Citrix Receiver für Windows 4.9 LTSR

Contents

Neue Features in 4.9 LTSR

June 21, 2019

Wichtige Informationen zu Citrix Receiver

Einstellung der Unterstützung für bestimmte TLS-Versionen in Citrix Cloud

Um die Sicherheit von Verbindungen mit Citrix Cloud zu erhöhen, wird ab dem 15. März 2019 jegliche Kommunikation über TLS 1.0 und 1.1 von Citrix blockiert. Die Einstellung der Unterstützung hat jedoch keine Auswirkungen auf Benutzer von Kunden, die Citrix Receiver für Windows 4.9 LTSR verwenden. Weitere Informationen finden Sie unter Einstellung der Unterstützung für bestimmte TLS-Versionen in Citrix Cloud.

Cumulative Update 7 ist jetzt verfügbar

Cumulative Update 7 (CU7) für Citrix Receiver für Windows 4.9 LTSR wurde am 21. Juni 2019 veröffentlicht. CU7 enthält über ein Dutzend Fixes für von Kunden gemeldete Probleme und trägt zur Stabilität und größerer Benutzerfreundlichkeit dieses LTSR bei. Aufbauend auf Citrix Receiver für Windows 4.9 enthält CU7 zehn Fixes von CU6, mehr als ein Dutzend Fixes von CU5 und CU4, 20 Fixes von CU3, 18 Fixes von CU2 und mehr als 15 Fixes von CU1. CU7 ist auf der Citrix Website unter Download zum Herunterladen verfügbar.

Kompakteres Installationsprogramm

In diesem Release wurde die Größe des Installationsprogramms von Citrix Receiver für Windows auf 39,9 MB reduziert. Dies stellt eine Verringerung um 15 % im Vergleich zu früheren Releases dar.

Neuer externer Beacon für StoreFront-Konto

In einem StoreFront-Konto wird ping.citrix.com anstelle von www.citrix.com als externer Beacon verwendet.

Ab Citrix Receiver für Windows Version 4.9 sind keine benutzerkonfigurierbaren Änderungen erforderlich.

Bei Verwendung einer Vorgängerversion von Citrix Receiver für Windows empfiehlt Citrix, den externen Beacon www.citrix.com durch ping.citrix.com zu ersetzen.

Weitere Informationen zum externen Beacon finden Sie im Knowledge Center-Artikel CTX218708.

Weitere Informationen zur Konfiguration des externen Beacon in StoreFront finden Sie unter Konfigurieren von Beacons.

> **Hinweis**
>
> Ignorieren Sie diesen Hinweis, wenn www.citrix.com nicht als externer Beacon für das StoreFront-Konto konfiguriert ist.

Behobene Probleme

May 23, 2019

Citrix Receiver für Windows 4.9 LTSR CU6 Hotfix 1 (4.9.6001)

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU6

Sicherheitsprobleme

- Dieser Fix behebt ein Sicherheitsproblem. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX251986. [LD1518]

Citrix Receiver für Windows 4.9 LTSR CU6

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU5

HDX MediaStream Windows Media-Umleitung

- Der clientseitige Inhaltsabruf bei Windows Media-Umleitung schlägt u. U. fehl. Das Problem tritt auf, wenn Sie Multimediadateien wiedergeben, die Skriptstreams enthalten, die aus einem Live-Webstream archiviert wurden. [LC7948]

Installieren, Deinstallieren und Aktualisieren

- Bei einem Upgrade von Citrix Receiver für Windows auf Version 4.9 LTSR wird der Registrierungsschlüssel, der für benutzerdefinierte virtuelle Kanäle erforderlich ist, möglicherweise nicht beibehalten. [LD0633]

Tastatur

- Wenn das Feature **Lokaler IME** oder das Feature **Lokale Tastaturlayoutsynchronisierung** aktiviert ist und Sie drücken eine Tastenkombination, die die rechte Strg- und die rechte Umschalttaste enthält, bleibt die Umschalttaste möglicherweise in der Abwärtsposition hängen. [LD0585]
- Wenn die Option **Ja, ich bevorzuge das lokale Tastaturlayout statt des Tastaturlayouts des Remoteservers** aktiviert ist, wird das zuletzt eingegebene Zeichen möglicherweise nicht korrekt verarbeitet. Das Problem tritt auf, wenn Sie von Koreanisch nach Englisch wechseln, indem Sie auf die rechte Alt-Taste klicken. Das Problem besteht nach der Anwendung dieses Updates u. U. weiterhin, wenn Sie die Maus verwenden. [LD0825]

