieren.

USB

Mit der USB-Unterstützung können Benutzer mit zahlreichen USB-Geräten interagieren, wenn sie mit einem virtuellen Desktop verbunden sind. Benutzer können USB-Geräte an ihren Computer anschließen. Diese werden dann zum virtuellen Desktop umgeleitet, nachdem die automatische Umleitung manuell über die Konfigurationsdateieinstellungen aktiviert wurde. Die automatische

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Umleitung von USB-Geräten ist standardmäßig deaktiviert. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören:

- Flashlaufwerke
- Smartphones
- PDAs
- Drucker
- Scanner
- MP3-Player
- Sicherheitsgeräte
- Tablets

Für die USB-Umleitung ist Citrix Virtual Apps and Desktops 7.6 oder höher erforderlich.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz oder hoher Geschwindigkeit unterstützt. Normalerweise ist jedoch die Standardaudio- oder Webcamumleitung besser geeignet.

Die folgenden Gerätetypen werden direkt in Sitzungen mit virtuellen Apps und Desktops unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards
- Headsets
- Webcams

> **Hinweis:**
>
> USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie unter CTX119722.

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über Citrix Virtual Apps and Desktops bzw. Citrix DaaS unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting der Netzwerkkarte wäre in diesem Fall nicht angebracht. Die folgenden USB-Gerätetypen können standardmäßig nicht für virtuelle Apps und Desktops verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs

Um die Standardliste von USB-Geräten für Remoting zu aktualisieren, bearbeiten Sie die Datei `usb.conf` im Ordner `$ICAROOT/`. Weitere Informationen finden Sie unter “Aktualisieren der für Remoting

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

verfügbaren USB-Geräteliste".

Um Remoting von USB-Geräten zu virtuellen Desktops zuzulassen, aktivieren Sie die USB-Richtlinienregel. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

Funktionsweise der USB-Unterstützung

Wenn ein Benutzer ein USB-Gerät anschließt, wird es anhand der USB-Richtlinie überprüft. Und, falls zugelassen, an den virtuellen Desktop umgeleitet. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Angenommen, ein Benutzer schließt ein USB-Gerät an einem Desktop an, auf den im Desktopgerätemodus zugegriffen wird. In diesem Fall wird das Gerät automatisch zum virtuellen Desktop umgeleitet, nachdem die automatische Umleitung manuell über die Konfigurationsdatei aktiviert wurde. Die automatische Umleitung von USB-Geräten ist standardmäßig deaktiviert. Gehen Sie wie folgt vor, um die automatische Umleitung von USB-Geräten zu konfigurieren:

1. Navigieren Sie zur Konfigurationsdatei `$Home/.ICAClient/wfclient.ini`.
2. Fügen Sie folgenden Eintrag hinzu:

   DesktopApplianceMode=True
3. Gehen Sie zur Konfigurationsdatei `/opt/Citrix/ICAClient/usb.conf`.
4. Legen Sie eine der folgenden Geräteregeln fest:

   - CONNECT: Legen Sie das Schlüsselwort CONNECT fest, um die automatische Umleitung eines Geräts zu aktivieren, wenn eine Sitzung beginnt.
   - ALLOW: Legen Sie das Schlüsselwort ALLOW fest, um die automatische Umleitung eines Geräts erst nach Beginn einer Sitzung zuzulassen
     Wenn jedoch das Schlüsselwort CONNECT oder ALLOW festgelegt ist, wird das Gerät automatisch umgeleitet, wenn es während einer Sitzung getrennt und wieder verbunden wird.

   Beispielgeräteregel:
   CONNECT: vid=046D pid=0002 # Bestimmtes Gerät gemäß vid/pid zulassen
   ALLOW: vid=046D pid=0102 # Bestimmtes Gerät gemäß vid/pid zulassen

Das Sitzungsfenster muss den Fokus haben, wenn der Benutzer das USB-Gerät für die Umleitung anschließt, es sei denn, der Desktop Appliance Mode wird verwendet.

Bekannte Einschränkung:

Bei der USB-Umleitung funktionieren die in der Datei `usb.conf` definierten Richtlinien möglicherweise nicht und die USB-Geräte werden u. U. nicht in die Sitzung umgeleitet. Dieses Problem tritt auf,

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

wenn die Datei `usb.conf` mehr als 2000 Zeichen enthält. Als Workaround entfernen Sie die vorhandenen Kommentare zu den Richtlinien, um die Anzahl der Zeichen in der Datei `usb.conf` zu reduzieren.

Massenspeichergeräte

Angenommen, ein Benutzer trennt die Verbindung zu einem virtuellen Desktop, während ein USB-Massenspeichergerät noch am lokalen Desktop angeschlossen ist. In diesem Fall wird das Gerät nicht an den virtuellen Desktop umgeleitet, wenn der Benutzer die Verbindung wiederherstellt. Um sicherzustellen, dass das Massenspeichergerät an den virtuellen Desktop umgeleitet wird, muss der Benutzer es entfernen und nach der Wiederherstellung der Verbindung wieder anschließen.

> **Hinweis:**
>
> Wenn Sie ein Massenspeichergerät an eine Linux-Workstation anschließen, die keine Remoteverbindungen von USB-Massenspeichergeräten zulässt, wird das Gerät von der Citrix Workspace-App nicht akzeptiert. Möglicherweise wird ein separater Linux-Dateibrowser geöffnet. Citrix empfiehlt daher, Benutzergeräte so zu konfigurieren, dass die Einstellung **Wechselmedien beim Einlegen einbinden** standardmäßig deaktiviert ist. Wählen Sie dazu auf Geräten mit Debian auf der Debian-Menüleiste, Folgendes: **System > Einstellungen > Wechseldatenträger und -medien**. Deaktivieren Sie auf der Registerkarte **Speichermedien** unter **Wechseldatenträger** das Kontrollkästchen **Wechselmedien beim Einlegen einbinden**.

Beachten Sie für die Client-USB-Geräteumleitung Folgendes.

> **Hinweise:**
>
> Angenommen, die Serverrichtlinie für die Client-USB-Geräteumleitung ist aktiviert. In diesem Fall werden Massenspeichergeräte wie USB-Geräte auch dann umgeleitet, wenn die Clientlaufwerkzuordnung aktiviert ist.

USB-Klassen

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln zugelassen:

- Audio (Geräteklasse 01)

  Umfasst Mikrofone, Lautsprecher, Kopfhörer und MIDI-Controller.

- Physikalische Schnittstelle (Geräteklasse 05)

  Diese Geräte ähneln Eingabegeräten (HIDs), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit. Dazu gehören u. a. Force-Feedback-Joysticks und -Exoskelette sowie Bewegungsplattformen.

- Bilder (Geräteklasse 06)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen 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 über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet. Die USB-Unterstützung wird nicht benötigt.

- Drucker (Geräteklasse 07)

  Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. Mehrfunktionsdrucker haben ggf. einen internen Hub oder sind Composite-Geräte. In beiden Fällen verwendet das Druckerelement meistens die Druckerklasse und das Scanner- oder Faxelement verwendet eine andere Klasse, z. B. Bilder.

  Drucker funktionieren normalerweise ohne USB-Unterstützung.

- Massenspeicher (Geräteklasse 08)

  Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke. Weitere Geräte sind über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, die auch eine Massenspeicherschnittstelle darstellen. Zu diesen Geräten gehören Mediaplayer, digitale Kameras und Mobiltelefone. 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. Die USB-Unterstützung wird daher nicht benötigt.

  Wichtig: Einige Viren werden aktiv mit allen Typen des Massenspeichers übertragen. Überlegen Sie genau, ob der Einsatz von Massenspeichergeräten (per Clientlaufwerkzuordnung oder USB-Unterstützung) im Unternehmen wirklich erforderlich ist. Zur Verringerung dieses Risikos kann auf dem Server konfiguriert werden, dass Dateien über die Clientlaufwerkzuordnung ausgeführt werden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Benutzer derzeit einen USB 3.0-Treiber über generische USB-Umleitung an den Linux VDA umleiten möchten, stecken sie den USB-Speicherstick in einen USB 3.0-Steckplatz.

- Content Security (Geräteklasse 0d)

  Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.

- Personal Healthcare (Geräteklasse 0f)

  Hierzu gehören beispielsweise folgende medizinische Geräte:

  - Blutdruckmessgeräte
  - Pulsmessgeräte
  - Schrittzähler
  - Geräte zur Überwachung der Medikamenteneinnahme
  - Spirometer

- Anwendung und herstellerspezifisch (Geräteklasse fe und ff)

  Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese Geräte werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

USB-Geräteklassen

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a)

  Umfasst Modems, ISDN-Adapter, Netzwerkkarten und einige Telefone und Faxgeräte.

  Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein Gerät möglicherweise die Verbindung zum virtuellen Desktop bereitstellt.

- HID (Human Interface Devices) (Geräteklasse 03)

  Umfasst viele Eingabe- und Ausgabegeräte. Typische Eingabegeräte oder HIDs (Human Interface Devices) sind folgende:

  - Tastaturen
  - Mäuse
  - Zeigegeräte
  - Grafiktabletts
  - Sensoren

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - Game Controller
  - Tasten
  - Steuerfunktionen

  Die Unterklasse 01 wird “Boot Interface”-Klasse genannt und für Tastaturen und Mäuse 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 sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.

- USB-Hub (Geräteklasse 09)

  Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.

- Chipkarte (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.

- Video (Geräteklasse 0e)

  Die Videoklasse umfasst Geräte, mit denen Videos und videobezogenes Material verwendet werden, z. B.:

  - Webcams
  - Digitale Camcorder
  - Analoge Videokonverter
  - Einige Fernsehtuner
  - Einige digitale Kameras, die Videostreaming unterstützen

  Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung.

- Kabelloser Controller (Geräteklasse e0)

  Hierzu gehören viele kabellose Controller, u. a. Ultra-Breitband-Controller und Bluetooth.

  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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Liste der USB-Geräte

Sie können den Bereich der USB-Geräte aktualisieren, die für Remoting zu Desktops verfügbar sind. Bearbeiten Sie zum Aktualisieren des Bereichs die Liste der Standardregeln in der Datei `usb.conf` auf dem Benutzergerät in `$ICAROOT/`.

Sie aktualisieren die Liste, indem Sie neue Richtlinienregeln hinzufügen, die USB-Geräte zulassen oder ablehnen, die nicht Teil des Standardumfangs sind. Von einem Administrator auf diese Weise erstellte Regeln steuern, welche Geräte dem Server angeboten werden. Die Regeln auf dem Server steuern dann, welche Geräte akzeptiert werden.

Die standardmäßige Richtlinienkonfiguration für nicht zulässige Geräte lautet folgendermaßen:

DENY: class=09 # Hub-Geräte

DENY: class=03 subclass=01 # HID-Bootgerät (Tastaturen und Mäuse)

DENY: class=0b # Smartcard

DENY: class=e0 # Wireless-Controller

DENY: class=02 # Kommunikations- und CDC-Steuerung

DENY: class=03 # UVC (webcam)

DENY: class=0a # CDC-Daten

ALLOW: # Letztes Fallback: alles andere zulassen

USB-Richtlinienregeln

Tipp: Wenn Sie Richtlinienregeln erstellen, verwenden Sie die USB-Klassencodes. Sie finden sie auf der USB-Website unter
http://www.usb.org/. Richtlinienregeln in der Datei `usb.conf` auf dem Benutzergerät haben das Format {ALLOW:|DENY:} gefolgt von einer Reihe von Ausdrücken, die auf Werten für die folgenden Tags basieren:

Tag	Beschreibung
VID	Vendor-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Tag	Beschreibung
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie eine Richtlinienregel erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen, die als Trennzeichen verwendet werden, werden ignoriert. Sie dürfen aber nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class=08 SubClass=05 eine gültige Regel; Deny: Class=0 8 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.

Beispiel

Das folgende Beispiel zeigt einen Abschnitt der Datei `usb.conf` auf dem Benutzergerät. Um diese Regeln zu implementieren, müssen dieselben Regeln wie auf dem Server vorhanden sein.

```
ALLOW: VID=1230 PID=0007 \## ANOther Industries, ANOther Flash Drive

DENY: Class=08 SubClass=05 \## Mass Storage Devices

DENY: Class=0D \## All Security Devices
```

Startmodi

Mit “Desktop Appliance Mode” können Sie anpassen, wie ein virtueller Desktop zuvor angeschlossene USB-Geräte behandelt. Legen Sie `DesktopApplianceMode = Boolean` im Abschnitt **WFClient** in der Datei `$ICAROOT/config/module.ini` auf jedem Benutzergerät wie folgt fest.

TRUE	Alle USB-Geräte, die bereits angeschlossen sind, sind beim Start verfügbar. Die Geräte stehen nur dann beim Starten zur Verfügung, wenn sie nicht durch eine Ablehnungsregel in den USB-Richtlinien auf dem Server (Registrierungseintrag) oder dem Benutzergerät (Konfigurationsdatei der Richtlinienregeln) deaktiviert wurden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

FALSE	Beim Start sind keine USB-Geräte verfügbar.

> **Hinweis:**
>
> Legen Sie das Schlüsselwort CONNECT fest, um die automatische Umleitung eines Geräts zu aktivieren, wenn eine Sitzung beginnt. Legen Sie außerdem das Schlüsselwort ALLOW fest, um die automatische Umleitung eines Geräts erst nach Beginn einer Sitzung zuzulassen. Wenn jedoch das Schlüsselwort CONNECT oder ALLOW festgelegt ist, wird das Gerät automatisch umgeleitet, wenn es während einer Sitzung getrennt und wieder verbunden wird.

Automatische Umleitung von USB-Geräten konfigurieren

Früher wurde ein Gerät, das während einer Sitzung getrennt und wieder verbunden wurde, automatisch umgeleitet. Das Gerät wurde daher automatisch mit dem VDA verbunden. Ab Release 2207 der Citrix Workspace-App müssen Sie die automatische Umleitung manuell über die Konfigurationsdatei aktivieren. Die automatische Umleitung von USB-Geräten ist standardmäßig deaktiviert.

Gehen Sie wie folgt vor, um die automatische Umleitung von USB-Geräten (normale Geräte und Verbundgeräte) zu konfigurieren:

1. Gehen Sie zu der Konfigurationsdatei $Home/.ICAClient/wfclient.ini.
2. Fügen Sie folgenden Eintrag hinzu:

   DesktopApplianceMode=True
3. Gehen Sie zur Konfigurationsdatei /opt/Citrix/ICAClient/usb.conf.
4. Legen Sie eine der folgenden Geräteregeln fest:
   - CONNECT: Legen Sie das Schlüsselwort CONNECT fest, um die automatische Umleitung eines Geräts zu aktivieren, wenn eine Sitzung beginnt.
   - ALLOW: Legen Sie das Schlüsselwort ALLOW fest, um die automatische Umleitung eines Geräts erst nach Beginn einer Sitzung zuzulassen

   Wenn jedoch das Schlüsselwort CONNECT oder ALLOW festgelegt ist, wird das Gerät automatisch umgeleitet, wenn es während einer Sitzung getrennt und wieder verbunden wird.

Beispiel für Geräteregeln:

CONNECT: vid=046D pid=0002 # Bestimmtes Gerät gemäß vid/pid zulassen‘

ALLOW: vid=046D pid=0102 # Bestimmtes Gerät gemäß vid/pid zulassen‘

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Umleitung von USB-Verbundgeräten

Ab Version 2207 erlaubt die Citrix Workspace-App das Aufteilen (Splitting) von USB-Verbundgeräten. Ein USB-Verbundgerät kann mehrere Funktionen ausführen. Dies wird erreicht, indem jede Funktion über eine andere Schnittstelle verfügbar gemacht wird. Beispiele für USB-Verbundgeräte sind HID-Geräte, die Audio-/Videoeingang und -ausgang umfassen.

Derzeit ist die Umleitung von USB-Verbundgeräten nur in Desktopsitzungen verfügbar. Die aufgeteilten Geräte werden im Desktop Viewer angezeigt.

Früher wurde ein Gerät, das während einer Sitzung getrennt und wieder verbunden wurde, automatisch umgeleitet. Das Gerät wurde daher automatisch mit dem VDA verbunden. In diesem Release müssen Sie die automatische Umleitung manuell über die Konfigurationsdatei aktivieren. Die automatische Umleitung von USB-Verbundgeräten ist standardmäßig deaktiviert.

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 Einstellung ist 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. Die lokale Nutzung des Geräts wird durch diese Aktion 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. Dies 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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

übrigen untergeordneten Geräte können durch diese Einstellung 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 USB-Standardgeräte auch werden die Verbundgeräte von in den Geräterichtlinien der Citrix Workspace-App festgelegten Geräteregeln 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.

Gehen Sie wie folgt vor, um die Geräteregeln zu ändern:

1. Gehen Sie zur Datei /opt/Citrix/ICAClient/usb.conf.
2. Aktualisieren Sie die Geräteregeln nach Bedarf.

Beispiele für Geräteregeln:

```
ALLOW: vid=046D pid=0102 ## Allow a specific device by vid/pid

ALLOW: vid=0505 class=03 subclass=01 ## Allow any pid for vendor 0505 w/
subclass=01

DENY: vid=0850 pid=040C ## deny a specific device (including all child
devices)

DENY: class=03 subclass=01 prot=01 ## deny any device that matches all
filters

CONNECT: vid=0911 pid=0C1C ## Allow and auto-connect a specific device

ALLOW: vid=0286 pid=0101 split=01 ## Split this device and allow all
interfaces

ALLOW: vid=1050 pid=0407 split=01 intf=00,01 ## Split and allow only 2
interfaces
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
CONNECT: vid=1050 pid=0407 split=01 intf=02 ## Split and auto-connect
interface 2

DENY: vid=1050 pid=0407 split=1 intf=03 ## Prevent interface 03 from being
remoted
```

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

Filterparameter	Beschreibung
vid=xxxx	Hersteller-ID des USB-Geräts (vierstelliger Hexadezimalcode)
pid=xxxx	Produkt-ID des USB-Geräts (vierstelliger Hexadezimalcode)
rel=xxxx	Release-ID des USB-Geräts (vierstelliger Hexadezimalcode)
class=xx	Klassencode des USB-Geräts (zweistelliger Hexadezimalcode)
subclass=xx	Unterklassencode des USB-Geräts (zweistelliger Hexadezimalcode)
prot=xx	Protokollcode des USB-Geräts (zweistelliger Hexadezimalcode)
split=1 (oder split=0)	Aufteilen (oder Nichtaufteilen) eines Verbundgeräts
intf=xx[,xx,xx,…]	Auswahl einer bestimmten Gruppe untergeordneter Schnittstellen eines Verbundgeräts (durch Kommas getrennte Liste mit zweistelligen Hexadezimalcodes)

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

Das USB Implementers Forum (USB-IF) bietet unter Defined Class Codes eine Liste definierter Klassen-, Unterklassen- und Protokollwerte. USB-IF bietet außerdem eine Liste registrierter Hersteller-IDs. Hersteller-, Produkt-, Release- und Schnittstellen-ID eines Geräts finden Sie auch mit kostenlosen Tools wie lsusb.

```
1  <username@username>-ThinkPad-T470:/var/log$ lsusb
2
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW

Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.

Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera

Bus 001 Device 003: ID 8087:0a2b Intel Corp.

Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver

Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver

Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.

Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

<!--NeedCopy-->
```

```
    | <username@username>-ThinkPad-T470:/var/log$ lsusb -t

    /:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000
       M

    /:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M

    /:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M

    |__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage,
       5000M

    /:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M

    |__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M

        |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=
           usbhid, 12M
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
16
17          |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=
                usbhid, 12M
18
19          |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=
                usbhid, 12M
20
21          |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12
                M
22
23          |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=,
                 12M
24
25          |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12
                M
26
27          |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12
                M
28
29          |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=
                usbhid, 12M
30
31      |__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=
            usbhid, 12M
32
33      |__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
            usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
            usbhid, 12M
36
37      |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39      |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41      |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43      |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45      |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
            |
46
47  <!--NeedCopy-->
```

Die letzten beiden Parameter gelten (sofern vorhanden) nur für USB-Verbundgeräte. Der split-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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.

Beispiel: USB-Verbundgerät mit sechs Schnittstellen (z. B. Bloomberg 4-Tastatur):

- Schnittstelle 0 – Bloomberg 4-Tastatur-HID
- Schnittstelle 1 – Bloomberg 4-Tastatur-HID
- Schnittstelle 2 – Bloomberg 4-HID
- Schnittstelle 3 – Bloomberg 4-Tastatur-Audiokanal
- Schnittstelle 4 – Bloomberg 4-Tastatur-Audiokanal
- Schnittstelle 5 – Bloomberg 4-Tastatur-Audiokanal
- Folgende Regeln werden für diese Gerätetypen empfohlen:

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=01 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=02 ## Bloomberg 4 HID

DENY: vid=1188 pid=9545 split=01 intf=03 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=04 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=05 ## Bloomberg 4 Keyboard Audio
Channel
```

Umleitung von USB-Verbundgeräten mit Citrix Viewer

Gehen Sie wie folgt vor, um die USB-Geräte über den Abschnitt **Geräte** zu verbinden:

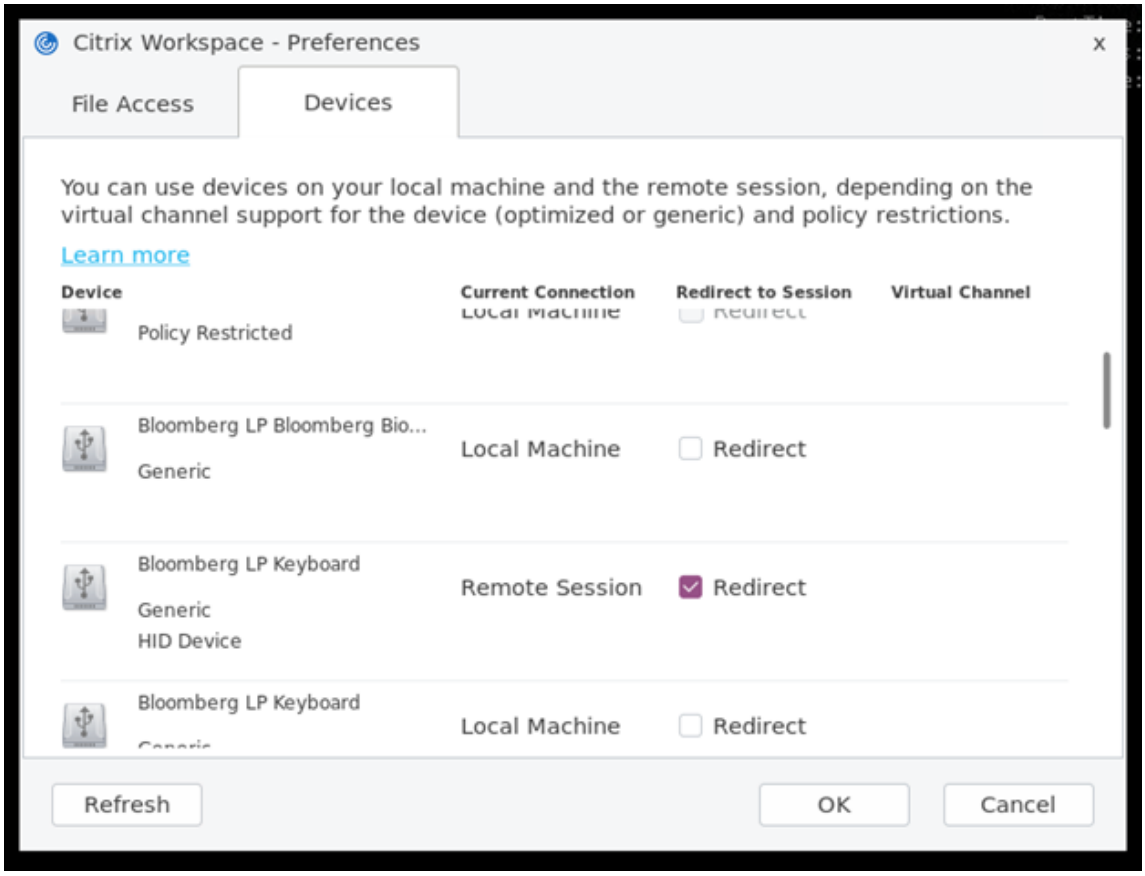
1. Gehen Sie in einer Desktopsitzung unter **Geräte** zum Desktop Viewer.
   Die aufgeteilten USB-Geräte werden angezeigt.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. Um ein Gerät zu verbinden, wählen Sie den zugehörigen Menüeintrag.

Gehen Sie wie folgt vor, um die USB-Geräte über den Abschnitt **Einstellungen** zu verbinden:

1. Gehen Sie zum Abschnitt **Einstellungen > Geräte**.
   Die aufgeteilten USB-Geräte werden angezeigt.



2. Aktivieren Sie die Kontrollkästchen der gewünschten Geräte.
3. Klicken Sie auf **OK**.

Die ausgewählte Konfiguration wird auf die Geräteverbindung angewendet.

> **Hinweis:**
>
> Deaktivieren Sie den Menüeintrag oder die Kontrollkästchen des Geräts, das Sie trennen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> möchten.

Webcams

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen müssen Benutzer Webcams mit USB-Unterstützung anschließen. Deaktivieren Sie HDX RealTime-Webcamvideokomprimierung, um Webcams mit USB-Unterstützung zu verbinden.

Webcamumleitung

Im Folgenden ein paar Hinweise zur Webcamumleitung:

- Die Webcamumleitung ist mit und ohne RTME kompatibel.
- Die Webcamumleitung funktioniert für 32-Bit- und 64-Bit-Anwendungen. Zum Beispiel für Skype und GoToMeeting. Verwenden Sie einen 32-Bit-Browser bzw. 64-Bit-Browser, um die Webcamumleitung online zu verifizieren. Beispiel: `https://webcamtests.com/`.
- Die Verwendung der Webcam ist pro Anwendung exklusiv. Wenn in Skype beispielsweise eine Webcam ausgeführt wird und Sie GoToMeeting starten, müssen Sie Skype beenden, um die Webcam in GoToMeeting zu verwenden.

Webcamumleitung für 64-Bit-Apps

Ab Release 2305 wird die Webcamumleitung für 64-Bit-Anwendungen unterstützt.

Systemanforderungen

- `GStreamer` Framework Version 0.1.x oder 1.x, je nach aktuell im System installierter Version.
- `ICAClient`-Version höher als 2106, falls `GStreamer` 1.x verwendet wird
- `Gstreamer`-Version und Plug-Ins:
  - `gstreamer1.0-plugins-base`
  - `gstreamer1.0-plugins-bad`
  - `gstreamer1.0-plugins-good`
  - `gstreamer1.0-plugins-ugly`
  - `gstreamer1.0-vaapi plugin` und `libva`-Bibliothek
  - x264-Bibliothek

> **Hinweis:**
>
> Die Versionen von `GStreamer`-Plug-In und `GStreamer`-Framework müssen übereinstimmen. Wenn Sie beispielsweise `Gstreamer`1.2.4 installieren, müssen alle `Gstreamer`1.x-Plug-Ins ebenfalls Version 1.2.4 verwenden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Konfiguration der Webcamumleitung

Führen Sie die folgenden Schritte aus, um die Webcamumleitung für 64-Bit-Apps in der Citrix Workspace-App für Linux zu aktivieren und zu konfigurieren.

Schritt 1: ICAClient-Konfiguration überprüfen

Stellen Sie den Wert `AllowAudioInput` auf **True** ein, um die Webcamumleitung zu aktivieren Standardmäßig wird dieser Wert während der Installation von `ICAClient` auf **True** festgelegt.

Wenn der Wert `AllowAudioInput` auf **False** festgelegt ist, gehen Sie wie folgt vor, um die Webcamumleitung zu aktivieren:

1. Gehen Sie zur Konfigurationsdatei `~/.ICAClient/wfclient.ini` und bearbeiten Sie sie.
2. Setzen Sie den Wert von `AllowAudioInput` auf **True**.

   AllowAudioInput=True

Schritt 2: Überprüfen der Theora-Encoder-Konfiguration

Nachdem Sie `ICAClient` erfolgreich installiert haben und der Wert `AllowAudioInput` auf **True** eingestellt ist, ist standardmäßig der Theora-Encoder konfiguriert. Dieser Encoder ist ein softwarebasierter Encoder mit akzeptabler Leistung. Dieser Encoder unterstützt jedoch nur 32-Bit-Apps auf einem VDA.

Gehen Sie wie folgt vor, um zu überprüfen, ob der Theora-Encoder 32-Bit-Apps unterstützt:

1. Installieren Sie Firefox 32-Bit auf einem VDA.
2. Rufen Sie die Webcam-Testsite unter `https://webcamtests.com/` auf.

Der Theora-Encoder unterstützt die Funktion zur Webcamumleitung für 64-Bit-Apps auf einem VDA nicht. Konfigurieren Sie den H264-Encoder zur Unterstützung der Webcamumleitung für 64-Bit-Apps auf dem VDA.

Schritt 3: Konfigurieren des H264-Encoders

Der H264-Encoder unterstützt die Webcamumleitung für 64-Bit-Apps auf dem VDA. Um den H264-Encoder zu aktivieren, müssen Sie Folgendes tun:

1. Gehen Sie zur Konfigurationsdatei `~/.ICAClient/wfclient.ini` und bearbeiten Sie sie.
2. Setzen Sie den Wert von `HDXH264InputEnabled` auf **True**.

   HDXH264InputEnabled=True

Gehen Sie wie folgt vor, um zu überprüfen, dass der H264-Encoder 64-Bit-Apps unterstützt:

1. Installieren Sie Firefox 64-Bit auf einem VDA.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. Rufen Sie die Webcam-Testsite unter `https://webcamtests.com/` auf.

Schritt 4: Systemabhängigkeiten überprüfen

Wenn die Webcamumleitung nach der Konfiguration des H264-Encoders keine 64-Bit-Apps auf dem VDA unterstützt, überprüfen Sie die Systemabhängigkeiten.

Die Webcamumleitung für die 64-Bit-App basiert auf dem `GStreamer`-Framework. `ICAClient` verwendet das `GStreamer`-Framework Version 0.1.x oder 1.x, je nach aktuell im System installierter Version.

Schritt 4.1: ICAClient-Version überprüfen

Überprüfen Sie, ob die `ICAClient`-Version größer als 2106 ist, falls `GStreamer` 1.x verwendet wird. Frühere Versionen von `ICAClient` schlagen möglicherweise fehl.

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die `ICAClient`-Version auf dem in Ihrem System installierten `GStreamer`-Framework basiert:

1. Geben Sie die folgenden Befehle an einer Befehlszeile ein:

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
ls -alh
<!--NeedCopy-->
```

2. Überprüfen Sie, ob `gst_read symlink` mit `gst_read1.0` oder `gst_read0.1.` verknüpft ist, wie in der folgenden Abbildung dargestellt:

```
28K Jan 26  2021 ctxlogd
.3M Jan 26  2021 ctx_rehash
.8M Jan 26  2021 ctxwebhelper
.0K Jan 26  2021 deploy-AppProtectionService.sh
26K Jan 26  2021 echo_cmd
30K Jan 26  2021 gst_aud_play
30K Jan 26  2021 gst_aud_read
 38 Feb 19 14:55 gst_play -> /opt/Citrix/ICAClient/util/gst_play1.0
55K Jan 26  2021 gst_play0.10
55K Jan 26  2021 gst_play1.0
 38 Feb 19 14:55 gst_read -> /opt/Citrix/ICAClient/util/gst_read1.0
51K Jan 26  2021 gst_read0.10
55K Jan 26  2021 gst_read1.0
32K Jan 26  2021 hdxcheck.sh
.1M Feb 22 10:50 HdxRtcEngine
32K Jan 26  2021 HdxRtcEngine.org
```

Sie können das Skript `workspaceappcheck.sh` auch im Verzeichnis `util` ausführen und die Ausgabe des Abschnitts überprüfen, der sich auf `GStreamer`-Abhängigkeiten bezieht.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix empfiehlt, `ICAClient` Version größer oder gleich 2106 und `GStreamer` 1.x zu verwenden.

