# Citrix Workspace-App für Linux

## Contents



© 1999-2019 Citrix Systems, Inc. All rights reserved. 

# Neue Features der Citrix Workspace-App für Linux

May 23, 2019

## Neue Features in Release 1903

### 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. Diese Verschlüsselungssammlungen wurden in Citrix Receiver Version 13.10 als veraltet klassifiziert. Abwärtskompatibilität ist jedoch vorhanden.

In diesem Release wurden die TLS_RSA_-Verschlüsselungssammlungen vollständig entfernt. Stattdessen unterstützt dieses Release die erweiterten TLS_ECDHE_RSA_-Verschlüsselungssammlungen. Wenn Ihre Umgebung nicht mit den TLS_ECDHE_RSA_-Verschlüsselungssammlungen konfiguriert ist, werden die Starts von Clients aufgrund schwacher Verschlüsselung nicht unterstützt. Dieses Release unterstützt 1536-Bit-RSA-Schlüssel für die Clientauthentifizierung.

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)

Weitere Informationen, siehe Konfigurieren von Verschlüsselungssammlungen.

> **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 unterUnterstützung des DTLS-Protokolls.

### Bloomberg-Audioumleitung

Dieses Feature ermöglicht den Einsatz von Bloomberg v4-Audioschnittstellen über mehrere Sitzungen hinweg. Das Audio der Sitzungen wird über den optimierten Kanal zur Bloomberg-Schnittstelle geleitet. Die Fingerabdruckschnittstelle wird wie bisher zu einer einzelnen Sitzung umgeleitet.

> **Hinweis:**
>
> Dieses Feature ist standardmäßig für x86-, x64- und ARMHF-Plattformen deaktiviert.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Weitere Informationen zum Konfigurieren der Bloomberg-Audioumleitung finden Sie in den Anleitungen unter Umleitung der Bloomberg v4-Tastatur über generisches USB bei Unterstützung der selektiven Umleitung.

#### Anmeldeseite

In diesem Release wird eine neue Anmeldeseite in der Self-Service-Benutzeroberfläche eingeführt.

#### Dauer der Trennung

Durch das Beheben bestimmter Probleme in diesem Release wurde die Trennzeit erheblich verkürzt.

### Neue Features in Release 1901

#### Unterstützung für Citrix Analytics

Die Citrix Workspace-App für Linux ist so instrumentiert, dass Protokolle sicher an Citrix Analytics übertragen werden, wenn bestimmte Ereignisse von der App ausgelöst werden. Die Protokolle werden analysiert und auf Citrix Analytics-Servern gespeichert, wenn diese aktiviert sind. Weitere Informationen zu Citrix Analytics finden Sie unter Citrix Analytics.

#### Workspace Launcher mit Citrix Gateway

Citrix hat Workspace Launcher (WebHelper) in Version 1809 eingeführt. In Version 1901 funktioniert Citrix Workspace Launcher nicht nur über direkte Verbindungen zu StoreFront, sondern auch über Citrix Gateway. Mit diesem Feature wird die ICA-Datei automatisch gestartet und die Citrix Workspace-App erkannt.

#### Verbesserungen bei der Protokollierung II

Die Verbesserungen bei der Protokollierung II erweitert die Protokollierungsverbesserungen und bessere Protokollierungsfeatures. Das Feature bietet Unterstützung für die Protokollierung für viele Module und vereinfacht das Sammeln von Protokollen. Es hilft Benutzern bei der Problembehandlung und unterstützt den Support bei komplizierten Problemen durch die Bereitstellung detaillierter Protokolle.

Informationen zum Aktivieren der Protokollierung finden Sie unter Aktivieren der Protokollierung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Tastaturlayoutsynchronisierung zwischen Client und VDA

Bisher wurden die Tastaturlayouts auf dem Windows VDA bzw. dem Linux VDA und dem Clientgerät manuell synchronisiert. Wurde beispielsweise das Tastaturlayout auf dem Clientgerät von Englisch auf Deutsch geändert, nicht jedoch auf dem VDA, konnten Probleme bei der Tastenzuordnung auftreten, bis das Tastaturlayout auch auf dem VDA auf Deutsch umgestellt wurde.

Ab diesem Release ist das Problem behoben. Das Tastaturlayout auf dem VDA wird automatisch mit dem des Clientgeräts synchronisiert. Jedes Mal, wenn sich das Tastaturlayout auf dem Clientgerät ändert, ändert sich automatisch auch das Layout auf dem VDA.

> **Hinweis:**
>
> Dieses Feature erfordert VDA-Version 7.16 oder höher.

Weitere Informationen finden Sie unter Tastaturlayoutsynchronisierung zwischen Client und VDA.

### Neue Features in Release 1810

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

### Neue Features in Release 1809

Das Verbinden dieser Version der Citrix Workspace-App für Linux mit den Citrix Workspace-Diensten ist ein experimentelles Feature.

#### Einführung von Workspace Launcher

Bisher ermöglichte das zusammen mit der Citrix Workspace-App für Linux bereitgestellte Browser-Plug-In Benutzern das Starten veröffentlichter Desktops und Anwendungen. Dieses Plug-In basierte auf dem Netscape Plugin Application Programming Interface (NPAPI).

Die Mozilla Corporation hat angekündigt, dass die NPAPI-Unterstützung ab Version 52 des Firefox-Browsers eingestellt wird. Andere Browser haben die Unterstützung für NPAPI ebenfalls eingestellt.

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.

Informationen zum Konfigurieren von StoreFront finden Sie unter **Solution – 2** > **a) Administrator configuration** im Knowledge Center-Artikel CTX237727.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **Hinweis:**
>
> Citrix Workspace Launcher funktioniert derzeit nur bei einer direkten Verbindung zu StoreFront. Es wird nicht in anderen Situationen, z. B. bei Verbindungen über Citrix Gateway, 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. Wechseln 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.

### Neue Features in Release 1808

#### Citrix Workspace-App

Citrix Receiver ist jetzt die Citrix Workspace-App.
Mit der Citrix Workspace-App werden die Funktionen von Citrix Receiver erweitert, sodass Sie noch produktiver arbeiten können. Die Citrix Workspace-App umfasst sämtliche Funktionen von Citrix Receiver und bildet die Grundlage für neue Funktionen in zukünftigen Citrix Virtual Apps and Desktops-Releases und im gesamten Citrix Workspace.

Die Citrix Workspace-App vereinfacht die Versionsverwaltung, und das verwendete YYMM-Format macht diese Version zur Citrix Workspace-App 1808. Die vorherige Version hatte die Dateiversionsnummer 13.10.0.20.

Bestehende Benutzer oder Endpunkte von Citrix Receiver für Linux können nahtlos zur neuen Version der Citrix Workspace-App für Linux wechseln, indem sie ein direktes Upgrade durchführen.

Upgrade auf die Citrix Workspace-App:

- Laden Sie die Citrix Workspace-App von der Citrix Downloadseite herunter und installieren Sie die App, um von Citrix Receiver auf die Citrix Workspace-App zu aktualisieren.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Die Citrix Workspace-App besitzt ein neues Symbol im blauen Farbton. Es ersetzt das frühere schwarze Citrix Receiver-Symbol.

Der **Citrix Workspace**-Bildschirm wird beim ersten Start der App, beim Upgrade oder bei der Deinstallation und Neuinstallation der App angezeigt, um Sie über den Wechsel zu informieren. Klicken Sie auf **Verstanden**, um die Workspace-App weiter zu verwenden, oder auf **Weitere Infos**, um mehr zu erfahren.

Das Verbinden dieser Version der Citrix Workspace-App für Linux mit den Citrix Workspace-Diensten ist ein experimentelles Feature.

#### Unterstützung für die selektive Bloomberg v4-Tastaturumleitung

Dieses Feature ermöglicht den Einsatz der Bloomberg v4-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.

> **Hinweis:**
>
> Dieses Feature ist standardmäßig für x86- und x64-Plattformen aktiviert und für ARMHF-Plattformen deaktiviert.

Weitere Informationen finden Sie unter Unterstützung für die selektive Bloomberg v4-Tastaturumleitung.

## Behobene Probleme

April 2, 2019

### Behobene Probleme in Release 1903

- Nach dem Beenden einer Microsoft Office 365 PowerPoint-Präsentation, die in einem veröffentlichten Chrome-Seamlessbrowser ausgeführt wird, wird die Anzeige möglicherweise nicht aktualisiert. Unter Umständen werden Elemente auf dem Bildschirm dupliziert und Mausklicks funktionieren nicht wie erwartet. [LD0777]
- Mehrere unerwünschte Fenster, die zu keinem Prozess oder keiner Anwendung gehören, werden möglicherweise auf der Taskleiste angezeigt. [LD1176]
- Die Citrix Workspace-App für Linux schlägt möglicherweise mit Verbindungsfehler 0.0.0.2 fehl. [LD1122]

Weitere Informationen finden Sie unter Kryptographische Aktualisierung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Behobene Probleme in Release 1901

- USB-Geräte, die an einen Endpunkt angeschlossen und einer VDA-Sitzung zugeordnet sind, können u. U. nicht in die Sitzung umgeleitet werden. Das Problem tritt auf, wenn Sie ein USB-Gerät innerhalb der Sitzung umbenennen und es dann trennen und erneut anschließen. [LD0111]
- Bestimmte Anwendungen von Drittanbietern funktionieren möglicherweise nicht ordnungsgemäß, wenn Sie sie über die Citrix Workspace-App für Linux starten. Das Problem tritt auf, wenn die Anwendungen die Prüfungen für das Hauptanwendungsfenster nicht bestehen, da dann keine Taskleistensymbole für diese Anwendungen erstellt werden. [LD0545]
- Client-zu-Server-Dateitypzuordnung funktioniert nur einmal pro Benutzer und Anmeldung. Informationen zum Öffnen einer lokalen Datei mit der zugehörigen veröffentlichten Anwendung finden Sie unter Zuordnen einer veröffentlichten Anwendung zu Dateitypen und Aktivieren von Dateitypzuordnung. [RFLNX-1363]

### Behobene Probleme in Release 1810

- Für bestimmte Zeitzonen wird möglicherweise eine falsche Uhrzeit für Kalendertermine angezeigt, wenn Sie die Versionen 1808 oder 1809 der Citrix Workspace-App für Linux verwenden. [LD0467]
- Versuche, Daten von Citrix Receiver für Linux über einen benutzerdefinierten virtuellen Kanal zu senden, schlagen möglicherweise fehl. [RFLNX-2288]

### Behobene Probleme in Release 1809

- Der Prozess wfica.exe wird beim Starten einer veröffentlichten Anwendung möglicherweise unerwartet beendet. Das Problem tritt auf, wenn mehrere Benutzer sich den Linux-Host teilen, auf dem Citrix Receiver für Linux 13.10 installiert ist. [LD0176]

### Behobene Probleme in Release 1808

- Bei aktivierter H.264-Codierung im Vollbildmodus wird der Textcursor in Anwendungen wie der Eingabeaufforderung und anderen Texteditoren nicht angezeigt. Als Workaround ist die Unterstützung kleiner Frames - eine Funktion des HDX “DeepCompressionV2”-Codecs - auf dem VDA deaktiviert (bis das Problem in der Citrix Workspace-App behoben ist). [RFLNX-2172]
- Das Flag **udtMSS** ist standardmäßig in der Datei All_Regions.ini aktiviert, damit die Citrix Workspace-App den Wert in der StoreFront-Datei default.ica file übernehmen kann. [RFLNX-2228]

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- Das Authentifizierungsdialogfeld ist hinter dem Sitzungsfenster im Vollbildmodus verborgen, wenn Sie ohne Eingabe Ihrer Anmeldeinformationen in die Sitzung klicken.
- Der Desktop Viewer, der auf bestimmten Bildschirmen zufällig verschwand, wird jetzt normal angezeigt.
- Wenn Sie eine Sitzung auf bestimmten Bildschirmen speichern, wird die Sitzung nach dem Neustart auf allen Bildschirmen angezeigt.
- Wenn Sie Benutzerabonnementdetails löschen, kann die Sitzung nicht erfolgreich gestartet werden.
- Wenn Sie auf **Layout speichern** klicken, reagiert die Sitzung nicht mehr. Dieses Problem tritt auf, wenn Sie mehrere Sitzungen von verschiedenen StoreFront-Instanzen aus starten, von denen nicht alle "Layout speichern" unterstützen.

## Bekannte Probleme

May 23, 2019

### Bekannte Probleme in Release 1903

- Beim Verwenden von Fedora 29 und höheren Versionen wird die Citrix Workspace-App für Linux unerwartet mit der Fehlermeldung "SIGSEGV" beendet. Dieses Problem tritt auf, weil Fedora Version 29 und höhere Versionen aufgrund von Inkompatibilität mit dem vom Betriebssystem zur Verfügung gestellten libidn-Paket derzeit nicht unterstützt werden. [LD0705]
- Das Citrix Optimization SDK-Paket enthält eine falschen Version von UIDialogLibWebKit.so. Führen Sie als Workaround die folgenden Schritte aus:

1. Laden Sie das Citrix Optimization SDK-Paket Version 18.10 von der Seite Downloads herunter.
2. Gehen Sie zum Pfad CitrixPluginSDK/UIDialogLib/GTK:

   ```
   cd CitrixPluginSDK/UIDialogLib/GTK
   ```

3. Löschen Sie alle Objektdateien:

   ```
   rm -rf *.o
   ```

4. Gehen Sie zum WebKit-Ordner:

   ```
   cd ../WebKit
   ```

5. Entfernen Sie die vorhandene Datei UIDialogLibWebKit.so:

   ```
   rm -rf UIDialogLibWebKit.so
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

6. Verwenden Sie den folgenden Befehl im WebKit-Verzeichnis:

   ```
   make all
   ```

   Die neue UIDialogLibWebKit.so wird generiert.

7. Kopieren Sie die neue Bibliothek in das Verzeichnis **$ICAROOT/lib**.

> **Hinweis:**
>
> Bevor Sie den Self-Service starten, beenden Sie die Prozesse AuthManagerDaemon und ServiceRecord. [RFLNX-2822]

### Bekannte Probleme in Release 1901

- In diesem Release wurden keine neuen Probleme festgestellt.

### Bekannte Probleme in Release 1810

- Sitzungen können möglicherweise über das Citrix Gateway keine Verbindung zu StoreFront herstellen. Das Problem tritt auf, wenn die Clientauthentifizierung obligatorisch ist. Als Workaround legen Sie die Clientauthentifizierung auf **Optional** fest oder deaktivieren Sie sie. [RFLNX-2431]

### Bekannte Probleme in Release 1809

- Die Funktion “In Dialogfeldern automatisch zur Standardschaltfläche springen” funktioniert manchmal nicht. [LD0843]

### Bekannte Probleme in Release 1808

- Beim Verwenden von storebrowse mit PNA-URL und einem abgelaufenen Kennwort wird der Bildschirm **Abgelaufenes Kennwort ändern** nicht angezeigt. [LC9129]

## Systemanforderungen und Kompatibilität

March 11, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

## Anforderungen

| Hardware | Requirements |
|---|---|
| Linux kernel | - Version 2.6.29 or later |
| Disk Space | - A minimum of 55 MB<br>- Additional 110 MB if you expand/extract the installation package on the disk<br>- A minimum of 1 GB RAM for system-on-a-chip (SoC) devices that use HDX MediaStream Flash Redirection |
| Color video display | - 256 color video display or higher |

| Libraries and Codec | Requirements |
|---|---|
| Libraries | - glibcxx 3.4.15 or later<br>- glibc 2.11.3 or later<br>- gtk 2.20.1 or later<br>- libcap1 or libcap2<br>- udev support |
| Self-service user interface | - libwebkit or libwebkitgtk 1.0<br>- libxml2 2.7.8<br>- libxerces-c 3.1 |
| Codec libraries | - Advanced Linux Sound Architecture (ALSA) libasound2<br>- Speex<br>- Vorbis codec libraries |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Components | Requirements |
|---|---|
| H.264 | For x86 devices:<br>- A minimum processor speed of 1.6 GHz<br>- Single-monitor sessions<br>- Display resolutions for example, 1280 x 1024 pixels |
| | For the HDX 3D Pro feature:<br>- A minimum processor speed of 2 GHz<br>- A native hardware with accelerated graphics driver |
| | For ARM devices:<br>- A hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro<br><br>**Note:**<br>Performance improves after using faster processor clock speeds. |
| HDX MediaStream Flash Redirection | For all HDX MediaStream Flash Redirection requirements, see http://support.citrix.com/article/CTX134786.<br><br>Citrix recommends testing with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes. |
| Customer Experience Improvement Program (CEIP) integration | - zlib 1.2.3.3<br>- libtar 1.2 and later<br>- libjson 7.6.1 or later |
| HDX RealTime Webcam Video Compression | - A Video4Linux compatible Webcam<br>- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| | |
|---|---|
| | Or<br><br>GStreamer 1.0 (or a later 1.x version), including the distribution's “plugins-base,” “plugins-good,” “plugins-bad,” “plugins-ugly,” and “gstreamer-libav” packages |
| HDX MediaStream Windows Media Redirection | - GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection<br><br>Or<br><br>GStreamer 1.0 (or a later 1.x version), including the distribution's “plugins-base,” “plugins-good,” “plugins-bad,” “plugins-ugly,” and “gstreamer-libav” packages<br><br>**Note:** If GStreamer is not included in your Linux distribution, you can download it from https://gstreamer.freedesktop.org/download/.<br><br>Use of certain codes (for example, those in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help. |
| Browser content redirection | - webkit2gtk version 2.16.6<br>- glibcxx 3.4.20 or later |
| Philips SpeechMike | - Visit the Philips web site to install the relevant drivers |

### Kompatibilitätsmatrix

Die Citrix Workspace-App für Linux 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.

### StoreFront und Webinterface

Sie können den browserbasierten Zugriff auf die Citrix Workspace-App für Linux 1808 und höher (mit oder ohne Citrix Gateway-Plug-In) in Kombination mit StoreFront Receiver für Web und dem Webinterface verwenden.

StoreFront:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- StoreFront 3.x, 2.6, 2.5 und 2.1

  Bietet direkten Zugriff auf StoreFront-Stores.

- StoreFront konfiguriert mit Workspace für Web

  Bietet Zugriff auf StoreFront-Stores über einen Webbrowser. Informationen zu den Beschränkungen dieser Bereitstellung finden Sie im Abschnitt “Wichtige Überlegungen” unter Citrix Receiver für Web-Sites.

Webinterface mit dem NetScaler VPN-Client:

- Webinterface 5.4 für Windows mit Webinterface-Sites

  Bietet Zugriff auf virtuelle Desktops und Apps über einen Webbrowser.

- Webinterface 5.4 für Linux mit XenApp Services- oder Citrix Virtual Desktops Service-Sites

### Bereitstellen der Citrix Workspace-App für Linux

Methoden der Bereitstellung der Citrix Workspace-App für Benutzer:

- Herunterladen der Citrix Workspace-App von der Citrix-Downloadseite und Konfiguration unter Verwendung einer E-Mail- oder Dienstadresse mit StoreFront.
- Angebot der Installation von Citrix Workspace für Web (mit StoreFront konfiguriert).
- Angebot der Installation der Citrix Workspace-App von Citrix Webinterface 5.4

## Verbindungen und Zertifikate

March 11, 2019

### 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
  - Webinterface 5.4 für Windows mit Webinterface oder XenApp Services
- Für sichere Remote- oder lokale Verbindungen:
  - Citrix Gateway 12.0
  - NetScaler Gateway 10.1 und höher

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 der Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installiert sein, um mit der Citrix Workspace-App auf Citrix Ressourcen zuzugreifen.

> **Hinweis:**
>
> Wenn das Zertifikat des Remotegateways beim Herstellen der Verbindung nicht verifiziert werden kann (da das Stammzertifikat nicht im lokalen Schlüsselspeicher vorhanden ist), wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Wenn der Benutzer weiterarbeitet, werden die Apps angezeigt, können jedoch nicht gestartet werden. Das Stammzertifikat muss im Zertifikatspeicher des Clients installiert werden.

### Stammzertifikate auf Benutzergeräten

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

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

### Installieren von Stammzertifikaten auf Benutzergeräten

Informationen zum Installieren von Stammzertifikaten auf Benutzergeräten und zum Konfigurieren von Zertifikaten auf dem Webinterface finden Sie unter Installieren von Stammzertifikaten in der Dokumentation zur Citrix Workspace-App für Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App für Linux unterstützt Zertifikate mit Platzhalterzeichen. Diese sollten jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden. In der Praxis kann die Verwendung von Alternativen, z. B. von Zertifikaten mit einer Liste der Servernamen in der Subject Alternative Name-Erweiterung, 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-Dokumentation.

#### Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

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

> **Wichtig:**
>
> Bestätigen Sie vor der Installation der Citrix Workspace-App für Linux, 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 für Linux jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases der Citrix Workspace-App für Linux wird dann auch überprüft, ob die Zertifikate vertrauenswürdig sind. Wenn nicht alle Zertifikate vertrauenswürdig sind, 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 der Citrix Workspace-App für Linux u. U. fehl.

Angenommen, ein Gateway ist mit gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen. Dabei wird genau ermittelt, welches Stam-

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

mzertifikat die Citrix Workspace-App für Linux verwendet:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Beispielstammzertifikat”

Die Citrix Workspace-App für Linux überprüft dann, ob alle Zertifikate gültig sind. Die Citrix Workspace-App für Linux überprüft ebenfalls, ob dem “Beispielstammzertifikat” bereits vertraut wird. Wenn die Citrix Workspace-App für Linux 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 für Linux-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.

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

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

Die Citrix Workspace-App für Linux verwendet dann diese beiden Zertifikate. Dann sucht die App nach einem Stammzertifikat auf dem Benutzergerät. Wird ein gültiges Zertifikat gefunden, das auch vertrauenswürdig ist (z. B. “Beispielstammzertifikat”), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt der Citrix Workspace-App für Linux das benötigte Zwischenzertifikat zur Verfügung und ermöglicht auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

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

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- “Falsches Stammzertifikat”

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

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

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

> **Wichtig:**
>
> - Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat. Dies ist für Situationen vorgesehen, wenn mehr als ein Stammzertifikat vorhanden ist und ein früher ausgestelltes Stammzertifikat zur gleichen Zeit wie ein später ausgestelltes Stammzertifikat verwendet wird. 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”.

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

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

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

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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

- “Beispielserverzertifikat”

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

## Installation und Einrichtung

April 17, 2019

Die folgenden Pakete sind verfügbar.

| Paketname | Inhalt |
|---|---|
| **Debian-Pakete (Ubuntu, Debian, Linux Mint usw.)** | |
| icaclient_19.3.0.5_amd64.deb | Self-Service-Support, 64 Bit, x86_64 |
| icaclient_19.3.0.5_i386.deb | Self-Service-Support, 32 Bit, x86 |
| icaclient_19.3.0.5_armhf.deb | Self-Service-Support, ARM HF |
| icaclientWeb_19.3.0.5_amd64.deb | nur Web Receiver, 64 Bit, x86_64 |
| icaclientWeb_19.3.0.5_i386.deb | nur Web Receiver, 32 Bit, x86 |
| icaclientWeb_19.3.0.5_armhf.deb | nur Web Receiver, ARM HF |
| ctxusb_2.7.5_amd64.deb | USB-Paket, 64 Bit, x86_64 |
| ctxusb_2.7.5_i386.deb | USB-Paket, 32 Bit, x86 |
| ctxusb_2.7.5_armhf.deb | USB-Paket, ARM HF |
| **Redhat-Pakete (Redhat, SUSE, Fedora usw.)** | |
| ICAClient-rhel-19.3.0.5-0.x86_64.rpm | Self-Service-Support, basierend auf Red Hat (einschl. Linux-VDA), 64 Bit, x86_64 |
| ICAClient-rhel-19.3.0.5-0.i386.rpm | Self-Service-Support, basierend auf RedHat, 32 Bit, x86 |
| ICAClientWeb-rhel-19.3.0.5-0.x86_64.rpm | nur Web Receiver, basierend auf Red Hat, 64 Bit, x86_64 |
| ICAClientWeb-rhel-19.3.0.5-0.i386.rpm | nur Web Receiver, basierend auf RedHat, 32 Bit, x86 |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Paketname | Inhalt |
|---|---|
| ICAClient-suse-19.3.0.5-0.x86_64.rpm | Self-Service-Support, basierend auf SUSE, 64 Bit, x86_64 |
| ICAClient-suse-19.3.0.5-0.i386.rpm | Self-Service-Support, basierend auf SUSE, 32-Bit, x86 |
| ICAClient-suse11sp3-19.3.0.5-0.x86_64.rpm | Self-Service-Support, basierend auf SUSE 11 sp3 (einschl. Linux-VDA), 64 Bit, x86_64 |
| ICAClient-suse11sp3-19.3.0.5-0.i386.rpm | Self-Service_Support, basierend auf SUSE 11 sp3, 32-Bit, x86 |
| ICAClientWeb-suse-19.3.0.5-0.x86_64.rpm | nur Web Receiver, basierend auf SUSE, 64 Bit, x86_64 |
| ICAClientWeb-suse-19.3.0.5-0.i386.rpm | nur Web Receiver, basierend auf SUSE, 32 Bit, x86 |
| ctxusb-2.7.5-1.x86_64.rpm | USB-Paket, 64 Bit, x86_64 |
| ctxusb-2.7.5-1.i386.rpm | USB-Paket, 32 Bit, x86 |
| **Tarballs (Skriptinstallation für jede Distribution)** | |
| linuxx64-19.3.0.5.tar.gz | 64 Bit Intel |
| linuxx86-19.3.0.5.tar.gz | 32 Bit Intel |
| linuxarmhf-19.3.0.5.tar.gz | ARM HF |

Der Unterschied zwischen den Paketen für die Web Workspace-App und für Self-Service ist, dass die Pakete mit Unterstützung für Self-Service die dafür erforderlichen Abhängigkeiten enthalten (zusätzlich zu den für die Web Workspace-App erforderlichen Abhängigkeiten). Die Abhängigkeiten für Self-Service sind eine Obermenge der für die Web Workspace-App erforderlichen Abhängigkeiten. Die installierten Dateien sind jedoch identisch.

Wenn Sie nur Unterstützung für die Web Workspace-App benötigen oder Ihre Distribution nicht die erforderlichen Pakete für Self-Service umfasst, installieren Sie nur das Paket für die Web Workspace-App.

> **Hinweis:**
>
> Wenn Ihre Distribution es zulässt, installieren Sie die Citrix Workspace-App vom Debian- oder RPM-Paket. Diese Dateien sind einfacher zu verwenden, da sie automatisch alle erforderlichen Pakete installieren.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> Wenn Sie den Installationsort steuern möchten, installieren Sie die Citrix Workspace-App vom Tarball-Paket.
>
> Verwenden Sie nicht beide Installationsmethoden auf derselben Maschine. Wenn Sie beispielsweise die Citrix Workspace-App für Linux mit einem Tarball-Paket auf einer Maschine installieren, auf der die Citrix Workspace-App für Linux bereits mit einem Debian-Paket installiert wurde, treten wahrscheinlich Fehlermeldungen und unerwünschtes Verhalten auf.

### Installieren der Citrix Workspace-App für Linux von einem Debian-Paket

Wenn Sie die Workspace-App mit dem Debian-Paket unter Ubuntu installieren, ist es u. U. bequemer, die Pakete im Ubuntu Software Center zu öffnen.

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

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

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 der folgenden 3 Pakete aus, indem Sie `gdebi packagename.deb` eingeben. Beispiel:
   - `gdebi icaclient\\_18.9.0.6\\_amd64.deb`
   - `gdebi icaclientWeb\\_18.9.0.6\\_i386.deb`
   - `gdebi ctxusb\\_2.7.6\\_amd64.deb`

   > **Hinweis:**
   >
   > Um in den obigen Beispielen dpkg zu verwenden, ersetzen Sie “gdebi” mit “dpkg -i”.

   Sie müssen das icaclient-Paket oder das icaclientWeb-Paket installieren. Das ctxusb-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.
4. Wenn Sie dpkg verwenden, installieren Sie fehlende Abhängigkeiten durch Eingabe von sudo **apt-get -f install**.
5. Akzeptieren Sie die Lizenzvereinbarung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Installieren der Citrix Workspace-App für Linux von einem RPM-Paket

Wenn Sie die Citrix Workspace-App vom RPM-Paket auf SUSE installieren, verwenden Sie das Hilfsprogramm YaST oder Zypper, nicht das RPM-Hilfsprogramm. Das RPM-Hilfsprogramm installiert nur das RPM-Paket. Es lädt die benötigten Abhängigkeiten nicht herunter und installiert sie nicht. Wenn die erforderlichen Abhängigkeiten fehlen, tritt ein Fehler auf.

> **Hinweis:**
>
> Ein Beispiel für eine Installation mit einem RPM-Paket finden Sie im Citrix Blog-Artikel Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop.

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

> **Hinweis:**
>
> Wenn in einer Fehlermeldung angezeigt wird, dass libwebkitgtk-1.0.so.0 für eine Installation auf Red Hat-basierten Distributionen (RHEL, CentOS, Fedora, usw.) erforderlich ist, fügen Sie das EPEL-Repository hinzu (weitere Informationen finden Sie unter https://fedoraproject.org/wiki/EPEL), das das fehlende Paket bereitstellt oder zur Webversion des Pakets wechselt.

### Einrichten des EPEL-Repositorys auf Red Hat

1. Laden Sie das entsprechende RPM-Quellpaket hier herunter:

   https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F

2. Beispiel für Red Hat Enterprise 7.x:

   **yum localinstall epel-release-latest-7 .noarch.rpm**

   > **Tipp:**
   >
   > RPM Package Manager installiert keine fehlende erforderliche Software. Citrix empfiehlt für den Download und die Installation die Verwendung von **zypper install <Dateiname>** an einer Befehlszeile unter OpenSUSE oder **yum localinstall <Dateiname>** unter Fedora/Red Hat.

Installieren der Workspace-App mit dem RPM-Paket nach dem Setup des EPEL-Repositorys

1. Melden Sie sich als privilegierter Benutzer (root) an.
2. Führen Sie die Installation der folgenden drei Pakete aus, indem Sie “zypper” in package-name.rpm eingeben.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **Hinweis:**
>
> Ein Benutzer muss das icaclient-Paket oder das icaclientWeb-Paket installieren. Das ctxusb-Paket ist optional und bietet Unterstützung für die generische USB-Umleitung.

3. Öffnen Sie ein Terminal-Fenster.

   Für SUSE-Installationen:

   zypper in ICAClient-suse-18.9.0.6-0.x86_64.rpm

   zypper in ICAClient-suse-18.9.0.6-0.i386.rpm

   zypper in ctxusb-2.7.6-1.x86_64.rpm

   Für Red Hat-Installationen:

   yum localinstall ICAClient-rhel-18.9.0.6-0.i386.rpm

   yum localinstall ICAClientWeb-rhel-18.9.0.6-0.i386.rpm

   yum localinstall ctxusb-2.7.6-1.i386.rpm

4. Akzeptieren Sie die Lizenzvereinbarung.

**Installieren der Citrix Workspace-App für Linux von 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. Entpacken Sie die TAR.GZ-Datei und extrahieren Sie den Dateiinhalt 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 (Workspace-App installieren) und drücken Sie die Eingabetaste.
5. Geben Sie den Pfad und den Namen des gewünschten Installationsverzeichnisses ein und drücken Sie die Eingabetaste oder drücken Sie die Eingabetaste, um die Workspace-App im Standardverzeichnis zu installieren.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Das Standardverzeichnis für Installationen durch nicht-privilegierte Benutzer ist $HOME/ICAClient/platform. “platform” ist ein systemgenerierter Bezeichner des installierten Betriebssystems. Beispiel: $HOME/ICAClient/linuxx86 für die Plattform Linux/x86)

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

6. Geben Sie “y” ein und drücken Sie die Eingabetaste, wenn Sie zum Fortfahren aufgefordert werden.
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 installiert haben, können Sie entscheiden, ob Sie GStreamer in die Citrix Workspace-App integrieren und damit die HDX Mediastream-Multimediabeschleunigung bereitstellen. Um die Citrix Workspace-App mit GStreamer zu integrieren, geben Sie an der Eingabeaufforderung “y” ein.

   > **Hinweis:**
   >
   > Auf einigen Plattformen kann die Installation des Clients mit einer Tarball-Distribution dazu führen, dass das System hängen bleibt, 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**. Nachdem der Befehl ausgeführt wurde, sollten Sie den Tarball-Setup erneut ausführen können, ohne dass das System hängen bleibt.

9. Wenn Sie sich als privilegierter Benutzer (root) anmelden, können Sie entscheiden, ob Sie die USB-Unterstützung für mit Citrix Virtual Apps and Desktops 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 Warnung 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 Setupprogramms “3” ein und drücken Sie die Eingabetaste.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

# Anpassen einer Citrix Workspace-App für Linux-Installation

January 22, 2019

Sie können eine Konfiguration vor der Installation anpassen, indem Sie den Inhalt des Citrix Workspace-App-Pakets bearbeiten und die Dateien dann neu verpacken. Alle Installationen, die Sie mit diesem bearbeiteten Paket ausführen, enthalten dann Ihre Änderungen.

## Anpassen einer Citrix Workspace-App für Linux-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. linuxx86.13.2.0.nnnnnn.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, wenn Sie ein Zertifikat einer Zertifizierungsstelle verwenden möchten, die nicht Teil der standardmäßigen Citrix Workspace-App-Installation ist. Informationen, wie Sie dem Paket ein TLS-Stammzertifikat hinzufügen, finden Sie unter “Installieren von Stammzertifikaten auf Benutzergeräten” auf der Citrix Website mit der Produktdokumentation.
   Weitere Informationen über integrierte Zertifikate finden Sie unter “Konfigurieren und Aktivieren von SSL und TLS” auf der Citrix Website mit der Produktdokumentation.
3. Öffnen Sie die PkgID-Datei.
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. Ein spezielles Format muss für diese Informationen nicht verwendet werden.
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. Wenn Sie diese Datei nicht aktualisieren, können bei der Installation des neuen Pakets 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
   - Unterpaket (hierfür muss immer cor eingestellt sein)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 *
> Hierbei ist “newpackage” der Name der neuen Paketdatei der Citrix Workspace-App.

## Starten der Citrix Workspace-App für Linux

December 21, 2018

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

Wenn die Citrix Workspace-App nicht im Standardverzeichnis installiert wurde, muss die Umgebungsvariable ICAROOT auf das richtige Installationsverzeichnis verweisen.

> **Tipp:**
>
> Die folgenden Anweisungen gelten nicht für mit Webpaketen oder Tarball ausgeführte Installationen, sondern wenn die Anforderungen für den Self-Service nicht erfüllt sind.

### Starten der Citrix Workspace-App an einer Terminal-Eingabeaufforderung

Geben Sie Folgendes an der Terminal-Eingabeaufforderung ein:

```
/opt/Citrix/ICAClient/selfservice
```

Hierbei ist /opt/Citrix/ICAClient das Verzeichnis, in dem Sie die Citrix Workspace-App installiert haben. Drücken Sie dann die Eingabetaste.

### Starten der Citrix Workspace-App vom Linux-Desktop

Mithilfe eines Dateimanagers können Sie die Citrix Workspace-App von einer Desktopumgebung für Linux aus starten.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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.

## Verwenden der Citrix Workspace-App für Linux als ICA-zu-X-Proxy

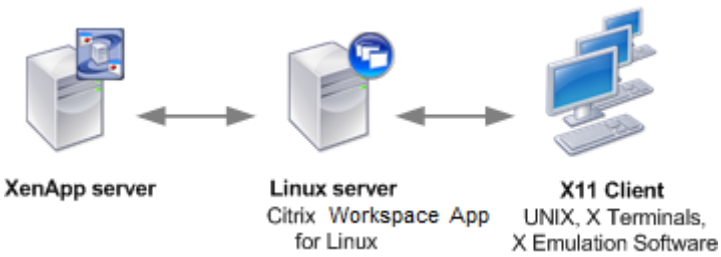
February 18, 2019

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 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 mehrere Kopien der Citrix Workspace-App gleichzeitig auf einem System ausführen und dabei festlegen, dass jede Kopie die Ausgabe an ein anderes Gerät sendet.

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.
- Wenn Sie UNIX-Workstations einsetzen möchten, für die es die Citrix Workspace-App nicht gibt, benötigen Sie einen eigenen Server, der als Proxy dient. Hier wäre ein PC, auf dem Linux ausgeführt wird, denkbar.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Unterstützte Features

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. Dies ist bei Einsatz von X-Terminals kein Problem (diese haben normalerweise keine lokalen Laufwerke). Wenn Sie Anwendungen anderen UNIX-Workstations bereitstellen, können Sie Folgendes tun:

- Einhängen der lokalen UNIX-Workstation über NFS auf der als Proxy dienenden Workstation und dann Verweisen einer Clientlaufwerkzuordnung auf den NFS-Einhängepunkt (Mount Point) 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.
- Die Umleitung von Multimedia-Eingaben funktioniert voraussichtlich nicht, da hierfür auf der Maschine, die die Citrix Workspace-App ausführt, eine Webcam erforderlich ist. 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>

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

4. Wenn die Citrix Workspace-App nicht im Standardverzeichnis installiert wurde, muss die Umgebungsvariable ICAROOT auf das richtige Installationsverzeichnis verweisen.
5. Suchen Sie das Verzeichnis, in dem die Citrix Workspace-App installiert ist. Geben Sie an einer Eingabeaufforderung “selfservice &” ein.

## Konfigurieren des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

September 7, 2018

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit Citrix die Qualität und Leistung seiner Produkte verbessern kann. Weitere Informationen zum CEIP finden Sie unter Citrix Programm zur Verbesserung der Benutzerfreundlichkeit.

Sie werden standardmäßig automatisch beim CEIP registriert, wenn Sie die Citrix Workspace-App für Linux installieren. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation der Citrix Workspace App. Die für aktive Benutzer gesammelten Daten werden alle sieben Tage auf den CIS-Server hochgeladen.

Registrierungseinstellung zur Steuerung der Registrierung in CEIP:

- Speicherort: <ICAROOT>/config/module.ini
- Abschnitt: CEIP
- Eintrag: EnableCeip
- Wert: Enable (Standard) / Disable

Die folgenden anonymen Informationen werden gesammelt. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren. Wenn EnableCeip auf “Disable” festgelegt ist, werden nur die Citrix Workspace-App-Versionsinformationen gesammelt.

| Datenpunkt | Beschreibung |
|---|---|
| Maschinen-ID | Identifiziert die Maschine, von der die Daten stammen. |
| Linux-Kernelversion | Die Zeichenfolge steht für die Kernelversion der Maschine. |
| Linux-OS-Name und -Version | Zeichenfolge, die den Linux-OS-Namen und die Linux-OS-Version der Maschine angibt. |
| Datum der Datensammlung | Das Datum, an dem die Datenerfassung erfolgt. |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Datenpunkt | Beschreibung |
| --- | --- |
| CPU-Modellname | Das CPU-Modell der Clientmaschine. |
| Systemspeicherinformationen | Sammelt Systemspeicherinformationen, u. a. gesamter RAM, verfügbarer RAM, Puffer-RAM, gemeinsam verwendeter RAM, gesamter Auslagerungsspeicher, verfügbarer Auslagerungsspeicher und die Anzahl der aktuellen Prozesse. |
| Bildschirmauflösung | Die Bildschirmauflösung der Clientmaschine. |
| Desktopumgebung | Informationen, ob die aktuell verwendete Desktopumgebung vom Typ -XDG_CURRENT_DESKTOP oder DESKTOP_SESSION ist. |
| Browserversion | Ruft Informationen über den verwendeten Browser ab: Firefox, Chrome usw. |
| USB-Geräteinformationen | Ruft Informationen zu den auf dem Clientsystem verfügbaren USB-Ports ab. |
| Flash-Version | Ruft Informationen zur verwendeten Flash-Version ab. |
| Gebietsschemaversion | Die Version des Gebietsschemas. |
| Sprachinformationen | Tastaturzuordnung und entsprechende Informationen. |
| Schemainformationen | Die Schemainformationen für die Citrix Workspace-App. |
| Multimediaumleitung | Boolescher Wert, der anzeigt, ob dieses Feature aktiviert ist. |
| Webcamumleitung | Boolescher Wert, der anzeigt, ob die Webcamumleitung aktiviert ist. |
| Flash-Umleitung | Boolescher Wert, der anzeigt, ob die Flash-Umleitung aktiviert ist. |
| MediaStream | Boolescher Wert, der anzeigt, ob MediaStream aktiviert ist. Dies schließt SpeedScreen-Audio- und Videofunktionen ein. |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

## Deinstallieren der Citrix Workspace-App für Linux

December 21, 2018

Dieses Verfahren wurde mit dem Tarball-Paket getestet. Entfernen Sie das RPM- und Debian-Paket mit den Standardtools des Betriebssystems.

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 eine vom System erstellte Kennung für das installierte Betriebssystem. Beispiel: $HOME/ICAClient/linuxx86 für die Plattform Linux/x86 Das Standardverzeichnis für Installationen durch privilegierte Benutzer ist /opt/Citrix/ICAClient.

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.

> **Hinweis:**
>
> Um die Citrix Workspace-App für Linux zu deinstallieren, müssen Sie als der Benutzer angemeldet sein, der die Installation durchgeführt hat.

## Verbinden

March 11, 2019

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

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

Die Homepage der Citrix Workspace-App zeigt virtuelle Desktops und Anwendungen an, die Benutzern basierend auf deren Kontoeinstellungen (d. h. dem Server, mit dem sie eine Verbindung herstellen) und basierend auf den von Citrix Virtual Apps and Desktops-Administratoren konfigurierten Einstellungen zur Verfügung stehen. Mit der Seite Einstellungen > Konten können Benutzer die Konfiguration selbst vornehmen, indem sie die URL eines StoreFront-Servers oder, wenn die E-Mail-basierte Kontenermittlung konfiguriert ist, ihre E-Mail-Adresse eingeben.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **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 PNAgent wird die Store-URL angezeigt, die den Store eindeutig identifiziert.

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 für Linux und Citrix Virtual Apps and Desktops-Servern konfigurieren. Sie können diese Einstellungen ggf. für einzelne Verbindungen ändern.

Die Informationen im übrigen Teil enthalten Verfahren für typische, von Benutzern der Citrix Workspace-App ausgeführte Aufgaben. Obwohl sich die Aufgaben und Verantwortungsbereiche von Administratoren und Benutzern überschneiden können, wird der Ausdruck “Benutzer” in diesem Abschnitt dort verwendet, wo Aufgaben beschrieben werden, die normalerweise von Benutzern und nicht von Administratoren ausgeführt werden.

- Verbinden mit Ressourcen per Eingabeaufforderung oder Browser
- Problembehandlung bei Verbindungen mit Ressourcen
- Anpassen der Citrix Workspace-App mit Konfigurationsdateien

## Verbinden mit Ressourcen per Eingabeaufforderung oder Browser

December 21, 2018

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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

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

```
./util/storebrowse –addstore <Store-URL>
```

1. Rufen Sie die eindeutige ID des Desktops oder der Anwendung auf, mit dem bzw. der Sie eine Verbindung herstellen möchten. Dies 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>
     ```

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

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

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

   ```
   ./util/storebrowse –L <Desktop- oder Anwendungs-ID> <Store-URL>
   ```

Wenn Sie keine Verbindung zu einem Server herstellen können, muss der Administrator möglicherweise die Angaben für den Serverstandort oder den SOCKS-Proxyserver ändern. Weitere Informationen finden Sie unter
Herstellen von Verbindungen über 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, sodass die ICA-Dateien die ausführbare Citrix Workspace-App-Datei wfica starten. 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

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

```
setenv 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).

## Problembehandlung bei Verbindungen mit Ressourcen

September 7, 2018

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.

© 1999-2019 Citrix Systems, 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

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

   Die verwendeten Server und die für jeden Server aktiven Sitzungen werden aufgelistet.

2. Führen Sie einen der folgenden Schritte aus:

   - Wählen Sie einen Server aus und trennen Sie die Verbindung, melden Sie sich ab oder zeigen Sie die Eigenschaften des Servers an.
   - Wählen Sie eine Anwendung aus und schließen Sie das Fenster, in dem der Desktop bzw. die Anwendung angezeigt wird.

## Anpassen mit Konfigurationsdateien

December 21, 2018

### 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.

### Anwenden von Standardwerten auf alle Citrix Workspace-App-Benutzer

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **Hinweis:**
>
> Sie brauchen All_Regions.ini keinen Eintrag hinzufügen, damit ein Konfigurationswert aus der Datei module.ini gelesen wird. Sie können dies jedoch tun, es sei denn, Sie möchten zulassen, dass andere Konfigurationsdateien den Wert in module.ini überschreiben. Wenn mit einem Eintrag in All_Regions.ini ein spezifischer Wert festgelegt wird, wird der Wert in module.ini nicht verwendet.

### Anwenden von Änderungen auf neue Citrix Workspace-App-Benutzer

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 zukünftigen Citrix Workspace-App-Benutzer angewendet.

### Anwenden von Änderungen auf alle Verbindungen bestimmter Benutzer

Wenn Ihre Änderungen für alle Verbindungen für einen bestimmten Benutzer gelten sollen, bearbeiten Sie die Datei wfclient.ini im Verzeichnis $HOME/.ICAClient des Benutzers. Die Einstellungen in dieser Datei gelten für zukünftige Verbindungen für diesen Benutzer.

### Überprüfen von Einträgen in Konfigurationsdateien

Wenn Sie die Werte für Einträge in wfclient.ini beschränken möchten, können Sie die zulässigen Optionen oder Optionsbereiche in der Datei All_Regions.ini festlegen. Wenn Sie nur einen möglichen Wert angeben, wird dieser Wert verwendet. $HOME/.ICAClient/All_Regsions.ini kann nur mit den in $ICAROOT/config/All_Regions.ini angegebenen Werten übereinstimmen oder sie reduzieren. Beschränkungen können nicht aufgehoben werden. Weitere Informationen finden Sie in der Datei All_Regions.ini im Verzeichnis $ICAROOT/config.

> **Hinweis:**
>
> Wenn ein Eintrag in mehr als einer Konfigurationsdatei enthalten ist, hat der Wert in wfclient.ini Vorrang vor dem Wert in module.ini.

### Parameter in den Dateien

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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Standardwerte werden, sofern nicht anders angegeben, automatisch für alle fehlenden Parameter eingesetzt. Wenn ein Parameter keinen Wert besitzt, wird automatisch der Standardwert angewendet. Beispiel: Wenn auf “InitialProgram” ein Gleichheitszeichen (=) ohne Wert folgt, wird der Standardwert (nach der Anmeldung kein Programm ausführen) angewendet.

### Rangfolge

Über All_Regions.ini wird bestimmt, welche Parameter 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. Werte in dieser Datei haben Vorrang vor:
    - ICA- Datei der Verbindung
    - wfclient.ini
2. module.ini Die Werte in dieser Datei werden verwendet, wenn sie nicht in All_Regions.ini, der ICA- Datei der Verbindung oder in wfclient.ini festgelegt wurden. Sie 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, um sicherzustellen, dass sie nicht von einem Server festgelegt wurden.

## Konfigurieren

February 18, 2019

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.

### Konfigurieren von Citrix Virtual Apps-Verbindungen mit dem Webinterface

Dieser Abschnitt gilt nur für Bereitstellungen, die Citrix Virtual Apps Services auf dem Webinterface oder “legacy PNAgent” auf StoreFront verwenden.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Mit Optionen wie self-service, storebrowse und pnabrowse können Benutzer über einen Server, auf dem eine Citrix Virtual Apps Services-Site ausgeführt wird, eine Verbindung zu veröffentlichten Ressourcen (veröffentlichten Anwendungen und Serverdesktops) herstellen. Diese Programme können Verbindungen direkt starten oder sie können zum Erstellen von Menüelementen verwendet werden, über die Benutzer auf veröffentlichte Ressourcen zugreifen können. Mit pnabrowse können für diesen Zweck auch Desktopelemente erstellt werden.

Einstellbare Optionen für alle Benutzer, die Citrix Virtual Apps im Netzwerk ausführen, sind in der Konfigurationsdatei config.xml festgelegt, die auf dem Webinterface-Server gespeichert ist. Wenn ein Benutzer eines dieser Programme startet, liest es die Konfigurationsdaten vom Server und aktualisiert anschließend die Einstellungen und die Benutzeroberfläche in regelmäßigen Abständen wie in der Datei config.xml festgelegt.

> **Wichtig:**
>
> Die Datei config.xml gilt für alle Verbindungen, die von der Citrix Virtual Apps Services-Site definiert werden.

### Veröffentlichen von Inhalten

Eine Citrix Virtual Apps Services-Site 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 für Linux erkennt nicht alle Dateitypen. Das System erkennt nur dann den Dateityp der veröffentlichten Inhalte und die Benutzer können die Inhalte nur dann über die Citrix Workspace-App anzeigen, wenn eine Zuordnung zwischen einer veröffentlichten Anwendung und dem Dateityp der veröffentlichten Datei besteht. 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 veröffentlichten Inhalt nur anzeigen, wenn eine geeignete Anwendung veröffentlicht ist.

### Konfigurieren der Verwendung von Smartcards

Um die Smartcard-Unterstützung in Citrix Workspace-App für Linux zu konfigurieren, müssen Sie den StoreFront-Server über die StoreFront-Konsole so konfigurieren, dass Smartcard-Authentifizierung zulässig ist. Aktivieren Sie das erforderliche Protokoll über die StoreFront-Konsole.

> **Hinweis:**
>
> Smartcards werden nicht für Konfigurationen mit der Citrix Virtual Apps Services-Site für Webinterface (früher Program Neighborhood Agent) oder mit der “Legacy-PNAgent”-Site unterstützt,

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> die von einem StoreFront-Server bereitgestellt werden können.

Die Citrix Workspace-App für Linux unterstützt Smartcardleser, die mit PCSC-Lite kompatibel sind, und Smartcards mit PKCS#11-Treibern für die entsprechende Linux-Plattform. Standardmäßig sucht die Citrix Workspace-App für Linux nach `opensc-pkcs11.so` in einem der Standardspeicherorte. Damit die Citrix Workspace-App für Linux `opensc-pkcs11.so` in einem Speicherort findet, der kein Standardspeicherort ist, oder aber einen anderen PKCS#11-Treiber findet, speichern Sie den Speicherort in einer Konfigurationsdatei:

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 zur Datei. Sie können auch einen absoluten Pfad verwenden, der mit "/" beginnt.

Sie konfigurieren das Verhalten der Citrix Workspace-App für Linux, wenn die Smartcard entfernt wird, indem Sie SmartCardRemovalAction in der Konfigurationsdatei wie folgt aktualisieren:

1. Suchen Sie die Konfigurationsdatei: $ICAROOT/config/AuthManConfig.xml
2. Suchen Sie die Zeile <key>SmartCardRemovalAction</key> und fügen Sie dem Element <value> "noaction" oder "forcelogoff" hinzu, das direkt der Zeile folgt.

Das Standardverhalten ist "noaction". Keine Aktion wird zum Löschen der gespeicherten Anmeldeinformationen und Token unternommen, die hinsichtlich der Smartcard beim Entfernen der Smartcard erstellt werden. Mit der Aktion "forcelogoff" werden alle Anmeldeinformationen und Token beim Entfernen der Smartcard in StoreFront entfernt.

### Einführung von Workspace Launcher

Bisher ermöglichte das zusammen mit der Citrix Workspace-App für Linux bereitgestellte Browser-Plug-In Benutzern das Starten veröffentlichter Desktops und Anwendungen. Dieses Plug-In basierte auf dem Netscape Plugin Application Programming Interface (NPAPI).

Die Mozilla Corporation hat angekündigt, dass die NPAPI-Unterstützung ab Version 52 des Firefox-Browsers eingestellt wird. Andere Browser haben die Unterstützung für NPAPI ebenfalls eingestellt. Daher hat Citrix den Workspace Launcher (WebHelper) eingeführt.

Citrix Workspace Launcher funktioniert über direkte Verbindungen zu StoreFront und über Citrix Gateway.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

# Optimieren

May 23, 2019

Durch Optimieren Ihrer Umgebung erhalten Sie die beste Leistung der Citrix Workspace-App und bieten die beste Benutzererfahrung.