Sitzung/Verbindung

- Die Host-zu-Client-Umleitung funktioniert möglicherweise nicht, wenn Anwendungen von Drittanbietern verwendet werden. Das Problem tritt auf, wenn diese Anwendungen eine spezielle Web-URL verwenden, die HTTPS- und HTTP-Adressen enthält. [LD0484]
- Wenn Anwendungsfortbestehen konfiguriert ist, können veröffentlichte Anwendungen eine vorhandene Datei möglicherweise nicht erneut öffnen, nachdem die Sitzung getrennt wurde. [LD0742]
- Sie verwenden das Windows 7-Grunddesign und deaktivieren die Hardwarebeschleunigung (GDI-Modus) auf dem Benutzergerät. Wenn Sie zwischen den lokalen und veröffentlichten Seamlessanwendungen wechseln, treten möglicherweise Anzeigeprobleme auf. [LD0853]
- Wenn Sie die NVIDIA-GPUs auf dem VDA verwenden und den neuesten NvENC in der GPU optimieren, kann es zu fehlerhafter h.264-DXVA-Dekodierung kommen.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRender

  Name: MaxNumRefFrames

  Typ: DWORD

  Wert: Zwischen 2 und 8 [LD0943]

Benutzererfahrung

- Wenn Sie ein Nicht-Seamlessanwendungsfenster maximieren, ist das Anwendungsfenster fehlerhaft. [LD0755]

- Wenn Sie einen veröffentlichten Windows 7-Desktop starten, kann es zu Verzögerungen kommen, wenn Sie einen Mauszeiger innerhalb der Citrix Receiver für Windows-Sitzung ziehen. [LD0923]

Citrix Receiver für Windows 4.9 LTSR CU5

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU4

Inhaltsumleitung

- Wenn Sie das Standardprogrammfenster schließen, während Sie die für Dateitypzuordnung aktivierte Erweiterung zum ersten Mal starten, wird bei nachfolgenden Starts dieser Erweiterung u. U. diese Fehlermeldung angezeigt:

  Auf das angegebene Gerät bzw. den Pfad oder die Datei kann nicht zugegriffen werden. Sie verfügen ggf. nicht über ausreichende Berechtigungen, um auf das Element zugreifen zu können. [LD0026]

Tastatur

- Beim Verwenden eines Barcodelesers gehen möglicherweise Daten verloren, wenn eine große Datenmenge gesendet wird. [LD0243]

Sitzung/Verbindung

- Nach dem Upgrade von Citrix Receiver für Windows auf Version 4.9.1000 zeigt der CDViewer möglicherweise einen grauen Bildschirm an, wenn Sie sich abmelden. [LC9290]
- Versuche, eine Anwendung zu starten, schlagen möglicherweise fehl und folgende Fehlermeldung wird angezeigt:

  Die Anwendung kann nicht gestartet werden. Wenden Sie sich mit den folgenden Informationen an den Helpdesk: Citrix Receiver kann nicht geöffnet werden.

  - Um den Fix zu aktivieren, muss der Administrator den folgenden Registrierungsschlüssel festlegen:

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    Name: EngineTimeout

    Typ: DWORD

    Wert: Mehr als 20 Sekunden

  - Um den Fix zu aktivieren, muss der Benutzer den folgenden Registrierungsschlüssel festlegen:

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    Name: EngineTimeout

    Typ: DWORD

    Wert: Über 20 Sekunden, z. B. EngineTimeout=20 [LC9771]

- Starten von mehreren Anwendungen auf einem gehosteten, freigegebenen Desktop. Wenn Sie zwischen den Clients wechseln oder einen Trenn- bzw. Wiederherstellungsvorgang durchführen, wird möglicherweise folgende Fehlermeldung angezeigt:

  Citrix HDX Engine funktioniert nicht mehr.
  Eine Ausnahme führte dazu, dass das Programm nicht mehr ordnungsgemäß funktioniert. Please close the program. [LC9772]

- Anwendungen, die mit Citrix Receiver für Windows gestartet werden, werden möglicherweise auf den sekundären Monitor gespiegelt. [LC9893]

- Wenn die Seamlessanwendung minimiert wird, wird sie als Miniaturversion der Anwendung angezeigt. Stattdessen sollte sie als minimiertes Fenster oder auf der Taskleiste angezeigt werden. [LD0034]

- Die veröffentlichte Instanz einiger Drittanbieteranwendungen wird bei Verwendung einer NVIDIA-Grafikkarte mit der GPU u. U. als transparente Anwendung geöffnet. [LD0175]

- Die lokalen Anwendungsverknüpfungen, die über das Symbol der Systemsteuerung erstellt werden, können nicht mit dem in Citrix Studio konfigurierten **KEYWORDS:Prefer** gestartet werden. [LD0288]

- Wenn Sie mit der administrativen Gruppenrichtlinienobjektvorlage einen zweiten Store hinzufügen, fehlen u. U. die Beacons und andere Informationen im zweiten Store. [LD0413]

Systemausnahmen

- Wenn die Richtlinie für bidirektionale Inhaltsumleitung aktiviert ist, wird der Prozess Redirector.exe möglicherweise unerwartet beendet, wenn Sie versuchen, eine Webseite im lokalen Web zu öffnen. In dem Fall funktioniert die bidirektionale Inhaltsumleitung nicht und die folgende Fehlermeldung wird angezeigt:

  Citrix FTA, URL Redirector funktioniert nicht mehr. [LD0420]

- Der wfica32.exe-Prozess kann unerwartet beendet werden. Das Problem tritt auf, wenn die Proxyeinstellungen konfiguriert sind und Sie versuchen, in Citrix Receiver für Web eine neue Sitzung zu starten. [LD0548]

Benutzeroberfläche

- Die Mausklicks erzeugen möglicherweise keine Antworten in der Remotesitzung. Dieses Problem kann auftreten, wenn Sie das Fenster **Einstellungen** über die Symbolleiste Desktop Viewer öffnen und die Einstellung **MouseTimer** auf einen anderen Wert als den Standard festlegen. [LD0260]
- Wenn Sie die Option **Receiver zurücksetzen** auswählen, fordert Citrix Receiver für Windows möglicherweise die Installation des .NET Framework 3.5 unter Microsoft Windows Version 10. [LD0690]

Citrix Receiver für Windows 4.9 LTSR CU4

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU3

Probleme bei Clientgeräten

- Bei Verwendung der aktivierten Richtlinie **Automatische Anzeige der Tastatur** wird die automatische Bildschirmtastatur möglicherweise nicht in einer Sitzung eingeblendet. [LC9925]

HDX MediaStream Windows Media-Umleitung

- Die umgeleiteten Multicast-Streams, die eingebettete Skripts enthalten, können möglicherweise den Inhalt vom Client nicht abrufen. Anstelle des Videos wird ein schwarzer Bildschirm angezeigt. [LC9775]

Tastatur

- Vor diesem Fix unterstützte die Bloomberg-Tastatur 4 (Starboard) nur den PC-Modus. Mit diesem Fix unterstützt die Bloomberg-Tastatur 4 (Starboard) den PC- und den KVM-Modus. [LC9984]

Anmeldung und Authentifizierung

- Wenn Sie mit Citrix Receiver für Windows ein Konto hinzufügen, wird bei der Eingabe der Store-URL möglicherweise folgende Fehlermeldung angezeigt: **Es konnte kein Kontakt mit dem Authentifizierungsdienst hergestellt werden.** Dieses Problem tritt auf, wenn eine StoreFront-URL mit der Textzeichenfolge `citrix.com` beginnt. [LC9631]

Sitzung/Verbindung

- Bei der Konfiguration “KEYWORDS:prefer” in Citrix Studio werden die Befehlszeilenoption oder das in der Anwendungsverknüpfung auf dem lokalen Benutzergerät angegebene Argument möglicherweise nicht berücksichtigt. [LD0060]
- Dieser Fix führt die folgenden Änderungen durch:
  - Wenn Sie edtMSS und OutBufLength benutzerdefiniert festlegen, wird OutBufLength von edtMSS überschrieben.
  - Parameternamen in den Dateien All_regions.ini und defaulit.ica sowie in der Systemregistrierung werden von udt* in edt* geändert.

  Hinweis:
  Nach einem Upgrade als Administrator werden der Benutzerregistrierungsschlüssel und die Einträge unter folgendem Registrierungsschlüssel nicht von udt* in edt* umbenannt: HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT. Außerdem wird der Parameterwert nicht beibehalten. [LD0098]
- Die über das Gruppenrichtlinienobjekt hinzugefügten Stores werden möglicherweise nicht entfernt, auch wenn Sie den Store im Gruppenrichtlinienobjekt aktualisieren oder entfernen. [LD0147]

Systemausnahmen

- Citrix Receiver für Windows wird möglicherweise unerwartet beendet, wenn Sie sich an einem Store anmelden. [LC8271]
- Citrix Receiver für Windows wird möglicherweise unerwartet beendet und es wird folgende Fehlermeldung angezeigt: **Citrix HDX Engine funktioniert nicht mehr.**

  Das Problem tritt auf, wenn sich im Grafikmodul ein Trap befindet. [LC9466]
- Der wfica32.exe-Prozess wird möglicherweise unerwartet beendet, wenn Sie sich vom System abmelden. [LC9892]

TWAIN

- Citrix Receiver für Windows 4.7 oder höher kann die Scanner möglicherweise nicht umleiten. Dieses Problem tritt auf, wenn die Twain 2.0-Treiber nicht auf dem Benutzergerät vorhanden sind. [LC8215]

Benutzererfahrung

- Wenn Sie eine VPN-Verbindung mit bestimmten Drittanbieteranwendungen herstellen, ist Citrix Receiver für Windows möglicherweise rund 15 Minuten lang nicht verwendbar. [LC9302]
- Wenn Sie eine Verbindung von Citrix Receiver für Windows zu einem Linux-VDA 7.17 oder höher herstellen, kann die GPU-Auslastung der Citrix HDX Engine hoch sein. [LC9506]
- Bei Verwendung des Eingabemethoden-Editors (IME) für Japanisch wird in einer Anwendung im Seamlessmodus eingegebener Text möglicherweise nicht angezeigt. Das Problem tritt bei kleinen Schriftgraden auf.