Schritt 4.2: Gstreamer-Version und Plug-Ins überprüfen

Abgesehen vom `GStreamer` 1.x-Framework müssen Sie die folgenden erforderlichen Plug-Ins installieren:

- `Gstreamer1.0-plugins-base`
- `Gstreamer1.0-plugins-bad`
- `Gstreamer1.0-plugins-good`
- `Gstreamer1.0-plugins-ugly`
- `Gstreamer1.0-vaapi plugin`
- `ibva library`
- `x264 library`

Weitere Informationen zur Installation der genannten `plugins` finden Sie im `GStreamer` Installationshandbuch.

> **Hinweis:**
>
> Die Versionen von `GStreamer`-Plug-In und `GStreamer`-Framework müssen übereinstimmen. Wenn Sie beispielsweise `Gstreamer1.2.4` installieren, müssen alle `Gstreamer1.x`-Plug-Ins ebenfalls Version 1.2.4 verwenden.

Führen Sie den folgenden Befehl aus, um die aktuelle Version des `GStreamer`-Frameworks abzufragen:

```
gst-inspect-1.0 --gst-version
<!--NeedCopy-->
```

Informationen zur Problembehandlung finden Sie unter Webcam im Abschnitt zur Problembehandlung.

Hintergrundunschärfe für Webcamumleitung

Ab Version 2303 unterstützt die Citrix Workspace-App für Linux Hintergrundunschärfe für die Webcamumleitung. Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Navigieren Sie zur Konfigurationsdatei `~/.ICAClient/wfclient.ini`.
2. Fügen Sie der Datei wfclient.ini den folgenden Eintrag hinzu:

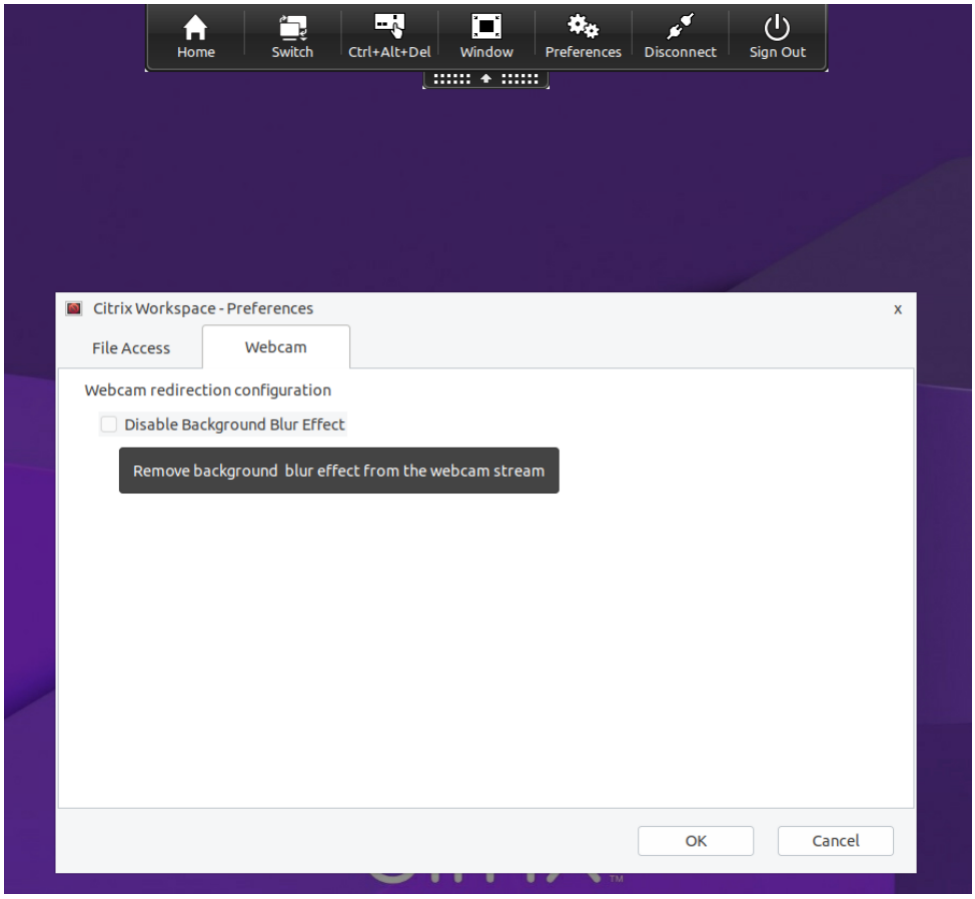
```
HDXWebCamEnableBackgndEffect=True
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Die Konfigurationseinstellung aktiviert die Hintergrundunschärfe für die Webcamumleitung für Clients mit und ohne Benutzeroberfläche.

Gehen Sie wie folgt vor, um die Hintergrundunschärfe in der Sitzung für die Webcamumleitung per GUI zu deaktivieren:

1. Klicken Sie in **Desktop Viewer** auf **Einstellungen**. Das Dialogfeld **Citrix Workspace - Einstellungen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Webcam**. Das folgende Dialogfeld wird angezeigt.



3. Aktivieren Sie das Kontrollkästchen **Hintergrundunschärfeeffekt deaktivieren**, um die Hintergrundunschärfe für die Webcamumleitung zu deaktivieren.
4. Klicken Sie auf **OK**.

Unterstützung für MJPEG-Webcams

Ab Version 2308 werden MJPEG-Webcams im H264-Stream unterstützt. Eine interne MJEPG-Komprimierung in der Webcam verbessert die Bildqualität und erhöht die Bildrate. Dieses Feature

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

ist standardmäßig aktiviert. Wenn die Webcam jedoch MJPEG nicht unterstützt, ist diese Funktion deaktiviert.

Xcapture

Das Citrix Workspace-App-Paket enthält eine Hilfsanwendung, xcapture. Diese Anwendung unterstützt den Austausch grafischer Daten zwischen der Serverzwischenablage und nicht ICCCM-konformen X Window-Anwendungen auf dem X-Desktop. Mit xcapture können Sie folgende Funktionen ausführen:

- Aufnehmen von Dialogfeldern und Bildschirmbereichen und Kopieren zwischen dem Benutzerdesktop (einschließlich nicht-ICCCM-kompatibler Anwendungen) und einer Anwendung, die in einem Verbindungsfenster ausgeführt wird
- Kopieren von Grafiken zwischen einem Verbindungsfenster und den X-Grafikbearbeitungsprogrammen xmag oder xv

Starten von xcapture von der Befehlszeile:

Geben Sie an der Eingabeaufforderung `/opt/Citrix/ICAClient/util/xcapture` ein und drücken Sie die EINGABETASTE, wobei /opt/Citrix/ICAClient das Verzeichnis ist, in dem Sie die Citrix Workspace-App installiert haben.

Kopieren von Informationen vom Benutzerdesktop:

1. Klicken Sie im xcapture-Dialogfeld auf **Von Bildschirm**. Der Cursor wird als Fadenkreuz dargestellt.
2. Wählen Sie eine der folgenden Optionen:
    - Auswählen eines Fensters: Verschieben Sie den Cursor auf das Fenster, das Sie kopieren möchten, und klicken Sie auf die mittlere Maustaste.
    - Auswählen eines Bereichs: Ziehen Sie den Cursor bei gedrückter linker Maustaste über den Bereich, den Sie kopieren möchten.
    - Aufheben der Auswahl: Klicken Sie mit der rechten Maustaste. Beim Ziehen der Maus können Sie die Auswahl aufheben, indem Sie vor dem Loslassen der mittleren oder linken Maustaste mit der rechten Maustaste klicken.
3. Klicken Sie im xcapture-Dialogfeld auf **Nach ICA**. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.
4. Verwenden Sie nach dem Abschluss der Übertragung in einer über das Verbindungsfenster gestarteten Anwendung den entsprechenden Befehl zum Einfügen.

Kopieren von Informationen aus xv in eine Anwendung in einem Verbindungsfenster:

1. Kopieren Sie die Informationen in “xv”.
2. Klicken Sie im Dialogfeld xcapture auf Von XV und dann auf Nach ICA. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. Verwenden Sie nach dem Abschluss der Übertragung in einer über das Verbindungsfenster gestarteten Anwendung den entsprechenden Befehl zum Einfügen.

Kopieren von Informationen aus einer Anwendung in einem Verbindungsfenster in xv:

1. Kopieren Sie die Informationen von der Anwendung im Verbindungsfenster.
2. Klicken Sie im Dialogfeld xcapture auf Von ICA und dann auf Nach XV. Während der Informationsverarbeitung ändert sich die Farbe der xcapture-Schaltfläche.
3. Fügen Sie nach Abschluss der Übertragung die Informationen in “xv” ein.

Cursor

Unterstützung der Cursor-Farbumkehrung

Bisher erschien in der Citrix Workspace-App ein gepunkteter Cursor, der dieselbe Farbe wie der Schwarz-Weiß-Hintergrund eines Textes hatte. Es war daher schwierig, die Position des Cursors zu finden.

Ab Version 2112 wird die Cursorfarbe je nach Hintergrundfarbe eines Textes umgekehrt. Dadurch können Sie den Cursor im Text leicht lokalisieren. Standardmäßig ist dieses Feature deaktiviert.

Voraussetzungen:

- Wenn `.ICAClient` bereits im Basisordner des aktuellen Benutzers vorhanden ist:

  Löschen Sie die Datei `All_Regions.ini`

  Oder

  Um die Datei `All_Regions.ini` beizubehalten, fügen Sie am Ende des Abschnitts [Virtual Channels\Thinwire Graphics] die folgenden Zeilen hinzu:

  InvertCursorEnabled=

  InvertCursorRefreshRate=

  InvertCursorMode=

Wenn der Ordner `.ICAClient` nicht vorhanden ist, weist dies auf eine Neuinstallation der Citrix Workspace-App hin. In diesem Fall wird die Standardeinstellung für das Feature beibehalten.

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

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Gehen Sie zum Abschnitt [Thinwire3.0] und legen Sie folgenden Eintrag fest:

   InvertCursorEnabled=True

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Der Cursor wird nicht umgekehrt, wenn der Wert für die Richtlinie **Videocodec zur Komprimierung verwenden** in Citrix Studio auf `Do not use video codec` festgelegt ist.

Maus

Relative Maus

Durch die Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Funktion ist für Anwendungen erforderlich, die relative Mauseingabe statt absoluter Eingabe erfordern.

> **Hinweis:**
>
> Dieses Feature ist nur in Sitzungen verfügbar, die unter Citrix Virtual Apps and Desktops 7.8 oder höher bzw. Citrix DaaS ausgeführt werden. Es ist standardmäßig deaktiviert.

Aktivieren des Features:

Fügen Sie der Datei `$HOME/.ICAClient/wfclient.ini` im Abschnitt [WFClient] folgenden Eintrag hinzu: RelativeMouse=1.

Damit wird das Feature aktiviert, zum Verwenden müssen Sie es jedoch noch einschalten. Weitere Informationen zum Aktivieren relativer Mausfunktionen finden Sie im Abschnitt Alternative relative Mauswerte.

Einschalten des Features:

Geben Sie Strg/F12 ein.

Nachdem das Feature aktiviert ist, drücken Sie erneut Strg/F12, um die Serverzeigerposition mit dem Client zu synchronisieren. Die Server- und Clientzeigerpositionen werden bei Verwendung einer relativen Maus nicht synchronisiert.

Deaktivieren des Features:

Geben Sie Strg-Umschalt/F12 ein.

Das Feature wird ebenfalls deaktiviert, wenn ein Sitzungsfenster den Fokus verliert.

Alternative relative Mauswerte

Alternativ gibt es folgende Werte für RelativeMouse:

- RelativeMouse=2 Aktiviert das Feature und schaltet es ein, wenn ein Sitzungsfenster den Fokus erhält.
- RelativeMouse=3 Aktiviert das Feature und es bleibt immer eingeschaltet.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- RelativeMouse=4 Aktiviert oder deaktiviert das Feature, wenn der clientseitige Mauszeiger angezeigt oder ausgeblendet wird. In diesem Modus kann die relative Maus für Anwendungsoberflächen im Gamingstil in Ich-Perspektive automatisch aktiviert oder deaktiviert werden.

Durch Eingeben folgender Einstellungen können Sie Tastaturbefehle ändern:

- RelativemouseOnChar=F11
- RelativeMouseOnShift=Shift
- RelativemouseOffChar=F11
- RelativeMouseOffShift=Shift

Die unterstützten Werte für **RelativemouseOnChar** und **RelativemouseOffChar** sind unter [Hotkey Keys] in der Datei config/module.ini in der Citrix Workspace-App-Installationsstruktur aufgeführt. Die Werte für **RelativeMouseOnShift** und **RelativeMouseOffShift** legen die zu verwendenden Zusatztasten fest und werden unter der Überschrift [Hotkey Shift States] aufgeführt.

Tastatur

Tastaturverhalten

Generieren der Tastenkombination Strg+Alt+Entfernen remote

1. Entscheiden Sie, welche Tastenkombination Strg+Alt+Entf auf dem remoten virtuellen Desktop generieren soll.
2. Konfigurieren Sie in der jeweiligen Konfigurationsdatei UseCtrlAltEnd im Abschnitt WFClient:
    - True bedeutet, dass mit Strg+Alt+Ende die Tastenkombination Strg+Alt+Entfernen an den Remotedesktop weitergegeben wird.
    - False bedeutet, dass mit Strg+Alt+Eingabetaste die Tastenkombination Strg+Alt+Entfernen an den Remotedesktop weitergegeben wird.

Generische Umleitung

Konfigurieren der Bloomberg v4-Tastatur über die generische USB-Umleitung auf der Clientseite:

Als Voraussetzung muss die Richtlinie im Delivery Controller der Domäne (DDC) aktiviert sein.

1. Suchen Sie die VID und PID der Bloomberg-Tastatur. In Debian und Ubuntu führen Sie hierfür den folgenden Befehl aus:

    ```
    lsusb
    ```

2. Wechseln Sie zu $ICAROOT und bearbeiten Sie die Datei usb.conf.
3. Fügen Sie folgenden Eintrag zur Datei usb.conf hinzu, um die USB-Umleitung für die Bloomberg-Tastatur zuzulassen und speichern Sie die Datei.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

ALLOW: vid=1188 pid=9545

4. Starten Sie den `ctxusbd`-Daemon auf dem Client neu. In Debian und Ubuntu führen Sie hierfür den folgenden Befehl aus:

   ```
   systemctl restart ctxusbd
   ```

5. Starten Sie eine Clientsitzung. Stellen Sie sicher, dass die Sitzung im Fokus ist, während Sie die umzuleitende Bloomberg v4-Tastatur anschließen.

> **Hinweis:**
>
> Sie können die folgende Konfiguration hinzufügen, um den Befehl `selectconfiguration` zu deaktivieren:
>
> `ALLOW: vid=1100 pid=0101 disableselectconfig=1`.
>
> Der Befehl `selectconfiguration` wird im VDA zur Konfiguration von USB-Geräten verwendet.

Selektive Umleitung

Dieses Feature ermöglicht den Einsatz der Bloomberg v4- und v5-Tastaturschnittstelle über mehrere Sitzungen hinweg. Damit kann die Tastatur flexibel in allen Remotesitzungen verwendet werden, außer bei Fingerabdruck- und Audioschnittstellen. Fingerabdruck- und Audioschnittstellen werden wie bisher zu einzelnen Sitzungen umgeleitet.

Aktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei `$HOME/.ICAClient/wfclient.ini` wie folgt.

   ```
   1 BloombergRedirection=true
   2 <!--NeedCopy-->
   ```

2. Führen Sie alle unter Generische Umleitung aufgeführten Schritte aus.

Deaktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei `$HOME/.ICAClient/wfclient.ini` wie folgt.

   ```
   1 BloombergRedirection=false
   2 <!--NeedCopy-->
   ```

2. Führen Sie alle unter Generische Umleitung aufgeführten Schritte aus.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Sie den Wert auf false festlegen, wird die Funktionalität auf das Verhalten in den Vorgängerversionen des Clients zurückgesetzt und alle Schnittstellen werden zu einer einzigen Sitzung umgeleitet.

Unterstützung von Tastenkombination zum Umschalten zwischen Vollbild- und Fenstermodus

Bisher konnten Sie im Desktop Viewer die Schaltfläche **Fenster** oder **Vollbild** verwenden, um zwischen **Vollbildmodus** und **Fenstermodus** zu wechseln.

Ab Version 2308 der Citrix Workspace-App können Sie mit der Tastenkombination Strg+F2 zwischen **Vollbildmodus** und **Fenstermodus** wechseln. Wenn sich die Desktopsitzung beispielsweise im **Vollbildmodus** befindet und Sie Strg+F2 drücken, wird der **Vollbildmodus** der Desktopsitzung beendet.

Das Feature ist in der Standardeinstellung deaktiviert.

Aktivieren des Features:

1. Wenn `.ICAClient` bei der Installation der neuen Version der Citrix Workspace-App für Linux bereits im Basisordner des aktuellen Benutzers vorhanden ist:

   Löschen Sie die Datei All_Regions.ini.
   Oder:
   Behalten Sie die Datei AllRegions.ini bei, und fügen Sie die folgenden Zeilen am Ende des Abschnitts [Client Engine\Application Launching] hinzu:

   ```
   1     FullScreenShortcutSupport=*
   2  <!--NeedCopy-->
   ```

2. Navigieren Sie zur Datei /opt/Citrix/ICAClient/config/All_Regions.ini und ändern Sie den Wert von FullScreenShortcutSupport wie folgt:

   ```
   1   FullScreenShortcutSupport=true
   2  <!--NeedCopy-->
   ```

   Der Standardwert der Tastenkombination ist Strg+F2.

Sie können die Tastenkombination auch anpassen. Die Tastenkombinationen bestehen aus zwei verschiedenen Teilen wie **KeyPassthroughEscapeShift** und **KeyPassthroughEscapeChar** in der Datei `All_Regions.ini`.

Die beiden Schlüssel, die Sie verwenden, müssen aus der folgenden Liste stammen:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Name	Abschnitt	Wert
KeyPassthroughEscapeShift	[Virtual Channels\Keyboard] in All_Regions.ini	[Alt, Strg, Umschalt, Alt+Strg, Alt+Umschalt, Strg+Umschalt, Alt+Strg+Umschalt], Standardwert: Strg
KeyPassthroughEscapeChar	[Virtual Channels\Keyboard] in All_Regions.ini	[F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, Minus, Plus, Tab, Pause], Standardwert: F2, Hinweis: Minus und Plus sind die Tasten auf dem Ziffernblock.

Wenn Sie beispielsweise „Strg+Umschalt+F3" als Tastenkombination verwenden möchten, müssen die Konfigurationselemente wie folgt lauten:

- KeyPassthroughEscapeShift=Strg+Umschalt
- KeyPassthroughEscapeChar=F3

Einschränkung:

- Wenn Sie eine Tastenkombination verwenden, die mit den Tastenkombinationen des Client-Betriebssystems in Konflikt steht oder eine systemeigene Tastenkombination enthält, funktioniert das Umschalten in den **Vollbildmodus** möglicherweise nicht, da das Client-Betriebssystem bei der Verwendung dieser Tastenkombination Vorrang hat. Wenn Sie beispielsweise "Strg+F3" als Tastenkombination des Linux-Betriebssystems verwenden, können Sie "Strg+F3" oder "Umschalt+Strg+F3" nicht in der Citrix Workspace-App zum Wechsel in den **Vollbildmodus** verwenden.
- Strg+Alt+F'*' oder *Alt+Strg+F*" (wobei sich F'*' auf F1-F12 bezieht) sind Tastenkombinationen, die in Linux zum Wechsel zwischen virtuellen Terminals verwendet werden. Diese Tastenkombinationen dürfen nicht für das Umschalten in den **Vollbildmodus** verwendet werden.
- Alt+Strg+Plus oder Alt+Strg+Minus (Plus und Minus sind die Tasten auf dem Ziffernblock) sind im Linux-System den Symbolen XF86Next_VMode/XF86Prev_VMode zugeordnet und nicht für Tastenkombinationen verfügbar. Diese Kombinationen dürfen also nicht für das Umschalten in den **Vollbildmodus** verwendet werden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Browserinhaltsumleitung

Chromium Embedded Framework (CEF) für die Browserinhaltsumleitung

In Versionen vor Version 1912 wurde bei der Browserinhaltsumleitung (BCR) ein WebKitGTK+-basiertes Overlay verwendet, um den Inhalt wiederzugeben. Bei Thin Clients gab es jedoch Leistungsprobleme. Ab Version 1912 wird für die Browserinhaltsumleitung ein CEF-basiertes Overlay verwendet. Diese Funktionalität bereichert die Benutzererfahrung bei der Browserinhaltsumleitung. Sie trägt dazu bei, dass Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen werden.

Ab Version 2106 ist die CEF-basierte Browserinhaltsumleitung voll funktionsfähig. Das Feature ist in der Standardeinstellung aktiviert.

Bei Bedarf können Sie die im Workspace-App-Paket bereitgestellte Datei `libffmpeg.so` durch eine geeignete Datei `libffmpeg.so` im Pfad `$ICAROOT/bcr/libffmpeg.so` ersetzen, die die erforderlichen Codecs enthält.

> **Hinweis:**
>
> Dieses Feature wird auf der ARMHF-Plattform nicht unterstützt.

Aktivieren der CEF-basierten Browserinhaltsumleitung

Aktivieren der CEF-basierten Browserinhaltsumleitung:

1. Navigieren Sie zur Datei `$ICAROOT/config/All_Regions.ini`. $ICAROOT steht hier für das Standardinstallationsverzeichnis der Citrix Workspace-App.
2. Gehen Sie zum Abschnitt `[Client Engine\WebPageRedirection]` und legen Sie folgenden Eintrag fest:

   UseCefBrowser=True

Einschränkung:

- Web-Apps, die Popups verwenden, funktionieren bei Verwendung der Browserinhaltsumleitung möglicherweise nicht.

Bekannte Probleme:

- Wenn Sie in `~/.ICAClient/All_Regions.ini` die Option `UseCefBrowser` auf **True** festlegen, funktioniert der japanische, chinesische und koreanische IME in Eingabefeldern möglicherweise nicht. Die Citrix Workspace-App für Linux unterstützt den japanischen, chinesischen und koreanischen IME nicht, wenn sichere SaaS mit dem eingebetteten Citrix-Browser verwendet wird.
- Wenn Sie versuchen, eine Webseitenumleitung mit CEF-basierter Browserinhaltsumleitung zu starten, wird möglicherweise ein unbekannter Zertifikatsfehler angezeigt. Das Problem tritt bei

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

der Citrix Workspace-App Version 2106 und höher auf.
Führen Sie als Workaround den folgenden Befehl am Terminal aus, um das selbstsignierte Zertifikat in `nssdb` zu importieren:

```
certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/
   Downloads/badssl.cer
<!--NeedCopy-->
```

Argumente in den Befehlen:

- `-A` - Hinzufügen eines Zertifikats zur Datenbank.
- `-n` - Der Name des Zertifikats. Dieses Argument ist optional und kann verwendet werden, um den Spitznamen hinzuzufügen.
- `"badssl.cer"` - Der Name des Zertifikats, das von der Site badssl.com exportiert wird.
- `-t "C,,"` - `-t` steht für TRUSTARGS und C steht für CA- bzw. ZS-Zertifikat. Weitere Informationen finden Sie in der Google-Dokumentation.
- `-d ~/.pki/nssdb` - Der Speicherort der Datenbank.
- `-i` - Kennzeichnet die Eingabedatei. Dieses Argument dient dazu, den Speicherort und den Namen der Zertifikatsdatei hinzuzufügen.

Informationen zur Browserinhaltsumleitung (BCR) finden Sie unter Browserinhaltsumleitung in der Dokumentation zu Citrix Virtual Apps and Desktops.

Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren

Ab Version 2303 der Citrix Workspace-App müssen Sie den Pfad des Speichers für temporäre Daten für CEF-basierte Browser konfigurieren. Gehen Sie wie folgt vor, um den Pfad zu konfigurieren:

1. Navigieren Sie zur Datei `$ICAROOT/config/All_Regions.ini`. `$ICAROOT` steht hier für das Standardinstallationsverzeichnis der Citrix Workspace-App.
2. Gehen Sie zum Abschnitt `[Client Engline\WebPageRedirection]` und fügen Sie folgenden Eintrag hinzu:

```
CefCachePath = <folder for CEF based BCR tmp files>
<!--NeedCopy-->
```

Automatische Wiederverbindung

In diesem Abschnitt wird die automatische HDX Broadcast-Wiederverbindung von Clients beschrieben. Citrix empfiehlt, dass Sie dieses Feature mit der HDX Broadcast -Sitzungszuverlässigkeit verwenden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Benutzer können von Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit dem Feature zur automatischen HDX Broadcast-Wiederverbindung von Clients kann die Citrix Workspace-App für Linux unabsichtlich getrennte Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden.

Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können. Mit einer festgelegten Anzahl von Versuchen versucht Citrix Workspace, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Wenn eine Benutzerauthentifizierung erforderlich ist, wird dem Benutzer bei der automatischen Wiederverbindung ein Dialogfeld zur Eingabe der Anmeldeinformationen angezeigt. Die automatische Wiederverbindung findet nicht statt, wenn Benutzer Anwendungen beenden, ohne sich abzumelden. Benutzer können sich nur mit getrennten Sitzungen wieder verbinden.

Standardmäßig wartet die Citrix Workspace-App für Linux 30 Sekunden, bevor versucht wird, die Verbindung zu einer getrennten Sitzung wiederherzustellen. Es werden drei Versuche gemacht, die Verbindung wiederherzustellen.

Bei einer Verbindung über Access Gateway steht ACR nicht zur Verfügung. Zum Schutz gegen Netzwerkausfälle sollten Sie sicherstellen, dass die Sitzungszuverlässigkeit auf dem Server und Client aktiviert und auf dem Access Gateway konfiguriert ist.

Weitere Informationen zur Konfiguration der automatische HDX Broadcast-Wiederverbindung von Clients finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

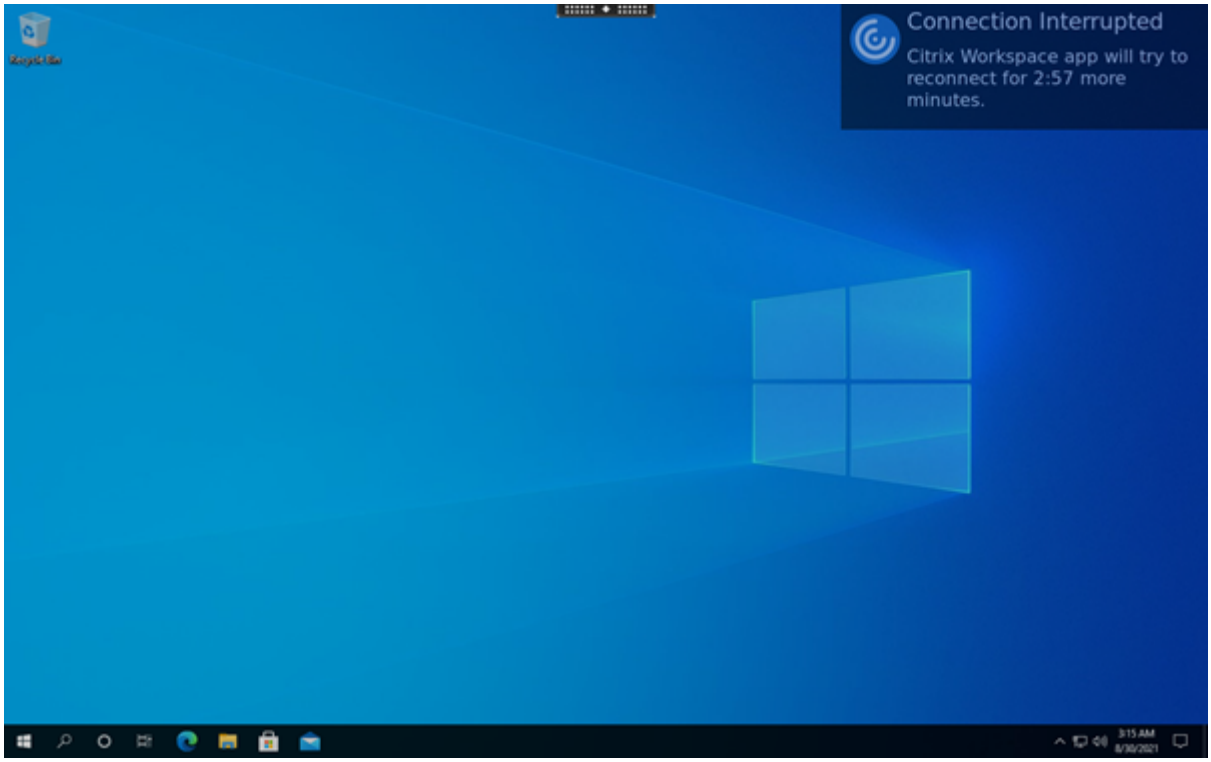
Sitzungszuverlässigkeit

In diesem Abschnitt wird die HDX Broadcast-Sitzungszuverlässigkeit beschrieben, die standardmäßig aktiviert ist.

Die HDX Broadcast-Sitzungszuverlässigkeit bedeutet, dass den Benutzern das Fenster einer veröffentlichten Anwendung angezeigt wird, selbst wenn die Verbindung zur Anwendung unterbrochen ist. Beispiel: Benutzer, die eine drahtlose Verbindung verwenden und in einen Tunnel fahren, können die Verbindung im Tunnel verlieren. Die Verbindung wird bei der Ausfahrt aus dem Tunnel wiederhergestellt. Während der Ausfallzeit werden die Daten des Benutzers, die gedrückten Tasten und andere Interaktionen gespeichert und die Anwendung erscheint als fixiert. Wenn die Verbindung wiederhergestellt ist, werden diese Interaktionen in der Anwendung wiedergegeben.

Sie können nun Bildschirmänderungen sehen, wenn die Sitzungszuverlässigkeit beginnt. Durch diese Verbesserung wird das Sitzungsfenster abgeblendet und ein Countdowntimer zeigt die Zeit bis zum nächsten Wiederverbindungsversuch an.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



> **Tipp**
>
> Sie können die für eine inaktive Sitzung verwendete Graustufe mit der Richtlinie **UI-Transparenzstufe während Wiederverbindung** ändern. Der Standardwert ist 80. Der Höchstwert ist 100 (transparentes Fenster) und der Mindestwert kann 0 sein (schwarzes Fenster).

Bei erfolgreicher Wiederverbindung einer Sitzung verschwindet die Benachrichtigung über den Countdown. Sie können wie gewohnt mit dem Desktop interagieren.

Ab Version 2109 ist die Benachrichtigung über die Sitzungszuverlässigkeit standardmäßig aktiviert.

So deaktivieren Sie diese Erweiterung:

1. Navigieren Sie zur Konfigurationsdatei `/opt/Citrix/ICAClient/config/module.ini`.
2. Ändern Sie im Abschnitt [WFClient] die folgende Einstellung:

```
SRNotification=False
```

> **Hinweis:**
>
> Dieses Feature wird nur für Citrix Virtual Desktops unterstützt.

Bei Konfiguration der automatischen Wiederverbindung von Clients und der Sitzungszuverlässigkeit hat die Sitzungszuverlässigkeit bei einem Verbindungsproblem Vorrang. Die Sitzungszuverlässigkeit versucht, eine Verbindung zu der vorhandenen Sitzung wieder herzustellen. Das Erkennen eines Verbindungsproblems kann bis zu 25 Sekunden dauern. Dann wird nach einem definierbaren

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Zeitraum (der Standard ist 180 Sekunden) eine Wiederverbindung versucht. Wenn die Sitzungszuverlässigkeit keine Wiederverbindung herstellen kann, versucht die automatische Wiederverbindung von Clients eine Wiederverbindung.

Wenn die HDX Broadcast-Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

Citrix Workspace-Benutzer können die Servereinstellungen nicht außer Kraft setzen.

> **Wichtig:**
>
> Für die HDX Broadcast-Sitzungszuverlässigkeit muss das Common Gateway Protocol (mit Richtlinieneinstellungen) auf dem Server aktiviert sein. Bei Deaktivierung von Common Gateway Protocol wird die HDX Broadcast-Sitzungszuverlässigkeit auch deaktiviert.

Verwenden von Sitzungszuverlässigkeitsrichtlinien

Mit der Richtlinieneinstellung “Sitzungszuverlässigkeit - Verbindungen” können Sie die Sitzungszuverlässigkeit aktivieren.

Der Standardwert für die Einstellung Sitzungszuverlässigkeit - Timeout ist 180 Sekunden (drei Minuten). Bei Bedarf können Sie den Zeitraum verlängern, über den die Sitzungszuverlässigkeit eine Sitzung geöffnet lässt. Sie werden nicht zur erneuten Authentifizierung aufgefordert.

> **Tipp**
>
> Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass Sie abgelenkt werden und das Benutzergerät verlassen. Es besteht dann das Risiko, dass unbefugte Benutzer Zugang zu der Sitzung erhalten.

Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter “Sitzungszuverlässigkeit - Portnummer” geändert.

Weitere Informationen zum Konfigurieren von Sitzungszuverlässigkeitsrichtlinien finden Sie unter Einstellungen der Richtlinie “Sitzungszuverlässigkeit”.

> **Hinweis:**
>
> Die Sitzungszuverlässigkeit ist standardmäßig auf dem Server aktiviert. Sie deaktivieren dieses Feature, indem Sie die vom Server verwaltete Richtlinie konfigurieren.

Multimedialeistung

Die Citrix Workspace-App enthält zahlreiche Technologien, die in den heutigen medienreichen Benutzerumgebungen eine High-Definition-Benutzererfahrung ermöglichen. Diese Technologien verbessern die Benutzererfahrung bei Verbindungen mit gehosteten Anwendungen und Desktops:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- HDX MediaStream Windows Media-Umleitung
- HDX MediaStream Flash-Umleitung
- HDX RealTime-Webcamvideokomprimierung
- H.264

> **Hinweis:**
>
> Citrix unterstützt die Koexistenz von RealTime Optimization Pack (RTOP) mit der Citrix Workspace-App für Linux Version 1901 und höher und mit `GStreamer` 0.1.

HDX MediaStream Windows Media-Umleitung

Mit HDX MediaStream Windows Media-Umleitung sind keine hohen Bandbreiten mehr erforderlich, um auf virtuellen Desktops, auf die von Linux-Benutzergeräten zugegriffen wird, Multimediainhalte aufzunehmen und wiederzugeben. Die Windows Media-Umleitung bietet einen Mechanismus zum Abspielen der Medienlaufzeitdateien auf dem Benutzergerät und nicht auf dem Server. Dadurch werden die Bandbreitenanforderungen für die Wiedergabe von Multimediadateien reduziert.

Windows Media-Umleitung verbessert die Leistung von Windows Media Player und anderen kompatiblen Playern, die auf virtuellen Windows-Desktops ausgeführt werden. Es werden eine Vielzahl von Formaten unterstützt, u. a.:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAV-Sounddateien

Die Citrix Workspace-App enthält die textbasierte Übersetzungstabelle MediaStreamingConfig.tbl, die Windows-spezifische Medienformat-GUIDs in MIME-Typen übersetzt, die `GStreamer` verwenden kann. Sie können die Übersetzungstabelle bearbeiten, um folgende Aktionen auszuführen:

- Hinzufügen bisher unbekannter oder nicht unterstützter Medienfilter/-dateiformate zur Übersetzungstabelle
- Blockieren problematischer GUIDs, um Fallback auf serverseitige Wiedergabe zu erzwingen
- Hinzufügen weiterer Parameter zu vorhandenen MIME-Strings, um Probleme mit schwierigen Formaten durch Ändern der `GStreamer`-Parameter eines Streams beheben zu können
- Verwalten und Bereitstellen benutzerdefinierter Konfigurationen basierend auf den Mediendateitypen, die von `GStreamer` auf einem Benutzergerät unterstützt werden

Mit dem clientseitigem Inhaltabruf können Sie zulassen, dass das Benutzergerät Medien direkt von URLs im Format `<http://>`, `<mms://>` oder `<rtsp://>` streamt, statt die Medien über einen Citrix Server zu streamen. Der Server leitet das Benutzergerät an die Medien um und sendet Steuerbefehle (einschließlich Wiedergabe, Pause, Stopp, Lautstärke, Suchen). Der Server verarbeitet je-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

doch keine Mediendaten. Dieses Feature erfordert erweiterte GStreamer-Multimediabibliotheken auf dem Gerät.

Einrichten von HDX MediaStream Windows Media-Umleitung:

1. Installieren Sie auf jedem erforderlichen Benutzergerät GStreamer 0.10, ein Open-Source-Multimedia-Framework. Normalerweise installieren Sie GStreamer vor der Citrix Workspace-App, damit die Citrix Workspace-App bei der Installation entsprechend konfiguriert werden kann.

   GStreamer ist in den meisten Linux-Distributionen enthalten. Ansonsten können Sie GStreamer auch von http://gstreamer.freedesktop.org herunterladen.

2. Um den clientseitigen Inhaltsabruf zu aktivieren, installieren Sie die erforderlichen GStreamer Protocol Source-*Plug-Ins* für die Dateitypen, die Benutzer auf dem Gerät wiedergeben. Mit dem Hilfsprogramm gst-launch können Sie prüfen, ob ein Plug-In installiert und funktionsbereit ist. Wenn gst-launch die URL wiedergeben kann, ist das erforderliche Plug-In funktionsbereit. Führen Sie beispielsweise gst-launch-0.10 playbin2 uri=<http://example-source/file.wmv> aus und vergewissern Sie sich, dass das Video einwandfrei wiedergegeben wird.

3. Wählen Sie bei der Installation der Citrix Workspace-App auf dem Gerät die Option GStreamer, wenn Sie das Tarball-Skript verwenden. Für .deb- und .rpm-Pakete erfolgt die Auswahl automatisch.

Beachten Sie Folgendes beim clientseitigen Inhaltsabruf:

- Standardmäßig ist dieses Feature aktiviert. Sie können es in All-Regions.ini im Abschnitt "Multimedia" mit der Option SpeedScreenMMACSFEnabled deaktivieren. Wenn Sie für diese Option "False" einstellen, wird die Windows Media-Umleitung für die Medienverarbeitung verwendet.
- Standardmäßig verwenden alle MediaStream-Features das GStreamer-Protokoll "playbin2". Sie können für alle MediaStream-Features (bis auf den clientseitigen Inhaltabruf) zum früheren Protokoll playbin zurückkehren. Das Feature "Clientseitiger Abruf" verwendet weiterhin playbin2, wobei die Option SpeedScreenMMAEnablePlaybin2 im Multimedia-Bereich der Datei All-Regions.ini verwendet wird.
- Die Citrix Workspace-App erkennt keine Playlistdateien oder Streamkonfigurationsdateien wie .asx- oder .nsc-Dateien. Benutzer müssen eine Standard-URL angeben, die nicht auf diese Dateitypen verweist. Überprüfen Sie mit gst-launch, ob eine URL gültig ist.

Hinweis zu GStreamer 1.0:

- Für die HDX MediaStream Windows Media-Umleitung wird standardmäßig GStreamer 0.10 verwendet. GStreamer 1.0 wird nur verwendet, wenn GStreamer 0.10 nicht verfügbar ist.
- Wenn Sie GStreamer 1.0 verwenden möchten, folgen Sie den nachstehenden Anweisungen:

1. Navigieren Sie zum Installationsverzeichnis der GStreamer-Plug-Ins. Der Speicherort der Plug-Ins hängt von Ihrer Distribution, der Architektur des Betriebssystems und der

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Installationsweise von GStreamer ab. Der Installationspfad ist normalerweise /usr/lib/x86_64-linux-gnu/gstreamer-1.0 oder $HOME/ .local/share/gstreamer-1.0.

2. Navigieren Sie zum Installationsverzeichnis der Citrix Workspace-App für Linux. Das Standardverzeichnis für Installationen durch privilegierte Benutzer (root) ist /opt/Citrix/ICAClient. Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist $HOME/ICAClient/-platform (wobei die Plattform z. B. linuxx64 sein kann). Weitere Informationen finden Sie unter Installation und Einrichtung.
3. Installieren Sie libgstflatstm1.0.so, indem Sie eine symbolische Verknüpfung im Verzeichnis der GStreamer-Plug-Ins erstellen: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so. Für diesen Schritt sind u. U. erhöhte Berechtigungen erforderlich, z. B. mit sudo.
4. Verwenden Sie gst_play1.0 als Player: ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play. Für diesen Schritt sind u. U. erhöhte Berechtigungen erforderlich, z. B. mit sudo.

- Um GStreamer 1.0 für die HDX RealTime-Webcamvideokomprimierung zu verwenden, nutzen Sie gst_read1.0 als Leser: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

Aktivieren von GStreamer 1.x

In Releases vor 1912 war GStreamer 0.10 die Standardversion für die Multimediaumleitung. Ab Version 1912 können Sie GStreamer 1.x als Standardversion konfigurieren.

Einschränkungen:

- Bei der Videowiedergabe funktioniert die Option zum Vor- und Zurückspulen möglicherweise nicht wie erwartet.
- Wenn Sie die Citrix Workspace-App auf ARMHF-Geräten starten, funktioniert GStreamer 1.x möglicherweise nicht wie erwartet.

Installieren von GStreamer 1.x

Installieren Sie das GStreamer1.x-Framework und die folgenden Plug-Ins von https://gstreamer.freedesktop.org/documentation/installing/on-linux.html:

- Gstreamer-plugins-base
- Gstreamer-plugins-bad
- Gstreamer-plugins-good
- Gstreamer-plugins-ugly
- Gstreamer-libav

Lokales Erstellen von Binärdateien

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Bei einigen Linux-Betriebssystemdistributionen, z. B. SUSE und openSUSE, findet das System die `GStreamer`-Pakete möglicherweise nicht in der Standardquellliste. Laden Sie in diesem Fall den Quellcode herunter und erstellen Sie alle Binärdateien lokal:

1. Laden Sie den Quellcode von https://gstreamer.freedesktop.org/src/ herunter.
2. Extrahieren Sie den Inhalt.
3. Navigieren Sie zu dem Verzeichnis mit dem extrahierten Paket.
4. Führen Sie die folgenden Befehle aus:

```
$sudo ./configure
$sudo make
$sudo make install
<!--NeedCopy-->
```

Standardmäßig sind die generierten Binärdateien unter */usr/local/lib/gstreamer-1.0/*.

Weitere Informationen zur Behandlung von Problemen finden Sie im Knowledge Center-Artikel CTX224988.

Konfigurieren von GStreamer 1.x

Um `GStreamer` 1.x für die Verwendung mit der Citrix Workspace-App zu konfigurieren, wenden Sie die folgende Konfiguration über die Shell-Eingabeaufforderung an:

- $ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.
- $ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play

Hierbei gilt:

- ICACLIENT_DIR ist der Installationspfad der Citrix Workspace-App für Linux.
- GST_PLUGINS_PATH ist der Plug-In-Pfad von `GStreamer`. Auf einer 64-Bit-Debian-Maschine ist dies beispielsweise */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

Einschränkungen:

- In Releases vor Version 2106 schlägt die Webcamumleitung möglicherweise fehl und die Sitzung wird u. U. getrennt, wenn Sie `GStreamer` Version 1.15.1 oder höher verwenden.

HDX MediaStream Flash-Umleitung

HDX MediaStream-Flash-Umleitung sorgt dafür, dass Adobe Flash-Inhalte lokal auf den Benutzergeräten wiedergegeben werden. So erhalten Benutzer High Definition-Audio und -Video, ohne dass die Bandbreitenanforderungen steigen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt. Weitere Informationen finden Sie unter Systemanforderungen.
2. Fügen Sie in der Datei `wfclient.ini` im Abschnitt [WFClient] (für alle Verbindungen eines bestimmten Benutzers) oder in der Datei `All\\_Regions.ini` im Abschnitt [Client Engine\Application Launching] (für alle Benutzer in Ihrer Umgebung) folgende Parameter hinzu:

   - **HDXFlashUseFlashRemoting=Ask**: **Never**; **Always**

     Aktiviert HDX MediaStream für Flash auf dem Benutzergerät. Standardmäßig ist dieser Wert auf **Nie**festgelegt. Benutzer werden zudem beim Aufrufen von Webseiten mit Flash-Inhalten in einem Dialogfeld gefragt, ob sie die Flash-Inhalte optimieren möchten.

   - **HDXFlashEnableServerSideContentFetching=Disabled**; **Enabled**

     Aktiviert oder deaktiviert den serverseitigen Inhaltsabruf für die Citrix Workspace-App. Die Standardeinstellung ist **Disabled**.

   - **HDXFlashUseServerHttpCookie=Disabled**; **Enabled**

     Aktiviert oder deaktiviert HTTP-Cookie-Umleitung. Die Standardeinstellung ist **Disabled**.

   - **HDXFlashEnableClientSideCaching=Disabled**; **Enabled**

     Aktiviert oder deaktiviert die clientseitige Zwischenspeicherung für von der Citrix Workspace-App abgerufene Inhalte. Die Standardeinstellung ist **Enabled**.

   - **HDXFlashClientCacheSize= [25-250]**

     Definiert die Größe des Clientcaches in MB. Die Größe kann zwischen 25 MB und 250 MB liegen. Wenn die maximale Größe erreicht ist, werden bereits im Cache vorhandene Daten gelöscht, um Platz für neue Inhalte zu schaffen. Die Standardeinstellung ist **100**.

   - **HDXFlashServerSideContentCacheType=Persistent**: **Temporary**; **NoCaching**

     Definiert den Zwischenspeicherungstyp, den die Citrix Workspace-App für mit serverseitigem Inhaltsabruf abgerufene Inhalte verwendet. Die Standardeinstellung ist **Persistent**.

     Hinweis: Dieser Parameter ist nur erforderlich, wenn **HDXFlashEnableServerSideContentFetching** auf **Enabled** gesetzt ist.

3. Flash-Umleitung ist standardmäßig deaktiviert. Ändern Sie in der Datei /config/module.ini die Einstellung FlashV2=Off in FlashV2=On, um das Feature zu aktivieren.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

HDX RealTime-Webcamvideokomprimierung

HDX RealTime bietet eine Webcam-Videokomprimierungsoption zur Verbesserung der Bandbreiteneffizienz bei Videokonferenzen. Diese Option stellt sicher, dass Benutzer bei der Verwendung von Anwendungen wie GoToMeeting mit HDFaces und Skype for Business eine optimale Leistung erzielen.

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt.
2. Stellen Sie sicher, dass der virtuelle `Multimedia`-Kanal aktiviert ist. Zum Aktivieren öffnen Sie die Datei `$ICAROOT/config/module.ini` und überprüfen, ob `MultiMedia` im Abschnitt [ICA3.0] auf `On` festgelegt ist.
3. Aktivieren Sie die Audioeingabe durch Klicken auf **Mikrofon und Webcam verwenden** auf der Seite "Mikrofon und Webcam" des Dialogfelds **Einstellungen**.

Deaktivieren Sie die HDX RealTime-Webcamvideokomprimierung

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen müssen Benutzer Webcams mit USB-Unterstützung anschließen. Führen Sie folgende Schritte aus, um die Verbindung herzustellen:

- Deaktivieren Sie die HDX RealTime-Webcamvideokomprimierung
- Aktivieren Sie die USB-Unterstützung für Webcams

1. Fügen Sie der entsprechenden INI-Datei im Abschnitt [WFClient] den folgenden Parameter hinzu:

   AllowAudioInput=False

   Weitere Informationen finden Sie unter Standardeinstellungen.

2. Öffnen Sie die Datei `usb.conf`, die normalerweise unter `$ICAROOT/usb.conf` verfügbar ist.
3. Entfernen Sie die folgende Zeile oder kommentieren Sie sie aus:

   > DENY: class=0e # UVC (standardmäßig über HDX RealTime-Webcamvideokomprimierung)

4. Speichern und schließen Sie die Datei.

Sichere SaaS mit integriertem Citrix Browser (experimentelles Feature)

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. Hierfür können sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die Citrix Workspace-App für Linux unterstützt die Verwendung von SaaS-Anwendungen unter Einsatz des Access Control Service. Über diesen Dienst können Administratoren eine geschlossene Erfahrung mit Single Sign-On und Inhaltsinspektion bereitstellen.

Voraussetzung:

Stellen Sie sicher, dass das Paket `libgtkglext1` verfügbar ist.

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 beliebter Anwendungen.

> **Hinweis:**
>
> SaaS mit Citrix Browser Engine wird nur auf x64- und x86-Plattformen und nicht auf ArmHardFloatPort-Hardware (ARMHF) unterstützt.

Weitere Informationen zum Konfigurieren von SaaS-Apps mit Access Control Service finden Sie in der Dokumentation zur Zugriffssteuerung.

Weitere Informationen zu SaaS-Apps mit der Citrix Workspace-App finden Sie unter Workspacekonfiguration in der Dokumentation zur Citrix Workspace-App für Windows.

H.264

Die Citrix Workspace-App unterstützt die H.264-Grafikanzeige einschließlich der von Citrix Virtual Apps and Desktops 7 bereitgestellten HDX 3D Pro-Technologie. Bei dieser Unterstützung wird der standardmäßig aktivierte Tiefenkomprimierungscodec verwendet. Dieses Feature liefert im Vergleich zum JPEG-Codec eine bessere Leistung bei reichhaltigen und professionellen Grafikanwendungen in WAN-Netzwerken.

> **Hinweis:**
>
> In H.264 unterstützt die Citrix Workspace-App für Linux nur das YUV 420-Format und nicht das YUV 444-Format.

Folgen Sie den Anweisungen in diesem Abschnitt, um das Feature zu deaktivieren und zur Grafikverarbeitung stattdessen den JPEG-Codec zu verwenden. Sie können auch die Textprotokollierung deaktivieren und gleichzeitig den Tiefenkomprimierungscodec weiterverwenden. Mit dieser Einstellung lässt sich der CPU-Bedarf senken, wenn Grafiken mit komplexen Bildern aber relativ wenig oder unwichtigem Text verarbeitet werden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Wichtig:**
>
> Verwenden Sie zum Konfigurieren dieses Features keine verlustfreie Einstellung in der Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Richtlinie "Bildqualität". Wenn Sie eine verlustfreie Einstellung wählen, ist die H.264-Codierung auf dem Server deaktiviert und funktioniert für die Citrix Workspace-App nicht.

Deaktivieren der Unterstützung für den Tiefenkomprimierungscodec

Legen Sie **H264Enabled** in der Datei `wfclient.ini` auf **False** fest. Dadurch wird auch die Textprotokollierung deaktiviert.

Ausschließliches Deaktivieren der Textprotokollierung:

Legen Sie bei aktiviertem Tiefenkomprimierungscodec in der Datei `wfclient.ini` **TextTrackingEnabled** auf **False** fest.

Bildschirmkacheln

Sie können die Verarbeitung von JPEG-codierten Bildschirmkacheln mit den Features "Bitmapdecodierung direkt zum Bildschirm", "Batchverarbeitung der Kacheldecodierung" und "Verzögertes `XSync`" verbessern.

1. Stellen Sie sicher, dass Ihre JPEG-Bibliothek diese Features unterstützt.
2. Setzen Sie in wfclient.ini im Abschnitt Thinwire3.0 DirectDecode und BatchDecode auf True.

   Hinweis: Das Aktivieren von "Batchverarbeitung der Kacheldecodierung" aktiviert gleichzeitig "Verzögertes `XSync`".

Protokollierung

In früheren Versionen wurden die Dateien `debug.ini` und `module.ini` zum Konfigurieren der Protokollierung verwendet.

Ab Version 2009 können Sie die Protokollierung über eines der folgenden Verfahren konfigurieren:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

Ab Version 2009 wird die Konfigurationsdatei `debug.ini` auch aus dem Installationspaket der Citrix Workspace-App entfernt.

Die Protokollierung erfasst Bereitstellungsdetails, Konfigurationsänderungen und Administratoraktivitäten für die Citrix Workspace-App in einer Protokollierungsdatenbank. Drittanbieterentwickler können diesen Protokollierungsmechanismus über das Protokollierungs-SDK nutzen, das im Platform Optimization SDK der Citrix Workspace-App enthalten ist.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Verwenden Sie die Protokollinformationen für Folgendes:

- Diagnostizieren und Beheben von Problemen, die nach Änderungen auftreten. Das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen.
- Bericht über Administratoraktivitäten.

Bei Installation der Citrix Workspace-App mit Root-Benutzerrechten werden die Protokolle in `/var/log/citrix/ICAClient.log` gespeichert. Andernfalls werden die Protokolle in `${ HOME } /.ICAClient/logs/ICAClient.log` gespeichert.

Wenn Citrix Workspace-App installiert ist, wird ein Benutzer namens `citrixlog` zur Verarbeitung der Protokollierungsfunktionen erstellt.

Befehlszeilenoberfläche

1. Navigieren Sie an der Eingabeaufforderung zum Pfad `/opt/Citrix/ICAClient/util`.
2. Führen Sie den folgenden Befehl aus, um die Protokolleinstellungen festzulegen.

   ```
   ./setlog help
   ```

Alle verfügbaren Befehle werden angezeigt.

Die folgende Tabelle listet verschiedene Module und die entsprechenden Traceklassenwerte auf: Verwenden Sie die folgende Tabelle, um einen bestimmten Befehlszeilenprotokollwert festzulegen:

Modul	Protokollklasse
Assertions	LOG_ASSERT
Audio Monitor	TC_CM
BCR with CEF	TC_CEFBCR
Clientaudiozuordnung	TC_CAM
Connection Center	TC_CONNCENTER
Client Communication Port	TC_CCM
Clientlaufwerkzuordnung	TC_CDM
Clip	TC_CLIP
Clientdruckerzuordnung	TC_CPM
Clientdruckerzuordnung	TC_CPM
Schriftart	TC_FONT
Frame	TC_FRAME

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Modul	Protokollklasse
Graphics Abstraction	TC_GA
Eingabemethoden-Editor	TC_IME
IPC	TC_IPC
Tastaturzuordnung	TC_KEY
Lizenzierungstreiber	TC_VDLIC
Multimedia	TC_MMVD
Mauszuordnung	TC_MOU
MS Teams	TC_MTOP
Andere Bibliotheken	TC_LIB
Protokolltreiber	TC_PD
PNA Store	TC_PN
Standardereignisprotokolle	LOG_CLASS
SRCC	TC_SRCC
SSPI Login	TC_CSM
Smartcard	TC_SCARDVD
Selfservice	TC_SS
Selfservice Extension	TC_SSEXT
StorefrontLib	TC_STF
Transport Driver	TC_TD
Thinwire	TC_TW
Transparent Window Interface	TC_TUI
Virtueller Kanal	TC_VD
PAL	TC_VP
Benutzeroberfläche	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
USB Daemon	TC_CTXUSB
Video Frame Driver	TC_VFM
Webkit	TC_WEBKIT

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Modul	Protokollklasse
WinStation Driver	TC_WD
`Wfica`	TC_NCS
`Wfica` Engine	TC_WENG
`Wfica` Shell	TC_WFSHELL
Web helper	TC_WH
Zero Latency	TC_ZLC

Grafische Benutzeroberfläche (GUI)

Gehen Sie zu **Menü** > **Einstellungen**. Das Dialogfeld **Citrix Workspace - Einstellungen** wird angezeigt.

Mit zunehmender Detailtiefe sind folgende Werte verfügbar:

- Disabled
- Nur Fehler
- Normal
- Verbose

Standardmäßig ist für die **Protokollierung** die Option **Nur Fehler** festgelegt.

Da bei der Ablaufverfolgung große Datenmengen generiert werden können, kann sie sich erheblich auf die Leistung der Citrix Workspace-App auswirken. Die Option **Ausführlich** sollte daher nur für die Problembehandlung verwendet werden.

Klicken Sie nach Auswahl der gewünschten Protokollierungsstufe auf **Speichern und Schließen**. Die Änderungen werden in der Sitzung dynamisch angewendet.

Klicken Sie auf das Symbol “Einstellungen” neben dem Dropdownmenü für die **Protokollierung**. Das Dialogfeld **Citrix-Protokolleinstellungen** wird angezeigt.

> **Hinweis:**
>
> Wenn Sie die Datei `ICAClient.log` löschen, müssen Sie den Protokollierungsdienst `ctxlogd` neu starten.
>
> Wenn Sie beispielsweise ein systemd-fähiges Setup verwenden, führen Sie folgenden Befehl aus:
>
> `systemctl restart ctxlogd`.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Aktivieren der Protokollierung für Version 2006 und früher:

Wenn Sie Version 2006 und früher verwenden, aktivieren Sie die Protokollierung wie folgt:

1. Laden Sie die Citrix Workspace-App auf Ihre Linux-Maschine herunter und installieren Sie sie.
2. Legen Sie die Umgebungsvariable `ICAROOT` auf das Installationsverzeichnis fest.

   Beispiel: `/opt/Citrix/ICAClient`.

   Standardmäßig ist die Traceklasse `TC_ALL` aktiviert, um alle Tracingberichte bereitzustellen.
3. Um Protokolle für ein bestimmtes Modul zu sammeln, öffnen Sie die Datei `debug.ini` unter `$ICAROOT` und fügen Sie die erforderlichen Ablaufverfolgungsparameter zum Abschnitt `[wfica]` hinzu.

   Fügen Sie die Traceklassen mit einem "+"-Symbol hinzu. Beispiel: `+TC_LIB`.

   Sie können unterschiedliche Klassen hinzufügen, indem Sie sie durch einen senkrechten Strich trennen.
   Beispiel: `+TC_LIB|+TC_MMVD`.

Die folgende Tabelle listet die `wfica`-Module und die entsprechenden Traceklassenwerte auf:

Modul	Wert für Traceklassen
Grafik	TC_TW
EUEM	TC_EUEM
WFICA (Sitzungsstart)	TC_NCS
Drucken	TC_CPM
Verbindungssequenz - WD	TC_WD
Verbindungssequenz - PD	TC_PD
Verbindungssequenz - TD	TC_TD
Proxy-bezogene Dateien	TC_PROXY
Virtueller Multimedientreiber /Webcam	TC_MMVD
Virtuelle Treiber	TC_VD
Clientlaufwerkzuordnung	TC_CDM
Audio	TC_CAM
COM (Kommunikationsport)	TC_CCM
Seamless	TC_TWI
Smartcard	TC_SCARDVD

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die folgende Tabelle listet das Connection Center-Modul und die entsprechenden Traceklassenwerte auf:

Modul	Wert für Traceklassen
Connection Center	TC_CSM

Die folgende Tabelle listet Traceklassenwerte für setWebHelper auf:

Wert für Traceklassen
Legen Sie logSwitch auf 1 (zum Aktivieren) oder 0 (zum Deaktivieren) fest.
Beispiel: logSwitch = 1

Problembehandlung:

Wenn `ctxlogd` nicht mehr reagiert, werden die Protokolle im syslog erfasst.

Weitere Informationen zum Abrufen neuer und aktualisierter Protokolle bei nachfolgenden Starts finden Sie unter Syslog-Konfiguration.

Syslog-Konfiguration

Standardmäßig werden alle syslog-Protokolle unter /var/log/syslog gespeichert. Sie können Pfad und Namen der Protokolldatei konfigurieren, indem Sie die folgende Zeile im Abschnitt [RULES] in der Datei `/etc/rsyslog.conf` bearbeiten. Beispiel:

```
1 user.* -/var/log/logfile_name.log
```

Speichern Sie Ihre Änderungen und starten Sie den syslog-Dienst mit dem folgenden Befehl neu:

```
sudo service rsyslog restart
```

Wichtige Punkte:

- Um sicherzustellen, dass ein neuer syslog-Dienst verfügbar ist, löschen Sie syslog und führen Sie folgenden Befehl aus: `sudo service rsyslog restart`.
- Um doppelte Benachrichtigungen zu vermeiden, fügen Sie **$RepeatedMsgReduction on** am Anfang der Datei `rsyslog.conf` hinzu.
- Stellen Sie sicher, dass die Zeile **$ModLoad imuxsock.so** am Anfang der Datei `rsyslog.conf` nicht auskommentiert ist.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Remoteprotokollierung

So aktivieren Sie die Remoteprotokollierung:

- **Serverseitige Konfiguration:** Entfernen Sie die Kommentarzeichen für die folgenden Zeilen in der Datei rsyslog.conf des Syslog-Servers:

  ```
  $ModLoad imtcp

  $InputTCPServerRun 10514
  ```

- **Clientseitige Konfiguration:** Fügen Sie die folgende Zeile in der Datei `rsyslog.conf` hinzu, indem Sie localhost durch die IP-Adresse des Remoteservers ersetzen:

  ```
  *.* @@localhost:10514
  ```

Sammeln von Protokolldateien

Bisher gab es kein Tool zum Sammeln der Protokolldateien in der Citrix Workspace-App. Protokolldateien waren in verschiedenen Ordnern. Sie mussten Protokolldateien manuell aus verschiedenen Ordnern sammeln.

Ab Version 2109 bietet die Citrix Workspace-App das Tool collectlog.py zum Sammeln von Protokolldateien aus verschiedenen Ordnern. Sie können das Tool über die Befehlszeile ausführen. Die Protokolldateien werden als eine komprimierte Protokolldatei generiert. Sie können es vom lokalen Server herunterladen.

Voraussetzungen

- Python3
- Erfordert zusätzlichen Speicherplatz zum Speichern der Protokolle

Ab Version 2109 werden zwei neue Dateien zum Sammeln von Protokolldateien mit dem Tool collectlog.py hinzugefügt:

- Datei `logcollector.ini`: speichert den Namen und Pfad der Protokolldatei.
- Datei `collectlog.py`: sammelt die Protokolldateien und speichert sie als komprimierte `cwalog_{ timestamp } .tar.gz`-Datei.

Standardmäßig wird die Komponente `[hdxteams]` in der Datei `logcollector.ini` hinzugefügt, um Protokolldateien für Microsoft Teams zu sammeln. Sie können jedoch mit dem folgenden Verfahren auch andere Komponenten in der Datei `logcollector.ini` hinzufügen:

1. Navigieren Sie zur Datei `${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini`.
2. Fügen Sie die Komponente, die Sie zum Sammeln von Protokolldateien benötigen, gemäß folgendem Beispiel hinzu:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[component_name]

log_name1 = “log_path1”

log_name2 = “log_path2”

Wenn Sie Version 2109 verwenden, sammeln Sie Protokolldateien mit dem folgenden Verfahren:

1. Laden Sie die Citrix Workspace-App auf Ihre Linux-Maschine herunter und installieren Sie sie.
2. Navigieren Sie an der Befehlszeile zum Pfad `/opt/Citrix/ICAClient/util`.
3. Führen Sie den folgenden Befehl aus:
   `./collctlog.py -h`.

   Die folgenden Informationen zur Verwendung von Befehlen werden angezeigt:

   ```
   usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE]optional arguments: -h,
    --help show this help message and exit -c CONFIG, --config CONFIG The
   logcollector.ini path & file -a ARCHIVE, --archive ARCHIVE The archive
   path & file
   ```

4. Führen Sie wie erforderlich die folgenden Befehle aus:

   - `./collectlog.py`: sammelt Protokolldateien mit der Konfigurationsdatei aus dem Standardpfad und speichert sie als komprimierte Protokolldateien im Standardpfad.
   - `./collectlog.py -c /user_specified_path/logcollector.ini`: sammelt Protokolldateien mit der Konfigurationsdatei aus einem benutzerdefinierten Pfad und speichert sie als komprimierte Protokolldateien im Standardpfad.
   - `./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_spec /`: sammelt Protokolldateien mit der Konfigurationsdatei aus einem benutzerdefinierten Pfad und speichert sie als komprimierte Protokolldateien im benutzerdefinierten Pfad.

   > **Hinweis:**
   >
   > Der Standardpfad der Konfigurationsdatei `logcollector.ini` ist `/opt/Citrix/ICAClient/config/logcollector.ini`. Der Standardpfad der komprimierten Protokolldatei ist `/tmp`.

5. Navigieren Sie zum Ordner `/tmp` und sammeln Sie die komprimierte `cwalog_{ timestamp } .tar.gz`-Datei.

> **Hinweis:**
>
> Die Protokolldateien werden im Ordner `/tmp` mit dem Dateinamen `cwalog_{ timestamp } .tar.gz` gespeichert.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Microsoft Teams optimieren

Citrix bietet eine Optimierung für die Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops bzw. Citrix DaaS der Citrix Workspace-App. Die Optimierung für Microsoft Teams ähnelt der Komponente HDX RealTime Optimization für Microsoft Skype for Business. Der Unterschied besteht darin, dass wir alle notwendigen Komponenten für die Optimierung von Microsoft Teams im VDA und in der Workspace-App für Linux bündeln.

Die Citrix Workspace-App für Linux unterstützt Audio-, Video- und Bildschirmfreigabefunktionen mit der Optimierung für Microsoft Teams.

> **Hinweis:**
>
> - Die Optimierung für Microsoft Teams wird nur auf der x64-Linux-Distributionen unterstützt.
> - Die Microsoft-Optimierung wird in Citrix Virtual Apps and Desktops und in Citrix DaaS unterstützt.
> - Für Thin Clients, die Dell Wyse verwenden, verwenden Sie den **Citrix Configuration Editor**, um alle Parameter in der Datei `/var/.config/citrix/hdx_rtc_engine/config.json` zu bearbeiten. Weitere Informationen finden Sie in der Dokumentation von Dell.

Weitere Informationen zum Aktivieren der Protokollierung erhalten Sie, wenn Sie die Schritte unter Protokollierung für Microsoft Teams ausführen.

Weitere Informationen zu Systemanforderungen finden Sie unter Anforderungen für die Microsoft Teams-Optimierung.

Weitere Informationen finden Sie unter Optimierung für Microsoft Teams und Microsoft Teams-Umleitung.

Verbesserung der Audiokonfiguration

Wenn in Microsoft Teams die Optionen für die automatische Verstärkungsregelung und Rauschunterdrückung konfiguriert, übernimmt das von Citrix umgeleitete Microsoft Teams die konfigurierten Werte. Andernfalls sind diese Optionen standardmäßig aktiviert. Ab Citrix Workspace-App 2104 ist die Echounterdrückung jedoch standardmäßig deaktiviert. Ab Citrix Workspace-App 2112 können Administratoren die Standardeinstellungen mit den folgenden Schritten ändern, um Audioprobleme zu beheben (Roboterstimme, hohe CPU-Last, die zu abgehacktem Audio führt, usw.):

1. Navigieren Sie zur Datei /var/.config/citrix/hdx_rtc_engine/config.json.
2. Legen Sie folgende Optionen fest:
   - Wert für `EnableAEC` auf 1 zum Aktivieren und auf 0 zum Deaktivieren der Echounterdrückung
   - Wert für `EnableAGC` auf 1 zum Aktivieren und auf 0 zum Deaktivieren der automatischen Verstärkungsregelung

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Wert für `EnableNS` auf 1 zum Aktivieren und auf 0 zum Deaktivieren der Rauschunterdrückung

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


      "EnableAEC":1,"EnableAGC":1,"EnableNS":1

 }

<!--NeedCopy-->
```

Wenn die Verbindung steht, prüfen Sie im `webrpc`-Protokoll (`/tmp/webrpc/<current date>/`) die folgenden Einträge, um zu verifizieren, dass die Änderungen wirksam wurden:

```
/tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
   14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
   constraints, aec=1, agc=1, ns=1
<!--NeedCopy-->
```

Geschätzte Codierungsleistung für Microsoft Teams

`HdxRtcEngine` ist die WebRTC Media Engine, die in die Citrix Workspace-App eingebettet ist und die Microsoft Teams-Umleitung verarbeitet. `HdxRtcEngine.exe` kann die beste Auflösung für ausgehende Videos (Kodierung) schätzen, die die CPU des Endpunkts ohne Überlastung aufrechterhalten kann. Mögliche Werte sind 240p, 360p, 720p und 1080p.

Die Schätzung der Leistung basiert auf Makroblockcode, um die beste Auflösung zu bestimmen, die beim jeweiligen Endpunkt erzielt werden kann. Die Codec-Aushandlung während der Einrichtung eines Anrufs umfasst die höchstmögliche Auflösung. Die Codec-Aushandlung kann zwischen Peers oder zwischen Peer und Konferenzserver stattfinden.

Die folgende Tabelle enthält die vier Leistungskategorien für Endpunkte mit eigener **maximal** verfügbarer Auflösung:

Endpunktleistung	Maximale Auflösung	Registrierungsschlüsselwert
Fast	1080p (1920x1080 16:9 @ 30 F/s)	3

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpunktleistung	Maximale Auflösung	Registrierungsschlüsselwert
Medium	720p (1280x720 16:9 @ 30 F/s)	2
Slow	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

Um den Codierungsauflösungswert für ausgehende Videos z. B. auf 360p festzulegen, führen Sie den folgenden Befehl vom Terminal aus:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


    "OverridePerformance":1

 }

<!--NeedCopy-->
```

Protokollierung für Microsoft Teams

Aktivieren der Protokollierung für Microsoft Teams:

1. Navigieren Sie zur Datei `/opt/Citrix/ICAClient/debug.ini`.
2. Ändern Sie den Abschnitt `[HDXTeams]` wie folgt:

```
[HDXTeams]
; Retail logging for HDXTeams 0/1 = disabled/enabled
HDXTeamsLogSwitch = 1
; Debug logging; , It is in decreasing order
; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
   LS_VERBOSE = 0
WebrtcLogLevel = 0
; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
WebrpcLogLevel = 0

<!--NeedCopy-->
```

Die Protokollierung kann auch aktiviert werden, indem Sie die folgende Zeile zur Datei config.json hinzufügen:

```
{

"WebrpcLogLevel": 0,"WebrtcLogLevel": 0
 }

<!--NeedCopy-->
```

Hinzufügen der Abhängigkeit “libunwind-12 library” für llvm-12

Ab Release 2111 gibt es für llvm-12 die neue Abhängigkeit “libunwind-12 library”. Sie ist jedoch nicht standardmäßig im ursprünglichen Repository vorhanden. Installieren Sie libunwind-12 library mit den folgenden Schritten manuell im Repository:

1. Öffnen Sie das Terminal.
2. Geben Sie die folgende Zeile ein, um die Repository-Schlüsseldatei für `llvm` zu installieren:

```
 wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key|sudo apt-key
     add
<!--NeedCopy-->
```

3. Geben Sie die folgende Zeile ein, um die Repository-Quellliste für `llvm` zu konfigurieren:

```
 sudo vim /etc/apt/sources.list
<!--NeedCopy-->
```

4. Fügen Sie die folgende Zeile hinzu:

```
deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
<!--NeedCopy-->
```

5. Führen Sie den folgenden Befehl aus, um libunwind-12 library zu installieren:

```
sudo apt-get update -y
sudo apt-get install libunwind-12
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Schnittstelle für bevorzugtes Netzwerk konfigurieren

Ab Citrix Workspace-App 2303 können Sie eine Schnittstelle für das bevorzugte Netzwerk für den Mediendatenverkehr konfigurieren. Sie können dann zu einem anderen Netzwerk wechseln, wenn Sie mehrere Netzwerkverbindungen haben und die Leistung der Standardverbindung nicht gut ist. Aktivieren der Verbesserung:

1. Navigieren Sie zur Datei `/var/.config/citrix/hdx_rtc_engine/config.json`.
2. Gehen Sie zu folgendem Abschnitt:

```
1         mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3          vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5         {
6
7
8              " NetworkPreference" :1
9
10           }
11
12 <!--NeedCopy-->
```

3. Aktualisieren Sie den Wert “NetworkPreference” nach Bedarf mit einem der folgenden Werte:
   - 1: Ethernet
   - 2: Wi-Fi
   - 3: Cellular
   - 4: VPN
   - 5: Loopback
   - 6: Any

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

Erweiterungen für die Microsoft Teams-Optimierung

- Ab Version 2101 für die Citrix Workspace-App:
  - Das Installationspaket der Citrix Workspace-App enthält die Klingeltöne von Microsoft Teams.
  - Die Audioausgabe wechselt automatisch zu neu angeschlossenen Audiogeräten und eine geeignete Lautstärke wird eingestellt.
  - HTTP-Proxyunterstützung für anonyme Authentifizierung.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Ab Version 2103 für die Citrix Workspace-App ist der VP9-Videocodec standardmäßig deaktiviert.
- Ab Version 2104 für die Citrix Workspace-App ist die Echounterdrückung standardmäßig deaktiviert. Wir empfehlen, dass Sie nicht die integrierten Lautsprecher und das Mikrofon für Anrufe verwenden. Verwenden Sie stattdessen Kopfhörer. Dieser Fix soll Probleme bei der Audiowiedergabe korrigieren, die bei Thin Clients festgestellt wurden.
- Ab Version 2106 für die Citrix Workspace-App:
  - Wenn Sie auf **Bildschirmfreigabe**geklickt haben, war die Vorschau eines Standard- oder Hauptmonitors nur für die Bildschirmfreigabe verfügbar.

    Ab dieser Version wird eine Vorschau aller Bildschirme im Menü der Bildschirmauswahl angezeigt. Sie können einen beliebigen Bildschirm für die Bildschirmfreigabe in der VDA-Umgebung auswählen. Auf dem ausgewählten Bildschirm wird ein rotes Quadrat angezeigt und ein kleines Bild des ausgewählten Bildschirminhalts wird im Menü für die Bildschirmauswahl angezeigt.

    Im Seamlessmodus können Sie einen der Bildschirme zur Freigabe auswählen. Wenn der Desktop Viewer den Fenstermodus ändert (maximieren, wiederherstellen oder minimieren), wird die Bildschirmfreigabe beendet.
- Ab Version 2112 für die Citrix Workspace-App:

  > **Hinweis:**
  >
  > Die folgenden Features sind 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.

  - **Anfordern der Steuerung in Microsoft Teams**

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

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

    Wenn Sie die Steuerung übernommen haben, können Sie Elemente auf dem freigegebenen Bildschirm auswählen, bearbeiten und andere Änderungen vornehmen. Wenn Sie fertig sind, klicken Sie auf **Steuerung freigeben**.

    Einschränkungen:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * Benutzer auf einem Linux-Client können anderen Benutzern keine *Steuerung übergeben*. Mit anderen Worten, nachdem der Benutzer auf dem Linux-Client mit der Freigabe von Inhalten begonnen hat, ist die Option **Steuerung übergeben** in der Symbolleiste für die Freigabe nicht vorhanden. Dies wird durch eine Microsoft-Einschränkung verursacht.
    * 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.

  – **Unterstützung für dynamisches e911**

    Ab diesem Release unterstützt die Citrix Workspace-App 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 auf dem VDA ausgeführten Microsoft Teams-Clients. 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 für Linux erfüllt die Microsoft Teams-Optimierung mit HDX die Bestimmungen von Ray Baum's Law. Um dieses Feature zu unterstützen, muss die LLDP-Bibliothek in die Betriebssystemverteilung des Thin Clients aufgenommen werden.

- Ab Version 2203 für die Citrix Workspace-App:

  Chat und Besprechungen mit mehreren Fenstern für Microsoft Teams

  Ab diesem Release können Sie mehrere Fenster für Chats und Besprechungen in Microsoft Teams benutzen, wenn die HDX-Optimierung in Citrix Virtual Apps and Desktops 2112 oder höher verwendet wird. Das Fenster-Pop-Out ist auf verschiedenerlei Art möglich. Einzelheiten zum Ausklappen von Fenstern finden Sie unter Microsoft Teams Pop-Out Windows for Chats and Meetings.

  Benutzer älterer Versionen der Citrix Workspace-App oder des Virtual Delivery Agent (VDA) sollten bedenken, dass Microsoft den Einzelfenstercode künftig nicht mehr unterstützt. Ab dem Zeitpunkt der globalen Verfügbarkeit dieses Features haben Sie jedoch mindestens neun Monate Zeit für ein Upgrade auf eine VDA- bzw. Citrix Workspace-App-Version, die mehrere Fenster unterstützt (2203 und höher).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

- Ab Version 2207 für die Citrix Workspace-App:

  Unterstützung für sekundären Klingelton:

  Sie können das Feature "Sekundärer Klingelton" verwenden, um ein zweites Gerät für die Benachrichtigung über eingehende Anrufe auszuwählen, wenn Microsoft Teams optimiert ist (Citrix HDX optimiert in Info/Version). Angenommen, Sie haben einen Lautsprecher als sekundären Klingelton eingerichtet und Ihr Endpunkt ist mit einem Kopfhörer verbunden. In diesem Fall sendet Microsoft Teams das eingehende Rufsignal an den Lautsprecher, obwohl Ihre Kopfhörer das primäre Peripheriegerät für den Audioanruf sind. In den folgenden Fällen können Sie keinen sekundären Klingelton festlegen:

  - Wenn Sie nicht mit mehreren Audiogeräten verbunden sind
  - Wenn das Peripheriegerät nicht verfügbar ist (z. B. Bluetooth-Headset)

  > **Hinweis:**
  >
  > Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Informationen zum Datum der Updateveröffentlichung finden Sie unter Microsoft 365-Roadmap. Die Revision der Dokumentation und die Ankündigung finden Sie außerdem unter CTX253754.

- Ab Version 2207 für die Citrix Workspace-App:

  - App-Freigabe aktiviert: Ab Citrix Workspace-App 2209 für Linux bzw. Citrix Virtual Apps and Desktops 2109 können Sie Apps über die **Bildschirmfreigabe** in Microsoft Teams freigeben.
  - **Verbesserungen der Unterstützung hoher DPI-Werte:** Wenn das Feature "Hoher DPI-Wert" aktiviert ist und Sie 4K-Bildschirme verwenden, werden Microsoft Teams-Videoüberlagerungen an der gewünschten Position und in der richtigen Größe angezeigt. Unabhängig von den Anzeigeeinstellungen (Einzel- oder Multimonitor-Anordnungen) erscheinen Überlagerungen immer korrekt und werden nicht vergrößert oder an einer unerwünschten Position angezeigt. Um diese Verbesserung zu aktivieren, stellen Sie sicher, dass der Parameter `DPIMatchingEnabled` in der Konfigurationsdatei `wfclient.ini` auf **True** festgelegt ist. Weitere Informationen finden Sie unter Unterstützung für DPI-Anpassung.
  - **WebRTC SDK-Upgrade:** Die Version von WebRTC, die für optimiertes Microsoft Teams verwendet wird, wurde auf Version M98 aktualisiert.

- Ab Version 2305 für die Citrix Workspace-App:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Verbesserter Energiesparmodus für optimierte Microsoft Teams-Anrufe**

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

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

- **Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen**

Ab Release 2305 ist die Simulcast-Unterstützung standardmäßig für optimierte Microsoft Teams-Videokonferenzen aktiviert. Dadurch werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

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

> **Hinweis:**
>
> Dieses Feature ist erst nach Veröffentlichung eines Microsoft Teams-Updates verfügbar. Weitere Informationen zum voraussichtlichen Releasedatum finden Sie durch Suchen nach “Microsoft 365 roadmap” auf . Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

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

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

Ab Release 2307 unterstützt die Citrix Workspace-App die Wiedergabe der kurzen Töne wie gewünscht. Diese Unterstützung aktiviert auch die sekundäre Ruftonfunktion.

Voraussetzungen:

Installieren Sie die neueste Version von Microsoft Teams.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Das oben erwähnte Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in CTX253754 Informationen über das Dokumentationsupdate und die Ankündigung.

Unterstützung für den virtuellen NSAP-Kanal (NetScaler App Experience)

Der virtuelle NSAP-Kanal war bisher als experimentelles Feature erhältlich und wird ab Version 2006 vollständig unterstützt. Alle HDX Insight-Daten entstammen dem virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Dieser Ansatz verbessert die Skalierbarkeit und Leistung von Sitzungen. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert. Um das Feature zu deaktivieren, legen Sie das VDNSAP-Flag in der Datei module.ini auf `NSAP=Off` fest.

Weitere Informationen finden Sie unter HDX Insight in der Dokumentation zu Linux Virtual Delivery Agent und unter HDX Insight in der Dokumentation zum Citrix Application Delivery Management Service.

Layoutspeicherung im Multimonitormodus

Mit diesem Feature werden die Angaben zum Bildschirmlayout einer Sitzung über Endpunkte hinweg beibehalten. Die Sitzung wird dann gemäß Konfiguration stets auf denselben Monitoren angezeigt.

Voraussetzung:

Dieses Feature erfordert Folgendes:

- StoreFront v3.15 oder höher.
- Wenn `.ICAClient` bereits im Basisordner des aktuellen Benutzers vorhanden ist:

  Löschen Sie die Datei All_Regions.ini.

  oder

  Zum Beibehalten der Datei `All_Regions.ini` fügen Sie die folgenden Zeilen am Ende des Abschnitts [Client Engine\Application Launching] hinzu:

  SubscriptionUrl =

  PreferredWindowsBounds =

  PreferredMonitors=

  PreferredWindowState=

  SaveMultiMonitorPref=

Wenn der Ordner `.ICAClient` nicht vorhanden ist, weist dies auf eine Neuinstallation der Citrix Workspace-App hin. In diesem Fall wird die Standardeinstellung für das Feature beibehalten.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Anwendungsfälle

- Starten Sie eine Sitzung auf einem beliebigen Bildschirm im Fenstermodus und speichern Sie die Einstellung.
  Wenn Sie die Sitzung erneut starten, wird sie im selben Modus, auf demselben Bildschirm und an derselben Position angezeigt.
- Starten Sie eine Sitzung auf einem beliebigen Bildschirm im Vollbildmodus und speichern Sie die Einstellung.
  Wenn Sie die Sitzung erneut starten, wird sie im Vollbildmodus auf demselben Bildschirm angezeigt.
- Ziehen Sie eine Sitzung im Fenstermodus über mehrere Bildschirme und wechseln Sie dann in den Vollbildmodus. Die Sitzung wird dann im Vollbildmodus auf allen Bildschirmen angezeigt. Wenn Sie die Sitzung erneut starten, wird sie im Vollbildmodus über alle Bildschirme hinweg angezeigt.

> **Hinweise:**
>
> - Das Layout wird bei jeder Speicherung überschrieben und nur auf dem aktiven StoreFront gespeichert.
> - Wenn Sie weitere Desktopsitzungen von demselben StoreFront-Store auf unterschiedlichen Bildschirmen starten, werden beim Speichern des Layouts in einer Sitzung die Layoutinformationen aller Sitzungen gespeichert.

Layout speichern

Aktivieren der Layoutspeicherung:

1. Installieren Sie StoreFront Version 3.15 oder höher (gleich oder höher als v3.15.0.12) auf einem kompatiblen Delivery Controller (DDC).
2. Laden Sie den Build der Citrix Workspace-App 1808 oder höher für Linux von der Downloadseite herunter und installieren Sie ihn auf der Linux-Maschine.
3. Legen Sie die ICAROOT-Umgebungsvariable auf den Installationsort fest.
4. Überprüfen Sie, ob die Datei **All_Regions.ini** im Ordner **.ICAClient** vorhanden ist. Wenn ja, löschen Sie sie.
5. Suchen Sie in der Datei **$ICAROOT/config/All_Regions.ini** nach dem Feld **SaveMultiMonitorPref**. Der Standardwert in diesem Feld ist “True” (das Feature ist aktiviert). Ändern Sie den Wert in “False”, um das Feature auszuschalten.
   Wenn Sie den Wert für **SaveMultiMonitorPref** ändern, müssen Sie die Datei **All_Regions.ini** im Ordner **.ICAClient** löschen, um Wertkonflikte und eine mögliche Profilsperrung zu verhindern. Aktivieren oder deaktivieren Sie das Flag **SaveMultiMonitorPref**, bevor Sie Sitzungen starten.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. Starten Sie eine neue Desktopsitzung.
7. Klicken Sie in der Desktop Viewer-Symbolleiste auf **Layout speichern**, um das aktuelle Sitzungslayout zu speichern. Am rechten unteren Bildrand wird die Speicherung in einer Meldung bestätigt.
   Wenn Sie auf "Layout speichern" klicken, wird das Symbol grau angezeigt. Die Farbänderung bedeutet, dass ein Speichervorgang ausgeführt wird. Nach der Speicherung des Layouts wird das Symbol wieder normal angezeigt.
8. Trennen Sie die Sitzung oder melden Sie sich ab.
   Starten Sie die Sitzung erneut. Sie wird dann im selben Modus, auf demselben Bildschirm und an derselben Position angezeigt.

Einschränkungen und nicht unterstützte Szenarien:

- Für Sitzungen im Fenstermodus wird das Speichern eines Layouts über mehrere Bildschirme hinweg aufgrund von Einschränkungen beim Linux-Anzeigemanager nicht unterstützt.
- Das bildschirmübergreifende Speichern von Sitzungsinformationen bei Bildschirmen mit unterschiedlicher Auflösung wird in diesem Release nicht unterstützt und kann zu unvorhersehbarem Verhalten führen.
- Kundenbereitstellungen mit weiteren StoreFront-Stores

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.

Workspace Launcher

Citrix führt den Workspace Launcher (WebHelper) ein, um veröffentlichte Desktops und Anwendungen zu starten.

Bisher ermöglichte das zusammen mit der Citrix Workspace-App für Linux bereitgestellte Browser-Plug-In, das auf der NPAPI basiert, Benutzern das Starten veröffentlichter Desktops und Anwendungen.

Als Lösung führt Citrix daher den Workspace Launcher (WebHelper) ein. Um dieses Feature zu aktivieren, konfigurieren Sie StoreFront so, dass Anforderungen an den Workspace Launcher gesendet werden, um die installierte Citrix Workspace-App zu erkennen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Ab Version 1901 ist der Citrix Workspace Launcher kompatibel für direkte Verbindungen zu StoreFront und Citrix Gateway. Mit diesem Feature wird die ICA-Datei automatisch gestartet und die Citrix Workspace-App erkannt.

Informationen zum Konfigurieren von StoreFront finden Sie unter **Solution – 2** > **a) Administrator configuration** im Knowledge Center-Artikel CTX237727.

> **Hinweis:**
>
> Citrix Workspace Launcher funktioniert derzeit nur bei einer direkten Verbindung zu StoreFront. In anderen Situationen (z. B. bei Verbindungen über Citrix Gateway) wird er nicht unterstützt.

Deaktivieren des neuen Workspace-Weboberflächenmodus

Wenn Sie die Citrix Workspace-App für Linux mit der ausführbaren Self-Service-Datei des Thin Client eines Drittanbieters starten, reagiert die Anwendung möglicherweise aufgrund 100%iger CPU-Auslastung nicht mehr.

Sie umgehen das Problem, indem Sie zurück zum alten Benutzeroberflächenmodus wechseln:

1. Entfernen Sie zwischengespeicherte Dateien mit dem folgenden Befehl:
   `rm -r ~/.ICAClient`
2. Navigieren Sie zur Datei `$ICAROOT/config/AuthManconfig.xml`.
3. Ändern Sie den Schlüsselwert `CWACapableEnabled` in “false”.
4. Starten Sie die Citrix Workspace-App für Linux. Die ausführbare Self-Service-Datei lädt die alte Benutzeroberfläche.

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert. Wenn Sie dieses Feature aktivieren, wird das Clienttastaturlayout automatisch mit den virtuellen Apps und Desktops synchronisiert.

Ab Version 2203 unterstützt die Citrix Workspace-App die folgenden drei Synchronisierungsmodi für das Tastaturlayout:

- **Nur einmal beim Sitzungsstart synchronisieren** - Basierend auf dem Wert `KeyboardLayout` in der Datei wfclient.ini wird das Clienttastaturlayout beim Start der Sitzung mit dem Server synchronisiert. Wenn der Wert `KeyboardLayout` auf `0` festgelegt ist, wird die Systemtastatur mit dem VDA synchronisiert. Wenn der Wert `KeyboardLayout` auf eine bestimmte Sprache festgelegt ist, wird die sprachspezifische Tastatur mit dem VDA synchronisiert. Änderungen, die Sie während der Sitzung am Clienttastaturlayout vornehmen, werden nicht sofort wirksam. Um die Änderungen zu übernehmen, melden Sie sich von der App ab und wieder an. Der Modus **Nur**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

einmal beim Sitzungsstart synchronisieren ist das Standardtastaturlayout, das für die Citrix Workspace-App ausgewählt wurde.