## Zuordnen von Benutzergeräten

Die Citrix Workspace-App unterstützt Clientgerätzuordnung für Verbindungen zu Citrix Virtual Apps and Desktops-Servern. Mit der Clientgerätzuordnung 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. Vergewissern Sie sich, 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 (unter Citrix Virtual Apps and Desktops) auswirken. Wenn Sie eines dieser Features (oder beide) benötigen, deaktivieren Sie SELinux, bevor Sie es auf dem Server konfigurieren.

### Zuordnen von Clientlaufwerken

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf dem Citrix Virtual Apps- oder Citrix Virtual Desktops-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 Clientlaufwerkzuordnung werden alle auf dem lokalen Benutzergerät bereitgestellten Verzeichnisse, einschließlich CDs, DVDs oder USB-Sticks, in Sitzungen für den Benutzer verfügbar, wenn der lokale Benutzer Zugriffsrechte hat. Wenn ein Server für die Clientlaufwerkzuordnung konfiguriert ist, können Benutzer auf lokal gespeicherte Dateien zugreifen, diese in ihren Sitzungen bearbeiten und dann entweder auf einem lokalen Laufwerk oder einem Laufwerk auf dem Server speichern.

Es gibt zwei Arten von Laufwerkzuordnung:

- Die statische Clientlaufwerkzuordnung ermöglicht es Administratoren, einen beliebigen Teil des Dateisystems auf dem Benutzergerät bei der Anmeldung einem bestimmten Laufwerksbuchstaben auf dem Server zuzuordnen. Sie können damit beispielsweise das gesamte Basisverze-

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

ichnis oder einen Teil davon sowie die Bereitstellungspunkte von Hardwaregeräten, wie CD-ROMs, DVDs oder USB-Sticks, zuordnen.
- Die dynamische Clientlaufwerkzuordnung überwacht die Verzeichnisse, in denen Hardwaregeräte 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 oder Citrix Virtual Desktops 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 unter Citrix Virtual Apps and Desktops.

Benutzer können Laufwerke im Dialogfeld Einstellungen zuordnen.

> **Hinweis:**
>
> Standardmäßig wird durch das Aktivieren der statischen Clientlaufwerkzuordnung auch die dynamische Clientlaufwerkzuordnung aktiviert. Damit beim Aktivieren der statischen Clientlaufwerkzuordnung die dynamische Clientlaufwerkzuordnung nicht aktiviert wird, legen Sie “DynamicCDM” in wfclient.ini auf “False” fest.

#### Zuordnen von Clientdruckern

Die Citrix Workspace-App unterstützt das Drucken auf Netzwerkdruckern und auf lokal an Benutzergeräte angeschlossenen Druckern. Citrix Virtual Apps 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 außerdem erforderlich machen, dass Sie das benutzerseitige Zuordnen lokaler Druckerports nicht zulassen. Hierfür stellen Sie auf dem Server die ICA-Richtlinieneinstellung “Client-COM-Ports automatisch verbinden” auf “Deaktiviert” ein.

#### Einschränken der Liste der auf dem Benutzergerät konfigurierten Drucker

1. Öffnen Sie die Konfigurationsdatei wfclient.ini in einem der folgenden Verzeichnisse:

© 1999-2019 Citrix Systems, 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=Drucker1:Drucker2:Drucker3

   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 von Clientdruckern auf Citrix Virtual Apps für Windows

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 für Windows jedoch 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 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 denen, die durch native Remotedesktopdienste erstellt werden, z. B. “HPLaserJet 4 von Clientname in Sitzung 3”.

   Weitere Informationen zum Hinzufügen von Druckern finden Sie in der Dokumentation zum Windows-Betriebssystem.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Zuordnen von Clientdruckern auf Citrix Virtual Apps für UNIX

In UNIX-Umgebungen werden von der Citrix Workspace-App definierte Druckertreiber ignoriert. Das Drucksystem auf dem Benutzergerät muss in der Lage sein, das von der Anwendung erzeugte Druckformat zu verarbeiten.

Bevor Benutzer von Citrix Virtual Apps für UNIX auf einem Clientdrucker drucken können, muss der Systemadministrator diese Funktion aktivieren. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation im Abschnitt über Citrix Virtual Apps für UNIX.

### Zuordnen von Clientaudio

Die Clientaudiozuordnung ermöglicht es, dass auf Citrix Virtual Apps-Servern oder Citrix Virtual Desktops 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 Prozessorzeit auf dem Server in Anspruch genommen.

Sie können die Clientaudiozuordnung mit Richtlinien konfigurieren. Weitere Informationen finden Sie in der Dokumentation unter Citrix Virtual Apps and Desktops.

> **Hinweis:**
>
> Clientaudiozuordnung steht nicht bei einer Verbindung zu Citrix Virtual Apps für UNIX zur Verfügung.

### Festlegen eines anderen Geräts als das Standardaudiogerät

Das Standardaudiogerät ist 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 Anpassen der Workspace-App mit Konfigurationsdateien.
2. Fügen Sie die folgende Option hinzu. Wenn dieser Abschnitt nicht vorhanden ist, erstellen Sie ihn.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

[ClientAudio]

AudioDevice =

Die Informationen für Gerät befinden sich in der ALSA-Konfigurationsdatei auf Ihrem Betriebssystem.

> **Hinweis:**
>
> Der Speicherort für diese Informationen ist nicht auf allen Linux-Betriebssystemen einheitlich. Citrix empfiehlt, in der Dokumentation Ihres Betriebssystems nachzulesen, wo Sie diese Informationen finden können.

### Konfigurieren der USB-Unterstützung

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. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets.

USB-Umleitung erfordert entweder Citrix Virtual Apps 7.6 (oder höher) oder Citrix Virtual Desktops. Citrix Virtual Apps unterstützt nicht die USB-Umleitung von Massenspeichergeräten. Für die Unterstützung von Audiogeräten ist eine besondere Konfiguration erforderlich. Details hierzu finden Sie unter Citrix Virtual Apps 7.6-Dokumentation.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz und hoher Geschwindigkeit unterstützt. Normalerweise ist jedoch die Standardaudio- oder Webcamumleitung besser geeignet.

Die folgenden Gerätetypen werden direkt in einer Citrix Virtual Apps and Desktops-Sitzung 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 unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

über internes USB mit der Systemplatine verbunden haben. Remoting wäre in diesem Fall nicht angebracht. Die folgenden Typen von USB-Geräten können standardmäßig nicht in einer Citrix Virtual Apps and Desktops-Sitzung verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs

Um die Standardliste von USB-Geräten für Remoting zu aktualisieren, bearbeiten Sie die Datei usb.conf in $ICAROOT/. Weitere Informationen finden Sie unter "Aktualisieren der für Remoting verfügbaren USB-Geräteliste".

Um Remoting von USB-Geräten zu virtuellen Desktops zuzulassen, aktivieren Sie die USB-Richtlinienregel. Weitere Informationen finden Sie in der Dokumentation unter Citrix Virtual Apps and Desktops.

#### Funktionsweise der USB-Unterstützung

Wenn ein Benutzer ein USB-Gerät anschließt, wird es anhand der USB-Richtlinie überprüft und, sofern zulässig, an den virtuellen Desktop umgeleitet. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Bei Desktops, auf die über Desktop Appliance Mode zugegriffen wird, erfolgt die automatische Umleitung eines Geräts zum virtuellen Desktop, wenn ein Benutzer ein USB-Gerät anschließt. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.

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.

#### Massenspeichergeräte

Wenn ein Benutzer die Verbindung zu einem virtuellen Desktop trennt, während ein USB-Massenspeichergerät noch am lokalen Desktop angeschlossen ist, wird das Gerät nicht an den virtuellen Desktop umgeleitet, wenn der Benutzer die Verbindung wieder herstellt. 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 Remoteverbindungen von USB-Massenspeichergeräten nicht zulässt, wird das Gerät von der Workspace-App-Software nicht akzeptiert. Möglicherweise wird ein separater Linux-Dateibrowser geöffnet. Aus diesem Grund empfiehlt Citrix, dass Sie die Benutzergeräte so konfigurieren, dass die

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> 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.

> **Hinweis:**
>
> Wenn die Serverrichtlinie Client-USB-Geräteumleitung aktiviert ist, werden Massenspeichergeräte wie USB-Geräte umgeleitet, selbst wenn die Clientlaufwerkzuordnung aktiviert ist.

#### Webcams

Standardmäßig bietet die HDX RealTime-Webcamvideokomprimierung optimale Webcamleistung. In manchen Situationen jedoch, müssen Benutzer Webcams mit USB-Unterstützung anschließen. Hierzu müssen Sie HDX RealTime-Webcamvideokomprimierung deaktivieren. Weitere Informationen finden Sie unter Videokonferenzen mit HDX RealTime-Webcamvideokomprimierung.

#### Webcamumleitung

Im Folgenden ein paar Hinweise zur Webcamumleitung:

- Die Webcamumleitung funktioniert mit und ohne RTME.
- Die Webcamumleitung funktioniert für 32-Bit-Anwendungen. Zum Beispiel für Skype und GoToMeeting. Verwenden Sie einen 32-Bit-Browser, um die Webcamumleitung online zu verifizieren. Beispielsweise www.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.

#### Standardmäßig zugelassene 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 HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Hautskelette.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- Bilder (Geräteklasse 06)

  Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen oft die Bilderklasse, in der Bilder mit den Protokollen PTP (Picture Transfer Protocol) oder MTP (Media Transfer Protocol) zu einem Computer oder zu einem anderen Peripheriegerät übertragen werden. Kameras können auch als Massenspeichergeräte angezeigt werden. Eine Kamera kann möglicherweise über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

  Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet und die USB-Unterstützung wird nicht benötigt.

- Drucker (Geräteklasse 07)

  Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. 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 sowie 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, u. a. Medienplayer, 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 und USB-Unterstützung wird daher nicht benötigt.

  Wichtig: Einige Viren werden aktiv mit allen Typen des Massenspeichers übertragen. Überlegen Sie genau, ob die Verwendung von Massenspeichergeräten entweder über die Clientlaufwerkzuordnung oder die USB-Unterstützung im Unternehmen wirklich erforderlich ist. Zur Verringerung dieses Risikos kann auf dem Server konfiguriert werden, dass Dateien über die Clientlaufwerkzuordnung ausgeführt werden.

- Content Security (Geräteklasse 0d)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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 Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.

- Anwendung und herstellerspezifisch (Geräteklasse fe und ff)

  Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

**In der Standardeinstellung nicht zugelassene USB-Geräteklassen**

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a)

  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 HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktabletts, Sensoren, Game Controller, Tasten und 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)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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 mit Video zusammenhängendes Material manipuliert werden, u. a. Webcams, digitale Camcorder, analoge Videokonverter, einige Fernsehtuner und 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.

**Aktualisieren der für Remoting verfügbaren USB-Geräteliste**

Sie können den Umfang der USB-Geräte, die für Remoting auf Desktops zur Verfügung stehen, aktualisieren, indem Sie die Liste der Standardregeln in der Datei usb.conf auf dem Benutzergerät unter $ICAROOT/ bearbeiten.

Sie aktualisieren die Liste, indem Sie neue Richtlinienregeln hinzufügen, die USB-Geräte, die nicht Teil des Standardumfangs sind, zulassen oder ablehnen. 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)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

DENY: class=0a # CDC-Daten

ALLOW: # Letzter Ausweg: alles andere zulassen

**Erstellen von 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 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 |
| 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 # Weitere Industrie, Weiteres Flash-Laufwerk

DENY: Class=08 SubClass=05 # Massenspeichergeräte

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

DENY: Class=0D # Alle Sicherheitsgeräte

#### Konfigurieren von Startmodi

Mit “Desktop Appliance Mode” können Sie anpassen, wie ein virtueller Desktop zuvor angeschlossene USB-Geräte behandelt. Stellen Sie auf jedem Benutzergerät in der Datei $ICAROOT/config/module.ini im Abschnitt WfClient die Option DesktopApplianceMode = Boolean wie folgt ein.

| | |
|---|---|
| TRUE | USB-Geräte, die bereits angeschlossen sind, starten, vorausgesetzt dass das Gerät nicht durch eine Ablehnungsregel in den USB-Richtlinien auf dem Server (Registrierungseintrag) oder dem Benutzergerät (Konfigurationsdatei der Richtlinienregeln) deaktiviert ist. |
| FALSE | Keine USB-Geräte starten. |

### Bloomberg-Tastaturumleitung

> **Hinweis:**
>
> Die Bloomberg-Audioumleitung erfordert ähnliche Konfigurationsschritte.

Sie können die Bloomberg-Tastaturumleitung wie folgt durchführen:

- über die generische USB-Umleitung
- über die generische USB-Umleitung bei Unterstützung der selektiven Umleitung

#### Umleitung der Bloomberg v4-Tastatur über die generische USB-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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

3. Fügen Sie folgenden Eintrag zur Datei usb.conf hinzu, um die USB-Umleitung für die Bloomberg-Tastatur zuzulassen und speichern Sie die Datei.

   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.

### Umleitung der Bloomberg v4-Tastatur über generisches USB bei Unterstützung der selektiven Umleitung

Dieses Feature ermöglicht den Einsatz der Bloomberg v4-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.

> **Hinweis:**
>
> Dieses Feature ist standardmäßig für x86- und x64-Plattformen aktiviert und für ARMHF-Plattformen deaktiviert.

Aktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei config/All_Regions.ini wie folgt.

   BloombergRedirection=true

2. Führen Sie alle unter Umleitung der Bloomberg v4-Tastatur über die generische USB-Umleitung aufgeführten Schritte aus.

Deaktivieren des Features:

1. Bearbeiten Sie den Abschnitt BloombergRedirection in der Datei config/All_Regions.ini.
2. Setzen Sie den Wert BloombergRedirection auf false.

   BloombergRedirection = false

3. Führen Sie alle unter Umleitung der Bloomberg v4-Tastatur über die generische USB-Umleitung aufgeführten Schritte aus.

© 1999-2019 Citrix Systems, 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.

## Steigern der Leistung über Verbindungen mit geringer Bandbreite

Citrix empfiehlt die Verwendung der aktuellen Citrix Virtual Apps- oder Citrix Virtual Desktops-Version auf dem Server und der aktuellen Citrix Workspace-App-Version auf dem Benutzergerät.

Wenn Sie eine Verbindung mit geringer Bandbreite verwenden, können Sie durch eine geänderte Citrix Workspace-App-Konfiguration und -Verwendung eine Verbesserung der Leistung erzielen.

- **Konfigurieren Sie die Citrix Workspace-App-Verbindung**: Konfigurieren der Receiver-Verbindungen kann die Bandbreite reduzieren, die für ICA erforderlich ist und die Leistung verbessern
- **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 von Citrix Virtual Apps und der Citrix Workspace-App für Linux**: Citrix erweitert und verbessert die Leistung mit jedem Release und für viele Leistungsfeatures ist die neueste Receiver- und Serversoftware erforderlich

### Konfigurieren von Verbindungen

Auf Geräten mit beschränkter Rechenleistung oder geringer Bandbreite gibt es entweder Einbußen bei Leistung oder 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**: SpeedScreen-Latenzreduktion steigert die Leistung bei Verbindungen mit hoher Latenz, da schnell Feedback für eingegebene Daten und Mausklicks geboten wird. Aktivieren Sie dieses Feature mit dem SpeedScreen-Latenzreduktionsmanager. In der Standardeinstellung ist dies in der Citrix Workspace-App bei Verbindungen mit hoher Latenz für die Tastatur deaktiviert und nur für die Maus aktiviert. Weitere Informationen finden Sie in der Dokumentation “Citrix Workspace app for Linux OEM’s Reference Guide”.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- **Aktivieren Sie die Datenkomprimierung**: Mit der Datenkomprimierung wird die in der Verbindung übertragene Datenmenge reduziert. Für das Komprimieren und Dekomprimieren werden zusätzliche Prozessorressourcen benötigt. Dies 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 auf der XenApp Services-Site die Sitzungsoptionen fest.
- **Reduzieren Sie die Farbanzahl**: Reduzieren Sie die Anzahl der Farben auf 256. Legen Sie auf der Citrix Virtual Apps and Desktops-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.

#### Aktivieren von UDP-Audio

UDP-Audio kann die Qualität von Telefonanrufen über das Internet verbessern. Dabei wird UDP (User Datagram Protocol) statt TCP (Transmission Control Protocol) verwendet.

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.

1. Stellen Sie die folgenden Optionen in module.ini im Abschnitt ClientAudio ein:
   - Setzen Sie EnableUDPAudio auf “True”. Standardeinstellung ist “False”, wodurch UDP-Audio deaktiviert wird.
   - Geben Sie Minimum und Maximum für die Portnummern von UDP-Audioverkehr mit UDPAudioPortLow und UDPAudioPortHigh an. Standardmäßig werden Ports 16500 bis 16509 verwendet.
2. Stellen Sie Client- und Serveraudioeinstellungen wie folgt ein, sodass die resultierende Audioqualität “Mittel” ist (also weder hoch noch niedrig).

| | | Audioqualität auf dem Client | Audioqualität auf dem Client | Audioqualität auf dem Client |
|---|---|---|---|---|
| | | Hoch | Mittel | Niedrig |
| Audioqualität auf dem Server | Hoch | Hoch | Mittel | Niedrig |
| Audioqualität auf dem Server | Mittel | Mittel | Mittel | Niedrig |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| | | | | |
|---|---|---|---|---|
| | | Audioqualität auf dem Client | Audioqualität auf dem Client | Audioqualität auf dem Client |
| Audioqualität auf dem Server | Niedrig | Niedrig | Niedrig | Niedrig |

#### Konfigurieren von UDP auf dem Client

Fügen Sie Folgendes in der Datei $ICAROOT/config/module.ini hinzu:

Unter dem Abschnitt [ClientAudio]:

```
EnableUDPAudio=True
UDPAudioPortLow=int
UDPAudioPortHigh=int
```

Fügen Sie Folgendes in der Datei $HOME/.ICAClient/wfclient.ini hinzu:

Unter dem Abschnitt [WFClient]:

```
AllowAudioInput=True
EnableAudioInput=true
AudioBandWidthLimit=1
```

> **Hinweis:**
>
> Wenn der Ordner .ICAClient nicht vorhanden ist (nur beim Starten nach Erstinstallation), starten Sie die Citrix Workspace-App und schließen Sie die App. Dadurch wird der Ordner .ICAClient erstellt.