  Zum Implementieren dieses Fixes legen Sie folgende Registrierungsschlüssel fest:

  - *Auf 32-Bit-Systemen*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client

    Name: DisableD3DRenderWidthHeightCheck

    Typ: REG_DWORD

    Wert: 1
  - *Auf 64-Bit-Systemen*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow 6432Node\Citrix\ICA Client

    Name: DisableD3DRenderWidthHeightCheck

    Typ: REG_DWORD

    Wert: 1 [LC9882]

Benutzeroberfläche

- Das Tool **Konfigurationsprüfung** zur Prüfung der Single Sign-On-Konfiguration kann während der Prüfung hängenbleiben. [LC9625]

Citrix Receiver für Windows 4.9 LTSR CU3

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU2

Probleme bei Clientgeräten

- Bestimmte DVD-Videos werden möglicherweise nicht in einer Sitzung über ein zugeordnetes Client-Laufwerk wiedergegeben. [LC8912]

Inhaltsumleitung

- Wenn Sie bidirektionalen Inhalt an einen VDA umleiten, wird eine zweite URL in einem neuen Browser geöffnet, wenn der Browser bereits geöffnet ist. [LC9157]
- Bei der Verwendung von Citrix Receiver für Windows mit der Citrix XenApp Services-Site werden Anwendungen und Symbole u. U. teilweise Dateitypen zugeordnet. [LC9402]

Installieren, Deinstallieren und Aktualisieren

- Wenn Sie Citrix Receiver für Windows über den System Center Configuration Manager (SCCM) aktualisieren, fordert Receiver für Windows möglicherweise einen Systemneustart an. [LC9706]

Tastatur

- Versuche, die Serverstandardeinstellungen oder die gewünschten Tastaturlayouts mit APPSRV.INI oder ICA-Dateien zu verwenden, die von StoreFront heruntergeladen wurden, schlagen möglicherweise fehl.

  Folgende Einschränkungen gelten:

  - Sie müssen das Tastaturlayout in der Sitzung manuell über die Systemsteuerung festlegen, wenn Sie die Konfiguration zum ersten mal vornehmen, auch wenn Sie das Layout zuvor festgelegt haben.
  - Sie müssen die Synchronisierung des Tastaturlayouts in **Erweiterte Einstellungen** auf **Nein** festlegen. Wenn Sie das Layout auf **Ja** festlegen, wird der lokale IME umgeleitet. [LC9593]

Anmeldung und Authentifizierung

- Nach dem Neustart des Prozesses AuthManSvr.exe schlagen Versuche fehl, sich von Citrix Receiver für Windows abzumelden. [LC7981]

Drucken

- Wenn Sie versuchen, große Dokumente zu drucken, die den PDF-Drucker als Druckeinstellung verwenden, reagiert der Drucker möglicherweise nicht mehr oder folgende Fehlermeldung wird angezeigt:

  "Emf viewer has stopped working." [LC8882]

Sitzung/Verbindung

- Der Desktop verschwindet möglicherweise bald nachdem Sie den Desktop gestartet haben. Das Problem tritt aufgrund der doppelten TLS-Pakete auf, die von Citrix Receiver für Windows gesendet werden. [LC8724]
- Wenn Sie versuchen, einen Desktop in Microsoft Internet Explorer 11 zu starten, wird möglicherweise folgende Fehlermeldung angezeigt:

  "Die Verbindung zu ist fehlgeschlagen. Status: (Unbekannter Clientfehler 0)" [LC8841]
- Wenn Sie die Aggregation zwischen zwei Websites in StoreFront einrichten, wird die Vorabstartsitzung nicht erstellt. [LC8847]
- In einem Double-Hop-Szenario mit VDA für Desktop-OS im ersten Hop und einer innerhalb eines VDA gestarteten Anwendung im zweiten Hop kann der Bildschirm beim erneuten Verbinden mit dem ersten Hop, der auf dem VDA für Desktop-OS ausgeführt wird, einige Sekunden lang flackern. [LC9071]
- Versuche, Desktops mit Citrix Receiver für Windows zu starten, schlagen möglicherweise nach einem Timeout fehl. Das Problem tritt selbst dann auf, wenn Sie in StoreFront den Wert für das Starttimeout in der Einstellung **LaunchTimeoutMs** erhöhen. [LC9369]
- Nach dem Ändern des internen Beaconpunkts in StoreFront können Sie möglicherweise keine Anwendungen von Citrix Receiver für Windows starten, bis Sie Citrix Receiver neu gestartet haben. [LC9442]
- Wenn Sie mit den Tastenkombinationen Win+Tab oder Alt+Tab zwischen mehreren veröffentlichten Anwendungen wechseln, steigt die Anzahl an GDI-Objekten auf dem Client möglicherweise an, bis die Anwendungen nicht mehr reagieren und schwarze Pixel anzeigen. [LC9655]