- **Dynamische Synchronisierung zulassen** - Diese Option synchronisiert das Clienttastaturlayout mit dem Server, wenn Sie das Clienttastaturlayout ändern.
- **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

Voraussetzung:

- Aktivieren Sie die Unicode-Tastaturlayoutzuordnung auf dem Windows VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX226335.
- Aktivieren Sie die dynamische Tastaturlayoutsynchronisierung auf dem Linux VDA. Weitere Informationen finden Sie unter Dynamische Tastaturlayoutsynchronisierung.
- Die Synchronisierung des Tastaturlayouts hängt von der XKB lib ab.
- Wenn Sie einen Windows Server 2016 oder Windows Server 2019 verwenden, navigieren Sie zum Registrierungspfad `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`, fügen Sie einen DWORD-Wert mit dem Schlüsselnamen `DisableKeyboardSync` hinzu und legen Sie den Wert `0` fest.
- Wenn `.ICAClient` bereits im Basisordner des aktuellen Benutzers vorhanden ist:

  Löschen Sie die Datei All_Regions.ini.

  oder

  Um die Datei `All_Regions.ini` beizubehalten, fügen Sie am Ende des Abschnitts [Virtual Channels\Keyboard] die folgenden Zeilen hinzu:

  KeyboardSyncMode=

  KeyboardEventMode=

Konfigurieren des Tastaturlayouts

Die Citrix Workspace-App bietet sowohl Benutzeroberflächenelemente als auch Konfigurationseinstellungen, um die drei verschiedenen Synchronisationsmodi für das Tastaturlayout zu aktivieren

Konfigurieren der Tastaturlayoutsynchronisierung über die grafische Benutzeroberfläche:

1. Wählen Sie im Infobereich das Symbol der Citrix Workspace-App aus und dann die Option **Einstellungen**.

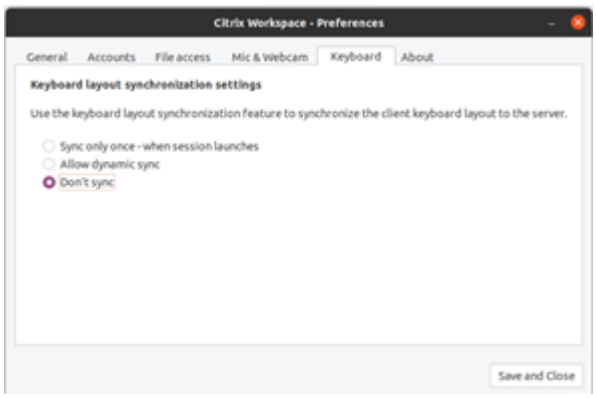
   Oder

   Öffnen Sie das Terminal, navigieren Sie zum Installationspfad und führen Sie den folgenden Befehl aus:

   ```
   util/configmgr
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Das Dialogfeld **Citrix Workspace - Einstellungen** wird angezeigt.



2. Klicken Sie auf die Registerkarte **Tastatur**.

   Die Seite **Einstellungen für die Synchronisierung des Tastaturlayouts** wird angezeigt

3. Wählen Sie eine der folgenden Optionen:

   - **Nur einmal beim Sitzungsstart synchronisieren** - Synchronisiert das Tastaturlayout nur einmal beim Sitzungsstart mit dem VDA. Der Tastatureingabemodus “Unicode” ist die empfohlene Option für den Modus **Nur einmal beim Sitzungsstart synchronisieren**.
   - **Dynamische Synchronisierung zulassen** - Synchronisiert das Tastaturlayout dynamisch mit dem VDA, wenn die Clienttastatur in einer Sitzung geändert wird. Der Tastatureingabemodus “Unicode” ist die empfohlene Option für den Modus **Dynamische Synchronisierung zulassen**.
   - **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout unabhängig vom im Client ausgewählten Tastaturlayout. Der Tastatureingabemodus “Scancode” ist die empfohlene Option für den Modus **Nicht synchronisieren**. Stellen Sie sicher, dass das Clienttastaturlayout mit dem Tastaturlayout auf dem VDA identisch ist, wenn Sie Unicode für die Option **Nicht synchronisieren** wählen.

4. Klicken Sie auf **Speichern und Schließen**.

Konfigurieren der Tastaturlayoutsynchronisierung mit Konfigurationsdateieinstellungen:

Bearbeiten Sie die Konfigurationsdatei `wfclient.ini`, um das erforderliche Tastaturlayout zu ermöglichen.

Nur einmal beim Sitzungsstart synchronisieren:

Wenn diese Funktion aktiviert ist, wird beim Starten einer Sitzung das aktive Tastaturlayout auf dem Clientgerät mit dem VDA synchronisiert. Basierend auf dem Wert `KeyboardLayout` in der Datei `wfclient.ini` wird das Clienttastaturlayout beim Start der Sitzung mit dem Server synchronisiert. Wenn der Wert `KeyboardLayout` auf `0` festgelegt ist, wird die Systemtastatur mit dem VDA synchronisiert. Wenn der Wert `KeyboardLayout` auf eine bestimmte Sprache festgelegt ist, wird die sprachspezifische Tastatur mit dem VDA synchronisiert.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Um diesen Modus auszuwählen, gehen Sie wie folgt vor:

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Fügen Sie die folgenden Einträge hinzu:

```
KeyboardSyncMode=Once
KeyboardEventMode=Unicode/Scancode
<!--NeedCopy-->
```

Der Tastatureingabemodus “Unicode” ist die empfohlene Option für den Modus **Nur einmal beim Sitzungsstart synchronisieren**.

Dynamische Synchronisierung zulassen:

Wenn das Feature aktiviert ist, ändert sich das Tastaturlayout der Sitzung automatisch zusammen mit dem auf dem Clientgerät.

Um diesen Modus auszuwählen, gehen Sie wie folgt vor:

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Fügen Sie die folgenden Einträge hinzu:

```
KeyboardSyncMode=Dynamic
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
<!--NeedCopy-->
```

Der Tastatureingabemodus “Unicode” ist die empfohlene Option für den Modus **Dynamische Synchronisierung zulassen**.

Nicht synchronisieren:

Wenn diese Funktion aktiviert ist, wird das VDA-seitige Tastaturlayout verwendet, unabhängig von dem Tastaturlayout, das auf dem Clientgerät ausgewählt ist.

Um diesen Modus auszuwählen, gehen Sie wie folgt vor:

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Fügen Sie die folgenden Einträge hinzu:

```
KeyboardSyncMode=No
KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
<!--NeedCopy-->
```

Der Tastatureingabemodus “Scancode” ist die empfohlene Option für den Modus **Nicht synchronisieren**. Stellen Sie sicher, dass das Clienttastaturlayout mit dem Tastaturlayout auf dem VDA identisch ist, wenn Sie Unicode für die Option **Nicht synchronisieren** konfigurieren.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn Sie `KeyboardSyncMode=""` (leer) in der Datei `wfclient.ini` festlegen, wird der Modus auf das vorherige Verhalten zurückgesetzt. Beim ursprünglichen Verhalten wird das Tastaturlayout aus der Datei `$HOME/.ICAClient/wfclient.ini` gelesen und zusammen mit anderen Clientinformationen beim Start der Sitzung an den VDA gesendet.

Tastatureingabemodus

Citrix empfiehlt den folgenden Tastatureingabemodus für die verschiedenen Tastaturlayoutsynchronisierungsoptionen:

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

Sie können die Konfiguration von `KeyboardEventMode` in der Datei `wfclient.ini` ändern. Um eine optimale Leistung zu erzielen, sollten Sie die von Citrix empfohlenen Modi die für verschiedene Szenarien, physische Tastaturen und Clientgeräte verwenden.

Client-IME für ostasiatische Sprachen

Der Client-Eingabemethoden-Editor (Input Method Editor, IME) verbessert die Eingabe und Anzeige von chinesischen, japanischen und koreanischen (CJK) Schriftzeichen in der Citrix Workspace-App für Linux. Sie können den Client-IME verwenden, wenn Sie einen bevorzugten IME im Linux-Client haben oder wenn der IME auf dem Remoteserver nicht verfügbar ist.

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

1. Navigieren Sie zur Konfigurationsdatei `$HOME/.ICAClient/wfclient.ini`.
2. Fügen Sie die folgenden Einträge hinzu:

```
KeyboardEventMode = Unicode
UseLocalIM = True
<!--NeedCopy-->
```

Wenn Ihre Client-Linux-Distribution keinen funktionierenden iBus hat, müssen Sie den Wert `KeyboardLayout` explizit entsprechend Ihrer IME-Sprache in der Konfigurationsdatei wfclient.ini festlegen:

- Chinesischer IME: `KeyboardLayout = Chinese (PRC)`
- Japanischer IME: `KeyboardLayout = Japanese (JIS)`
- Koreanischer IME: `KeyboardLayout = Korean`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Verbesserung zur Unterstützung der Tastaturlayoutsynchronisierung für GNOME 42

Ab Version 2305 unterstützt die Citrix Workspace-App für Linux die Synchronisierung des Tastaturlayouts für Desktops wie Ubuntu 22.04, das die Desktopumgebung GNOME 42 und höher verwendet.

Tastaturlayoutunterstützung für Windows VDA und Linux VDA

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Arabisch	ara	-	→	ar-SA	00000401	ara	-
Arabisch (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
Deutsch (Österreich)	at	-	→	de-AT	00000407	at	-
Belgisch (alt. ISO)	be	iso-alternate	→	fr-BE	0000080c	be	iso-alternativ
Belgisch	be	-	→	nl-BE	00000813	be	-
Bulgarisch	bg	-	→	bg-BG	00030402	bg	-
Bulgarisch (traditionelle Phonetik)	bg	phonetic	→	bg-BG	00040402	bg	phonetic
Bulgarisch (neue Phonetik)	bg	bas_phonetic	→	bg-BG	00020402	bg	bas_phonetic
Portugiesis (Brasilien)	br	-	→	pt-BR	00000416	br	-
Belarussisch	by	-	→	be-BY	00000423	by	-
Englisch (Kanada)	ca	eng	→	en-CA	00000409	ca	eng

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Kanadisch mehrsprachlich	ca	multix	→	fr-CA	00011009	ca	multix
Französisch (Kanada, Legacy)	ca	fr-legacy	→	fr-CA	00000c0c	ca	fr-legacy
Französisch (Kanada)	ca	-	→	fr-CA	00001009	ca	-
Französisch (Schweiz)	ch	fr	→	fr-CH	0000100c	ch	fr
Deutsch (Schweiz)	ch	-	→	de-CH	00000807	ch	-
Chinesisch (vereinfacht)	cn	-	→	en-US	00000409	us	-
Tschechisch	cz	-	→	cs-CZ	00000405	cz	-
Tschechisch (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty
Deutsch	de	-	→	de-DE	00000407	de	-
Deutsch (Macintosh)	de	mac	→	de-DE	00000407	de	mac
Dänisch	dk	-	→	da-DK	00000406	dk	-
Estnisch	ee	-	→	et-EE	00000425	ee	-
Spanisch (Lateinamerika)	es	-	→	es-ES	0000040a	es	-
Spanisch (Macintosh)	es	mac	→	es-ES	0000040a	es	mac
Finnisch	fi	-	→	fi-FI	0000040b	fi	-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Französisch	fr	-	→	fr-FR	0000040c	fr	-
Französisch (Macintosh)	fr	mac	→	fr-FR	0000040c	fr	mac
Englisch (UK)	gb	-	→	en-GB	00000809	gb	-
Englisch (Macintosh)	gb	mac	→	en-GB	00000809	gb	mac
Englisch (UK, erweitert mit Win-Tasten)	gb	extd	→	en-GB	00000452	gb	extd
Griechisch	gr	-	→	el-GR	00000408	gr	-
Kroatisch	hr	-	→	hr-HR	0000041a	hr	-
Ungarisch	hu	-	→	hu-HU	0000040e	hu	-
Irisch	ie	-	→	en-IE	00001809	ie	-
Hebräisch	il	-	→	he-IL	0002040d	il	-
Englisch (Indien, mit Rupie)	in	eng	→	en-IN	00004009	in	eng
Irakisch	iq	-	→	ar-IQ	00000401	iq	-
Isländisch	is	-	→	is-IS	0000040f	is	-
Italienisch	it	-	→	it-IT	00000410	it	-
Japanisch	jp	-	→	en-US	00000409	us	-
Japanisch (Macintosh)	jp	mac	→	en-US	00000409	us	mac

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Koreanisch	kr	-	→	en-US	00000409	us	-
Spanisch (Lateinamerika)	latam	-	→	es-MX	0000080a	latam	-
Litauisch	lt	-	→	lt-LT	00010427	lt	-
Litauisch (IBM LST 1205-92)	lt	ibm	→	lt-LT	00000427	lt	ibm
Litauisch (Standard)	lt	std	→	lt-LT	00020427	lt	std
Lettisch	lv	-	→	lv-LV	00020426	lv	-
Norwegisch	no	-	→	nb-NO	00000414	no	-
Polnisch	pl	-	→	pl-PL	00000415	pl	-
Polnisch (QWERTZ)	pl	qwertz	→	pl-PL	00010415	pl	qwertz
Portugiesisch	pt	-	→	pt-PT	00000816	pt	-
Portugiesisch (Macintosh)	pt	mac	→	pt-PT	00000816	pt	mac
Rumänisch (Standard)	ro	std	→	ro-RO	00010418	ro	std
Serbisch	rs	-	→	sr-Cyrl-RS	00000c1a	rs	-
Serbisch (Lateinisch)	rs	Lateinisch	→	sr-Latn-RS	0000081a	rs	Lateinisch
Russisch	ru	-	→	ru-RU	00000419	ru	-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Russisch (Schreibmaschine)	ru	typewriter	→	ru-RU	00010419	ru	Schreibmaschine
Russisch (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
Schwedisch	se	-	→	sv-SE	0000041d	se	-
Schwedisch (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
Slowenisch	si	-	→	sl-SI	00000424	si	-
Slowakisch	sk	-	→	sk-SK	0000041b	sk	-
Slowakisch (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
Thailändisch	th	-	→	th-TH	0000041e	th	-
Thailändisch (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
Tadschikisch	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
Türkisch	tr	-	→	tr-TR	0000041f	tr	-
Türkisch (F)	tr	f	→	tr-TR	0001041f	tr	f
Chinesisch (traditionell)	tw	-	→	en-US	00000409	us	-
Ukrainisch	ua	-	→	uk-UA	00000422	ua	-
Englisch (US)	us	-	→	en-US	00000409	us	-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Linux-Clienttastatur	Linux-Client Tastaturlayout	Linux-Client Tastaturvariante	Synchr. mit	Windows Gebietsschema-ID	Windows VDA-Tastaturlayout (ID)	Linux VDA-Tastaturlayout	Linux VDA-Tastaturvariante
Englisch (Macintosh)	us	mac	→	en-US	00000409	us	mac
Englisch (Dvorak)	us	dvorak	→	en-US	00010409	us	dvorak
Englisch (Dvorak, Linkshänder)	us	dvorak-l	→	en-US	00030409	us	dvorak-l
Englisch (Dvorak, Rechtshänder)	us	dvorak-r	→	en-US	00040409	us	dvorak-r
Englisch (US, int., mit unbelegten Tasten)	us	intl	→	nl-NL	00020409	us	intl
Vietnamesisch	vn	-	→	vi-VN	0000042a	vn	-

VDA-Tastaturlayout

Mit dem VDA-Tastaturlayout-Feature können Sie das Tastaturlayout des VDA unabhängig von den Tastaturlayouteinstellungen des Clients verwenden. Die folgenden Tastaturtypen werden unterstützt: PC/XT 101, 102, 104, 105, 106.

Verwenden des serverseitigen Tastaturlayouts:

1. Starten Sie die Datei wfclient.ini.
2. Ändern Sie den Wert des Attributs `KeyboardLayout` wie folgt:

   `KeyboardLayout=(Server Default)`

   Der Standardwert für das Attribut `KeyboardLayout` ist (Benutzerprofil).
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Dateien und Ordner zwischen zwei virtuellen Desktops kopieren und einfügen [Technical Preview]

Bisher konnten Sie nur Text zwischen zwei virtuellen Desktops kopieren. Ab diesem Release können Sie auch Dateien und Ordner zwischen zwei virtuellen Desktops kopieren und einfügen. Die maximale Datenmenge, die im Linux Virtual Delivery Agent in einem einzelnen Vorgang kopiert bzw. eingefügt werden kann, ist 200 MB. Weitere Informationen finden Sie in der Dokumentation zum Kopieren und Einfügen von Dateien.

Dieses Feature ist standardmäßig aktiviert.

> **Hinweis:**
>
> Das Kopieren und Einfügen von Dateien und Ordnern zwischen zwei virtuellen Desktops wird nur auf der x64-Linux-Distribution und auf Geräten mit ARM64-Architektur unterstützt, auf denen die Citrix Workspace-App für Linux ausgeführt wird.

Um das Feature zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zur Konfigurationsdatei `/opt/Citrix/ICAClient/config/module.ini`.
2. Ändern Sie den Wert für `VDGDT` in `Off`.

Sie können Feedback zu dieser Technical Preview mit dem Podio-Formular geben.

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

Dateitypzuordnungen

Citrix Virtual Apps Services kann auch eine Datei und nicht nur Anwendungen oder Desktops veröffentlichen. Dieser Vorgang wird als Veröffentlichen von Inhalt bezeichnet und ermöglicht pnabrowse, die veröffentlichte Datei zu öffnen.

Die Citrix Workspace-App erkennt nicht alle Dateitypen. Dem Dateityp der veröffentlichten Datei muss eine veröffentlichte Anwendung zugeordnet sein, damit gilt:

- Das System erkennt den Dateityp des veröffentlichten Inhalts.
- Benutzer können die Datei über die Citrix Workspace-App anzeigen.

Um beispielsweise eine veröffentlichte Adobe PDF-Datei mit der Citrix Workspace-App zu öffnen, muss eine Anwendung wie z. B. Adobe PDF Viewer veröffentlicht sein. Benutzer können den

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

veröffentlichten Inhalt nur anzeigen, wenn eine geeignete Anwendung veröffentlicht ist.

Aktivieren von Dateitypzuordnung auf dem Client:

1. Stellen Sie sicher, dass die App, die Sie zuordnen möchten, eine Favoriten-App oder eine abonnierte Anwendung ist.
2. Um die Liste der veröffentlichten Anwendungen und die Server-URL abzurufen, führen Sie die folgenden Befehle aus:

```
./util/storebrowse -l

./util/storebrowse -S <StoreFront URL>
<!--NeedCopy-->
```

3. Führen Sie den Befehl ./util/ctx_app_bind mit der folgenden Syntax aus:

   ```
   ./util/ctx_app_bind [-p] example_file|MIME-type published-application [
   server|server-URI]
   ```

   Beispiel:
   ```
   ./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.
   bvt.local/citrix/store/discovery
   ```

4. Stellen Sie sicher, dass für die Datei, die Sie öffnen möchten, die Clientlaufwerkzuordnung (CDM) aktiviert ist.
5. Doppelklicken Sie auf die Datei, um sie mit der zugeordneten Anwendung zu öffnen.

Zuordnen einer veröffentlichten Anwendung zu Dateitypen

Die Citrix Workspace-App liest die von Administratoren in Citrix Studio konfigurierten Einstellungen und wendet sie an.

Voraussetzung:

Stellen Sie sicher, dass Sie eine Verbindung mit dem Store-Server herstellen, auf dem die Dateitypzuordnung konfiguriert ist.

Verknüpfen einer Dateinamenerweiterung mit einer Citrix Workspace-App für Linux:

1. Veröffentlichen Sie die Anwendung.
2. Melden Sie sich bei Citrix Studio an.
3. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften**.
4. Wählen Sie **Ort**.
5. Fügen Sie “%**” im Feld “Befehlszeilenargument (optional)” hinzu, um die Befehlszeilenprüfung zu umgehen, und klicken Sie dann auf “OK”.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften**.
7. Wählen Sie **Dateitypzuordnung**.
8. Wählen Sie alle Erweiterungen aus, die die Citrix Workspace-App der Anwendung zuordnen soll.
9. Klicken Sie auf **Anwenden** und dann auf **Dateitypen aktualisieren**.
10. Führen Sie die unter Dateitypzuordnung beschriebenen Schritte aus, um die Dateitypzuordnung auf dem Client zu aktivieren.

> **Hinweis:**
>
> Die StoreFront-Dateitypzuordnung muss auf "EIN" festgelegt sein. In der Standardeinstellung ist die Dateitypzuordnung aktiviert.

Unterstützung für Citrix Analytics

Ab Version 2006 überträgt die Citrix Workspace-App Daten von ICA-Sitzungen, die Sie über einen Browser starten, an den Citrix Analytics-Dienst.

Weitere Informationen dazu, wie Citrix Analytics diese Informationen verwendet, finden Sie unter Self-Service-Suche für Leistung und Self-Service-Suche für Virtual Apps and Desktops.

Die Citrix Workspace-App für Linux ist für die sichere Übertragung von Protokollen an Citrix Analytics ausgelegt, wenn die App bestimmte Ereignisse auslöst. 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.

Transparente Benutzeroberfläche

Das Citrix ICA-Protokoll verwendet das Protokoll "Transparent User Interface Virtual Channel" [TUI VC], um Daten zwischen Citrix Virtual Apps and Desktops bzw. Citrix DaaS und Hostservern zu übertragen. Das TUI-Protokoll überträgt Komponentenmeldungen der Benutzeroberfläche [UI] für Remoteverbindungen.

Die Citrix Workspace-App für Linux unterstützt das TUI VC-Feature. Durch das Feature kann der Client die vom Server gesendeten TUI-Pakete empfangen und auf UI-Komponenten zugreifen. Durch diese Funktion können Sie die Anzeige des überlagernden Standardbildschirms steuern. Sie können das `VDTUI`-Flag in der Datei `module.ini` ein- und ausschalten: `VDTUI - On/Off`

Ab Version 1912 ist das **VDTUI**-Flag standardmäßig auf **On** gesetzt. Das Dialogfeld "<Anwendung> wird gestartet" wird daher beim Start einer App nicht mehr angezeigt. Stattdessen ist das Dialogfeld "Verbinden mit <Anwendung>" mit einer Fortschrittsanzeige zu sehen. Das Dialogfeld zeigt auch den

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Fortschritt des App-Starts an. Wenn Sie das Flag jedoch auf **Off** gesetzt hatten, wurde die Anmeldeaufforderung vom Dialogfeld “<Anwendung> wird gestartet” verdeckt.

Weitere Informationen zu virtuellen Kanälen finden Sie unter Virtuelle ICA-Kanäle von Citrix in der Dokumentation zu Citrix Virtual Apps and Desktops.

Erhöhung der Anzahl der unterstützten virtuellen Kanäle

In früheren Versionen des Clients wurden bis zu 32 virtuelle Kanäle in einer Sitzung unterstützt.

Ab Version 2103 können Sie bis zu 64 virtuelle Kanäle in einer Sitzung nutzen.

Authentifizieren

September 12, 2023

Ab Citrix Workspace-App 2012 können Sie das Authentifizierungsdialogfeld in der Citrix Workspace-App anzeigen und Details auf dem Anmeldebildschirm speichern. Dies sorgt für eine bessere Benutzererfahrung.

Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht neu eingeben müssen.

> **Hinweis:**
>
> Diese Verbesserung der Authentifizierung ist nur in Cloud-Bereitstellungen verfügbar.

Voraussetzung:

Installieren Sie die Bibliothek `libsecret`.

Dieses Feature ist standardmäßig aktiviert.

Verbesserung der Authentifizierung für Storebrowse

Ab Version 2205 befindet sich das Authentifizierungsdialogfeld in der Citrix Workspace-App und die Storedetails werden im Anmeldebildschirm angezeigt. Die Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht neu eingeben müssen.

Die verbesserte Authentifizierung unterstützt Storebrowse für die folgenden Vorgänge:

- `Storebrowse -E`: Listet die verfügbaren Ressourcen auf.
- `Storebrowse -L`: Startet eine Verbindung zu einer veröffentlichten Ressource.
- `Storebrowse -S`: Listet die abonnierten Ressourcen auf.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- `Storebrowse -T`: Beendet alle Sitzungen des angegebenen Stores.
- `Storebrowse -Wr`: Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [r] werden alle getrennten Sitzungen wieder verbunden.
- `storebrowse -WR`: Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [R] werden alle aktiven und alle getrennten Sitzungen wieder verbunden.
- `Storebrowse -s`: Abonniert die angegebene Ressource aus dem jeweiligen Store.
- `Storebrowse -u`: Kündigt das Abonnement der angegebenen Ressource aus dem jeweiligen Store.
- `Storebrowse -q`: Startet eine Anwendung über die direkte URL. Dieser Befehl funktioniert nur bei StoreFront-Stores.

> **Hinweis:**
>
> - Sie können die verbleibenden Storebrowse-Befehle weiterhin wie zuvor verwenden (mit AuthMangerDaemon).
> - Die Verbesserung der Authentifizierung ist nur auf Cloud-Bereitstellungen anwendbar.
> - Mit dieser Verbesserung wird das Feature der persistenten Anmeldung unterstützt.

Unterstützung für mehr als 200 Gruppen in Azure AD

Ab Version 2305 kann ein Azure AD-Benutzer, der Mitglied in mehr als 200 Gruppen ist, ihm zugewiesene Apps und Desktops anzeigen. Bisher konnte er diese Apps und Desktops nicht sehen.

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

Verbesserung der Authentifizierung für die Storebrowse-Konfiguration

Das Feature zur Verbesserung der Authentifizierung ist standardmäßig deaktiviert.

Wenn der Gnome-Schlüsselbund nicht verfügbar ist, wird der Token im Self-Service-Prozessspeicher gespeichert.

Um das Speichern des Token im Speicher zu erzwingen, deaktivieren Sie den Gnome-Schlüsselbund mit den folgenden Schritten:

1. Navigieren Sie zu `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Fügen Sie folgenden Eintrag hinzu:

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Smartcard

Um die Smartcard-Unterstützung in der Citrix Workspace-App für Linux zu konfigurieren, müssen Sie den StoreFront-Server über die StoreFront-Konsole konfigurieren.

Die Citrix Workspace-App unterstützt Smartcardleser, die mit PCSC-Lite- und PKCS#11-Treibern kompatibel sind. Standardmäßig sucht die Citrix Workspace-App nach `opensc-pkcs11.so` in einem der Standardspeicherorte.

Die Citrix Workspace-App kann `opensc-pkcs11.so` in einem nicht standardmäßigen Speicherort suchen oder sie kann einen anderen `PKCS\##11`-Treiber suchen. Sie können den jeweiligen Speicherort mit den folgenden Schritten speichern:

1. Suchen Sie die Konfigurationsdatei: `$ICAROOT/config/AuthManConfig.xml`.
2. Suchen Sie die Zeile <key>PKCS11module</key> und fügen Sie den Treiberspeicherort dem Element <value> hinzu, das direkt der Zeile folgt.

> **Hinweis:**
>
> Wenn Sie einen Dateinamen für den Treiberspeicherort eingeben, navigiert die Citrix Workspace-App im Verzeichnis `$ICAROOT/PKCS\ ##11` zu der Datei. Sie können auch einen absoluten Pfad verwenden, der mit "/" beginnt.

Nach dem Entfernen einer Smartcard konfigurieren Sie das Verhalten der Citrix Workspace-App, indem Sie `SmartCardRemovalAction` mit den folgenden Schritten aktualisieren:

1. Suchen Sie die Konfigurationsdatei: `$ICAROOT/config/AuthManConfig.xml`
2. Suchen Sie die Zeile <key>SmartCardRemovalAction</key> und fügen Sie `noaction` oder `forcelogoff` dem Element <value> hinzu, das direkt der Zeile folgt.

Das Standardverhalten ist `noaction`. Es werden keine Maßnahmen ausgeführt, um gespeicherte Anmeldeinformationen und generierte Token beim Entfernen der Smartcard zu löschen.

Mit der Aktion `forcelogoff` werden alle Anmeldeinformationen und Token in StoreFront beim Entfernen der Smartcard entfernt.

Aktivieren der Smartcardunterstützung

Die Citrix Workspace-App unterstützt verschiedene Smartcardleser, wenn die Verwendung von Smartcards sowohl auf dem Server als auch auf der Citrix Workspace-App aktiviert ist.

Sie können Smartcards zu folgenden Zwecken verwenden:

- Smartcard-Anmeldeauthentifizierung: Authentifiziert Sie bei Citrix Virtual Apps and Desktops- und Citrix DaaS-Servern (zuvor Citrix Virtual Apps and Desktops Service).
- Smartcard-Anwendungsunterstützung: Ermöglicht smartcardfähigen veröffentlichten Anwendungen den Zugriff auf lokale Smartcardgeräte.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die sicherheitsrelevanten Smartcarddaten müssen über einen sicheren, authentifizierten Kanal, z. B. TLS, übertragen werden.

Für die Smartcardunterstützung müssen folgende Voraussetzungen erfüllt sein:

- Die Smartcardleser und die veröffentlichten Anwendungen müssen dem PC/SC-Industriestandard entsprechen.
- Installieren Sie den passenden Treiber für die Smartcard.
- Installieren Sie das PCSC Lite-Paket.
- Installieren Sie den `pcscd`-Daemon, der Middleware für den Zugriff auf die Smartcard mit PC/SC bereitstellt, und führen Sie ihn aus.
- Auf einem 64-Bit-System muss die 64-Bit- und 32-Bit-Version des “libpscslite1”-Pakets vorhanden sein.

Weitere Informationen zur Konfiguration der Smartcardunterstützung auf Servern finden Sie unter Smartcards in der Dokumentation zu Citrix Virtual Apps and Desktops.

Verbesserung der Smartcardunterstützung

Ab Version 2112 unterstützt die Citrix Workspace-App die Plug&Play-Funktionalität für Smartcardleser.

Wenn Sie eine Smartcard einstecken, erkennt der Smartcardleser die Smartcard auf dem Server und Client.

Wenn Sie verschiedene Karten gleichzeitig einstecken, werden alle Karten erkannt.

Voraussetzungen:

Installieren Sie die Bibliothek `libpcscd` auf dem Linux-Client.

> **Hinweis:**
>
> Diese Bibliothek kann in aktuellen Versionen der meisten Linux-Distributionen vorinstalliert sein. In früheren Versionen einiger Linux-Distributionen wie Ubuntu 1604 müssen Sie die Bibliothek `libpcscd` jedoch möglicherweise installieren.

So deaktivieren Sie diese Erweiterung:

1. Navigieren Sie zum Ordner `<ICAROOT>/config/module.ini`.
2. Navigieren Sie zum Abschnitt `SmartCard`.
3. Legen Sie Folgendes fest: `DriverName=VDSCARD.DLL`.

Unterstützung für neue PIV-Karten

Ab Version 2303 unterstützt die Citrix Workspace-App die folgenden PIV-Karten (Personal Identification Verification):

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- IDEMIA-Smartcard der nächsten Generation
- DELL TicTok-Smartcard

Leistungsoptimierung für Smartcardtreiber

Version 2303 der Citrix Workspace-App enthält leistungsbezogene Korrekturen und Optimierungen für den `VDSCARDV2.DLL`-Smartcardtreiber. Diese Verbesserungen erhöhen die Leistung gegenüber `VDSCARD.DLL` Version 1.

Unterstützung für Multifaktorauthentifizierung (nFactor)

Die Multifaktorauthentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten.

Mit der Multifaktorauthentifizierung können Authentifizierungsschritte und die zugehörigen Anmeldeinformationsformulare vollständig vom Administrator konfiguriert werden.

Die native Citrix Workspace-App unterstützt dieses Protokoll über die Anmeldeformulare, die bereits für StoreFront implementiert sind. Die webbasierten Anmeldeseiten für virtuelle Citrix Gateway- und Traffic Manager-Server verwenden ebenfalls dieses Protokoll.

Weitere Informationen finden Sie in der Dokumentation zu Citrix ADC unter SAML-Authentifizierung und Multifaktorauthentifizierung (nFactor).

Unterstützung für die Authentifizierung mit FIDO2 in HDX-Sitzungen

Ab Version 2303 können Sie sich innerhalb einer HDX-Sitzung mit kennwortlosen FIDO2-Sicherheitsschlüsseln authentifizieren. Mit FIDO2-Sicherheitsschlüsseln können Unternehmensmitarbeiter sich ohne Eingabe von Benutzernamen oder Kennwort bei Apps und Desktops, die FIDO2 unterstützen, authentifizieren. Weitere Informationen zu FIDO2 finden Sie unter FIDO2-Authentifizierung.

> **Hinweis:**
>
> Wenn Sie die FIDO2-Geräteumleitung über USB verwenden, entfernen Sie die USB-Umleitungsregel des FIDO2-Geräts aus der Datei `usb.conf` im Ordner `$ICAROOT/`. Dieses Update hilft Ihnen beim Umschalten auf den virtuellen FIDO2-Kanal.

Standardmäßig ist die FIDO2-Authentifizierung deaktiviert. Gehen Sie wie folgt vor, um die FIDO2-Authentifizierung zu aktivieren:

1. Navigieren Sie zur Datei `<ICAROOT>/config/module.ini`.
2. Navigieren Sie zum Abschnitt `ICA 3.0`.
3. Legen Sie `FIDO2= On` fest.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

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

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

Einschränkung:

Möglicherweise können Sie das zweite Gerät nicht mit der FIDO2-Authentifizierung bei demselben Konto registrieren.

Benutzerdefinierte Authentifizierung

Die folgende Tabelle enthält einen Verweis auf die verfügbare benutzerdefinierte Authentifizierung für die Citrix Workspace-App:

Hilfsprogramm	SDK	Authentifizierungstyp	Verwendete Bibliotheken	Binärdateien	Erkennung des Authentifizierungstyps
Unterstützung für Fast Connect:	Credential Insertion SDK	Benutzername/Passthrough	libCredInject.so	cis	Parameter, die von Authentifikator-Integrationen von Drittanbietern verwendet werden
Benutzerdefiniertes Dialogfeld	Platform Optimization SDK	Benutzername/Kennwort/Smartcard	UIDialogLib and UIDialogLib-WebKit3.so	Nein	Automatische Erkennung - Wird von Thin Client-Partnern verwendet

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Hilfsprogramm	SDK	Authentifizierungstyp	Verwendete Bibliotheken	Binärdateien	Erkennung des Authentifizierungstyps
Storebrowse	Citrix Workspace-App	Benutzername/	Nein	Storebrowse	Parameter

Sichere Kommunikation

September 12, 2023

Zum Sichern der Kommunikation zwischen Ihrer Site und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen mit Sicherheitstechnologien wie Citrix Gateway integrieren.

> **Hinweis:**
>
> Citrix empfiehlt die Verwendung von Citrix Gateway zwischen StoreFront-Servern und Benutzergeräten.

- Eine Firewall: Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie die Citrix Workspace-App mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.
- Vertrauenswürdige Server.
- Nur Citrix Virtual Apps and Desktops bzw. Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service): (gilt nicht für XenDesktop 7) ein SOCKS-Proxyserver oder ein sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver oder Tunneling-Proxyserver für Transport Layer Security (TLS)). Mit Proxyservern schränken Sie den eingehenden und ausgehenden Zugriff auf das Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.
- Nur Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Bereitstellungen: Citrix Secure Web Gateway- oder SSL-Relay-Lösungen mit TLS-Protokollen. Die TLS-Versionen 1.0 bis 1.2 werden unterstützt.

Citrix Gateway

Citrix Gateway (ehemals Access Gateway) sichert Verbindungen mit StoreFront-Stores. Administratoren können hiermit zudem präzise den Benutzerzugriff auf Desktops und Anwendungen steuern.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Format https://gateway.company.com.
   - Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im 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.

2. 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.

Proxyserver

Proxyserver werden zur Einschränkung des Netzwerkzugriffs und für Verbindungen zwischen der Citrix Workspace-App und Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Bereitstellungen verwendet.

Die Citrix Workspace-App unterstützt das SOCKS- und HTTPS-Protokoll (Technical Preview) sowie Folgendes:

- Citrix Secure Web Gateway und Citrix SSL-Relay, das sichere Proxy-Protokoll
- NTLM-Authentifizierung (Windows NT Challenge/Response).

Gehen Sie wie folgt vor, um einen Proxy für den Start eines Desktops mit dem SOCKS-Protokoll zu konfigurieren:

1. Navigieren Sie zur Konfigurationsdatei `~/.ICAClient/All_Regions.ini`.
2. Aktualisieren Sie die folgenden Attribute:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

a) Aktualisieren Sie `ProxyType`. Sie können `SocksV5` als `ProxyType` verwenden.

b) Aktualisieren Sie `ProxyHost`. Sie können `ProxyHost` im folgenden Format hinzufügen:

`<IP>:<PORT>`. Beispiel: 10.122.122.122:1080

> **Hinweis:**
>
> - Um den Proxy zu verwenden, deaktivieren Sie EDT. Um EDT zu deaktivieren, setzen Sie das Attribut `HDXoverUDP` im Abschnitt `[Network\UDT]` der Konfigurationsdatei `~/.ICAClient/All_Regions.ini` auf *Off*.
> - Aktivieren Sie zur Gewährleistung einer sicheren Verbindung TLS.

HTTPS-Protokollunterstützung für Proxyserver

Bisher konnten Sie nur mithilfe des SOCKS-Protokolls eine Verbindung zu einem Proxyserver herstellen. Ab der Citrix Workspace-App 2308 können Sie auch über das HTTPS-Protokoll eine Verbindung zu einem Proxyserver herstellen.

Führen Sie folgende Schritte aus, um einen Desktop mit einem HTTPS-Protokoll zu öffnen:

1. Navigieren Sie zur Konfigurationsdatei ~/.ICAClient/All_Regions.ini.
2. Gehen Sie zum Abschnitt [Network\UDT].
3. Wählen Sie folgende Einstellungen:

```
HDXoverUDP=Off
<!--NeedCopy-->
```

4. Gehen Sie zum Abschnitt [Network\Proxy].
5. Aktualisieren Sie die folgenden Attribute:
   - Aktualisieren Sie den Wert für ProxyType. Sie können “Secure” als ProxyType verwenden.
   - Aktualisieren Sie den Wert für ProxyHost. Sie können den ProxyHost im folgenden Format hinzufügen:

`<IP>:<PORT>`. Beispiel: “192.168.101.37:6153”.

Sicherer Proxyserver

Durch das Konfigurieren des Secure Proxy-Protokolls wird gleichzeitig auch Unterstützung für Windows NT Challenge/Response (NTLM)-Authentifizierung aktiviert. Wenn dieses Protokoll zur Verfügung steht, wird es beim Start erkannt und ohne zusätzliche Konfiguration ausgeführt.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Wichtig:**
>
> NTLM-Unterstützung erfordert die Bibliotheken OpenSSL 1.1.1d und libcrypto.so. Installieren Sie die Bibliotheken auf dem Benutzergerät. Diese Bibliotheken sind oft in Linux-Distributionen enthalten. Sie können sie auch von http://www.openssl.org/ herunterladen.

Secure Web Gateway und SSL

Sie können die Citrix Workspace-App in eine Umgebung mit Citrix Secure Web Gateway oder dem SSL (Secure Sockets Layer)-Relay integrieren. Die Citrix Workspace-App unterstützt das TLS-Protokoll. TLS (Transport Layer Security) ist die neueste normierte Version des SSL-Protokolls. Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von SSL 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 (Federal Information Processing Standard). FIPS 140 ist ein Standard für die Kryptografie.

Secure Web Gateway

Sie können Citrix Secure Web Gateway im Normal- oder Relaymodus verwenden, um einen sicheren Kommunikationskanal zwischen der Citrix Workspace-App und dem Server bereitzustellen. Wenn Sie Secure Web Gateway im Modus **Normal** verwenden, muss die Citrix Workspace-App nicht konfiguriert werden.

Wenn Citrix Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Citrix Secure Web Gateway Proxy im Relaymodus verwenden. Wenn Sie den Relaymodus verwenden, fungiert der Citrix Secure Web Gateway-Server als Proxy und Sie müssen die Citrix Workspace-App konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Citrix Secure Web Gateway-Servers.
- Portnummer des Citrix Secure Web Gateway-Servers.

> **Hinweis:**
>
> Citrix Secure Web Gateway Version 2.0 unterstützt den Relaymodus nicht.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Beispiel: my_computer.my_company.com ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (my_computer), einen Second-Level-Domänennamen (my_company) und einen Top-Level-Domänennamen (com) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (my_company.com) wird als Domänenname bezeichnet.

SSL-Relay

Das Citrix SSL-Relay verwendet standardmäßig den TCP-Port 443 auf dem Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Server für TLS-gesicherte Kommunikation. Wenn das SSL-Relay eine TLS-Verbindung empfängt, werden die Daten entschlüsselt und dann an den Server übergeben.

Wenn Sie SSL-Relay so konfigurieren, dass ein anderer Port als 443 abgehört wird, müssen Sie die Citrix Workspace-App für diese geänderte Portnummer konfigurieren.

Mit dem Citrix SSL-Relay kann folgende Kommunikation gesichert werden:

- Zwischen einem TLS-fähigen Benutzergerät und einem Server

Weitere Informationen zum Konfigurieren und Sichern der Installation mit SSL-Relay finden Sie in der Citrix Virtual Apps-Dokumentation.

TLS

Bislang war die unterstützte TLS-Mindestversion 1.0 und die unterstützte TLS-Höchstversion 1.2. Ab Version 2203 ist die höchste unterstützte TLS-Version 1.3.

Die Versionen des TLS-Protokolls, die ausgehandelt werden können, können Sie steuern, indem Sie die folgenden Konfigurationsoptionen im Abschnitt [WFClient] hinzufügen:

- MinimumTLS=1.1
- MaximumTLS=1.3

Dies sind die Standardwerte, die als Code implementiert werden. Passen Sie sie nach Bedarf an.

> **Hinweise:**
>
> - Diese Werte werden bei jedem Programmstart gelesen. Wenn Sie sie nach dem Start von self-service oder storebrowse ändern, geben Sie Folgendes ein: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
> - Die Verwendung des SSLv3-Protokolls ist in der Citrix Workspace-App für Linux nicht zulässig.
> - TLS 1.0/1.1 funktioniert nur mit dem älteren VDI oder Citrix Gateway, die sie unterstützen.

Zum Auswählen der Verschlüsselungssammlung fügen Sie die folgende Konfigurationsoption im Abschnitt [WFClient] hinzu:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- SSLCiphers=GOV

Dieser Wert ist der Standardwert. Die Werte COM und ALL werden ebenfalls erkannt.

> **Hinweis:**
>
> Wenn Sie diese Konfiguration nach dem Start von self-service oder storebrowse ändern, müssen Sie wie bei der Konfiguration der TLS-Version Folgendes eingeben:
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

CryptoKit-Update

CryptoKit-Version 14.2 ist in OpenSSL 1.1.1d integriert.

Kryptographische Aktualisierung

Mit diesem Feature ändert sich das Protokoll zur sicheren Kommunikation grundlegend. Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten kein Forward Secrecy und werden als unsicher eingestuft.

Die TLS_RSA_-Verschlüsselungssammlungen wurden vollständig entfernt. Stattdessen werden die erweiterten TLS_ECDHE_RSA_-Verschlüsselungssammlungen unterstützt.

Wenn Ihre Umgebung nicht mit den TLS_ECDHE_RSA_-Verschlüsselungssammlungen konfiguriert ist, werden die Starts von Clients aufgrund schwacher Verschlüsselung nicht unterstützt. Für die Clientauthentifizierung werden 1536-Bit-RSA-Schlüssel unterstützt.

Die folgenden erweiterten Verschlüsselungssammlungen werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

DTLS v1.0 unterstützt die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS v1.2 unterstützt die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

TLS v1.3 unterstützt die folgenden Verschlüsselungssammlungen:

- TLS_AES_128_GCM_SHA256 (0x1301)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- TLS_AES_256_GCM_SHA384 (0x1302)

> **Hinweis:**
>
> Ab Version 1903 und höher wird DTLS von Citrix Gateway 12.1 und höher unterstützt. Informationen zu mit DTLS unterstützten Verschlüsselungssammlungen für Citrix Gateway finden Sie unter Unterstützung des DTLS-Protokolls.

Verschlüsselungssammlungen

Um verschiedene Verschlüsselungssammlungen zu aktivieren, ändern Sie den Wert für den Parameter `SSLCiphers` in `ALL`, `COM` oder `GOV`. Standardmäßig ist die Option in der Datei `All_Regions.ini` im Verzeichnis `$ICAROOT/config` auf `ALL` festgelegt.

Die folgenden Sätze von Verschlüsselungssammlungen werden von ALL, GOV und COM bereitgestellt:

- ALL
  - Alle 3 Verschlüsselungssammlungen werden unterstützt.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Informationen zur Problembehandlung finden Sie unter Verschlüsselungssammlungen.

Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten Forward Secrecy nicht. Diese Verschlüsselungssammlungen gelten heute branchenweit als veraltet. Um jedoch die Abwärtskompatibilität mit älteren Versionen von Citrix Virtual Apps and Desktops bzw. Citrix DaaS zu unterstützen, kann die Citrix Workspace-App diese Verschlüsselungssammlungen optional aktivieren.

Setzen Sie das Flag `Enable\\_TLS\\_RSA\\_` auf **False**, um die Sicherheit weiter zu erhöhen.

Im Folgenden finden Sie eine Liste der veralteten Verschlüsselungssammlungen:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Die beiden letzten Verschlüsselungssammlungen verwenden den RC4-Algorithmus und sind veraltet, weil sie unsicher sind. Sie könnten auch die Verschlüsselungssammlung TLS_RSA_3DES_CBC_EDE_SHA als veraltet betrachten. Mit Flags können Sie alle Kategorisierungen durchsetzen.

Weitere Informationen zum Konfigurieren von DTLS v1.2 finden Sie unter Adaptiver Transport in der Dokumentation zu Citrix Virtual Apps and Desktops.

Voraussetzung:

Wenn Sie Version 1901 oder früher verwenden, führen Sie die folgenden Schritte aus:

Wenn `.ICAClient` bereits im Basisverzeichnis des aktuellen Benutzers vorhanden ist:

- Löschen Sie die Datei `All\\_Regions.ini`

Oder

- Fügen Sie folgende Zeilen am Ende des Abschnitts [Network\SSL] hinzu, um die Datei `AllRegions.ini` beizubehalten:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

Wenn der Ordner `.ICAClient` nicht im Basisordner des aktuellen Benutzers vorhanden ist, weist dies auf eine Neuinstallation der Citrix Workspace-App hin. In diesem Fall wird die Standardeinstellung für die Features beibehalten.

Die folgende Tabelle enthält die Verschlüsselungssammlungen jeder Gruppe:
Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen

> **Hinweis:**
>
> Alle bisherigen Verschlüsselungssammlungen sind FIPS- und SP800-52-konform. Die ersten beiden Sammlungen sind nur für (D)TLS1.2-Verbindungen zulässig. Umfassende Informationen zur Unterstützung von Verschlüsselungssammlungen finden Sie in **Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen**.

Zertifikate

Wenn Sie einen Store mit SAML-Authentifizierung (mit AuthV3-Protokoll) verwenden, wird die folgende Fehlermeldung angezeigt: “Unacceptable TLS Certificate.”

Dieses Problem tritt auf, wenn Sie die Citrix Workspace-App 1906 und höher verwenden. Informationen zur Fehlerbehebung finden Sie in den folgenden Knowledge Center-Artikeln:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- CTX260336
- CTX231524
- CTX203362

Wenn der StoreFront-Server keine Zwischenzertifikate bereitstellen kann, die dem verwendeten Zertifikat entsprechen, oder wenn Sie Zwischenzertifikate für die Unterstützung von Smartcard-Benutzern installieren, führen Sie diese Schritte aus, bevor Sie einen StoreFront-Store hinzufügen:

1. Rufen Sie separat ein oder mehr Zwischenzertifikate im PEM-Format ab.

   > **Tipp:**
   >
   > Wenn Sie kein Zertifikat im PEM-Format finden, konvertieren Sie mit dem Hilfsprogramm `openssl` ein Zertifikat im CRT-Format in eine PEM-Datei.

2. Als Benutzer, der das Paket installiert (normalerweise root):

   a) Kopieren Sie eine oder mehrere Dateien zu $ICAROOT/keystore/intcerts.

   b) Führen Sie den folgenden Befehl als Benutzer, der das Paket installiert hat, aus:

   ```
   $ICAROOT/util/ctx_rehash
   ```

Wenn Sie ein Serverzertifikat einer Zertifizierungsstelle authentifizieren, dem von Benutzergeräten noch nicht vertraut wird, folgen Sie die nachfolgenden Anweisungen, bevor Sie einen StoreFront-Store hinzufügen.

1. Rufen Sie ein Stammzertifikat im PEM-Format ab.
   Tipp: Wenn Sie kein Zertifikat in diesem Format finden, konvertieren Sie mit dem Hilfsprogramm `openssl` ein Zertifikat im CRT-Format in eine PEM-Datei.
2. Als Benutzer, der das Paket installiert hat (normalerweise root):
   a) Kopieren Sie die Datei in $ICAROOT/keystore/cacerts.
   b) Führen Sie den folgenden Befehl aus:
   `$ICAROOT/util/ctx_rehash`

Verbesserungen am HDX Enlightened Data Transport-Protokoll (EDT)

Wenn `HDXoverUDP` in älteren Releases auf `Preferred` festgelegt ist, erfolgt der Datentransport über EDT. Wenn dies nicht möglich ist, erfolgt er über TCP.

Ab Version 2103 der Citrix Workspace-App werden bei aktivierter Sitzungszuverlässigkeit EDT und TCP bei folgenden Schritten parallel versucht:

- Erste Verbindung
- Sitzungszuverlässigkeitswiederverbindung
- Automatische Wiederverbindung von Clients

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Diese Verbesserung verkürzt die Verbindungszeit, wenn EDT bevorzugt wird. Ist der erforderliche zugrunde liegende UDP-Transport jedoch nicht verfügbar, muss TCP verwendet werden.

Nach dem Fallback auf TCP sucht der adaptive Transport standardmäßig alle fünf Minuten nach EDT.

MTU-Discovery durch EDT (Enlightened Data Transport)

Die Citrix Workspace-App Version 2109 unterstützt nun MTU-Discovery (Maximum Transmission Unit = maximale Übertragungseinheit) für Enlightened Data Transport (EDT). Das Feature erhöht die Zuverlässigkeit und Kompatibilität des EDT-Protokolls und bietet eine verbesserte Benutzererfahrung.

Weitere Informationen finden Sie im Abschnitt MTU-Discovery durch EDT in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung für EDT IPv6

Ab Version 2203 der Citrix Workspace-App wird EDT IPv6 unterstützt.

> **Hinweis:**
>
> IPv6 wird sowohl mit TCP als auch EDT unterstützt. IPv6 wird jedoch mit TCP über TLS und mit EDT über DTLS nicht unterstützt.

Storebrowse

September 12, 2023

Storebrowse ist ein einfaches Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Mit Storebrowse können Administratoren folgende Routinevorgänge automatisieren:

- Hinzufügen von Stores
- Auflisten der veröffentlichten Apps und Desktops eines konfigurierten Stores
- Abonnieren der Apps und Desktops eines konfigurierten Stores und Stornieren der Abos
- Aktivieren und Deaktivieren von Verknüpfungen für veröffentlichte Apps und Desktops
- Starten von veröffentlichten Anwendungen
- Wiederherstellen der Verbindung zu getrennten Sitzungen

Im Allgemeinen ist das Storebrowse-Hilfsprogramm im Ordner `/util` verfügbar. Dieser ist im Installationsverzeichnis. Beispiel: `/opt/Citrix/ICAClient/util`.

Voraussetzungen

Für das Storebrowse-Hilfsprogramm ist das Bibliothekspaket **libxml2** erforderlich.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Starten von veröffentlichten Desktops und Anwendungen

Es gibt zwei Möglichkeiten, eine Ressource zu starten:

- Sie können die Befehlszeilen- und Storebrowse-Befehle verwenden
- Sie können die Benutzeroberfläche verwenden, um eine Ressource zu starten.

Dieser Artikel beschreibt die Storebrowse-Befehle.

Storebrowse-Verbesserung für Servicekontinuität

Bisher wurden die Workspace-Verbindungsleasedateien mit den auf dem Remoteserver verfügbaren Dateien nur synchronisiert, wenn eine Verbindung mit dem Self-Service-Plug-In hergestellt wurde. Das Feature für die Servicekontinuität wurde daher beim Start von Apps oder Desktopsitzungen mit Storebrowse nicht unterstützt. Die meisten Thin Clients von Drittanbietern stellen über Storebrowse eine Verbindung zur Workspace-Plattform her, und das Feature für die Servicekontinuität war für sie nicht aktiviert.

Ab Version 2109 von Citrix Workspace-App werden die Workspace-Verbindungsleasedateien mit auf dem Remoteserver verfügbaren Dateien auch dann synchronisiert, wenn Sie eine Verbindung über Storebrowse herstellen. Mit diesem Feature können Thin Clients von Drittanbietern selbst dann auf Workspace zugreifen, wenn sie offline sind.

> **Hinweis:**
>
> - Diese Verbesserung ist nur verfügbar, wenn Servicekontinuität in Cloud-Bereitstellungen aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren von Servicekontinuität in der Dokumentation zu Citrix Workspace.

Verwendung von Befehlen

Im folgenden Abschnitt werden die Storebrowse-Befehle beschrieben, die Sie im Storebrowse-Hilfsprogramm verwenden können.

Store hinzufügen

`-a, --addstore`

Beschreibung:

Fügt einen Store mit Gateway- und Beacondetails zusammen mit dem ServiceRecord-Daemonprozess hinzu. Dieser Befehl gibt die vollständige URL des Stores zurück. Wenn das Hinzufügen eines Stores fehlschlägt, wird ein Fehler angezeigt.

Befehlsbeispiel für StoreFront:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Befehl:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Beispiel:

```
./storebrowse -a https://my.firstexamplestore.net
```

> **Hinweis:**
>
> Sie können mit dem Storebrowse-Hilfsprogramm mehrere Stores hinzufügen.

Hilfe

```
-?, -h, --help
```

Beschreibung:

Bietet Details zur Verwendung des Storebrowse-Hilfsprogramms.

Store auflisten

```
-l --liststore
```

Beschreibung:

Listet die Stores auf, die Sie hinzugefügt haben.

Befehlsbeispiel in StoreFront:

```
./storebrowse -l
```

Enumeration

```
-E --enumerate
```

Beschreibung:

Listet die verfügbaren Ressourcen auf. Standardmäßig werden die folgenden Werte angezeigt:

- Ressourcenname
- Anzeigename
- Ordner der Ressource

Wenn Sie weitere Informationen anzeigen möchten, fügen Sie den Befehl `-M --details` an den Befehl `-E` an.

> **Hinweis:**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Wenn Sie den Befehl **-E** ausführen, wird ein Authentifizierungsfenster angezeigt, wenn Sie Ihre Anmeldeinformationen nicht zuvor angegeben haben.

Geben Sie die gesamte Store-URL ein, die Sie mit dem Befehl **-liststore** erhalten.

Befehlsbeispiel für StoreFront:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Abonniert

`-S --subscribed`

Beschreibung:

Listet die abonnierten Ressourcen auf. Standardmäßig werden die folgenden Werte angezeigt:

- Ressourcenname
- Anzeigename
- Ordner der Ressource

Wenn Sie weitere Informationen anzeigen möchten, fügen Sie den Befehl `-M --details` an den Befehl `-E` an.

Befehlsbeispiel für StoreFront:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Details

`-M --details`

Beschreibung:

Dieser Befehl gibt mehrere Attribute der veröffentlichten Anwendungen zurück. Im Allgemeinen wird dieser Befehl mit den Befehlen **-E** und **-S** verwendet. Dieser Befehl umfasst ein Argument, das die Summe der Zahlen ist, die den erforderlichen Details entsprechen:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

> **Hinweise:**
>
> - Zum Erstellen von Menüeinträgen für abonnierte Anwendungen verwenden Sie das Argument CreateShortcuts(0x100000) mit den Befehlen **-S**, **-s** und **-u**.
> - Um alle Menüeinträge zu löschen, verwenden Sie RemoveShortcuts(0x200000) mit dem Befehl **-S**.

Befehlsbeispiel für StoreFront:

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

Im vorherigen Befehlsbeispiel ist 0x264 die Kombination aus DisplayName (0x200), AppIsDisabled (0x40), AppIsDesktop (0x20) und SoundType (0x4). Es wird eine Liste der abonnierten Ressourcen zusammen mit den Details ausgegeben.

Sie können den Befehl **-M** verwenden, um die Ressourcen mit den erforderlichen Details aufzulisten:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Hinweise:**
>
> - Sie können die Werte entweder im Dezimalformat oder im Hexadezimalformat darstellen. Beispiel: 512 für 0x200.
> - Wenn einige Details über storebrowse nicht verfügbar sind, ist der Ausgabewert Null.

Abonnieren

```
-s --subscribe
```

Beschreibung:

Abonniert die angegebene Ressource aus dem jeweiligen Store.

Befehlsbeispiel für StoreFront:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

Abonnement kündigen

```
-u --unsubscribe
```

Beschreibung:

Kündigt das Abonnement der angegebenen Ressource aus dem jeweiligen Store.

Befehlsbeispiel für StoreFront:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

Start

```
-L --launch
```

Beschreibung:

Startet eine Verbindung zu einer veröffentlichten Ressource. Das Hilfsprogramm wird dann automatisch geschlossen, während die erfolgreich verbundene Sitzung bestehen bleibt.

Befehlsbeispiel für StoreFront:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/
Store/discovery
```

Symbole

```
-i --icons
```

Beschreibung:

Mit diesem Befehl werden Desktop- und Anwendungssymbole im PNG-Format abgerufen. Dieser Befehl wird mit dem Befehl **-E** oder **-S** verwendet.

Verwenden Sie zum Abrufen von Symbolen mit bestimmten Größen und Tiefen das Argument “best” oder das Größenargument.

Argument “best”

Mit dem Argument “best” können Sie die auf dem Server verfügbaren Symbole mit der besten Größe abrufen. Sie können die Symbole später in die erforderlichen Größen konvertieren. Das Argument “best” ist nach Speicher- und Bandbreitengesichtspunkten die effizienteste Methode und vereinfacht die Skripterstellung. Die Dateien werden im Format <Ressourcenname>.png gespeichert.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Größenargument

Verwenden Sie zum Abrufen von Symbolen mit bestimmten Größen und Tiefen das Größenargument. Wenn der Server Symbole einer bestimmten Größe oder Tiefe nicht abrufen kann, wird ein Fehler angezeigt.

Das Größenargument wird als WxB angegeben, wobei Folgendes gilt:

- **W** ist die Breite (width) der Symbole. Alle Symbole sind quadratisch, daher wird nur ein Wert benötigt, um die Größe anzugeben.
- **B** ist die Farbtiefe. Sie wird als Anzahl der Bits pro Pixel angegeben.

> **Hinweis:**
>
> Der Wert **W** ist obligatorisch. Der Wert **B** ist optional.

Wenn Sie die Werte nicht angeben, werden Symbole aller verfügbaren Bildtiefen angezeigt. Die Dateien werden im Format <Ressourcenname>_WxWxB.png gespeichert.

Bei beiden Methoden werden die Symbole für jede Ressource, die mit dem Befehl **-E** oder **-S** zurückgegeben werden, im **PNG-Format** gespeichert.

Symbole werden im Ordner **.icaClient/cache/icons** gespeichert.

Befehlsbeispiel für StoreFront:

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

Sitzung wieder verbinden

`-W [r|R] --reconnect [r|R]`

Beschreibung:

Verbindet die getrennten aktiven Sitzungen des angegebenen Stores erneut. Mit der Option [r] werden alle getrennten Sitzungen wieder verbunden. Mit der Option [R] werden alle aktiven und alle getrennten Sitzungen wieder verbunden.

Befehlsbeispiel für StoreFront:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Sitzung trennen

```
-WD --disconnect
```

Beschreibung:

Trennt alle Sitzungen des angegebenen Stores.

Befehlsbeispiel für StoreFront:

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

Sitzung beenden

```
-WT --terminate
```

Beschreibung:

Beendet alle Sitzungen des angegebenen Stores.

Befehlsbeispiel für StoreFront:

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

Version

```
-v --version
```

Beschreibung:

Zeigt die Version des Storebrowse-Hilfsprogramms an.

Befehlsbeispiel für StoreFront:

```
./storebrowse -v
```

Stammverzeichnis

```
-r --icaroot
```

Beschreibung:

Gibt das Stammverzeichnis an, in dem die Citrix Workspace-App für Linux installiert ist. Wenn Sie nichts angegeben, wird das Stammverzeichnis zur Laufzeit ermittelt.

Befehlsbeispiel für StoreFront:

```
./storebrowse -r /opt/Citrix/ICAClient
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Benutzername, Kennwort, Domäne

```
-U --username, -P --password, -D --domain
```

Beschreibung:

Übergibt den Benutzernamen, das Kennwort und die Domänendetails an den Server. Diese Methode funktioniert nur mit einem PNA-Store. StoreFront-Stores ignorieren diesen Befehl. Die Details werden nicht zwischengespeichert. Geben Sie die Details bei jedem Befehl ein.

Befehlsbeispiel für StoreFront:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
 user1 -P password -D domain-name
```

Store löschen

```
-d --deletestore
```

Beschreibung:

Hebt die Registrierung eines Stores beim ServiceRecord-Daemon auf.

Befehlsbeispiel für StoreFront:

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Self-Service konfigurieren

```
-c --configselfservice
```

Beschreibung:

Dient zum Aufrufen und Konfigurieren der in StoreCache.ctx gespeicherten Einstellungen der Self-Service-Benutzeroberfläche. Das zugehörige Argument hat das Format <Eintrag[=Wert]>. Wenn nur ein Eintrag vorhanden ist, wird der aktuelle Wert der Einstellung aufgerufen. Wenn jedoch ein Wert vorhanden ist, wird der Wert verwendet, um die Einstellung zu konfigurieren.

Befehlsbeispiel für StoreFront:

```
./storebrowse -c SharedUserMode=True
```

CR-Datei hinzufügen

```
-C --addcr
```

Beschreibung:

Liest die bereitgestellte Citrix Receiver-Datei (CR) und fordert Sie zum Hinzufügen jedes Stores auf. Die Ausgabe ist wie beim Befehl **-a**, enthält aber mehrere Stores auf jeweils neuen Zeilen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Befehlsbeispiel für StoreFront:

```
./storebrowse -C <path to CR file>
```

Synchronisieren von Verbindungsleasedateien

```
-o --synclease
```

Beschreibung:

Startet die Synchronisierung der Workspace-Verbindungsleasedateien mit den Dateien, die auf dem Remoteserver für den angegebenen Store verfügbar sind. Mit diesem Befehl aktualisieren Sie den Standardspeicher und lösen die Leasedateisynchronisierung aus. Wenn Servicekontinuität deaktiviert ist, wird ein Fehler angezeigt.

Befehl:

```
./storebrowse -o *URL of Store *
```

Befehlsbeispiel für StoreFront:

```
./storebrowse -o https://my.firstexamplestore.net
```

Storebrowse-Daemon schließen

```
-K --killdaemon
```

Beschreibung:

Beendet den Storebrowse-Daemon. Alle Anmeldeinformationen und Tokens werden gelöscht.

Befehlsbeispiel für StoreFront:

```
./storebrowse -K
```

Fehlercodes auflisten

```
-e --listerrorcodes
```

Beschreibung:

Listet die registrierten Fehlercodes auf.

Befehlsbeispiel für StoreFront:

```
./storebrowse -e
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Storegateway

`-g --storegateway`

Beschreibung:

Legt das Standardgateway für einen Store fest, der bereits beim ServiceRecord-Daemon registriert ist.

Befehlsbeispiel für StoreFront:

```
./storebrowse -g “<unique gateway name>” https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Hinweis:**
>
> Der eindeutige Gatewayname (unique gateway name) muss in der Liste der Gateways für den angegebenen Store enthalten sein.

Schnellstart

`-q, --quicklaunch`

Beschreibung:

Startet eine Anwendung über die direkte URL. Dieser Befehl funktioniert nur bei StoreFront-Stores.

Befehlsbeispiel für StoreFront:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Daemonisieren

`-n --nosingleshot`

Beschreibung:

Daemonisiert immer den Storebrowse-Prozess.

Befehlsbeispiel für StoreFront:

```
./storebrowse -n
```

Dateiparameter

`-F --fileparam`

Beschreibung:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Startet eine Datei mit dem Dateipfad und der angegebenen Ressource.