Fügen Sie Folgendes in wfclient.ini hinzu. * Richtlinieneinstellung auf dem DDC:

```
Legen Sie ”Windows Media-Umleitung” auf ”Nicht zugelassen” fest
Legen Sie ”Audio über UDP” auf ”Zugelassen” fest
Legen Sie ”Audio über UDP - Real-time Transport” auf ”Aktiviert” fest
Legen Sie ”Audioqualität” auf ”Mittel” fest
```

#### 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- **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 dies 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 dies sehr lange dauern.
- **Vermeiden Sie das Abspielen von Multimediainhalten**. Die Wiedergabe von Multimediainhalten benötigt viel Bandbreite und kann die Leistung reduzieren.

### Steigern der Multimedialeistung

Die Citrix Workspace-App enthält zahlreiche Technologien, die in den heutigen medienreichen Benutzerumgebungen eine High-Definition-Benutzererfahrung ermöglichen. Diese verbessern die Benutzererfahrung bei Verbindungen mit gehosteten Anwendungen und Desktops:

- HDX MediaStream Windows Media-Umleitung
- HDX MediaStream Flash-Umleitung
- HDX RealTime-Webcamvideokomprimierung
- H.264-Unterstützung

> **Hinweis:**
>
> Citrix unterstützt die Koexistenz von RealTime Optimization Pack mit der Citrix Workspace-App für Linux Version 1901 und höher und mit GStreamer 0.1.

### Konfigurieren von 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. Mit Windows Media-Umleitung werden die Laufzeitdateien von Medieninhalten auf dem Benutzergerät statt auf dem Server abgespielt. Dies führt zu einer Reduktion der Bandbreitenanforderungen beim Abspielen von Multimediadateien.

Windows Media-Umleitung verbessert die Leistung des Windows Media-Players und anderer kompatibler Player, 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)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 zusätzlicher 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 jedoch keine Mediendaten. Dieses Feature erfordert erweiterte GStreamer-Multimediabibliotheken auf dem Gerät.

#### Einrichten von HDX Mediastream Windows Media-Umleitung

1. Installieren Sie GStreamer 0.10, ein Open-Source-Multimedia-Framework, auf jedem erforderlichen Benutzergerät. Normalerweise installieren Sie GStreamer vor der Citrix Workspace-App, damit der Installationsvorgang die Citrix Workspace-App für die Verwendung von GStreamer konfiguriert.

   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 Protocol Source-*Plug-Ins* für die Dateitypen, die Benutzer auf dem Gerät wiedergeben. Sie prüfen mit dem Hilfsprogramm gst-launch, 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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

"False" einstellen, wird die Windows Media-Umleitung für die Medienverarbeitung verwendet.

- Standardmäßig verwenden alle MediaStream-Features das GStreamer-Protokoll "playbin2". Sie können auf ein früheres playbin-Protokoll für alle MediaStream-Features außer dem clientseitigen Inhaltsabruf zurückgehen, der weiter playbin2 verwendet. Stellen Sie dazu in All-Regions.ini im Abschnitt "Multimedia" die Option SpeedScreenMMAEnablePlaybin2 ein.
- Die Citrix Workspace-App erkennt nicht 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.

Beachten Sie bei GStreamer 1.0:

- GStreamer 0.10 wird standardmäßig für die HDX MediaStream Windows Media-Umleitung 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 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 "platform" z. B. linuxx64 sein kann). Weitere Informationen finden Sie unter Installation und Einrichtung.
3. Installieren Sie libgstflatstm1.0.so, indem Sie einen symbolischen Link im Verzeichnis der GStreamer-Plug-Ins erstellen: ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflat
   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.

- Wenn Sie GStreamer 1.0 HDX RealTime-Webcamvideokomprimierung verwenden möchten, verwenden Sie gst_read1.0 als Leser: ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read.

#### Konfigurieren der 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.

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt. Weitere Informationen finden Sie unter Systemanforderungen.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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. Die Standardeinstellung ist **Never**. Benutzer werden beim Aufrufen von Webseiten mit Flash-Inhalten in einem Dialogfeld gefragt, ob sie diese 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.

#### Konfigurieren Sie HDX RealTime-Webcamvideokomprimierung

HDX RealTime bietet Webcamvideokomprimierung, mit der die Bandbreiteneffizienz während Videokonferenzen verbessert wird. So erhalten Benutzer optimale Leistung, wenn sie Anwendungen wie GoToMeeting mit HD Faces oder Skype for Business verwenden.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

1. Stellen Sie sicher, dass das Benutzergerät die Anforderungen für dieses Feature erfüllt.
2. Stellen Sie sicher, dass der virtuelle Multimedia-Kanal aktiviert ist. Öffnen Sie hierzu die Konfigurationsdatei module.ini im Verzeichnis $ICAROOT/config und überprüfen Sie, ob im Abschnitt [ICA3.0] die Option “MultiMedia” 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. Dazu müssen Sie die folgenden Schritte ausführen:

- 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:

   HDXWebCamEnabled=Off

   Weitere Informationen finden Sie unter Anpassen der Citrix Workspace-App mit Konfigurationsdateien.
2. Öffnen Sie die Datei usb.conf, die normalerweise unter $ICAROOT/usb.conf 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.

#### Konfigurieren der H.264-Unterstützung

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.

Befolgen Sie die 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. So lassen sich CPU-Kosten während der Verarbeitung von Grafiken mit komplexen Bildern aber relativ wenig oder unwichtigem Text senken.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **Wichtig:**
>
> Verwenden Sie zum Konfigurieren dieses Features keine verlustfreie Einstellung in der Citrix Virtual Apps and Desktops-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 in wfclient.ini für H264Enabled die Einstellung False fest. Dadurch wird auch die Textprotokollierung deaktiviert.

Ausschließliches Deaktivieren der Textprotokollierung

Legen Sie bei aktiviertem Tiefenkomprimierungscodec in wfclient.ini TextTrackingEnabled auf False fest.

### Optimieren der Leistung für 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: Aktivieren der Batchverarbeitung für die Kacheldecodierung aktiviert gleichzeitig verzögertes XSync.

### Aktivieren der Protokollierung

Aktivieren der Protokollierung für die Citrix Workspace-App für Linux:

1. Laden Sie die Citrix Workspace-App für Linux herunter und installieren Sie sie auf Ihrer Linux-Maschine. Legen Sie dabei die ICAROOT-Umgebungsvariable auf den Installationsordner fest. Beispiel: /opt/Citrix/ICAClient.

   Standardmäßig ist die Traceklasse TC_ALL aktiviert, um alle Traces bereitzustellen.

2. 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 mehrere Klassen hinzufügen, indem Sie sie durch einen senkrechten Strich trennen.
   Beispiel: +TC_LIB|+TC_MMVD.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Die folgende Tabelle listet verschiedene Module und die entsprechenden Traceklassenwerte auf:

| Section | Modules | TraceClasses value |
|---|---|---|
| wfica | Graphics | TC_TW |
| | EUEM | TC_EUEM |
| | WFICA (Session Launch) | TC_NCS |
| | Printing | TC_CPM |
| | Connection Sequence - WD | TC_WD |
| | Connection Sequence - PD | TC_PD |
| | Connection Sequence - TD | TC_TD |
| | Proxy related files | TC_PROXY |
| | MultiMedia Virtual Driver / Webcam | TC_MMVD |
| | Virtual Drivers | TC_VD |
| | Client Drive Mapping | TC_CDM |
| | Audio | TC_CAM |
| | COM (Communication Port) | TC_CCM |
| | Seamless | TC_TWI |
| | Smart Card | TC_SCARDVD |
| Connection center | Connection center | TC_CSM |
| WebHelper | Set logSwitch to 1 (to enable) or 0 (to disable)<br>Example: logSwitch = 1 | |

3. Öffnen Sie die Datei $ICAROOT/config/module.ini. Ändern Sie im Abschnitt [WFClient] den Wert **SyslogThreshold=0** in **SyslogThreshold=7**. Durch diese Änderung werden Protokolle für alle Ebenen generiert. Um nur Fehler zu protokollieren, legen Sie folgende Einstellung fest: **SyslogThreshold=3**.

4. Starten Sie den Citrix Workspace-App-Prozess (./selfservice unter $ICAROOT). Nach Beenden der Sitzung finden Sie die Protokolldatei unter /var/log/syslog. Bei nachfolgenden Starts werden die Protokolle an die Protokolldatei angehängt.

   Weitere Informationen zum Abrufen neuer und aktualisierter Protokolle bei nachfolgenden Starts finden Sie unter Weitere Informationen zur syslog-Konfiguration.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Weitere Informationen zur 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:

> user.* -/var/log/logfile_name.log

Speichern Sie Ihre Änderungen und starten Sie den syslog-Dienst mit dem folgenden Befehl neu:

```
1 sudo service rsyslog restart
```

#### Wichtige Punkte

Beachten Sie Folgendes:

- Um sicherzustellen, dass das generierte Systemprotokoll immer neu ist, löschen Sie syslog und führen Sie den Befehl “sudo service rsyslog restart” aus.
- 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.

#### Aktivieren der 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
  ```

### Konfigurieren der 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 dem- oder denselben Monitor(en) angezeigt.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**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 AllRegions.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 die Features beibehalten.

**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.

> **Hinweis:**
>
> Das Layout wird bei jeder Speicherung überschrieben und nur auf dem aktiven StoreFront gespeichert.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> Wenn Sie mehrere Desktopsitzungen von demselben StoreFront-Store auf unterschiedlichen Bildschirmen starten, werden beim Speichern des Layouts in einer Sitzung die Layoutinformationen aller Sitzungen gespeichert.

#### Konfigurieren des Features zur Layoutspeicherung

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 Seite Downloads 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.
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. Dies zeigt an, dass ein Speichervorgang ausgeführt wird. Nach der Speicherung des Layouts wird das Symbol wieder normal angezeigt.
   Wenn das Symbol für längere Zeit ausgegraut ist, finden Sie im Knowledge Center-Artikel CTX235895 Informationen zur Fehlerbehebung.
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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Verhalten führen.
- Kundenbereitstellungen mit mehreren 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.

## 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. Wechseln 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.

## V3-Authentifizierungsprotokoll

V3-Authentifizierung bezeichnet die dritte Hauptdefinition eines Anmeldeprotokolls für Citrix Gateway, das von der Citrix Workspace-App für Linux unterstützt wird.

V3 ist das Standardanmeldeprotokoll für Citrix Gateway in Kombination mit dem Authentifizierungsrichtlinien-Framework “N-Factor”, mit dem Authentifizierungsschritte und zugehörige Formulare zur Anmeldedatenerfassung vollständig konfigurierbar sind. Die systemeigene Citrix Workspace-App kann dieses Protokoll über die unterstützten Anmeldeformulare nutzen, die bereits für StoreFront implementiert sind. Die webbasierte Anmeldeseite für virtuelle Citrix Gateway- und Traffic Manager-Server verwendet ebenfalls dieses Protokoll mit Code, der auch von der Citrix Workspace-App für Linux verwendet wird.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Weitere Informationen finden Sie unter SAML-Authentifizierung und im Knowledge Center-Artikel NetScaler-Authentifizierung.

### Unterstützung für Citrix Analytics

Die Citrix Workspace-App für Linux ist so instrumentiert, dass Protokolle sicher an Citrix Analytics übertragen werden, wenn bestimmte Ereignisse von der App ausgelöst werden. Die Protokolle werden analysiert und auf Citrix Analytics-Servern gespeichert, wenn diese aktiviert sind. Weitere Informationen zu Citrix Analytics finden Sie unter Citrix Analytics.

### Tastaturlayoutsynchronisierung zwischen Client und VDA

Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, bei der Verwendung eines Windows VDA oder Linux VDA zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist in der Standardeinstellung deaktiviert.

#### 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 unterDynamische Tastaturlayoutsynchronisierung

Um dieses Feature zu aktivieren, fügen Sie der Datei module.ini die folgenden Zeilen hinzu:

```
[ICA 3.0]
KeyboardSync=On
[KeyboardSync]
DriverName = VDIME.DLL
```

Wenn Sie **KeyboardSync=On** in der Datei module.ini festlegen und **KeyboardLayout=(Benutzerprofil)** in der Datei **wfclient.ini** festlegen, erkennt der virtuelle Treiber vdime das aktive Tastaturlayout auf dem Client und sendet die Informationen an den VDA. Wenn sich das Tastaturlayout in einer Clientsitzung ändert, erkennt der vdime-Treiber dies und sendet das neue Layout sofort an den VDA.

Um diese Funktion zu deaktivieren, legen Sie **KeyboardSync=Off** in der Datei module.ini fest, damit das ursprüngliche Verhalten wiederhergestellt wird. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Verwendung

Wenn das Feature aktiviert ist, ändert sich das Tastaturlayout auf dem VDA automatisch zusammen mit dem auf dem Clientgerät.

#### Bekannte Einschränkungen

Die Tastaturlayoutsynchronisierung hängt von der XKB lib ab, die die automatische Synchronisierung des Tastaturlayouts zwischen dem VDA und dem Client ermöglicht.

#### Tastaturlayoutunterstützung für Linux VDA

**Hinweis:** In der folgenden Tabelle ist das Gebietsschema der Linux-Tastatur für alle Referenzen ein Bindestrich.

| Linux-Tastaturlayout | Linux-Tastatur / Linux VDA-Layout | Windows-Gebietsschema | Windows-Tastatur-ID | Linux VDA-Layout |
|---|---|---|---|---|
| ara | - | ar-SA | 00000401 | ara |
| ara | azerty | ar-DZ | 00020401 | ara |
| at | - | de-AT | 00000407 | at |
| be | iso-alternativ | fr-BE | 0000080c | be |
| be | - | nl-BE | 00000813 | be |
| bg | - | bg-BG | 00030402 | bg |
| bg | phonetic | bg-BG | 00040402 | bg |
| bg | bas_phonetic | bg-BG | 00020402 | bg |
| br | - | pt-BR | 00000416 | br |
| by | - | be-BY | 00000423 | by |
| ca | eng | en-CA | 00000409 | ca |
| ca | multix | fr-CA | 00011009 | ca |
| ca | fr-legacy | fr-CA | 00000c0c | ca |
| ca | - | fr-CA | 00001009 | ca |
| ch | fr | fr-CH | 0000100c | ch |
| ch | - | de-CH | 00000807 | ch |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Linux-Tastaturlayout | Linux-Tastatur / Linux VDA-Layout | Windows-Gebietsschema | Windows-Tastatur-ID | Linux VDA-Layout |
|---|---|---|---|---|
| cn | - | en-US | 00000409 | us |
| cz | - | cs-CZ | 00000405 | cz |
| cz | qwerty | cs-CZ | 00010405 | cz |
| de | - | de-DE | 00000407 | de |
| de | mac | de-DE | 00000407 | de |
| dk | - | da-DK | 00000406 | dk |
| ee | - | et-EE | 00000425 | ee |
| es | - | es-ES | 0000040a | es |
| es | mac | es-ES | 0000040a | es |
| fi | - | fi-FI | 0000040b | fi |
| fr | - | fr-FR | 0000040c | fr |
| fr | mac | fr-FR | 0000040c | fr |
| gb | - | en-GB | 00000809 | gb |
| gb | mac | en-GB | 00000809 | gb |
| gb | extd | en-GB | 00000452 | gb |
| gr | - | el-GR | 00000408 | gr |
| hr | - | hr-HR | 0000041a | hr |
| hu | - | hu-HU | 0000040e | hu |
| ie | - | en-IE | 00001809 | ie |
| il | - | he-IL | 0002040d | il |
| in | eng | en-IN | 00004009 | in |
| iq | - | ar-IQ | 00000401 | iq |
| is | - | is-IS | 0000040f | is |
| it | - | it-IT | 00000410 | it |
| jp | - | en-US | 00000409 | us |
| jp | mac | en-US | 00000409 | us |
| kr | - | en-US | 00000409 | us |
| latam | - | es-MX | 0000080a | latam |

© 1999-2019 Citrix Systems, Inc. All rights reserved.

| Linux-Tastaturlayout | Linux-Tastatur / Linux VDA-Layout | Windows-Gebietsschema | Windows-Tastatur-ID | Linux VDA-Layout |
|---|---|---|---|---|
| lt | - | lt-LT | 00010427 | lt |
| lt | ibm | lt-LT | 00000427 | lt |
| lt | std | lt-LT | 00020427 | lt |
| lv | - | lv-LV | 00020426 | lv |
| no | - | nb-NO | 00000414 | no |
| pl | - | pl-PL | 00000415 | pl |
| pl | qwertz | pl-PL | 00010415 | pl |
| pt | - | pt-PT | 00000816 | pt |
| pt | mac | pt-PT | 00000816 | pt |
| ro | std | ro-RO | 00010418 | ro |
| rs | - | sr-Cyrl-RS | 00000c1a | rs |
| rs | latin | sr-Latn-RS | 0000081a | rs |
| ru | - | ru-RU | 00000419 | ru |
| ru | typewriter | ru-RU | 00010419 | ru |
| ru | mac | ru-RU | 00000419 | ru |
| se | - | sv-SE | 0000041d | se |
| se | mac | sv-SE | 0000041d | se |
| si | - | sl-SI | 00000424 | si |
| sk | - | sk-SK | 0000041b | sk |
| sk | qwerty | sk-SK | 0001041b | sk |
| th | - | th-TH | 0000041e | th |
| th | pat | th-TH | 0001041e | th |
| tj | - | tg-Cyrl-TJ | 00000428 | tj |
| tr | - | tr-TR | 0000041f | tr |
| tr | f | tr-TR | 0001041f | tr |
| tw | - | en-US | 00000409 | us |
| ua | - | uk-UA | 00000422 | ua |
| us | - | en-US | 00000409 | us |

© 1999-2019 Citrix Systems, Inc. All rights reserved.

| Linux-Tastaturlayout | Linux-Tastatur / Linux VDA-Layout | Windows-Gebietsschema | Windows-Tastatur-ID | Linux VDA-Layout |
|---|---|---|---|---|
| us | mac | en-US | 00000409 | us |
| us | dvorak | en-US | 00010409 | us |
| us | dvorak-l | en-US | 00030409 | us |
| us | dvorak-r | en-US | 00040409 | us |
| us | intl | nl-NL | 00020409 | us |
| vn | - | vi-VN | 0000042a | vn |

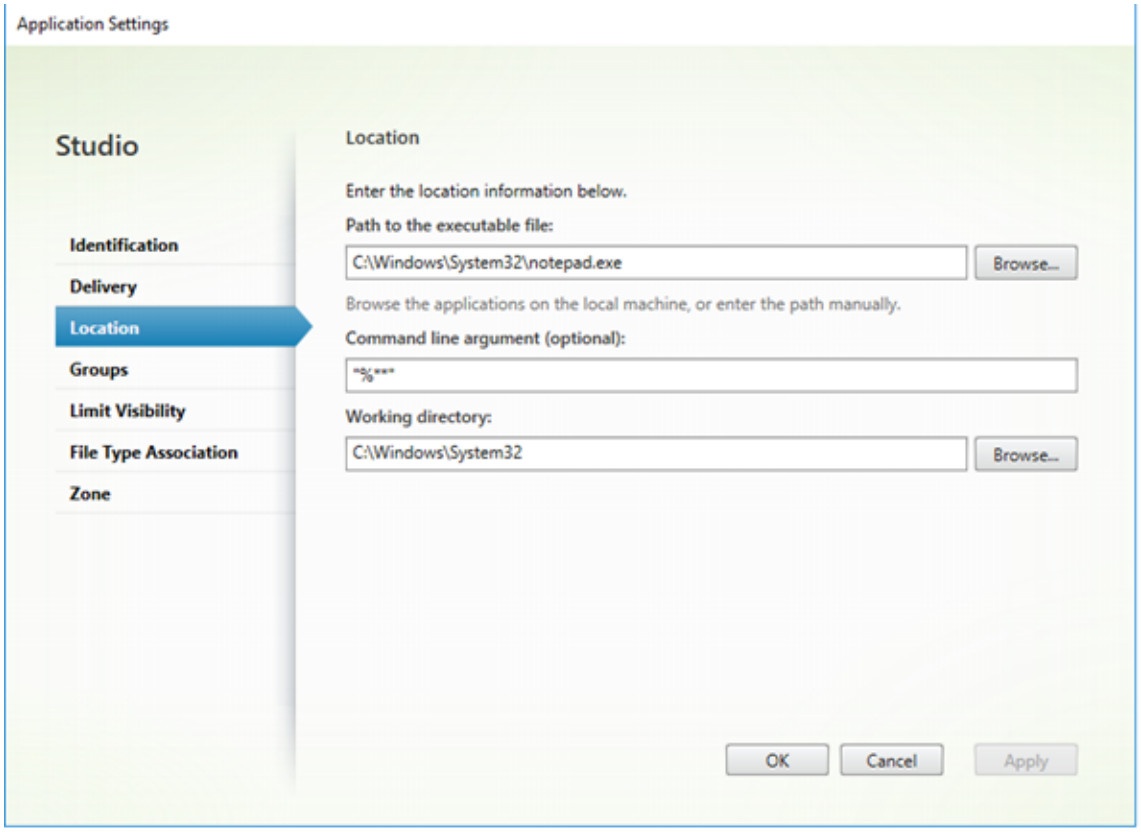
### Zuordnen einer veröffentlichten Anwendung zu Dateitypen

Die Citrix Workspace-App liest die von Administratoren in Citrix Studio konfigurierten Einstellungen und wendet sie an. Damit die Dateitypzuordnung in einer Sitzung angewendet wird, stellen Sie sicher, dass Sie eine Verbindung mit dem Store-Server herstellen, auf dem die Dateitypzuordnung konfiguriert ist.

Verknüpfen einer Dateierweiterung mit einer Citrix Workspace-App für Linux:

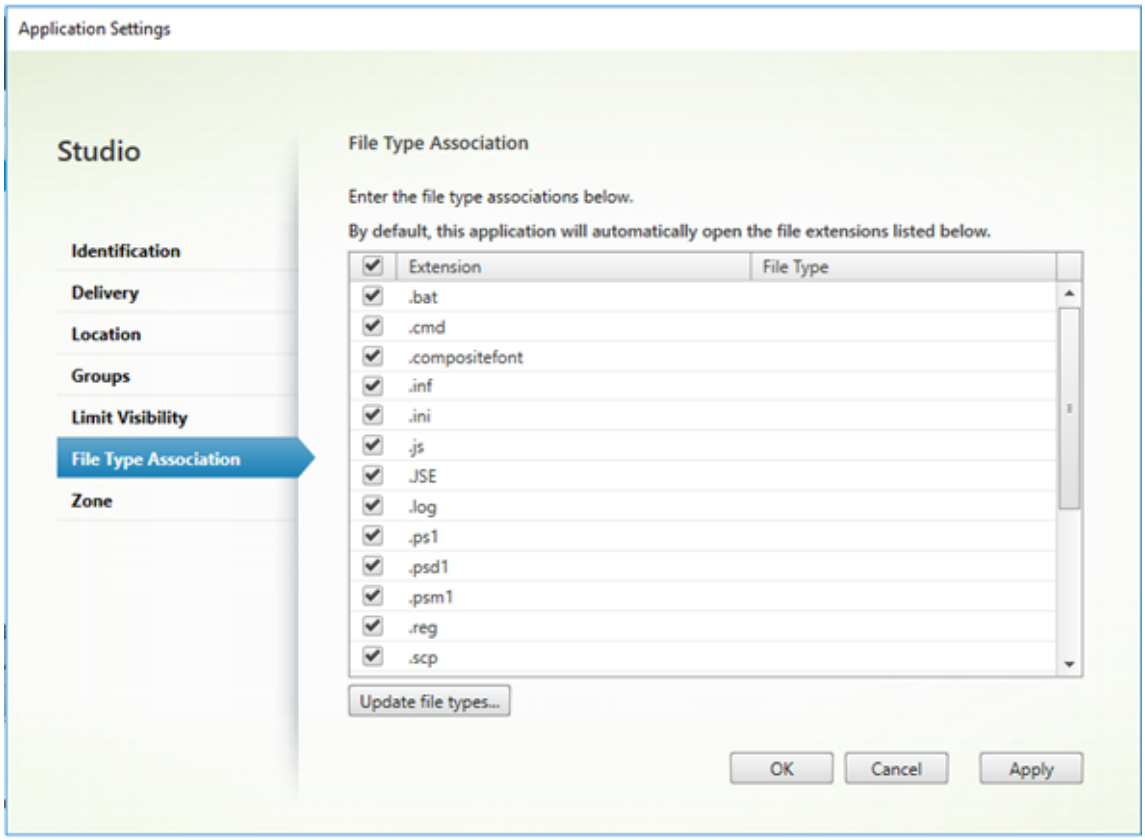
1. Veröffentlichen Sie die Anwendung.
2. Melden Sie sich bei Citrix Studio an.
3. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften** aus.
4. Wählen Sie **Speicherort**.
5. Fügen Sie “%**” im Feld “Befehlszeilenargument (optional)” hinzu, um die Befehlszeilenprüfung zu umgehen, und klicken Sie dann auf “OK”.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 




6. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Eigenschaften** aus.
7. Wählen Sie **Dateitypzuordnung**.
8. Wählen Sie die Erweiterungen aus, die die Citrix Workspace-App der Anwendung zuordnen soll (wählen Sie alle zutreffenden aus).

© 1999-2019 Citrix Systems, Inc. All rights reserved. 




9. Klicken Sie auf **Anwenden** und dann auf **Dateitypen aktualisieren**.
10. Führen Sie die unter Aktivieren von Dateitypzuordnung beschriebenen Schritte aus, um die Dateitypzuordnung auf dem Client zu aktivieren.

> **Hinweis:**
>
> Stellen Sie sicher, dass die StoreFront-Dateitypzuordnung auf “EIN” festgelegt ist. Standardmäßig ist die Dateitypzuordnung in Stores aktiviert, damit Inhalte nahtlos an die abonnierten Anwendungen der Benutzer umgeleitet werden, wenn sie lokale Dateien der zugeordneten Typen öffnen.

### Aktivieren von Dateitypzuordnung

Aktivieren von Dateitypzuordnung auf dem Client:

1. Stellen Sie sicher, dass die App, die Sie zuordnen möchten, ein Favorit 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
```

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

```
2
3 ./util/storebrowse  -S <StoreFront URL>
```

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.

## Verbessern der Benutzererfahrung

March 11, 2019

Sie können die Erfahrung der Benutzer mit den folgenden unterstützten Features verbessern:

### Festlegen von Einstellungen

Sie können Einstellungen festlegen, indem Sie im Citrix Workspace-App-Menü auf “Einstellungen” klicken. Sie können steuern, wie Desktops angezeigt werden, Verbindung mit verschiedenen Anwendungen und Desktops herstellen und den Datei- und Gerätezugriff verwalten.

#### Verwalten eines Kontos

Für den Zugriff auf Desktops und Anwendungen benötigen Sie ein XenDesktop- oder Citrix Virtual Apps-Konto. 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. Ihr Helpdesk stellt möglicherweise alternativ eine Provisioningdatei mit Kontoinformationen bereit, mit der Sie ein Konto erstellen können.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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. Es kann erforderlich sein, dass Sie sich bei dem Server authentifizieren.

### Ändern der Anzeige Ihrer Desktops

Dieses Feature steht nicht für Citrix Virtual Apps für UNIX-Sitzungen zur Verfügung.

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

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

Die Citrix Workspace-App hat nun eine Funktion zum **Aktivieren des Desktop Viewer** über die Symbolleiste, sodass Sie die Fensterkonfiguration Ihrer Remotesitzung dynamisch anpassen können.

### Desktop Viewer

Jedes Unternehmen hat andere Anforderungen. Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern. Die Benutzererfahrung beim Verbinden mit virtuellen Desktops und der Umfang der Benutzereingriffe beim Konfigurieren der Verbindungen hängen davon ab, wie Sie die Citrix Workspace-App für Linux einrichten.

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 mit mehreren Desktops über mehrere Citrix Virtual Apps and Desktops-Verbindungen arbeiten. 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.

Als Eingabehilfe von Desktop Viewer werden die Schaltflächen der Desktop Viewer-Symbolleiste in einem Popupfenster angezeigt, wenn Sie Strg+Alt+Untbr drücken.

Weitere Informationen zu erweiterten Konfigurationseinträgen zum Aktivieren oder Deaktivieren von Desktop Viewer oder zum Ändern der Zugriffstastenabfolge finden Sie im Linux OEM Guide.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Automatisches Wiederherstellen von Sitzungsverbindungen

Die Citrix Workspace-App kann Desktops und Anwendungen, deren Verbindung getrennt wurde (zum Beispiel bei einem Problem mit der Netzwerkinfrastruktur), wiederverbinden:

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

### Steuern des Zugriffs auf lokale Dateien

Ein virtueller Desktop oder eine Anwendung benötigt 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 aus:
   - Lesen/Schreiben: ermöglicht dem Desktop bzw. der Anwendung das Lesen bzw. Ändern der lokalen Dateien.
   - 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, wenn der Desktop oder die Anwendung Zugriff auf lokale Dateien benötigt, eine Aufforderung an.
2. Wenn Sie eine der Optionen, die Zugriff auf lokale Dateien ermöglichen, auswählen, können Sie außerdem beim Ansteuern von Speicherorten auf dem Benutzergerät Zeit einsparen. Klicken Sie auf Hinzufügen, geben Sie den Speicherort an und wählen Sie ein Laufwerk für die Zuordnung aus.

### Einrichten eines Mikrofons oder einer Webcam

Sie können die Art und Weise, wie ein virtueller Desktop oder eine virtuelle Anwendung auf das lokale Mikrofon oder die Webcam zugreift, ändern:

Wählen Sie auf der Seite Mikrofon & Webcam im Dialogfeld Einstellungen 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Einrichten von 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 aus:

- 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.

### Konfigurieren der ClearType-Schriftartenglättung

Mit ClearType-Schriftartenglättung (auch Subpixel-Rendering von Schriftarten genannt) wird eine höhere Qualität der Schriftartenanzeige erzielt als bei traditioneller Schriftartenglättung oder Anti-Aliasing. Sie können dieses Feature ein- und ausschalten. Sie können auch die Art der Glättung über die folgende Einstellung im Abschnitt [WFClient] der jeweiligen Konfigurationsdatei angeben:

FontSmoothingType = Nummer

wobei Nummer einen der folgenden Werte haben kann:

| 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: Vom Server kann FontSmoothingType über die ICA-Datei konfiguriert werden. Dies hat Vorrang vor dem Wert in der [WFClient]. Wenn der Wert vom Server auf 0 festgelegt wird, wird die lokale Einstellung von einer anderen Einstellung im [WFClient] bestimmt:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

FontSmoothingTypePref = Nummer

wobei Nummer einen der folgenden Werte haben kann:

| Wert | Ergebnis |
|---|---|
| 0 | Keine Glättung |
| 1 | Keine Glättung |
| 2 | Standardglättung |
| 3 | ClearType-Glättung (horizontale Subpixel-Technologie, Standard) |

## 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 Ihrer Benutzer angeben, damit diese auch bei Verwendung verschiedener Servertypen und Serverfarmkonfigurationen bestehen bleiben. 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

Der Vorgang besteht aus zwei Schritten. Zuerst aktivieren Sie die Umleitung spezieller Ordner mit einem Eintrag in module.ini; anschließend geben Sie die Speicherorte der Ordner im Abschnitt [WFClient] wie im Folgenden beschrieben an:

1. Fügen Sie module.ini (z. B. $ICAROOT/config/module.ini) folgenden Text hinzu:

   [ClientDrive]

   SFRAllowed = True

2. Fügen Sie im Abschnitt [WFClient] (z. B. $HOME/.ICAClient/wfclient.ini) folgenden Text hinzu:

   DocumentsFolder = Dokumente

   DesktopFolder = Desktop

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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.
- 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.

### Einrichten der 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. Diese Funktion ermöglicht Administratoren eine wesentlich effizientere Zuordnung der Citrix Ressourcen, wobei für Benutzer gleichzeitig eine Leistungsverbesserung erzielt wird.

Folgende URL-Typen können umgeleitet werden:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (Ältere Real Player)

Wenn die Citrix Workspace-App für Linux keine geeignete Anwendung hat oder nicht direkt auf den Inhalt zugreifen kann, wird die URL mit der Serveranwendung geöffnet.

Die Server-zu-Client-Inhaltsumleitung ist auf dem Server konfiguriert und standardmäßig in der Citrix Workspace-App aktiviert, falls der Pfad RealPlayer und mindestens einen Browser wie Firefox, Mozilla oder Netscape enthält.

> **Hinweis:**
>
> Weitere Informationen über RealPlayer für Linux finden Sie unter http://www.real.com/resources/unix/.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**Aktivieren der Server-zu-Client-Inhaltsumleitung, wenn der Pfad weder einen Browser noch RealPlayer enthält**

1. Öffnen Sie die Konfigurationsdatei wfclient.ini.
2. Bearbeiten Sie im Abschnitt [Browser] die folgenden Einstellungen:

   Path=path

   Command=command

   Dabei ist path das Verzeichnis, in dem sich die ausführbare Browserdatei befindet, und command ist der Name der ausführbaren Datei zur Verarbeitung umgeleiteter Browser-URLs, an die die vom Server gesendete URL angehängt wird. 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

   Dabei ist path das Verzeichnis, in dem sich die ausführbare RealPlayer-Datei befindet, und command ist der Name der ausführbaren Datei zur Verarbeitung umgeleiteter Multimedia-URLs, an die die vom Server gesendete URL angehängt wird.
4. Speichern und schließen Sie die Datei.

> **Hinweis:**
>
> Für beide Einstellungen für “Path” brauchen Sie nur das Verzeichnis anzugeben, in dem sich die ausführbaren Dateien für den Browser und RealPlayer befinden. Sie brauchen nicht dem vollständigen Pfad zu den ausführbaren Dateien anzugeben. Beispiel: Im Abschnitt [Browser] kann “Path” auf /usr/X11R6/bin statt auf /usr/X11R6/bin/netscape eingestellt sein. Außerdem können Sie mehrere Verzeichnisnamen in einer durch Doppelpunkte getrennten Liste angeben. Wenn diese Einstellungen 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

2. Ändern Sie die Einstellung CREnabled zu “Off”.
3. Speichern und schließen Sie die Datei.

### Steuern des Tastaturverhaltens

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 im Abschnitt WFClient UseCtrlAltEnd:
    - 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.