Smartcards

- Wenn Sie versuchen, einen veröffentlichten Desktop mit Smartcardauthentifizierung im Vollbildmodus zu starten, wird die PIN-Eingabeaufforderung möglicherweise nicht auf dem Desktop Viewer angezeigt. [LC8579]

Systemausnahmen

- Wenn über ein touchfähiges Gerät eine Verbindung mit einem VDA hergestellt wird, wird der Prozess wfica32 möglicherweise gelegentlich beendet. [LC9228]
- Der Prozess wfica32.exe wird möglicherweise sporadisch beendet. [LC9397]

Benutzererfahrung

- Das Citrix Receiver für Windows-Anwendungsfenster wird möglicherweise automatisch angezeigt, selbst wenn Sie die Anwendung nicht geöffnet haben. Das Problem tritt auf, wenn der Administrator veröffentlichte Anwendungen aus Citrix Studio entfernt oder deaktiviert. [LC8176]
- Die Symbole im Startmenü und in der Taskleiste flackern möglicherweise, wenn Sie die Anwendungen in Citrix Receiver für Windows aktualisieren. [LC8890]
- Der Mauszeiger fehlt in der Citrix Receiver für Windows-Sitzung oder wird zu klein angezeigt. Das kann passieren, wenn mehrere Monitore mit unterschiedlicher Auflösung auf Endpunkten unter Microsoft Windows 10 verwendet werden. [LC8915]
- Der Mauszeiger wird in der Citrix Receiver für Windows-Sitzung möglicherweise zu klein angezeigt. Dieses Problem kann auftreten, wenn Sie eine hohe Anzeigeauflösung auf den Endpunkten verwenden, auf denen Version 1607 von Microsoft Windows 10 oder höher ausgeführt wird.

  Folgende Einschränkungen gelten:

  - Der Mauszeiger wird klein, wenn Sie im invertierten Seamlessmodus mit der linken Maustaste klicken. Er wird wieder normal, wenn Sie die Maustaste loslassen.
  - Auf VDAs für Desktopbetriebssysteme und VDA für Serverbetriebssysteme mit einer Windows-Version vor Version 1607 von Windows 10 und Windows Server 2016 wird der Mauszeiger bei niedriger Auflösung leicht vergrößert.
  - In einem Szenario mit mehreren Monitoren kann der Mauszeiger nicht richtig skaliert werden, wenn die DPI der Monitore unterschiedlich sind. Das Problem tritt auf, wenn das Fenster über Monitore hinweg verschoben wird und kann durch Ändern der Größe des Anwendungsfensters korrigiert werden.
  - Auf dem Desktop Viewer in gestarteten Desktops ist der Mauszeiger immer noch klein. [LC9221]
- Dieser Fix bietet kleinere Leistungs- und Qualitätsverbesserungen für Enlightened Data Transport (EDT). [LC9417]

Citrix Receiver für Windows 4.9 LTSR CU2

Verglichen mit Citrix Receiver für Windows 4.9 LTSR CU1

Probleme bei Clientgeräten

- Wenn ein Benutzer bei einem VoIP-Anruf eine veröffentlichte Anwendung zur Audioaufnahme startet und die Aufzeichnung beginnt, ist das Mikrofonaudio des Benutzers nicht mehr zu hören.

Der Benutzer kann seinen Gesprächspartner hören. [LC8713]

HDX MediaStream Flash-Umleitung

- Wenn die Einstellung HDX MediaStream Flash-Umleitung aktiviert ist und Sie trennen die Sitzung, dann wird der Prozess PseudoContainer2.exe möglicherweise unerwartet beendet. [LC8802]

HDX MediaStream Windows Media-Umleitung

- Beim Senden von Nachrichten mit bestimmten Drittanbieteranwendungen ist kein Benachrichtigungston zu hören. Dieser Fix bietet verbesserte Unterstützung für Töne, die nur kurz wiedergegeben werden. [LC8468]

Lokale HDX Seamless-Apps

- Das Starten von Anwendungen kann fehlschlagen, wenn das Feature des lokalen App-Zugriffs **KEYWORDS:prefer="*pattern*"** mit einer 64-Bit-Anwendung verwendet wird, die beim Start konfiguriert werden muss. [LC8580]

Installieren, Deinstallieren und Aktualisieren

- Nach einem Upgrade von Citrix Receiver für Windows sind bestimmte, für benutzerdefinierte virtuelle Kanäle erforderliche Registrierungsschlüssel möglicherweise nicht mehr vorhanden. [LC8414]
- Nach der automatischen Updateinstallation von Citrix Receiver für Windows wird der Befehlszeilenschalter zur Installation **automatischer Updates** möglicherweise nicht beibehalten. Daher wird die Konfiguration für automatische Updates auf die Standardoption festgelegt. [LC9103]

Sitzung/Verbindung

- Das Starten einer Sitzung kann fehlschlagen und die folgende Fehlermeldung wird angezeigt:

  "The ICA file contains an invalid unsigned parameter."