Befehlsbeispiel für StoreFront:

```
./storebrowse -F “<path to file>” -L <Resource Name> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Workflow

Dieser Artikel beschreibt einen einfachen Workflow zum Starten einer App mit den Storebrowse-Befehlen:

1. `./storebrowse -a https://my.firstexamplestore.net`

   Fügt einen Store hinzu und stellt die vollständige URL des Stores bereit. Notieren Sie sich die vollständige URL, da sie in den folgenden Befehlen verwendet wird.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

   Listet alle veröffentlichten Apps und Desktops auf. Geben Sie Ihre Anmeldeinformationen mit dem Popupfenster ein, das für den registrierten Store angezeigt wird.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

   Startet die Ressource. Verwenden Sie “Resource_Name” aus der Ausgabe des vorherigen Befehls.

4. `./storebrowse -K`

   Dieser Befehl löscht die zuvor eingegebenen Anmeldeinformationen und beendet den Storebrowse-Daemon. Wenn Sie diesen Befehl nicht explizit eingeben, wird der Storebrowse-Prozess nach einer Stunde beendet.

Problembehandlung

September 12, 2023

Dieser Artikel enthält Informationen für Administratoren, die bei der Problembehandlung in der Citrix Workspace-App hilfreich sein können.

Verbindung

Die folgenden Verbindungsprobleme kommen vor.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

ICA-Start auf Fedora 29/30

Ein ICA-Start kann auf Fedora 29/30 fehlschlagen. Führen Sie als Workaround die folgenden Schritte aus:

1. Installieren Sie `compat-openssl10` mit dem Befehl.

   ```
   sudo yum install compat-openssl10.x86_64
   ```

2. Legen Sie fest, dass die Umgebungsvariable in `~/.bashrc` in jeder Sitzung geladen werden soll. Diese Aktion verweist auf die ältere `libcrypto`-Bibliothek.

   ```
   export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o
   ```

> **Hinweis:**
>
> Die Citrix Workspace-App funktioniert gut im X.Org-Server im Vergleich zum Wayland Compositor. Für Distributionen, die Wayland als Standardgrafikprotokoll verwenden, heben Sie die Auskommentierung für einen der folgenden Einträge auf:
>
> `WaylandEnable=false` in `/etc/gdm/custom.conf` oder in `/etc/gdm3/custom.conf`
>
> Melden Sie sich ab und dann an, um auf den X.Org-Server zu verweisen.

Veröffentlichte Ressourcen- oder Desktopsitzung

Wenn beim Herstellen einer Verbindung mit einem Windows-Server ein Dialogfeld mit der Meldung "Verbindung zu Server … wird hergestellt…" aber danach kein Verbindungsfenster angezeigt wird, müssen Sie den Server möglicherweise mit einer Clientzugriffslizenz (CAL) konfigurieren. Weitere Informationen zur Lizenzierung finden Sie unter Lizenzierung.

Sitzungswiederverbindung

Die Verbindung kann fehlschlagen beim Wiederverbinden mit Sitzungen, die eine höhere Farbtiefe als der von der Citrix Workspace-App angeforderten verwenden. Dieser Fehler tritt auf, wenn der verfügbare Speicher auf dem Server knapp wird.

Wenn die Wiederverbindung fehlschlägt, versucht die Citrix Workspace-App, die ursprüngliche Farbtiefe zu verwenden. Andernfalls versucht der Server, eine neue Sitzung mit der angeforderten Farbtiefe zu starten. Die ursprüngliche Sitzung bleibt in diesem Fall getrennt. Die zweite Sitzung kann auch fehlschlagen, wenn immer noch nicht genügend Speicher auf dem Server verfügbar ist.

Vollständiger Internetname

Citrix empfiehlt, DNS (Domain Name Server) auf Ihrem Netzwerk zu konfigurieren. Damit können die Namen von Servern aufgelöst werden, zu denen Sie eine Verbindung herstellen möchten. Wenn

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Sie DNS nicht konfiguriert haben, kann der Servername eventuell nicht in eine IP-Adresse aufgelöst werden. Alternativ können Sie den Server mit der IP-Adresse statt dem Namen angeben. Für TLS-Verbindungen ist ein vollqualifizierter Domänenname und keine IP-Adresse erforderlich.

Langsame Sitzungen

Wenn eine Sitzung nicht startet, bevor Sie die Maus bewegen, liegt möglicherweise ein Problem mit der Zufallszahlengenerierung im Linux-Kernel vor. Als Workaround führen Sie einen Entropie generierenden Daemon wie `rngd` (hardwarebasiert) oder `haveged` (von Magic Software) aus.

Verschlüsselungssammlungen

Wenn Ihre Verbindung mit der neuen kryptografischen Unterstützung fehlschlägt:

1. Es gibt verschiedene Tools, um zu überprüfen, welche Verschlüsselungssammlungen Ihr Server unterstützt, einschließlich der Folgenden:
   - `Ssllabs.com` (der Server muss Internetzugang haben)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. Suchen Sie in Linux Client WireShark nach dem Paket (Client Hello, Server Hello) mit dem Filter (ip.addr == `VDAIPAddress`), um den SSL-Abschnitt zu finden. Das Ergebnis enthält die Verschlüsselungssammlungen, die vom Client gesendet und vom Server akzeptiert werden.

Falsches Citrix Optimization SDK

Das Citrix Optimization SDK-Paket enthält eine falsche Version von `UIDialogLibWebKit.so`. Führen Sie als Workaround folgende Schritte aus:

1. Laden Sie das Citrix Optimization SDK-Paket Version 18.10 von der Downloadseite herunter.
   a) Gehen Sie zum Pfad CitrixPluginSDK/UIDialogLib/GTK:

   ```
   cd CitrixPluginSDK/UIDialogLib/GTK
   ```

   b) Löschen Sie alle Objektdateien:

   ```
   rm -rf *.o
   ```

   c) Gehen Sie zum WebKit-Ordner:

   ```
   cd ../WebKit
   ```

   d) Entfernen Sie die vorhandene Datei UIDialogLibWebKit.so:

   ```
   rm -rf UIDialogLibWebKit.so
   ```

   e) Verwenden Sie den folgenden Befehl im WebKit-Verzeichnis:

   ```
   make all
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die neue UIDialogLibWebKit.so wird generiert.

f) Kopieren Sie die neue Bibliothek in das Verzeichnis **$ICAROOT/lib**.

Schwache Verschlüsselungssammlungen für SSL-Verbindungen

Für das Herstellen einer TLS-Verbindung bietet die Citrix Workspace-App eine eingeschränkte Standardliste moderner Verschlüsselungssammlungen.

Wenn Sie eine Verbindung zu einem Server herstellen, der eine ältere Verschlüsselungssammlung erfordert, legen Sie im Abschnitt [WFClient\] einer Konfigurationsdatei die Konfigurationsoption `SSLCiphers=ALL` fest.

Die folgenden erweiterten Verschlüsselungssammlungen werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

Verbindungsverlust

Bei der Verwendung des EDT-Protokolls wird u. U. folgende Fehlermeldung angezeigt: Verbindung mit "…" wurde unterbrochen Das Problem könnte auftreten, wenn die Verbindung über einen Router erfolgt, wobei die maximale Übertragungseinheit für EDT kleiner ist als die Standardeinstellung von 1500 Bytes. Führen Sie folgende Schritte aus:

- Legen Sie `edtMSS=1000` in einer Konfigurationsdatei fest.

Verbindungsfehler

Verbindungsfehler können eine Vielzahl unterschiedlicher Fehlermeldungen erzeugen. Beispiele:

- Fehler bei Verbindung: Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten.
- Es konnte kein Kontakt mit dem Authentifizierungsdienst hergestellt werden.
- Ihr Konto kann nicht mit dieser Serveradresse hinzugefügt werden

Verschiedene Probleme können solche Fehler verursachen, einschließlich der Folgenden:

- Der lokale Computer und der Remotecomputer können kein gemeinsames TLS-Protokoll aushandeln. Weitere Informationen finden Sie unter TLS.
- Der Remotecomputer erfordert eine ältere Verschlüsselungssammlung für eine TLS-Verbindung. In diesem Fall legen Sie im Abschnitt `\[WFClient\]` einer Konfigurationsdatei die Konfigurationsoption `SSLCiphers=ALL` fest. Führen Sie `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` aus, bevor Sie die Verbindung neu starten.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Der Remotecomputer fordert falscherweise ein Clientzertifikat an. IIS darf Zertifikate nur für "Citrix", "Authentication" und "Certificate" **akzeptieren** oder **anfordern**.
- Andere Probleme:

Verbindungen mit geringer Bandbreite

Citrix empfiehlt, dass Sie die neueste Version von Citrix Virtual Apps and Desktops bzw. Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) auf dem Server verwenden. Verwenden Sie außerdem die aktuelle Citrix Workspace-App-Version auf dem Benutzergerät.

Wenn Sie eine Verbindung mit geringer Bandbreite verwenden, können Sie durch Anpassen der Konfiguration und Verwendungsart der Citrix Workspace-App eine Verbesserung der Leistung erzielen.

- **Konfigurieren Sie die Citrix Workspace-App-Verbindung**: Konfigurieren der Citrix Workspace-App-Verbindungen kann die Bandbreite reduzieren, die für ICA erforderlich ist, und verbessert die Leistung
- **Ändern Sie die Verwendung der Citrix Workspace-App**: Durch Ändern der Verwendung der Citrix Workspace-App können Sie die Bandbreite verringern, die für eine schnelle Verbindung benötigt wird.
- **Aktivieren Sie UDP-Audio**: Dieses Feature kann für eine gleichmäßige Latenz bei VoIP-Verbindungen (Voice over IP) in stark ausgelasteten Netzwerken sorgen.
- **Verwenden Sie die neuesten Versionen der Citrix Workspace-App für Linux und von Citrix Virtual Apps and Desktops bzw. Citrix DaaS**: Citrix erweitert und verbessert die Leistung mit jedem Release und für viele Leistungsfeatures ist die neueste Receiver- und Serversoftware erforderlich

Anzeige

Tearing

Tearing wird verursacht, wenn Teile von zwei (oder mehreren) unterschiedlichen Frames gleichzeitig auf dem Bildschirm in horizontalen Blöcken angezeigt werden. Dieses Problem ist besonders bei großen Bereichen von sich schnell änderndem Inhalt auf dem Bildschirm erkennbar.

Tearing wird vermieden, wenn Daten auf dem VDA erfasst werden. Tearing tritt nicht auf, wenn Daten an den Client weitergegeben werden. X11 (das Linux/Unix-Grafiksubsystem) bietet jedoch keine konsistente Möglichkeit der Erstellung von Frames, die Tearing verhindert.

Zum Verhindern von Tearing empfiehlt Citrix die Standardmethode, bei der der Anwendungsaufbau mit dem Aufbau des Bilds synchronisiert wird. Dies bedeutet, dass `vsvnc` den Aufbau des nächsten Frames startet. Abhängig von der auf dem Client verwendeten Grafikhardware und Ihrem verwendeten Fenstermanager stehen die folgenden zwei Lösungsansätze zur Verfügung, um ein Tearing zu verhindern:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- X11 GPU-Einstellungen
- Verwenden eines Kompositionsmanagers

X11 GPU-Konfiguration

Erstellen Sie für Intel HD-Grafiken in xorg.conf.d eine **20-intel.conf** genannte Datei mit folgenden Inhalten:

```
Section "Device"

 Identifier    "Intel Graphics"
 Driver        "intel"
 Option        "AccelMethod" "sna"
 Option        "TearFree" "true"

 EndSection
```

Navigieren Sie für NVIDIA-Grafiken zur Datei im Ordner xorg.conf.d, die die Option “MetaModes” für Ihre Konfiguration enthält. Fügen Sie für jeden durch Komma getrennten MetaMode Folgendes hinzu:

{ForceFullCompositionPipeline = On}

Beispiel:

Option “MetaModes” “DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}”

> **Hinweis:**
>
> Unterschiedliche Linux-Bereitstellungen verwenden unterschiedliche Pfade zu xorg.conf.d, z. B. /etc/X11/xorg.conf.d oder /user/share/X11/xorg.conf.d.

Kompositionsmanager

Verwenden Sie Folgendes:

- Compiz (integriert in Ubuntu Unity). Installieren Sie den “CompizConfig Settings Manager”.

  Führen Sie “CompizConfig Settings Manager” aus.

  Unter **General** > **Composition** deaktivieren Sie **Undirect Fullscreen Windows**.

> **Hinweis:**
>
> Seien Sie vorsichtig bei der Verwendung von “CompizConfig Settings Manager”, da das System u. U. nicht starten kann, wenn Sie Werte fehlerhaft ändern.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Compton (ein Add-On-Hilfsprogramm). Ausführliche Informationen finden Sie auf der Hauptseite bzw. in der Dokumentation von Compton. Führen Sie beispielsweise den folgenden Befehl aus:

  ```
  compton --vsync opengl --vsync -aggressive
  ```

Falsche Tastatureingaben

Wenn Sie keine englische Tastatur verwenden, stimmt die Bildschirmanzeige möglicherweise nicht mit der Tastatureingabe überein. In diesem Fall müssen Sie den verwendeten Tastaturtyp und das verwendete Tastaturlayout angeben. Weitere Informationen zur Angabe der Tastaturen finden Sie unter Steuern des Tastaturverhaltens.

Übermäßiges Aktualisieren der Darstellung

Einige Fenstermanager übertragen beim Verschieben von Seamlessfenstern ständig die neue Fensterposition, was zu einem wiederholten Neuaufbau der Darstellung führen kann. Sie können dieses Problem beheben, indem Sie den Fenstermanager zu einem Modus wechseln, bei dem beim Verschieben von Fenstern nur die Konturen gezeichnet werden.

Kompatibilität von Symbolen

Die Citrix Workspace-App erstellt Fenstersymbole, die mit den meisten Fenstermanagern verwendet werden können. Diese Symbole sind jedoch nicht vollständig mit den X Window-Kommunikationsrichtlinien für Clients (ICCCM, X Inter-Client Communication Convention Manual) kompatibel.

Volle Kompatibilität von Symbolen

Erreichen voller Kompatibilität von Symbolen:

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Bearbeiten Sie die folgende Zeile im Abschnitt [WFClient]: UseIconWindow=True
3. Speichern und schließen Sie die Datei.

Cursorfarbe

Der Cursor ist manchmal schlecht zu erkennen, wenn er dieselbe oder eine ähnliche Farbe wie der Hintergrund hat. Sie können dieses Problem lösen, indem Sie erzwingen, dass Bereiche des Cursors schwarz oder weiß sind.

Ändern der Farbe des Cursors

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Fügen Sie dem Abschnitt [WFClient] eine der folgenden Zeilen hinzu:

   CursorStipple=ffff,ffff (der Cursor wird schwarz angezeigt)

   CursorStipple=0,0 (der Cursor wird weiß angezeigt)
3. Speichern und schließen Sie die Datei.

Farbblitz

Wenn Sie den Mauszeiger über ein Verbindungsfenster verschieben, können in dem Fenster, das gerade nicht den Fokus hat, Farbwechsel auftreten. Dies ist eine bekannte Einschränkung bei der Verwendung von X Window System mit PseudoColor-Anzeigen. Falls möglich sollten Sie die Farbtiefe für die betroffene Verbindung erhöhen.

Farbwechsel bei TrueColor-Anzeige

Benutzer haben bei der Herstellung einer Verbindung zu einem Server die Option, 256 Farben zu verwenden. Voraussetzung für diese Option ist, dass die Videohardware Paletten unterstützt, damit Anwendungen zum Erzeugen animierter Anwendungen die Farbpalette wechseln können.

TrueColor-Anzeigen können die Funktion zum Erzeugen von Animationen durch schnelles Wechseln der Palette nicht emulieren. Software-Emulationen dieser Funktion gehen zu Lasten von Schnelligkeit und Datenverkehr im Netzwerk. Um diese Einschränkungen zu reduzieren, puffert die Citrix Workspace-App schnelle Palettenwechsel und aktualisiert die eigentliche Palette nur in Abständen von einigen Sekunden.

Falsche Anzeige

Die Citrix Workspace-App verwendet die EUC-JP- oder UTF-8-Zeichencodierung für japanische Zeichen, während der Server SJIS verwendet. Die Citrix Workspace-App kann diese Zeichensätze nicht übersetzen. Dies kann zu Problemen bei der Anzeige führen:

- wenn auf dem Server gespeicherte Dateien lokal angezeigt werden
- wenn lokal gespeicherte Dateien auf dem Server angezeigt werden

Dies Problem betrifft auch japanische Zeichen in Parametern, die bei der erweiterten Parameterübergabe verwendet werden.

Spannen der Sitzung

Sitzungen im Vollbildmodus gehen standardmäßig über alle Monitore. Es gibt außerdem für Befehlszeilen eine Steuerungsoption für die Anzeige auf mehreren Monitoren: -span. Hiermit können

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Vollbildschirmsitzungen über weitere Monitore gespannt werden.

Mit der Symbolleistenfunktionalität von Desktop Viewer können Sie in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore.

> **Wichtig:**
>
> Dies hat keinen Einfluss auf Sitzungen mit Seamless- oder normalen Fenstern (einschließlich Sitzungen mit maximierten Fenstern).

Die Option hat das folgende Format:
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]

Wenn `h` angegeben wird, wird eine Liste von Monitoren auf `stdout` ausgegeben. Wenn der gesamte Optionswert `h` ist, wird wfica beendet.

Wenn `o` angegeben wird, enthält das Sitzungsfenster das Attribut `override-redirect`.

> **Achtung:**
>
> - Die Verwendung dieser Option wird nicht empfohlen. Sie ist als letzte Option für problematische Fenstermanager vorgesehen.
> - Das Sitzungsfenster ist im Fenstermanager nicht sichtbar, hat kein Symbol und kann nicht neu angeordnet werden.
> - Es kann nur durch Beenden der Sitzung entfernt werden.

Wenn `a` angegeben wird, wird von der Citrix Workspace-App versucht, eine Sitzung zu erstellen, die alle Monitore abdeckt.

Dabei wird von der Citrix Workspace-App angenommen, dass der Rest des Werts der Option “-span” eine Liste der Monitornummern ist:

- Ein einzelner Wert gibt einen bestimmten Monitor an.
- Zwei Werte geben Monitore oben links und unten rechts in dem erforderlichen Bereich an.
- Vier Werte geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

Wenn `o` nicht angegeben wurde, fordert wfica mit der Meldung _NET_WM_FULLSCREEN_MONITORS ein entsprechendes Fensterlayout vom Fenstermanager an, wenn dies unterstützt wird. Sonst werden Größe- und Positionstipps verwendet, um das gewünschte Layout anzufordern.

Mit dem folgenden Befehl können Sie die Fenstermanager-Unterstützung testen:

```
xprop -root | grep \\_NET\\_WM\\_FULLSCREEN\\_MONITORS
```

Wenn es keine Ausgabe gibt, werden keine Fenstermanager unterstützt. Wenn keine Unterstützung vorhanden ist, benötigen Sie eventuell ein Fenster mit override-redirect. Sie können ein solches Fenster mit `-span o` einrichten.

Erstellen einer Sitzung über mehrere Monitore hinweg, an der Befehlszeile:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   /opt/Citrix/ICAClient/wfica -span h
   ```

   Es wird eine Liste mit Nummern der zurzeit an das Benutzergerät angeschlossenen Monitore auf stdout ausgegeben und wfica wird beendet.

2. Notieren Sie diese Monitornummern.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   /opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
   ```

   Die Werte w, x, y und z sind Monitornummern, die Sie in Schritt 1 oben erhalten haben. Der einzelne Wert w gibt einen bestimmten Monitor an. Zwei Werte w und x geben Monitore oben links und unten rechts in dem erforderlichen Bereich an. Vier Werte w, x, y und z geben Monitore an den oberen, unteren, linken und rechten Seiten des Bereichs an.

   > **Wichtig:**
   >
   > - Definieren Sie die Variable WFICA_OPTS, bevor Sie Self-Service über einen Browser starten. Bearbeiten Sie hierzu Ihre Profildatei, die üblicherweise unter $HOME/.bash_profile oder $HOME/.profile ist. Fügen Sie hier eine Zeile hinzu, um die Variable WFICA_OPTS zu definieren. Beispiel:
   >
   >   ```
   >   export WFICA_OPTS="-span a"
   >   ```
   >
   > - Diese Änderung betrifft sowohl virtuelle Apps als auch virtuelle Desktop-Sitzungen.
   > - Wenn Sie self-service oder storebrowse gestartet haben, entfernen Sie die gestarteten Prozesse, damit die neue Umgebungsvariable wirksam wird. Entfernen Sie die Prozesse mit folgendem Befehl:
   >
   > ```
   > killall AuthManagerDaemon ServiceRecord storebrowse
   > ```

Lokale Anwendungen

Der Vollbildmodus einer Sitzung kann möglicherweise nicht mit der Escape-Taste beendet werden, um lokale Anwendungen oder eine andere Sitzung zu verwenden. Dieses Problem tritt auf, da die clientseitige Systembenutzeroberfläche verborgen ist und das Feature “Tastaturtransparenz” den üblichen Tastaturbefehl, z. B. Alt+Tab, deaktiviert und den Befehl stattdessen an den Server sendet.

Deaktivieren Sie als Workaround das Feature “Tastaturtransparenz” vorübergehend mit Strg+F2, bis der Fokus wieder zum Sitzungsfenster zurückgeht. Als alternativen Workaround können Sie TransparentKeyPassthrough in $ICAROOT/config/module.ini auf No einstellen. Mit diesem Workaround wird das Feature “Tastaturtransparenz” deaktiviert. Sie müssen jedoch u. U. **die ICA-Datei überschreiben**, indem Sie diese Einstellung in der Datei All_regions.ini hinzufügen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Webcam

Aktualisieren der Standardwebcam

Derzeit unterstützt die Webcamumleitung in der Citrix Workspace-App für Linux jeweils nur eine Webcam. Die ausgewählte Standardwebcam ist dem Gerätepfad `/dev/video0` zugeordnet, der im Allgemeinen die in Laptops integrierte Webcam ist.

Um alle Geräte mit Videofunktionen im System aufzulisten, müssen Sie die v4l-Tools mit dem folgenden Befehl installieren:

```
sudo apt-get install v4l-util
<!--NeedCopy-->
```

Listen Sie die Videogeräte mit dem folgenden Befehl auf:

```
v4l2-ctl --list-devices
<!--NeedCopy-->
```

Sie erhalten möglicherweise eine Ausgabe wie die Folgende:

```
user@user-pc:~ $ v4l2-ctl --list-devices
UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
    /dev/video2
    /dev/video3
    /dev/media1
Integrated Camera: Integrated C (usb-0000:00:14.0-8):
    /dev/video0
    /dev/video1
    /dev/media0
<!--NeedCopy-->
```

Wie im vorherigen Beispiel gibt es zwei Webcams. Sie können jede von ihnen verwenden. Citrix empfiehlt, den ersten Index zu verwenden. Aufgrund eines bekannten Problems mit Ubuntu sehen Sie möglicherweise mehrere Indizes für eine Webcam. In diesem Beispiel können Sie /dev/video0 und /dev/video2 verwenden.

Gehen Sie wie folgt vor, um eine andere Videoquelle als Standard festzulegen:

1. Gehen Sie zur Konfigurationsdatei `~/.ICAClient/wfclient.ini` und bearbeiten Sie sie.
2. Fügen Sie im Abschnitt [WFClient] die folgende Einstellung hinzu:

   `HDXWebCamDevice=<device path>`

Fügen Sie beispielsweise `HDXWebCamDevice=/dev/video2` hinzu, um die `/dev/video2` zugeordnete Webcam in einem System festzulegen.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Testmöglichkeiten

Auf dem Client kann das Modul zur Webcamumleitung in verschiedenen Modi verwendet werden, um isolierte Komponenten unter Kundenumgebungsbedingungen zu testen.

Produktions- und Debugmodus

In diesem Modus wird das Video auf der VDA-Seite mit den tatsächlichen Puffern verglichen, die der Encoder auf der Clientseite erzeugt. Es ermöglicht das Testen der gesamten Pipeline.

Um diesen Modus zu aktivieren:

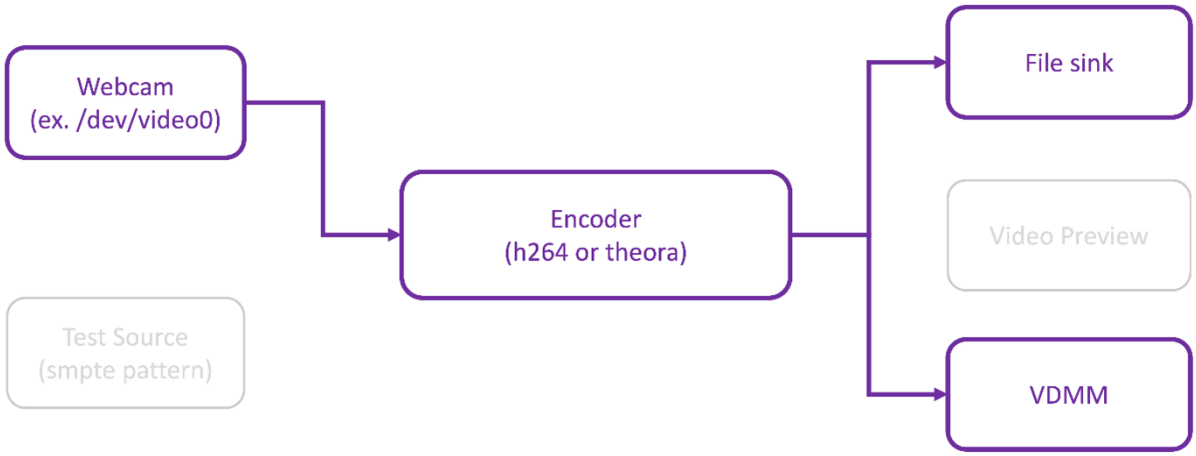
1. Gehen Sie zur Konfigurationsdatei `~/.ICAClient/wfclient.ini` und bearbeiten Sie sie.
2. Setzen Sie den Wert von `HDXWebcamDebug` auf **True**.

   HDXWebcamDebug = True

Nachdem dieser Modus aktiviert wurde, generiert der Encoder die folgenden Dateien mit den Puffern, je nach verwendetem Encoder:

- Für H264 Encoder: /tmp/file_mode_buffers.h264
- Für Theora-Encoder: /tmp/file_mode_buffers.theora

Das folgende Diagramm beschreibt den Produktions- und Debugmodus:



Webcam-Testmodus

In diesem Modus können Sie die Webcam isoliert von den übrigen Pipeline-Elementen testen.

```
./gst_read --buffers | -b BUFFERS_AMOUNT  [ --input_device | -i
   WEBCAM_DEVICE; default=/dev/video0]
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Um den Webcam-Testmodus zu aktivieren, führen Sie die folgenden Befehle über die Befehlszeilen aus:

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
`$./gst_read -b 100 /dev/video0
<!--NeedCopy-->
```

Nachdem dieser Modus aktiviert wurde, wird eine Videovorschau angezeigt und die folgende Datei mit den Rohpuffern von der Webcam erstellt:

/tmp/wewbcam_buffers.buff

Der einzige für den Webcam-Testmodus erforderliche Schalter sind die Optionen `--buffers (-b)`. Sie können auch das zu testende Webcam-Gerät angeben. Betrachten Sie zum Beispiel Folgendes:

- ./gst_read -buffers 150
- ./gst_read –buffers 100 –input_device /dev/video2

Das folgende Diagramm beschreibt den Webcam-Testmodus:

Encoder-Testmodus

In diesem Modus können Sie den Encoder isoliert von der Pipeline testen.

```
./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT;
    default=10 0 ]  [ --enableH264  | -e ]
<!--NeedCopy-->
```

Um den Encoder-Testmodus zu aktivieren, führen Sie die folgenden Befehle über die Befehlszeilen aus:

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

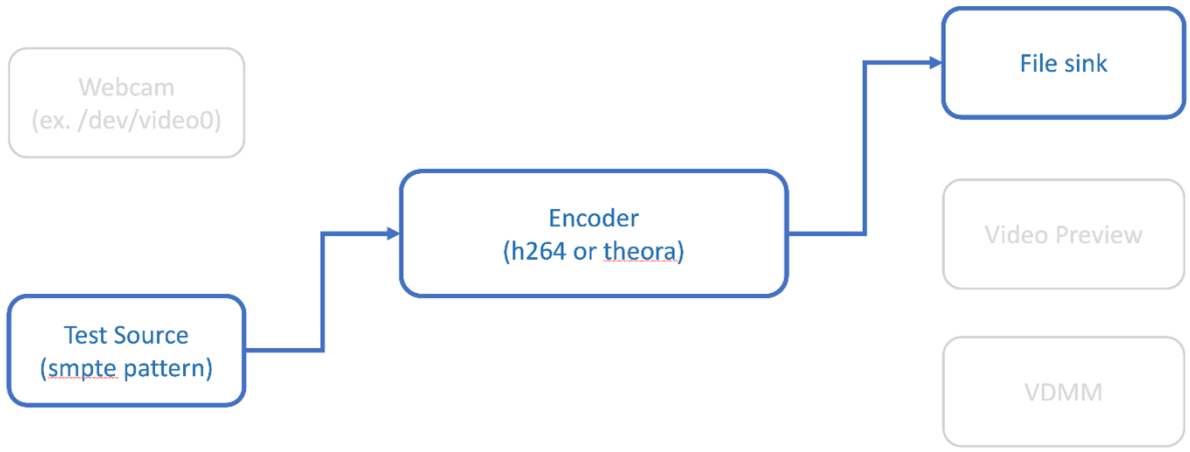
```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
./gst_read -o ~/file_buffers.h264 -e
 <!--NeedCopy-->
```

Der einzige Schalter, der für diesen Modus erforderlich ist, sind die Optionen `--output_file (-o)`. Sie können auch Theora- oder H264-Encoder und die Menge des zu generierenden Puffers testen. Betrachten Sie zum Beispiel Folgendes:

- Für H264: ./gst_read –output_file ~/file_buffers.h264 –buffers 200 –enableH264
- Für Theora: ./gst_read -o ~/file_buffers.theora -b 100

Das folgende Diagramm beschreibt den Encoder-Testmodus:



H264 Software Encoder

Wenn der softwarebasierte H264-Encoder nicht richtig funktioniert, müssen Sie die Abhängigkeiten mit den folgenden Schritten überprüfen:

1. Überprüfen Sie, ob das x264-Plug-In `GStreamer` als Teil von `gstreamer-plugins-ugly` im System vorhanden ist. Wenn es in der Bibliothek `libgstx264.so` verfügbar ist, führen Sie für die Verifizierung den folgenden Befehl aus:

   ```
   gst-inspect-1.0 x264
   <!--NeedCopy-->
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
:/opt/Citrix/ICAClient$ gst-inspect-1.0 x264
Plugin Details:
  Name                     x264
  Description              libx264-based H264 plugins
  Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
  Version                  1.14.5
  License                  GPL
  Source module            gst-plugins-ugly
  Source release date      2019-05-29
  Binary package           GStreamer Ugly Plugins (Ubuntu)
  Origin URL               https://launchpad.net/distros/ubuntu/+source/gst-plugins-ugly1.0

  x264enc: x264enc

  1 features:
  +-- 1 elements
```

2. Führen Sie den folgenden Befehl aus, um die Abhängigkeiten der Bibliothek `libgstx264.so` zu überprüfen:

```
ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
<!--NeedCopy-->
```

```
:/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
        linux-vdso.so.1 (0x00007ffcf23c5000)
        /usr/local/lib/AppProtection/libAppProtection.so (0x00007fde6482f000)
        libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007fde64596000)
        libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007fde6435e000)
        libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007fde64023000)
        libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007fde63dcf000)
        libx264.so.152 => /usr/lib/x86_64-linux-gnu/libx264.so.152 (0x00007fde63a2a000)
        libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007fde63826000)
        libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007fde6350f000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fde6311e000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007fde62eff000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007fde62cfb000)
        libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007fde629c3000)
        libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007fde6279b000)
        libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007fde62412000)
        libXi.so.6 => /usr/lib/x86_64-linux-gnu/libXi.so.6 (0x00007fde62202000)
        libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007fde61f8d000)
        liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007fde61d11000)
        libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007fde61973000)
        libgstaudio-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstaudio-1.0.so.0 (0x00007fde616fe000)
        libgsttag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgsttag-1.0.so.0 (0x00007fde614c3000)
        librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007fde612bb000)
        libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007fde610b3000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007fde60e41000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fde64c64000)
        libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007fde60c3d000)
        libXdmcp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmcp.so.6 (0x00007fde60a37000)
        libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007fde6081f000)
        libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007fde6060d000)
        libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007fde603f0000)
        libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007fde601db000)
```

Wenn die Datei `libgstx264.so` nicht vorhanden ist, müssen Sie gstreamer-plugins-ugly mit dem folgenden Befehl installieren:

```
sudo apt-get install gstreamer1
0-plugins-ugly
<!--NeedCopy-->
```

H264-Hardware-Encoder

1. Stellen Sie sicher, dass das Plug-In `vaapi GStreamer` als Teil von `gstreamer1.0-vaapi` im System vorhanden ist. Wenn es in der Bibliothek `libgstvaapi.so` verfügbar ist, führen Sie für die Verifizierung den folgenden Befehl aus:

```
gst-inspect-1.0 vaapi
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
:/opt/Citrix/ICAClient$ gst-inspect-1.0 vaapi
Plugin Details:
  Name                     vaapi
  Description              VA-API based elements
  Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
  Version                  1.14.5
  License                  LGPL
  Source module            gstreamer-vaapi
  Source release date      2019-05-29
  Binary package           gstreamer-vaapi
  Origin URL               http://bugzilla.gnome.org/enter_bug.cgi?product=GStreamer


  0 features:

:/opt/Citrix/ICAClient$
```