### Verwenden von xcapture

Das Citrix Workspace-App-Paket enthält das Hilfsprogramm xcapture, mit dem Grafikdaten zwischen der Zwischenablage des Servers und nicht-ICCCM-kompatiblen X Windows-Anwendungen auf dem X-Desktop ausgetauscht werden können. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 Dialogfeld xcapture 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.
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.

## Automatische Wiederverbindung von Benutzern

In diesem Abschnitt wird die automatische HDX Broadcast-Wiederverbindung von Clients beschrieben. Citrix empfiehlt, dass Sie dieses Feature mit der HDX Broadcast -Sitzungszuverlässigkeit verwenden.

Benutzer können von ICA-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,

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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.

### Sicherstellen der 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.

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 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. Weitere Informationen finden Sie in der
Citrix Virtual Apps and Desktops-Dokumentation.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> **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.

### 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 oder Citrix Virtual Desktops 7.8 (oder höher) ausgeführt werden. In der Standardeinstellung ist das Steuerelement 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.

> **Tipp:**
>
> Im Abschnitt Alternative relative Mauswerte finden Sie weitere Informationen zum Aktivieren der relativen Mausfunktion.

**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:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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.
- RelativeMouse=4 Aktiviert oder deaktiviert das Feature, wenn der clientseitige Mauszeiger angezeigt oder ausgeblendet wird. In diesem Modus kann die relative Maus automatisch aktiviert oder deaktiviert werden für Anwendungsoberflächen im Gamingstil in Ich-Perspektive.

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.

## Sicherheit

May 23, 2019

Zum Sichern der Kommunikation zwischen der Site und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen zur Site mit zahlreichen Sicherheitsverfahren integrieren, u. a.:

- Einen SOCKS-Proxyserver oder Secure Proxyserver (auch Security Proxyserver, HTTPS-Proxyserver oder TLS-Tunneling-Proxyserver genannt) 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.
- Citrix Secure Web Gateway- oder SSL-Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen. Die TLS-Versionen 1.0 bis 1.2 werden unterstützt.
- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

## Herstellen von Verbindungen über Proxyserver

Proxyserver werden zur Beschränkung des Netzwerkzugriffs sowie beim Herstellen von Verbindungen zwischen der Citrix Workspace-App und Citrix Virtual Apps- oder Citrix Virtual Desktops-Bereitstellungen verwendet. Die Citrix Workspace-App unterstützt das SOCKS-Protokoll zusammen mit Citrix Secure Web Gateway und Citrix SSL-Relay, das Secure Proxy-Protokoll und Windows NT Challenge/Response (NTLM)-Authentifizierung.

Die unterstützten Proxytypen sind durch die Inhalte von Trusted_Regions.ini und Untrusted_Regions.ini auf die Typen “Auto”, “None” und “Wpad” beschränkt. Wenn Sie die Typen “SOCKS”, “Secure” oder “Script” verwenden, bearbeiten Sie die genannten Dateien und fügen Sie die zusätzlichen Typen der Liste der zulässigen Typen hinzu.

> **Hinweis:**
>
> Aktivieren Sie zur Gewährleistung einer sicheren Verbindung TLS.

### Verbinden über einen sicheren 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.

> **Wichtig:**
>
> Um NTLM verwenden zu können, muss die OpenSSL-Bibliothek libcrypto.so auf dem Benutzergerät installiert sein. Diese Bibliothek ist häufig in Linux-Distributionen enthalten, kann aber bei Bedarf auch von http://www.openssl.org/ in einem neuen Fenster heruntergeladen werden.

## Verbinden mit Citrix Secure Web Gateway oder dem Citrix SSL-Relay

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

### Verbinden mit Citrix 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. Die Citrix Workspace-App muss nicht konfiguriert werden, wenn Sie Citrix Secure Web Gateway im Normalmodus verwenden und Benutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Citrix Secure Web Gateway-Servern verwendet die Citrix Workspace-App Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Informationen zum Konfigurieren der Proxyservereinstellungen für die Citrix Workspace-App finden Sie in der Webinterface-Dokumentation.

Wenn Citrix Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Citrix Secure Web Gateway Proxy im Relaymodus verwenden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps (Citrix Secure Web Gateway).

Wenn Sie den Relaymodus verwenden, fungiert der Citrix Secure Web Gateway-Server als Proxy und Sie müssen die Citrix Workspace-App für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Citrix Secure Web Gateway-Servers.
- Portnummer des Citrix Secure Web Gateway-Servers. Der Relaymodus wird von Citrix Secure Web Gateway, Version 2.0 nicht unterstützt.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

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.

### Verbinden mit dem Citrix SSL-Relay

Das Citrix SSL-Relay verwendet standardmäßig den TCP-Port 443 auf dem Citrix Virtual Apps-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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- Mit Webinterface zwischen dem Citrix Virtual Apps-Server und dem Webserver

Weitere Informationen zum Konfigurieren und Sichern der Installation mit SSL-Relay finden Sie in der Citrix Virtual Apps-Dokumentation. Weitere Informationen zum Konfigurieren des Webinterface für die TLS-Verschlüsselung finden Sie in der Webinterface-Dokumentation.

#### Konfigurieren und Aktivieren von TLS

Die Versionen des TLS-Protokolls, die ausgehandelt werden können, können Sie steuern, indem Sie die folgenden Konfigurationsoptionen im Abschnitt [WFClient] hinzufügen:

- MinimumTLS=1.0
- MaximumTLS=1.2

Diese Werte sind die Standardwerte, die als Code implementiert werden. Passen Sie sie nach Bedarf an.

> **Hinweis 1:**
>
> 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**.
>
> **Hinweis 2:**
>
> Die Verwendung des SSLv3-Protokolls ist in der Citrix Workspace-App für Linux nicht zulässig.

Die Citrix Workspace-App für Linux unterstützt DTLS 1.0 und TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen:

- RSA+AES256-SHA (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-1 für Digest)
- RSA+AES256-SHA256 (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-256 für Digest)
- RSA+AES128-SHA (RSA für Schlüsselaustausch, AES-128 für die Verschlüsselung, SHA-1 für Digest)
- RSA+DES-CBC3-SHA (RSA für Schlüsselaustausch, Triple DES für die Verschlüsselung, SHA-1 für Digest)
- RSA+RC4128-MD5 (RSA für Schlüsselaustausch, RC4-128 für die Verschlüsselung, MD5 für Digest)
- RSA+RC4128-SHA (RSA für Schlüsselaustausch, RC4-128 für die Verschlüsselung, SHA-1 für Digest)
- RSA+AES128_GCM-SHA256 (RSA für Schlüsselaustausch, AES-128 für die Verschlüsselung, SHA-256 für Digest)
- RSA+AES256_GCM-SHA384 (RSA für Schlüsselaustausch, AES-256 für die Verschlüsselung, SHA-384 für Digest)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Elliptic Curve Diffie-Hellman für Schlüsselaustausch, RSA für Authentifizierung, AES-256 und GCM SHA-384 für Digest)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (Elliptic Curve Diffie-Hellman für Schlüsselaustausch, RSA für Authentifizierung, AES-256 und GCM SHA-384 für Digest)
- TLS_RSA_AES256_CBC_SHA256 (RSA für Authentifizierung, AES-256 und CBC SHA-256 für Digest)

Die effektive Größe der Verschlüsselungsschlüssel für die oben aufgeführten SSL/TLS-Standardverschlüsselungssa
sind wie folgt definiert:

- RC4-Algorithmus: 128 Bits (Stromverschlüsselung)
- Triple DES-Algorithmus: 3 x 64 Bits (effektive Größe: 3 x 56 = 168 Bits) (Blockgröße: 64 Bits)
- AES-Algorithmus: 128 Bits oder 256 Bits (Blockgröße: 128 Bits)
- Für RSA-Schlüsselaustausch und Authentifizierung werden Schlüssellängen (Modulus) zwischen 1024 Bits und 4096 Bits unterstützt.
- Für ECDH-Schlüsselaustausch werden die elliptischen Kurven NIST P-256 und NIST P-384 (256 Bits und 384 Bits Schlüssellänge) unterstützt.

Zum Auswählen der Verschlüsselungssammlung fügen Sie die folgende Konfigurationsoption im Abschnitt [WFClient] hinzu:

- SSLCiphers=GOV

Dieser Wert ist der Standardwert. Die Werte COM und ALL werden ebenfalls erkannt.
**Hinweis**: Wenn Sie dies nach dem Start von selfservice oder storebrowse ändern, müssen Sie wie bei der Konfiguration der TLS-Version Folgendes eingeben:
**killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

#### 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 |

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Zertifikat | Zertifizierungsstelle |
|---|---|
| GeoTrust_Global_CA.pem | GeoTrust |
| DigiCertGlobalRootCA.pem | DigiCert Global Root CA |

Für die Verwendung der Zertifikate von diesen Zertifizierungsstellen ist es nicht erforderlich, Stammzertifikate zu beziehen und auf dem Benutzergerät zu installieren. Wenn Sie sich jedoch entscheiden, eine andere Zertifizierungsstelle zu verwenden, müssen Sie ein Stammzertifikat dieser Zertifizierungsstelle haben und es auf jedem Benutzergerät installieren.

Die Citrix Workspace-App für Linux unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

> **Hinweis:**
>
> Die Citrix Workspace-App für Linux 1808 und höher verwendet das Tool ctx_rehash wie in den folgenden Schritten beschrieben.

#### Verwenden eines Stammzertifikats

Wenn Sie ein Serverzertifikat authentifizieren, das von einer Zertifizierungsstelle ausgestellt wurde und dem von dem Benutzergerät noch nicht vertraut wird, befolgen Sie die nachfolgenden Anweisungen, bevor Sie einen StoreFront-Store hinzufügen.