  Bevor Sie die neue ADMX-Datei aktualisieren oder ersetzen, legen Sie die mit der ICA-Dateisignierung verbundenen Richtlinie "ICA-Dateisignierung aktivieren" auf "Nicht konfiguriert" fest.

Hinweis: Fix LC5338 ist für StoreFront 3.0.4000, StoreFront 3.9 und höhere Versionen geeignet. [LC5338]

- Wenn Sie den Prozess selfservice.exe von Citrix Receiver für Windows auf dem ersten Hop eines VDAs für Serverbetriebssysteme starten, kann das Trennen des ersten Hop dazu führen, dass Drittanbieteranwendungen oder die Windows-Aufgabenplanung "SelfService.exe – disconnectapps" ausführen, um die Verbindung des zweiten Hop zu trennen. Wenn Sie die Verbindung zum ersten Hop wiederherstellen, wird "SelfService.exe – reconnectapps" ausgeführt, um die Verbindung zum zweiten Hop wiederherzustellen. In diesem Szenario wird Citrix Receiver für Windows möglicherweise im Vordergrund und die wiederverbundenen Anwendungen werden im Hintergrund angezeigt. [LC8224]

Systemausnahmen

- Der wfica32-Prozess wird möglicherweise zeitweise beendet, wenn der virtuelle Mobile Receiver-Kanal verwendet wird. [LC8526]
- Benutzersitzungen können bei Verwendung der biometrischen Authentifizierung der Bloomberg-Tastatur unerwartet beendet werden. [LC8766]
- Benutzersitzungen werden möglicherweise unerwartet beendet, wenn Sie in einer USB-umgeleiteten Sitzung den Fingerabdruckscanner einer Bloomberg-Tastatur verwenden. [LC8928]

Benutzererfahrung

- Wenn Sie die angepasste Phrasenfunktion in der Sprachenleiste des Eingabemethoden-Editors (Input Method Editor, IME) verwenden, werden bestimmte Zeichen in einer Benutzersitzung zufällig gelöscht. [LC6155]
- Manuell auf Desktops und Taskleiste erstellte Verknüpfungen von Streaming-Anwendungen werden gelöscht. [LC7500]
- Wenn Sie Citrix Receiver für Windows starten, können Startmenü und Desktop-Verknüpfungen flackern, wenn die abonnierten Anwendungen Symbole mit bpp=4 im Receiver Self-Service-Fenster enthalten. [LC8480]
- Wenn bestimmte Anwendungen von Drittanbietern versuchen, eine große Anzahl von Zeichen an eine Sitzung mit aktivierten HDX Seamless-Apps zu senden, werden möglicherweise nur einige statt aller Zeichen an die Anwendung gesendet. [LC8560]
- Wenn ein veröffentlichter Desktop im Vollbildmodus auf einem Windows 7-Clientcomputer gestartet wird, kann die Wiedergabe eines umgeleiteten Flash-Videos dazu führen, dass Anwendun-

gen, für die **Immer oben** festgelegt ist, über dem Desktop Viewer-Fenster angezeigt werden. In der Standardeinstellung ist dieser Fix deaktiviert.

Zum Implementieren dieses Fixes legen Sie folgende Registrierungsschlüssel fest:

- *Auf 32-Bit-Systemen*:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenDesktop\DesktopViewer

  Name:PreventAlwaysOnTopWindowPopover

  Typ: DWORD

  Wert: 2; Um den Fix zu deaktivieren, setzen Sie den Wert des Registrierungsschlüssels auf 0 oder entfernen den Registrierungsschlüssel.

- *Auf 64-Bit-Systemen*:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenDesktop\DesktopViewer

  Name:PreventAlwaysOnTopWindowPopover

  Typ: DWORD

  Wert: 2; Um den Fix zu deaktivieren, setzen Sie den Wert des Registrierungsschlüssels auf 0 oder entfernen den Registrierungsschlüssel. [LC8616]

- Wenn Sie Anwendungen in Citrix Receiver für Windows aktualisieren, werden manuell an die Taskleiste angeheftete Microsoft Outlook-Anwendungssymbole möglicherweise nicht mehr angezeigt. [LC8785]

Benutzeroberfläche

- Anwendungen werden möglicherweise nicht im Startmenü angezeigt, wenn Sie die **Einstellungsoption** in Citrix Receiver für Windows ändern und StoreFront mit der Einstellung **Benutzerabonnements deaktivieren (vorgegebener Store)** für den Store konfigurieren. [LC8648]

Citrix Receiver für Windows 4.9 LTSR CU1

Verglichen mit Citrix Receiver für Windows 4.9 LTSR

Probleme bei Clientgeräten

- An eine Dockingstation oder einen USB-Hub angeschlossene Geräte wie eine Tastatur, eine Maus oder ein Monitor können nicht verwendet werden. Das Problem tritt auf, wenn die