2. Führen Sie den folgenden Befehl aus, um die Abhängigkeiten der libgstvaapi.so-Bibliothek zu überprüfen:

```
1     ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
2 <!--NeedCopy-->
```

```
/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
        linux-vdso.so.1 (0x00007ffd635fe000)
        /usr/local/lib/AppProtection/libAppProtection.so (0x00007f5eb1d5e000)
        libgstcodecparsers-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstcodecparsers-1.0.so.0 (0x00007f5eb1b1b000)
        libdrm.so.2 => /usr/lib/x86_64-linux-gnu/libdrm.so.2 (0x00007f5eb190a000)
        libudev.so.1 => /lib/x86_64-linux-gnu/libudev.so.1 (0x00007f5eb16ec000)
        libva-drm.so.2 => /usr/lib/x86_64-linux-gnu/libva-drm.so.2 (0x00007f5eb14e9000)
        libXrandr.so.2 => /usr/lib/x86_64-linux-gnu/libXrandr.so.2 (0x00007f5eb12de000)
        libXrender.so.1 => /usr/lib/x86_64-linux-gnu/libXrender.so.1 (0x00007f5eb10d4000)
        libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007f5eb0d9c000)
        libGL.so.1 => /usr/lib/x86_64-linux-gnu/libGL.so.1 (0x00007f5eb0b10000)
        libva-x11.so.2 => /usr/lib/x86_64-linux-gnu/libva-x11.so.2 (0x00007f5eb090a000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f5eb0706000)
        libEGL.so.1 => /usr/lib/x86_64-linux-gnu/libEGL.so.1 (0x00007f5eb04f2000)
        libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007f5eb02ee000)
        libva-wayland.so.2 => /usr/lib/x86_64-linux-gnu/libva-wayland.so.2 (0x00007f5eb00e9000)
        libva.so.2 => /usr/lib/x86_64-linux-gnu/libva.so.2 (0x00007f5eafec8000)
        libwayland-client.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-client.so.0 (0x00007f5eafcb9000)
        libgstgl-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstgl-1.0.so.0 (0x00007f5eafa53000)
        libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007f5eaf81b000)
        libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007f5eaf582000)
        libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007f5eaf30d000)
        libgstallocators-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstallocators-1.0.so.0 (0x00007f5eaf109000)
        libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007f5eaedce000)
        libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007f5eaeb7a000)
        libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007f5eae863000)
        libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007f5eae4c5000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f5eae2a6000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f5eadeb5000)
        libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007f5eadc8d000)
        libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007f5ead904000)
        libXi.so.6 => /usr/lib/x86_64-linux-gnu/libXi.so.6 (0x00007f5ead6f4000)
        librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007f5ead4ec000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f5eb2261000)
        libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007f5ead2da000)
        libGLX.so.0 => /usr/lib/x86_64-linux-gnu/libGLX.so.0 (0x00007f5ead0a9000)
        libGLdispatch.so.0 => /usr/lib/x86_64-linux-gnu/libGLdispatch.so.0 (0x00007f5eacdf3000)
        libXfixes.so.3 => /usr/lib/x86_64-linux-gnu/libXfixes.so.3 (0x00007f5eacbed000)
        libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007f5eac9e5000)
        libX11-xcb.so.1 => /usr/lib/x86_64-linux-gnu/libX11-xcb.so.1 (0x00007f5eac7e3000)
        libwayland-egl.so.1 => /usr/lib/x86_64-linux-gnu/libwayland-egl.so.1 (0x00007f5eac5e1000)
        libgbm.so.1 => /usr/lib/x86_64-linux-gnu/libgbm.so.1 (0x00007f5eac3d2000)
        libgudev-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgudev-1.0.so.0 (0x00007f5eac1c8000)
        libgstaudio-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstaudio-1.0.so.0 (0x00007f5eabf53000)
        libgsttag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgsttag-1.0.so.0 (0x00007f5eabd18000)
        liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007f5eaba9c000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f5eab82a000)
        libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007f5eab626000)
        libXdmcp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmcp.so.6 (0x00007f5eab420000)
        libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007f5eab208000)
        libwayland-server.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-server.so.0 (0x00007f5eaaff5000)
        libexpat.so.1 => /lib/x86_64-linux-gnu/libexpat.so.1 (0x00007f5eaadc3000)
        libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f5eaaba6000)
        libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007f5eaa991000)
gamilr@ubuntu:/opt/Citrix/ICAClient$
```

3. Lösen Sie alle fehlenden Abhängigkeiten.

Folgen Sie zur Installation und Konfiguration von `vaapi` dem `GStreamer vappi` Installationshand-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

buch.

Sammeln Sie interne Protokolle für GStreamer-Frameworks und gst_read

Alternativ zu regulären `ICAClient`-Protokollen müssen Sie die Protokolle aus dem Modul `gst_read` sammeln.

Gehen Sie wie folgt vor, um die Protokolle zu sammeln:

1. Öffnen Sie ein Terminal und führen Sie die folgenden Befehle aus:

```
export GST_DEBUG=2, gst_read_debug:6
<!--NeedCopy-->
```

```
export GST_DEBUG_FILE=~/gst_read.log
<!--NeedCopy-->
```

> **Hinweis:**
>
> Diese Variable legt den Grad der Protokollierung und die Datei zum Speichern fest. In diesem Fall setzen wir Level 2 für das Framework `GStreamer` und Level 7 für das Modul `gst_read`. Weitere Informationen finden Sie in dieser Dokumentation. Es wird empfohlen, nur Fehler- und Warnstufen für das interne Framework `GStreamer` und die Protokollebene für `gst_read` festzulegen.

2. Laden Sie eine ICA-Datei eines gültigen VDA herunter.
3. Führen Sie auf demselben Terminal den folgenden Befehl aus, um eine VDA-Sitzung zu starten:

```
cd /opt/Citrix/ICAClient
<!--NeedCopy-->
```

```
./wfica   <ICA file path>/vda.ica
<!--NeedCopy-->
```

Die Datei `gst_read.log` wird mit dem internen `GStreamer`-Framework und den `gst_read`-Protokollen generiert.

GStreamer Pipeline-Inspektionen

Gehen Sie wie folgt vor, um die Pipelines zu sehen, die das `GStreamer`-Framework erstellt:

1. Erstellen Sie einen Ordner zum Speichern der Dot-Dateien, zum Beispiel: `gstIntPipes`.
2. Öffnen Sie ein Terminal und exportieren Sie `GST_DEBUG_DUMP_DOT_DIR=<Absolute path>/gstIntPipes`. Diese Variable gibt an, wo `GStreamer` die Dot-Dateien speichern soll.

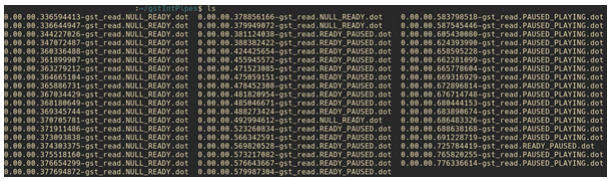
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. Laden Sie eine ICA-Datei eines gültigen VDA herunter.
4. Führen Sie auf demselben Terminal den folgenden Befehl aus, um eine VDA-Sitzung zu starten:

```
cd /opt/Citrix/ICAClient/
<!--NeedCopy-->
```

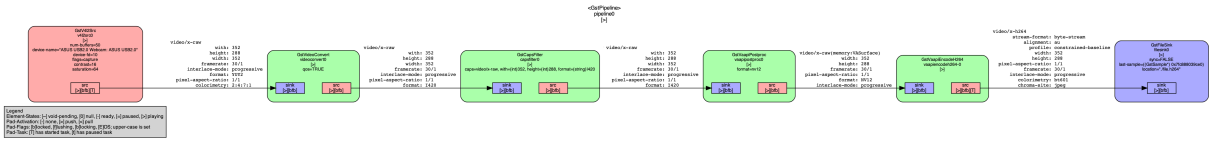
```
./wfica <ICA file path>/vda.ica
<!--NeedCopy-->
```

5. Das Verzeichnis `gstIntPipes` enthält die Dot-Dateien. `GStreamer` generiert eine Dot-Ddatei für jede Zustandsänderung in der Pipeline. Dadurch können Sie alle Prozesse beim Erstellen der Pipeline überprüfen. Im Folgenden finden Sie ein Beispiel für den Satz von Dot-Dateien:

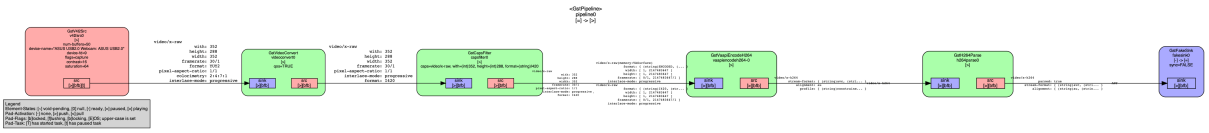


6. Installieren Sie ein Hilfsprogramm für Dot-Dateien, um eine visuelle Darstellung der Pipelines anzuzeigen. Zum Beispiel Graphviz. Die folgenden Bilder sind Beispiele für ein gutes und schlechtes Erstellen der Pipeline:

Pipeline wurde erfolgreich erstellt:



Pipeline kann keine Verbindung herstellen:



> **Hinweis:**
>
> Um die vorhergehenden Bilder oder andere Bilder zu vergrößern, klicken Sie mit der rechten Maustaste auf das Bild, wählen Sie **Bild in neuem Tab öffnen**und zoomen Sie den Browser nach Bedarf.

Wie in der vorherigen Abbildung gezeigt, kann die zweite Pipeline das Element `GstCapsFilter` und das Element `GstVaapiEncodeH264` nicht verknüpfen. Die Fähigkeiten werden niemals vollständig ausgehandelt. Weitere Informationen finden Sie in dieser Dokumentation.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Systemdiagnoseskript für RAVE

Citrix stellt das Skript `rave_troubleshooting.sh` bereit, mit dem Sie überprüfen können, ob die Systemkonfiguration und die Abhängigkeiten die Remote Audio- und Videoerweiterungen (RAVE) unterstützen.

> **Hinweis:**
>
> RAVE ist ein HDX-Feature zur Unterstützung der optimierten Webcamumleitung und der Windows Media Player-Umleitung für Citrix VDAs.

Gehen Sie wie folgt vor, um das Skript auszuführen:

1. Klicken Sie auf rave_troubleshooting.sh, um das Skript herunterzuladen.
2. Öffnen Sie das Terminal auf Ihrer Linux-Maschine.
3. Geben Sie `rave_troubleshooting.sh --help` oder `rave_troubleshooting.sh -h` ein, um die zugehörigen Befehlszeilenargumente anzuzeigen.
4. Machen Sie eine der folgenden Eingaben:
   - `rave_troubleshooting.sh -w` oder `rave_troubleshooting.sh --webcam` - Verwenden Sie diesen Befehl, um die Webcamumleitung zu überprüfen. Dies ist der Standardbefehl.
   - `rave_troubleshooting.sh -r` oder `rave_troubleshooting.sh --rave` - Verwenden Sie diesen Befehl, um das RAVE-Feature zu überprüfen. Es wird ein Popupfenster angezeigt, in dem ein h264-Testvideo zu sehen ist.

   Die Systemkonfiguration und Abhängigkeiten werden angezeigt.

Browser

Lokaler Browser

Beim Klicken auf einen Link in einer Windows-Sitzung wird der Inhalt in einem lokalen Browser angezeigt. Die Server-zu-Client-Inhaltsumleitung ist in der Datei wfclient.ini aktiviert. Diese Umleitung führt zur Ausführung einer lokalen Anwendung. Informationen zum Deaktivieren der Server-zu-Client-Inhaltsumleitung finden Sie unter Server-zu-Client-Inhaltsumleitung.

Zugriff auf veröffentlichte Ressourcen

Beim Zugreifen auf veröffentlichte Ressourcen werden Sie vom Browser aufgefordert, eine Datei zu speichern. Andere Browser als Firefox und Chrome müssen möglicherweise konfiguriert werden, bevor Sie auf eine veröffentlichte Ressource zugreifen können. Wenn Sie jedoch versuchen, eine Ressource durch Klicken auf das Symbol auf der Seite zu öffnen, fordert Sie der Browser zum Speichern der ICA-Datei auf.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Spezifische Browser

Wenn Sie Probleme mit einem bestimmten Webbrowser haben, geben Sie für die Umgebungsvariable BROWSER den lokalen Pfad und Namen des erforderlichen Browsers ein, bevor Sie `setupwfc` ausführen.

Firefox-Browser

Wenn Sie Desktops oder Anwendungen in Firefox starten und die Seite nicht reagiert, aktivieren Sie das ICA-Plug-In.

ICA-Plug-In Firefox

Wenn das ICA-Plug-In in Firefox aktiviert ist, werden Desktop- und Anwendungssitzungen möglicherweise nicht gestartet. Versuchen Sie in diesem Fall, das ICA-Plug-In zu deaktivieren.

Konfigurationsfehler

Diese Fehler können auftreten, wenn Sie einen Verbindungseintrag nicht richtig konfiguriert haben.

E_MISSING_INI_SECTION – Überprüfen der Konfigurationsdatei: "…". In der Konfigurationsdatei fehlt der Abschnitt "…".

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_MISSING_INI_ENTRY – Überprüfen der Konfigurationsdatei: "…". Der Abschnitt "…" muss einen Eintrag "…" enthalten.

Die Konfigurationsdatei wurde nicht richtig bearbeitet oder ist fehlerhaft.

E_INI_VENDOR_RANGE – Überprüfen der Konfigurationsdatei: "…". Der X Server-Herstellerbereich "…" in der Konfigurationsdatei ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Bitte wenden Sie sich an Citrix.

Konfigurationsfehler in wfclient.ini

Diese Fehler können auftreten, wenn Sie die Datei wfclient.ini nicht richtig bearbeitet haben.

E_CANNOT_WRITE_FILE – Datei kann nicht geschrieben werden: "…"

Es liegt ein Problem beim Speichern der Verbindungsdatenbank vor, z. B. nicht genügend Festplattenspeicher.

E_CANNOT_CREATE_FILE – Datei kann nicht erstellt werden: "…"

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Beim Erstellen einer Verbindungsdatenbank ist ein Problem aufgetreten.

E_PNAGENT_FILE_UNREADABLE – Citrix Virtual Apps-Datei kann nicht gelesen werden "…": Datei oder Verzeichnis nicht gefunden.

– oder –

Citrix Virtual Apps-Datei "…" kann nicht gelesen werden: Zugriff verweigert.

Sie versuchen, eine Ressource über einen Desktopeintrag oder ein Menü zu öffnen. Die Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Datei für die Ressource steht jedoch nicht zur Verfügung. Aktualisieren Sie die Liste der veröffentlichten Ressourcen. Wählen Sie im Menü **Ansicht** die Option "Anwendungsaktualisierung" und versuchen Sie erneut, die Ressource zu öffnen. Falls der Fehler weiterhin besteht:

- Überprüfen Sie die Eigenschaften des Desktopsymbols oder des Menüelements.
- Überprüfen Sie die Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Datei, auf die das Symbol oder Element verweist.

Andere

Verbindungsprobleme

Möglicherweise treten auch die folgenden Probleme auf.

Schließen einer Sitzung

Mit dem Programm *wfica* können Sie feststellen, ob die Citrix Workspace-App vom Server angewiesen wurde, eine Sitzung zu schließen. Dieses Programm protokolliert, wenn es vom Server den Befehl erhalten hat, die Sitzung zu beenden.

Damit diese Informationen vom Syslog aufgezeichnet werden, fügen Sie *SyslogThreshold* mit dem Wert 6 im Abschnitt [WFClient] der Konfigurationsdatei hinzu. Durch diese Einstellung wird das Protokollieren von Meldungen mit der Priorität LOG_INFO oder höher aktiviert. Der Standardwert für *SyslogThreshold* ist 4 (=LOG_WARNING).

Damit *wfica* die Informationen als Standardfehler sendet, fügen Sie *PrintLogThreshold* mit dem Wert 6 im Abschnitt [WFClient] hinzu. Der Standardwert für *PrintLogThreshold* ist 0 (=LOG_EMERG).

Weitere Informationen zur Protokollierung finden Sie unter Protokollierung. Weitere Informationen zur Konfiguration von syslog finden Sie unter Syslog-Konfiguration.

Konfigurationsdateieinstellungen

Für jeden Eintrag in wfclient.ini muss ein entsprechender Eintrag in All_Regions.ini gemacht werden, damit die Einstellung wirksam wird. Außerdem muss für jeden Eintrag in den Abschnitten [Thin-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

wire3.0], [ClientDrive] und [TCP/IP] von wfclient.ini ein entsprechender Eintrag in canonicalization.ini gemacht werden, damit die Einstellung wirksam wird. Weitere Informationen finden Sie in den Dateien All_Regions.ini und canonicalization.ini im Verzeichnis $ICAROOT/config.

Veröffentlichte Anwendungen

Beim Zugriff einer veröffentlichten Anwendung auf einen seriellen Port kann die Anwendung fehlschlagen (je nach der Anwendung mit oder ohne Fehlermeldung), wenn der Port durch eine andere Anwendung gesperrt ist. Überprüfen Sie in solchen Fällen, ob eine Anwendung den seriellen Port vorübergehend gesperrt hat. Oder ob eine Anwendung den seriellen Port gesperrt hat und dann beendet wurde, ohne ihn freizugeben.

Um dieses Problem zu lösen, beenden Sie die Anwendung, die den seriellen Port derzeit belegt. Bei UUCP-Sperren ist nach dem Beenden der Anwendung eventuell noch eine Sperrdatei vorhanden. Der Speicherort dieser Sperrdateien hängt vom verwendeten Betriebssystem ab.

Starten der Citrix Workspace-App

Wenn die Citrix Workspace-App nicht gestartet werden kann, wird die Fehlermeldung “Application default file could not be found or is out of date” angezeigt. In diesem Fall ist die Umgebungsvariable ICAROOT möglicherweise nicht richtig definiert. Diese Variable muss richtig definiert werden, wenn Sie die Citrix Workspace-App nicht im Standardverzeichnis installiert haben. Citrix empfiehlt hierfür zwei Lösungsvorschläge:

- Definieren Sie ICAROOT als Installationsverzeichnis.

  Um zu überprüfen, ob die Umgebungsvariable ICAROOT richtig definiert wurde, versuchen Sie, die Citrix Workspace-App von einer Terminalsitzung zu starten. Wenn die Fehlermeldung weiterhin angezeigt wird, ist die Umgebungsvariable ICAROOT wahrscheinlich nicht richtig definiert.

- Installieren Sie die Citrix Workspace-App im Standardverzeichnis neu. Weitere Informationen zur Installation der Citrix Workspace-App finden Sie unter Installation und Einrichtung.

  Wenn die Citrix Workspace-App vorher im Standardverzeichnis installiert worden war, sollten Sie vor der Neuinstallation das Verzeichnis `/opt/Citrix/ICAClient` oder `$HOME/ICAClient/platform` entfernen.

Citrix CryptoKit (früher SSLSDK)

Um die Versionsnummer für das ausgeführte Citrix CryptoKit (ehemals SSLSDK) oder OpenSSL festzustellen, führen Sie den folgenden Befehl aus:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

Sie können diesen Befehl auch für AuthManagerDaemon oder PrimaryAuthManager ausführen

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Tastenkombinationen

Ihre Tastenkombinationen funktionieren unter Umständen nicht richtig, wenn der Fenstermanager dieselben Tastenkombinationen für systemeigene Funktionen verwendet. Im KDE-Fenstermanager werden beispielsweise die Kombinationen von STRG+UMSCHALT+F1 bis STRG+UMSCHALT+F4 verwendet, um zwischen den Desktops 13 bis 16 zu wechseln. Wenn dieses Problem auftritt, versuchen Sie Folgendes:

- Mit dem Übersetzungsmodus auf der Tastatur werden lokale Tastenkombinationen serverseitigen Tastenkombinationen zugeordnet. Beispielsweise wird im Übersetzungsmodus standardmäßig STRG+UMSCHALT+F1 serverseitig der Tastenkombination ALT+F1 zugeordnet. Um diese Zuordnung in eine andere lokale Tastenkombination zu ändern, aktualisieren Sie den folgenden Eintrag im Abschnitt [WFClient] der Datei $HOME/.ICAClient/wfclient.ini. Durch diese Einstellung wird die lokale Tastenkombination Alt+Strg+F1 der Kombination Alt+F1 zugeordnet:
  - Ändern Sie Hotkey1Shift=Ctrl+Shift in Hotkey1Shift=Alt+Ctrl.
- Im direkten Modus werden alle Tastenkombinationen direkt an den Server gesendet. Sie werden nicht lokal verarbeitet. Legen Sie zum Konfigurieren des direkten Modus im Abschnitt [WFClient] der Datei $HOME/.ICAClient/wfclient.ini TransparentKeyPassthrough auf Remote fest.
- Konfigurieren Sie den Fenstermanager so, dass Standardtastaturkombinationen unterdrückt werden.

Kroatische Remotetastatur

Diese Vorgehensweise stellt sicher, dass ASCII-Zeichen korrekt an remote virtuelle Desktops mit kroatischen Tastaturlayouts gesendet werden.

1. Setzen Sie im Abschnitt WFClient der entsprechenden Konfigurationsdatei UseEUKSforASCII auf True.
2. Setzen Sie UseEUKS auf 2.

Japanische Tastatur

Zum Konfigurieren einer japanischen Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Japanese (JIS)

ABNT2-Tastatur

Zum Konfigurieren einer ABNT2-Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Lokale Tastatur

Wenn sich einige Tasten auf der lokalen Tastatur nicht wie erwartet verhalten, wählen Sie das passendste Serverlayout aus der Liste in $ICAROOT/config/module.ini aus.

Windows Media Player

Die Citrix Workspace-App hat möglicherweise nicht die nötigen GStreamer-Plug-Ins, um ein gewünschtes Format zu verarbeiten. Normalerweise fordert der Server dann ein anderes Format an. Manchmal wird bei der anfänglichen Prüfung irrtümlich ein passendes Plug-In festgestellt. Dieses Problem sollte erkannt werden und auf dem Server eine Fehlermeldung auslösen, die darauf hinweist, dass beim Wiedergeben der Datei mit Windows Media Player ein Problem aufgetreten ist. Ein erneutes Wiedergeben der Datei in der Sitzung funktioniert normalerweise, weil das Format von der Citrix Workspace-App abgelehnt wird. Der Server wird daraufhin ein anderes Format anfordern oder das Medium selbst bereitstellen.

In seltenen Fällen wird kein passendes Plug-In erkannt und die Datei wird nicht richtig wiedergegeben, obwohl sich die Fortschrittsanzeige in Windows Media Player wie erwartet bewegt.

Vermeiden der Fehlermeldung oder des Wiedergabefehlers in zukünftigen Sitzungen:

1. Fügen Sie beispielsweise in der Datei $Home/.ICAClient/wfclient.ini vorübergehend die Konfigurationsoption “SpeedScreenMMAVerbose=On” im Abschnitt [WFClient] hinzu.
2. Starten Sie wfica über einen selfservice, der von einem Terminal aus gestartet wurde.
3. Geben Sie ein Video wieder, das diesen Fehler auslöst.
4. Bestimmen Sie in der Ausgabe der Ablaufverfolgung den MIME-Typ des fehlenden Plug-Ins oder den MIME-Typ, der unterstützt werden sollte, aber nicht wiedergegeben wird (z. B. “video/x-h264..”).
5. Bearbeiten Sie $ICAROOT/config/MediaStreamingConfig.tbl. Fügen Sie dazu in der Zeile mit dem MIME-Typ ein “?” zwischen dem “:” und dem MIME-Typ ein. Diese Einstellung deaktiviert das Format.
6. Wiederholen Sie die vorherigen Schritte 2 bis 5 für andere Medienformate, die diesen Fehler verursachen.
7. Verteilen Sie die bearbeitete Datei MediaStreamingConfig.tbl auf andere Maschinen, die dieselben GStreamer-Plug-Ins haben.

> **Hinweis:**
>
> Nachdem Sie den MIME-Typ identifiziert haben, können Sie möglicherweise ein GStreamer-Plug-In installieren und ihn decodieren.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Skript zur Überprüfung der Systemanforderungen für die Windows Media Player-Umleitung

Mit Release 2307 wird ein neues Bash-Skript eingeführt, um die Konfiguration zu überprüfen, die für die Windows Media Player-Umleitungsfunktion in der Citrix Workspace-App für Linux erforderlich ist. Damit können Sie die Problembehandlung bei der Windows Media Player-Umleitungsfunktion beschleunigen. Zur Überprüfung der Konfiguration können Sie dieselbe Datei rave_troubleshooting.sh verwenden, die unter [Systemdiagnoseskript für RAVE]/de-de/citrix-workspace-app-for-linux/troubleshooting.html#system-diagnostic-script-for-rave) verfügbar ist.

Einstellung für seriellen Anschluss

Zum Konfigurieren eines seriellen Anschlusses fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=1

ComPort1=device

Zum Konfigurieren von mehreren seriellen Anschlüssen fügen Sie die folgenden Einträge der Konfigurationsdatei$ICAROOT/config/module.ini hinzu:

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Fehler

Dieser Abschnitt enthält weitere Fehlermeldungen, die bei der Verwendung der Citrix Workspace-App möglicherweise häufiger angezeigt werden.

Es ist ein Fehler aufgetreten. Fehler 11 (E_MISSING_INI_SECTION). Weitere Informationen finden Sie in der Dokumentation. Anwendung wird beendet.

Bei der Ausführung der Citrix Workspace-App über die Befehlszeile lässt dieser Fehler in der Regel darauf schließen, dass die in der Befehlszeile angegebene Beschreibung in der Datei appsrv.ini nicht gefunden wurde.

E_BAD_OPTION – Die Option "…" ist ungültig.

Fehlendes Argument für Option "…".

E_BAD_ARG – Die Option "…" hat ein ungültiges Argument: "…".

Ungültiges Argument für Option "…".

E_INI_KEY_SYNTAX – Der Schlüssel "…" in der Konfigurationsdatei "…" ist ungültig.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Erstellen Sie eine Konfigurationsdatei.

E_INI_VALUE_SYNTAX – Der Wert "…" in der Konfigurationsdatei "…" ist ungültig.

Die X Server-Händlerinformationen in der Konfigurationsdatei sind fehlerhaft. Erstellen Sie eine Konfigurationsdatei.

E_SERVER_NAMELOOKUP_FAILURE – Verbindung zu Server "…" kann nicht hergestellt werden.

Der Servername kann nicht aufgelöst werden.

In mindestens eine Datei kann nicht geschrieben werden: "…". Beheben Sie Probleme in Bezug auf Berechtigungen oder den verfügbaren Speicherplatz auf dem Datenträger und versuchen Sie es erneut.

Überprüfen Sie, ob die Festplatte voll ist oder ob Probleme mit den Rechten bestehen. Wenn Sie das Problem gefunden und gelöst haben, wiederholen Sie den Vorgang, der die Fehlermeldung ausgelöst hat.

Die Verbindung zum Server wurde unterbrochen. Stellen Sie die Verbindung wieder her und versuchen Sie es erneut. In diesen Dateien fehlen u. U. Daten: "…".

Stellen Sie die Verbindung wieder her und wiederholen Sie den Vorgang, der den Fehler ausgelöst hat.

Diagnoseinformationen

Wenn Sie beim Verwenden der Citrix Workspace-App Probleme feststellen, werden Sie vom Technischen Support möglicherweise gebeten, Diagnoseinformationen bereitzustellen. Diese Informationen unterstützen dieses Team bei der Diagnose und helfen, das Problem zu beheben.

Abfrage von Diagnoseinformationen zur Citrix Workspace-App:

1. Geben Sie im Installationsverzeichnis util/lurdump ein. Es empfiehlt sich, diese Änderung auszuführen, während eine Sitzung geöffnet ist und möglichst während das Problem auftritt.

   Es wird eine Datei generiert, die detaillierte Diagnoseinformationen bereitstellt, u. a. Version, Inhalt der Citrix Workspace-App-Konfigurationsdateien und die Werte der verschiedenen Systemvariablen.

2. Überprüfen Sie, ob diese Datei vertrauliche Informationen enthält, bevor Sie sie an den technischen Support senden.

Problembehandlung bei Verbindungen mit Ressourcen

Benutzer können aktive Verbindungen mit dem Connection Center verwalten. Dieses Feature ist ein nützliches Tool, mit dem Benutzer und Administratoren Probleme mit langsamen oder fehlerhaften

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Verbindungen beheben können. Mit Connection Center, können Benutzer folgende Verbindungsverwaltungsaufgaben durchführen:

- Schließen einer Anwendung
- Abmelden von einer Sitzung. Dabei wird die Sitzung beendet und alle geöffneten Anwendungen werden geschlossen.
- Trennen der Verbindung mit einer Sitzung. Mit diesem Schritt wird die ausgewählte Verbindung mit dem Server getrennt, ohne offene Anwendungen zu schließen (außer wenn der Server zum Schließen von Anwendungen bei Verbindungstrennung konfiguriert ist).
- Anzeigen der Verbindungsübertragungsstatistik

SDK und API

June 6, 2023

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 Kanalanwendungen sind auf Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Servern (ehemals Citrix Virtual Apps and Desktops Service).

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 (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Funktionierender Quellcode für mehrere Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen finden Sie unter Citrix Virtual Channel SDK for Citrix Workspace app for Linux.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Befehlszeilenreferenz

Weitere Informationen zu Befehlszeilenreferenz und Parametern finden Sie unter Citrix Workspace app for Linux Command Reference.

Platform Optimization SDK

Im Rahmen der HDX SoC-Initiative für die Citrix Workspace-App für Linux haben wir das "Platform Optimization SDK" entwickelt.

Dieses SDK ermöglicht ein Ökosystem kostengünstiger Geräte mit niedrigem Energieverbrauch, hoher Leistung und innovativen Formfaktoren.

Das Platform Optimization SDK kann von Entwicklern genutzt werden, um die Leistung von Linux-basierten Geräten zu verbessern. Entwickler können mit dem SDK Plug-In-Erweiterungen für die ICA-Engine-Komponente (`wfica`) der Citrix Workspace-App erstellen. Plug-Ins werden als freigegebene Bibliotheken entwickelt, die von `wfica` dynamisch geladen werden.

Mit diesen Plug-Ins können Sie die Leistung Ihrer Linux-Geräte optimieren, indem Sie die folgenden Funktionen aktivieren:

- Beschleunigtes Decodieren von JPEG- und H.264-Daten, mit denen das Sitzungsbild erstellt wird
- Steuern der Speicherzuordnung zum Erstellen des Sitzungsbilds
- Verbessern der Leistung durch Steuern der unteren Ebene beim Erstellen des Sitzungsbilds
- Bereitstellen von Diensten für die Grafikausgabe und Benutzereingabe für Betriebssystemumgebungen, die X11 nicht unterstützen

Weitere Informationen finden Sie unter Citrix Workspace app for Linux - Platform Optimization SDK.

Referenz für ICA-Einstellungen

June 6, 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)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).