1. Beziehen Sie das Stammzertifikat im PEM-Format.
   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
   ```

#### Verwenden Sie ein Zwischenzertifikat

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. Besorgen Sie sich die einzelnen Zwischenzertifikate im PEM-Format.
   Tipp: Wenn Sie kein Zertifikat in diesem Format finden, konvertieren Sie mit dem Hilfsprogramm openssl ein Zertifikat im CRT-Format in eine PEM-Datei.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

2. Als Benutzer, der das Paket installiert hat (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`

#### Aktivieren der Smartcardunterstützung

Die Citrix Workspace-App für Linux unterstützt verschiedene Smartcardleser. Wenn die Smartcard-Unterstützung sowohl auf dem Server als auch in der Citrix Workspace-App aktiviert ist, können Smartcards zu folgenden Zwecken eingesetzt werden:

- Smartcard-Anmeldeauthentifizierung: Verwendung von Smartcards zur Authentifizierung von Benutzern an Citrix Virtual Apps-Servern.
- Smartcard-Anwendungsunterstützung: Zugriff auf lokale Smartcardgeräte über smartcard-fähige veröffentlichte Anwendungen.

Die sicherheitsrelevanten Smartcarddaten sollten 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.

Wichtig: Wenn Sie das Sun Ray-Terminal mit Sun Ray-Serversoftware (Version 2.0 oder höher) verwenden, installieren Sie zunächst das PC/SC SRCOM-Bypass-Paket, das unter http://www.sun.com/ zur Verfügung steht.

Weitere Informationen zur Konfiguration der Smartcardunterstützung auf den Servern finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

### Verbindung über Citrix Gateway

Citrix Gateway (früher Access Gateway) sichert Verbindungen mit StoreFront-Stores und ermöglicht Administratoren eine genaue Steuerung des Benutzerzugriffs auf Desktops und Anwendungen.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**Herstellen einer Verbindung mit Desktops und Anwendungen über Citrix Gateway**

1. Geben Sie die vom Administrator erhaltene Citrix Gateway-URL ein. Dafür stehen folgende Methoden zur Auswahl:

   - 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 wie beispielsweise https://gateway.company.com.
   - Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im Format wie beispielsweise 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 wahrscheinlich 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.

## 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. Diese Verschlüsselungssammlungen wurden in Citrix Receiver Version 13.10 als veraltet klassifiziert. Abwärtskompatibilität ist jedoch vorhanden.

In diesem Release wurden die TLS_RSA_-Verschlüsselungssammlungen vollständig entfernt. Stattdessen unterstützt dieses Release die erweiterten TLS_ECDHE_RSA_-Verschlüsselungssammlungen. Wenn Ihre Umgebung nicht mit den TLS_ECDHE_RSA_-Verschlüsselungssammlungen konfiguriert ist, werden die Starts von Clients aufgrund schwacher Verschlüsselung nicht unterstützt. Dieses Release unterstützt 1536-Bit-RSA-Schlüssel für die Clientauthentifizierung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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)

#### Konfigurieren von Verschlüsselungssammlungen

Um verschiedene Verschlüsselungssammlungen zu aktivieren, ändern Sie 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 Fehlerbehebung finden Sie unter Verschlüsselungssammlungen.

### Konfigurieren von veralteten Verschlüsselungssammlungen

> **Wichtig:**
>
> Ab Version 1903 wird Citrix nur die folgenden drei Verschlüsselungssammlungen unterstützen:
>
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 – GOV/ALL
> - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA – COM/ALL
>
> Der Abschnitt **Konfigurieren veralteter Verschlüsselungssammlungen** gilt nur für Version 1901 und früher. Ab Version 1903 werden nur die erweiterten TLS_ECDHE_RSA_-Verschlüsselungssammlungen unterstützt. Weitere Informationen, siehe Kryptographische Aktualisierung. Dieser Abschnitt dient nur als Referenz und ist nur für Kunden, die Version 1901 und ältere Versionen des Clients verwenden. Die unten genannten Verschlüsselungssammlungen sind veraltet und es besteht keine Abwärtskompatibilität.

Verschlüsselungssammlungen mit dem Präfix TLS_RSA_ bieten Forward Secrecy nicht. Diese Verschlüsselungssammlungen werden von der Branche mittlerweile allgemein als veraltet eingestuft. Um die Abwärtskompatibilität mit älteren Versionen von Citrix Virtual Apps and Desktops zu unterstützen, kann die Citrix Workspace-App für Linux diese Verschlüsselungssammlungen aktivieren.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Flags wurden erstellt, um die Verwendung veralteter Verschlüsselungssammlungen zu ermöglichen. In der Citrix Workspace-App 1808 für Linux sind diese Flags standardmäßig aktiviert. Die Kategorisierung der Verschlüsselungssammlungen als veraltet mit den AES- oder 3DES-Algorithmen wird jedoch nicht standardmäßig erzwungen. Sie können diese Flags jedoch ändern und verwenden, um die Kategorisierung strenger durchzusetzen.

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

> **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.

Informationen zum Konfigurieren von DTLS v1.2 finden Sie unter Adaptiver Transport.

**Voraussetzung**

Mit dem folgenden Schritt konfigurieren Sie dieses Feature auf dem Client:

Wenn .ICAClient bereits im Home-Verzeichnis 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**Konfigurieren von veralteten Verschlüsselungssammlungen**

1. Öffnen Sie die Datei **$ICAROOT/config/All_Regions.ini**.
2. Verwenden Sie im Abschnitt **Network\SSL** folgende drei Flags, um die veralteten Verschlüsselungssammlungen zu aktivieren oder zu deaktivieren:
   - **Enable_TLS_RSA_**: Die Standardeinstellung für das Flag Enable_TLS_RSA_ ist True.
     Legen Sie das Flag Enable_TLS_RSA_ auf True fest, um folgende Verschlüsselungssammlungen anzuzeigen:
     - 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

     > **Wichtig:**
     >
     > Legen Sie das Flag Enable_TLS_RSA_ auf True fest, um die anderen beiden Verschlüsselungssammlungen Enable_RC4-MD5 und Enable_RC4_128_SHA zu verwenden.

   - **Enable_RC4-MD5**: Die Standardeinstellung für das Flag Enable_RC4-MD5 ist **False**.
     Legen Sie dieses Flag auf True fest, um die Verschlüsselungssammlung RC4-MD5 zu aktivieren.
   - **Enable_RC4_128_SHA**: Die Standardeinstellung für das Flag Enable_RC4_128_SHA ist **False**.
     Legen Sie dieses Flag auf True fest, um die Verschlüsselungssammlung RC4_128_SHA zu aktivieren.
3. Speichern Sie die Datei.

Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

| Ciphersuite | Native Cyrpto Kit mode and cipher set | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Open | | FIPS | | | | SP800-52 | | |
| | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1) | Y | | Y | Y | | Y | Y | | Y |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1) | Y | | Y | Y | | Y | Y | | Y |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | Y | Y | | Y | Y | | Y | Y | |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2) | X | | | | | | | | |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2) | X | X | | | | | | | |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2) | X | | | | | | | | |
| TLS_RSA_WITH_AES_256_CBC_SHA (2) | X | | | | | | | | |
| TLS_RSA_WITH_AES_128_CBC_SHA (2) | X | X | | | | | | | |
| TLS_RSA_WITH_RC4_128_SHA (2) (3) | X | X | | | | | | | |
| TLS_RSA_WITH_RC4_128_MD5 (2) (3) | X | X | | | | | | | |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (2) | X | | | | | | | | |
| TLS_EMPTY_RENEGOTIATION_INFO_SCSV | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **Notes** | | | | | | | | | |
| (1) Ciphersuites that require TLS1.2/DTLS 1.2 | | | | | | | | | |
| (2) Ciphersuites disabled by default | | | | | | | | | |
| (3) Ciphersuites not available for DTLS protocol | | | | | | | | | |
| Y - Supported ciphersuites | | | | | | | | | |
| X-Deprecated ciphersuites | | | | | | | | | |

Tabelle 1 – Unterstützungsmatrix für Verschlüsselungssammlungen

> **Hinweis:**
>
> Alle oben genannten 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**.

# Problembehandlung

May 23, 2019

Dieser Artikel enthält Informationen für Administratoren zur Fehlerbehebung von Problemen in der Citrix Workspace-App für Linux.

## Verbindungsprobleme

Die folgenden Verbindungsprobleme kommen vor.

### Benutzer haben Probleme beim Herstellen einer Verbindung zu einer veröffentlichten Ressource oder einer 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,

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

müssen Sie den Server möglicherweise mit einer Clientzugriffslizenz (CAL) konfigurieren. Weitere Informationen zur Lizenzierung finden Sie unter Lizenzierung.

#### Wiederherstellung von Verbindungen zu Sitzungen ist manchmal nicht möglich

Manchmal sind Wiederverbindungen mit Sitzungen, die eine höhere Farbtiefe als der von der Citrix Workspace-App angeforderten verwenden, nicht möglich. Der Grund hierfür ist ein Speichermangel auf dem Server. 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 aber auch fehlschlagen, wenn immer noch nicht genügend Speicher auf dem Server verfügbar ist.

#### Verbindungsherstellung zu einem Server mit dem vollständigen Internetnamen ist nicht möglich

Citrix empfiehlt, DNS auf Ihrem Netzwerk zu konfigurieren, damit die Namen der Server, zu denen Sie eine Verbindung herstellen möchten, aufgelöst werden können. Wenn 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.

#### Bei der Verbindungsherstellung wird ein Proxyerkennungsfehler angezeigt

Wenn Ihre Verbindung für automatische Proxyerkennung konfiguriert ist und Sie beim Versuch, eine Verbindung herzustellen, die Fehlermeldung "Proxyerkennung fehlgeschlagen: JavaScript-Fehler" erhalten, kopieren Sie die Datei wpad.dat in das Verzeichnis $ICAROOT/util. Führen Sie den folgenden Befehl aus, wobei Hostname der Hostname des Servers ist, zu dem Sie eine Verbindung herstellen möchten:

> cat wpad.dat | ./pacexec pac.js FindProxyForURL http://hostname hostname 2>&1 | grep "undeclared variable"

Wenn Sie keine Ausgabe erhalten, liegt ein schwerwiegendes Problem in der Datei wpad.dat auf dem Server vor, das untersucht werden muss. Wenn Sie eine Ausgabe mit ungefähr folgendem Inhalt erhalten, können Sie das Problem jedoch beheben: "assignment to undeclared variable …". Öffnen Sie pac.js für jede in der Ausgabe aufgeführte Variable und fügen Sie am Anfang der Datei eine Zeile in folgendem Format hinzu, wobei "…" der Variablenname ist.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

> var …;

#### Sitzungsstart ist sehr langsam

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:
   - Ssllab.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.

#### Schwache Verschlüsselungssammlungen für SSL-Verbindungen

Für das Herstellen einer TLS-Verbindung bietet die Citrix Workspace-App für Linux standardmäßig einen moderneren und eingeschränkteren Satz von 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

#### Bei der Verwendung des UDT-Protokolls wird folgende Fehlermeldung angezeigt: Verbindung mit "…" wurde unterbrochen

Das Problem kann auftreten, wenn die Verbindung über einen Router erfolgt, wobei die maximale Übertragungseinheit für UDT kleiner ist als die Standardeinstellung von 1500 Bytes. Probieren Sie beides aus:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- Heben Sie die Auskommentierung des Eintrags udtMSS in $ICAROOT/config/All_Regions.ini und in $HOME/.ICAClient/All_Regions.ini auf.
- Legen Sie in einer Konfigurationsdatei folgende Einstellung fest: udtMSS=1000

#### 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 verhandeln. Weitere Informationen finden Sie unter Konfigurieren und Aktivieren von 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.
- Der Remotecomputer fordert falscherweise ein Clientzertifikat an. IIS sollte Zertifikate nur für “Citrix/Authentication/Certificate” akzeptieren oder anfordern.
- Andere Probleme:

### Anzeigeprobleme

#### Warum tritt Tearing auf dem Bildschirm auf?

Tearing wird verursacht, wenn Teile von zwei (oder mehreren) unterschiedlichen Frames gleichzeitig auf dem Bildschirm in horizontalen Blöcken angezeigt werden. Dies ist besonders bei großen Bereichen von sich schnell änderndem Inhalt auf dem Bildschirm erkennbar. Die Daten werden am VDA auf eine Weise erfasst, die Tearing verhindert, und sie werden an den Client auf eine Weise weitergegeben, dass kein Tearing auftritt. 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 initiiert. Abhängig von der auf dem Client verwendeten Grafikhardware und dem verwendeten Fenstermanager bietet Linux verschiedene Optionen. Diese Optionen lassen sich in zwei Lösungsgruppen einteilen:

- X11 GPU-Einstellungen

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 zu der 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.

- 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

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Falsches Anzeigen von Tastatureingaben bei der Verwendung der Tastatur

Wenn Sie keine englische Tastatur verwenden, stimmt die Bildschirmanzeige möglicherweise nicht mit der Tastatureingabe überein. In dieser Situation müssen Sie den verwendeten Tastaturtyp und das verwendete Tastaturlayout angeben. Weitere Informationen zur Angabe der Tastaturen finden Sie unter Steuern des Tastaturverhaltens.

#### Beim Verschieben von Seamlessfenstern wird der Bildschirm ständig neu aufgebaut

Einige Fenstermanager übertragen beim Verschieben von Fenstern ständig die neue Fensterposition, was zu einem wiederholten Neuaufbau des Bildschirms 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 für Linux erstellt Fenstersymbole, die mit den meisten Fenstermanagern verwendet werden können, aber nicht vollständig kompatibel mit den X Window-Kommunikationsrichtlinien für Clients (ICCCM, X Inter-Client Communication Convention Manual) sind.

#### 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.

#### Der Cursor ist schlecht sichtbar

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

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)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

3. Speichern und schließen Sie die Datei.

#### Farbwechsel auf dem Bildschirm

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.

#### Schnelle Farbwechsel bei TrueColor-Anzeigen

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.

#### Japanische Zeichen werden nicht richtig angezeigt

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 führen, wenn auf dem Server gespeicherte Dateien lokal angezeigt werden oder lokal gespeicherte Dateien auf dem Server angezeigt werden. Dies Problem betrifft auch japanische Zeichen in Parametern, die bei der erweiterten Parameterübergabe verwendet werden.

#### Benutzer möchten eine Sitzung erstellen, die bildschirmübergreifend angezeigt wird

Sitzungen im Vollbildmodus gehen standardmäßig über alle Monitore. Es gibt außerdem für Befehlszeilen eine Steuerungsoption für die Anzeige auf mehreren Monitoren: -span. Hiermit können Vollbildschirmsitzungen über mehrere Monitore gestreckt werden.

Mit der Symbolleistenfunktionalität von Desktop Viewer können Sie in einer Sitzung zwischen Fenstermodus und Vollbildmodus wechseln, einschließlich Multimonitorunterstützung für die Monitore. Einzelheiten finden Sie unter Verbessern der Benutzererfahrung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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 dies der einzige Optionswert ist, wird wfica anschließend beendet.

Wenn o angegeben wird, enthält das Sitzungsfenster das Weiterleitungsattribut “override-redirect”.

Achtung: Von der Verwendung dieses Optionswerts wird abgeraten. Er ist als letzter Ausweg 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 und 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 ein Fenster mit override-redirect. Sie können ein solches Fenster mit -span o einrichten.

Erstellen einer Sitzung, die sich über mehrere Monitore erstreckt, an der Befehlszeile

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]]]

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

wobei w, x, y und z Monitornummern sind, 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 und 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 selfservice starten oder über einen Browser eine Verbindung zum Webinterface herstellen. 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 Citrix Virtual Apps and Desktops-Sitzungen.

Wenn Sie selfservice oder storebrowse gestartet haben, entfernen Sie die von ihnen gestarteten Prozesse, damit die neue Umgebungsvariable wirksam wird. Entfernen Sie die Prozesse mit folgendem Befehl:

killall AuthManagerDaemon ServiceRecord storebrowse

#### Der Vollbildmodus einer Sitzung kann nicht mit der Escape-Taste beendet werden, um lokale Anwendungen oder eine andere Sitzung zu verwenden

Der Grund dafür ist, dass 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 zur Problembehebung 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. Das Feature “Tastaturtransparenz” wird hiermit deaktiviert. Sie müssen jedoch u. U. die ICA-Datei durch Hinzufügen dieser Einstellung in der Datei All_regions.ini überschreiben.

### Browserprobleme

#### 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. Dies führt zur Ausführung einer lokalen Anwendung. Informationen zum Deaktivieren der Server-zu-Client-Inhaltsumleitung finden Sie unter Einrichten der Server-zu-Client-Inhaltsumleitung.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Beim Zugreifen auf veröffentlichte Ressourcen fordert der Browser den Benutzer zum Speichern einer Datei auf

Andere Browser als Mozilla, Firefox und Chrome müssen möglicherweise konfiguriert werden, bevor Sie auf eine veröffentlichte Ressource zugreifen können. Wenn Sie eine Verbindung über das Webinterface herstellen, können Sie möglicherweise die Webinterface-Homepage mit der Liste der Ressourcen öffnen. 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.

#### Konfigurieren eines anderen Browsers für das Webinterface

Die Angaben hängen vom Browser ab, aber Sie können die MIME-Datentypen im Browser so einrichten, dass $ICAROOT/wfica als Hilfsprogramm ausgeführt wird, wenn der Browser auf Daten mit dem MIME-Typ “application/x-ica” oder eine ICA-Datei trifft.

#### Der Installer unterstützt einen bestimmten Browser nicht

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.

#### Beim Start von Desktops oder Anwendungen in Firefox geschieht nichts

Versuchen Sie ein Aktivieren des ICA-Plug-Ins.

#### Das ICA-Plug-In ist in Firefox aktiviert, jedoch können Desktop- und Anwendungssitzungen nicht gestartet werden

Versuchen Sie ein Deaktivieren des ICA-Plug-Ins.

### Andere Probleme

Folgende Probleme können ebenfalls auftreten.

#### Hat der Server die Citrix Workspace-App angewiesen, eine Sitzung zu schließen?

Sie können sich mit dem Programm *wfica* anmelden, wenn Receiver vom Server den Befehl erhalten hat, die Sitzung zu beenden.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

Damit diese Informationen vom Syslog aufgezeichnet werden, fügen Sie *SyslogThreshold* mit dem Wert 6 im Abschnitt [WFClient] der Konfigurationsdatei hinzu. Hierdurch wird die Protokollierung von Nachrichten 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 Aktivieren der Protokollierung. Weitere Informationen zur Konfiguration von syslog finden Sie unter Weitere Informationen zur syslog-Konfiguration.

#### Einstellungen der Konfigurationsdatei funktionieren nicht mehr

Für jeden Eintrag in wfclient.ini muss ein entsprechender Eintrag in All_Regions.ini gemacht werden, damit die Einstellung wirksam wird. Zusätzlich muss für jeden Eintrag in den Abschnitten [Thinwire3.0], [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.

#### Beim Ausführen veröffentlichter Anwendungen, die auf einen seriellen Port zugreifen, treten Probleme auf

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, dass keine Anwendungen vorhanden sind, die den seriellen Port vorübergehend gesperrt haben oder die den seriellen Port gesperrt haben und beendet wurden, ohne ihn wieder 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.

#### Die Citrix Workspace-App kann nicht gestartet werden

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. Die Variable muss richtig definiert werden, wenn Sie die Citrix Workspace-App nicht im Standardverzeichnis installiert haben. Citrix empfiehlt hierfür zwei Lösungsvorschläge:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

- 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 zum Installieren 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.

#### Ermitteln der Versionsnummer für das Citrix CryptoKit (früher SSLSDK) oder OpenSSL

Führen Sie den folgenden Befehl aus, um die Versionsnummer für das ausgeführte Citrix SSLSDK oder OpenSSL zu bestätigen:
strings libctxssl.so | grep “Citrix SSLSDK”

Sie können diesen Befehl auch für AuthManagerDaemon oder PrimaryAuthManager ausführen

#### Tastenkombinationen funktionieren nicht richtig

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. Auf diese Weise wird die lokale Tastenkombination Alt+Ctrl+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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

#### Remote-Tastatur für Kroatisch soll aktiviert werden

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.

#### Verwenden einer japanischen Tastatur auf dem Client

Zum Konfigurieren einer japanischen Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Japanese (JIS)

#### Verwenden einer ABNT2-Tastatur auf dem Client

Zum Konfigurieren einer ABNT2-Tastatur aktualisieren Sie den folgenden Eintrag in der Konfigurationsdatei wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

#### Einige Tasten auf der lokalen Tastatur verhalten sich nicht wie erwartet

Wählen Sie in der Liste in der Datei $ICAROOT/config/module.ini das passendste Serverlayout aus.

#### Windows Media Player gibt bestimmte Dateiformate nicht wieder

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. Dies sollte erkannt werden und auf dem Server eine Fehlermeldung auslösen, die darauf hinweist, dass Windows Media Player beim Wiedergeben der Datei ein Problem hatte. Erneutes Wiedergeben der Datei in der Sitzung funktioniert normalerweise, weil das Format von der Citrix Workspace-App abgelehnt wird und der Server dann ein anderes Format anfordert oder das Medium selbst wiedergibt.

Manchmal wird nicht erkannt, dass kein passendes Plug-In vorhanden ist, 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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. Dadurch wird das Format deaktiviert.
6. Wiederholen Sie die Schritte 2 bis 5 (oben) 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 u. U. ein GStreamer-Plug-In installieren und ihn decodieren.

#### Ich möchte eine Einstellung für einen seriellen Anschluss konfigurieren

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 bei der Verbindungskonfiguration

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**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: "…"

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-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. Sollte das Problem weiterhin auftreten, prüfen Sie die Eigenschaften des Desktopsymbols oder des Menüeintrags und Citrix Virtual Apps-Datei, auf die das Symbol oder der Eintrag verweist.

### PAC-Datei-Fehler

Folgende Fehler können auftreten, wenn Ihre Bereitstellung die automatische Proxykonfiguration mit PAC-Dateien verwendet:

**Proxyerkennungsfehler: Falsche Autokonfigurations-URL.**

Eine Adresse im Browser wurde mit einem falschen URL-Typ angegeben. Gültige Typen sind http:// und https://. Andere Typen werden nicht unterstützt. Ändern Sie die Adresse zu einem gültigen URL-Typ und versuchen Sie es erneut.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**Proxyerkennung fehlgeschlagen: HTTP-Download von PAC-Skript ist fehlgeschlagen: Verbindung fehlgeschlagen.**

Überprüfen Sie, ob Name oder Adresse falsch eingegeben wurden. Ist dies der Fall, berichtigen Sie die Adresse und versuchen Sie es erneut. Wenn dies nicht der Fall ist, könnte der Server ausgefallen sein. Versuchen Sie es später erneut.

**Proxyerkennungsfehler: PAC-Skript-HTTP-Download fehlgeschlagen: Pfad nicht gefunden.**

Die angeforderte PAC-Datei ist nicht auf dem Server. Wechseln Sie entweder den Server oder konfigurieren Sie den Browser neu.

**Proxyerkennungsfehler: PAC-Skript-HTTP-Download fehlgeschlagen.**

Die Verbindung wurde während des Downloads der PAC-Datei unterbrochen. Stellen Sie die Verbindung wieder her und versuchen Sie es erneut.

**Proxyerkennungsfehler: Leeres Autokonfigurationsskript.**

Die PAC-Datei ist leer. Wechseln Sie entweder den Server oder konfigurieren Sie den Browser neu.

**Proxyerkennungsfehler: Keine JavaScript-Unterstützung.**

Die ausführbare PAC-Datei oder die Textdatei pac.js fehlen. Installieren Sie die Citrix Workspace-App erneut.

**Proxyerkennungsfehler: JavaScript-Fehler.**

Die PAC-Datei enthält ungültiges JavaScript. Ändern Sie die PAC-Datei auf dem Server. Siehe auch Verbindungsprobleme.

**Proxyerkennungsfehler: Falsches Ergebnis vom Proxy-Autokonfigurationsskript.**

Eine ungültige Antwort wurde vom Server gesendet. Beheben Sie das Problem auf dem Server oder konfigurieren Sie den Browser neu.

### Andere 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 diese Meldung 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.**

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

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.**

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 Name des Servers konnte nicht aufgelöst werden.

**In mindestens eine Datei kann nicht geschrieben werden: "…". Beheben Sie Probleme beim Speicherplatz auf der Festplatte oder der Verbindung 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.

## Senden von Diagnoseinformationen an den technischen Support von Citrix

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, diesen Vorgang auszuführen, während eine Sitzung geöffnet ist und möglichst während das Problem auftritt.

   Es wird eine Datei generiert, die detaillierte Diagnoseinformationen enthält, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

# SDK und API

November 15, 2018

## Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für zusätzliche virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalanwendungen sind auf Citrix Virtual Apps oder Citrix Virtual Desktops-Servern. Diese Version des SDK bietet Unterstützung zum Schreiben neuer virtueller Kanäle für die Citrix Workspace-App für Linux. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an 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 zum SDK finden Sie unter Citrix Virtual Channel SDK for Citrix Workspace app for Linux.

## Befehlszeilenreferenz und -parameter

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, um ein Ökosystem kostengünstiger Geräte mit niedrigem Energieverbrauch, hoher Leistung und innovativen Formfaktoren zu ermöglichen.

Das Platform Optimization SDK kann von Entwicklern genutzt werden, um die Leistung von Linux-basierten Geräten zu verbessern, indem sie Plug-In-Erweiterungen für die ICA-Engine-Komponente

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

(wfica) der Citrix Workspace-App für Linux entwickeln. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

© 1999-2019 Citrix Systems, Inc. All rights reserved. 

**Locations**
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, 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).