Benutzersitzung im Vollbildmodus ausgeführt wird oder wenn das Sitzungsfenster im Fokus ist und wenn Sie die Dockingstation oder den Hub nach dem Starten der Benutzersitzung mit einer Clientmaschine verbinden. [LC8295]

Inhaltsumleitung

- Die Dateitypzuordnung funktioniert möglicherweise nicht, wenn Sie sich mit einem Roamingprofil bei Citrix Receiver für Windows anmelden. [LC8042]

HDX RealTime

- Wenn mehrere Webcams des gleichen Modells auf einem VDA installiert sind, wird möglicherweise nur die letzte Webcam in einer Sitzung erkannt und zugeordnet. Mit dem Fix können mehrere Webcams desselben Modells in einer Videokonferenzanwendung innerhalb einer Sitzung verwendet werden.

  > **Hinweis:**
  >
  > – Wenn Fix LC5008 installiert ist, können Sie Webcams möglicherweise nicht über die Registerkarte “Einstellungen” wechseln.
  > – Zum Implementieren dieses Fixes müssen Sie ein Server- und ein Clienthotfix mit Fix LC5008 installieren. [LC5008]

Sitzung/Verbindung

- Bei dem Versuch, Microsoft Internet Explorer als ein anderer als der zurzeit angemeldete Benutzer mit dem Befehl “Ausführen als” zu starten und wenn dabei auf dem System der Prozess Redirector.exe ausgeführt wird, wird u. U. der Browser gestartet, aber der Inhalt wird für ca. 20-30 Sekunden nicht geladen. [LC5227]
- Versuche, einen Desktop mit Mozilla Firefox zu starten, schlagen möglicherweise fehl. Das Problem tritt auf, wenn der Desktop Viewer eine zuvor erstellte ICA-Datei aus dem temporären Verzeichnis von Internet Explorer nicht löschen kann. Dies führt zu einem Fehler “Zugriff verweigert”, der das Kopieren der ICA-Datei beim Starten einer neuen Sitzung verhindert. [LC7883]
- Wenn Sie eine Anwendung über das Startmenü oder die Desktopverknüpfung starten, wird die Anwendung möglicherweise gestartet und folgende Fehlermeldung wird angezeigt:

  “Die Datei kann nicht gefunden werden. Überprüfen Sie, ob der korrekte Pfad und Dateiname angegeben wurde.” [LC8253]

- Wenn Citrix Receiver für Windows 4.8 installiert ist, funktionieren bestimmte Features eines Webportals für Mitarbeiter u. U. nicht einwandfrei. Wenn jedoch das Citrix ICA Client ActiveX-Steuerelement in Microsoft Internet Explorer deaktiviert ist, funktioniert die Website ordnungsgemäß. [LC8428]

Systemausnahmen

- Citrix Receiver für Windows wird u. U. unerwartet mit folgender Fehlermeldung geschlossen:

  Citrix HDX Engine funktioniert nicht mehr. [LC8040]

- In Citrix Receiver für Windows 4.8 tritt möglicherweise eine schwerwiegende Ausnahme mit einem blauen Bildschirm auf. Das Problem tritt auf, wenn Sie das System mit bestimmten Multifunktionstastaturmodellen neu starten und die Tastatur mehrmals vom System trennen und wieder anschließen. [LC8182]
- Wenn Sie während der Wiedergabe einer Audiodatei die Kopfhörer von einem Benutzergerät entfernen, reagiert die Sitzung möglicherweise nicht mehr, bis Sie die Sitzung trennen und erneut verbinden. [LC8243]
- Wenn Sie die Tastenkombination “Alt+Eingabetaste” in einer veröffentlichten Seamlessanwendung verwenden, wird der Prozess wfica32.exe möglicherweise unerwartet beendet. [LC8317]
- In einem Double-Hop-Szenario wird der Prozess wfica32.exe möglicherweise unerwartet beendet, wenn Sie eine Sitzung zwischen Clients wechseln. [LC8354]

Benutzererfahrung

- Wenn Sie Ton mit hoher Audioqualität aufnehmen, ist die Qualität der Tonaufnahme möglicherweise schlecht. [LC8241]
- Wenn Sie in einer Umgebung mit mehreren Monitoren ein Seamlessfenster vom Vollbild auf die ursprüngliche Größe zurücksetzen und dann das Fenster wieder zurück ziehen, um die gesamte Anwendung anzuzeigen, wird das Fenster möglicherweise nicht ordnungsgemäß angepasst. Infolgedessen ist nur ein Teil des Fensters sichtbar. Das Problem tritt bei Seamlessfenstern auf, die breiter als der Monitor sind und damit teilweise außerhalb des Bildschirms liegen. [LC8325]
- Wenn Sie Verknüpfungsoptionen in der Store-Datei web.config konfigurieren, werden Verknüpfungen für veröffentlichte Anwendungen möglicherweise nicht mehr im Startmenü und auf dem Desktop angezeigt.

  Hinweis: Dieser Fix bietet einen vollständigen Fix für LC7577. [LC8391]

- Wenn Sie bei der Verwendung von Epic Hyperspace eine Sitzung im Seamlessmodus starten, verhindert die Anwendung möglicherweise, dass andere Anwendungen, die lokal auf einem Endpunkt ausgeführt werden, im Vordergrund erscheinen. Epic Hyperspace bleibt dann so lange im Vordergrund, bis Sie die Anwendung minimieren. [LC8462]
- Wenn Sie eine Verbindung zu einem veröffentlichten Desktop herstellen, werden möglicherweise leere Bereiche auf dem Desktop angezeigt, die sich beim Ändern der Größe des Fensters ändern. Dieser Fehler tritt auf, wenn der Legacy-Grafikmodus verwendet wird. [LC8518]

Citrix Receiver für Windows 4.9 LTSR

Verglichen mit Citrix Receiver für Windows 4.8

HDX 3D Pro

- Wenn HDX 3D Pro auf einem VDA aktiviert ist, kann die Verwendung bestimmter Drittanbieter-Anwendungen dazu führen, dass die Verbindung zum VDA getrennt wird.

  Zum Implementieren dieses Fixes legen Sie folgende Registrierungsschlüssel fest:

  - *Bei 32-Bit-Windows:*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

    Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

    Name: Tw2IgnoreValidationErrors

    Typ: REG_SZ

    Wert: TRUE

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

    Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

    Name: Tw2IgnoreExecutionErrors

    Typ: REG_SZ

    Wert: TRUE
  - *Unter 64-Bit-Windows:*

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

    Name: Tw2IgnoreValidationErrors

    Typ: REG_SZ

    Wert: TRUE

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

Name: Tw2IgnoreExecutionErrors

Typ: REG_SZ

Wert: TRUE [LC7655]

Server- /Siteverwaltung

- Das Ablaufen eines Benutzerkennworts kann dazu führen, dass das Eingabefeld für "Kennwort ändern" nicht mehr reagiert. Das Problem tritt auf, wenn das neue Kennwort nicht die Anforderungen erfüllt. [LC7943]

Sitzung/Verbindung

- Wenn Sie eine Desktopgruppe einer externen Client-IP-Adresse zuweisen (gemäß der Schrittfolge im Knowledge Center-Artikel CTX128232), wird der veröffentlichte Desktop möglicherweise nicht gestartet, wenn Sie über NetScaler Gateway darauf zugreifen. Die folgende Fehlermeldung wird angezeigt:

  "App kann nicht gestartet werden" [LC5932]
- Citrix Receiver für Windows kann möglicherweise keine Verbindung zu StoreFront herstellen, wenn die Verbindung über ein Juniper SSL VPN erfolgt. Das Problem tritt auf, wenn die DNS-Auflösung für die StoreFront-URL fehlschlägt. [LC6711]
- Citrix Receiver für Windows wird möglicherweise unerwartet beendet, wenn die Verbindung zu einem VDA mit integrierter Webcam getrennt wird. Das Problem tritt auf, wenn die Verbindung getrennt wird, während die Webcam eingeschaltet ist. [LC6815]
- Bei aktiviertem Desktop Lock kann die Benutzersitzung automatisch getrennt werden, wenn die StoreFront-Sitzung abgelaufen ist. [LC6984]
- Bei Verwendung der Software Epic Hyperspace für medizinische Diktate kann es vorkommen, dass die Diktierfunktion auf dem Benutzergerät während der Aufzeichnung aufhört zu reagieren. [LC7435]
- Wenn Sie mit der Citrix ICA-Clientobjekt-API eine Clientsitzung über NetScaler starten und im Gruppenrichtlinienobjekt das Feature "Client Selective Trust" konfiguriert haben, wird die Sitzung möglicherweise nicht gestartet. [LC7575]
- Die Dateitypzuordnung kann das zugeordnete Dokument möglicherweise nicht öffnen, wenn Sie im Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle (32-Bit-Windows) bzw. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64-Bit-Windows) den Registrierungswert "DisableStubCreation" auf "True" festlegen. Das Problem

tritt auf, wenn im Registrierungsschlüssel HKEY_CURRENT_USER\SOFTWARE\Classes\Dazzle der Parameter "%1" für die jeweilige Dateinamenerweiterung fehlt.<*Appname*>.<*Dateierweiterung*>.1\shell\o [LC7619]

- Bei aktiviertem lokalem App-Zugriff können Größe und Position des VDA für Desktopbetriebssysteme bei Sitzungen im Vollbildmodus fehlerhaft sein. [LC7646]
- Wenn Sie einen Store über die Gruppenrichtlinieneinstellungen oder die Befehlszeile hinzufügen und die Wiederverbindung beim Anmelden an Windows konfigurieren, erfolgt die Wiederverbindung von Citrix Receiver für Windows bei der Windows-Anmeldung möglicherweise nicht automatisch. [LC7679]
- Nach dem Beenden des Energiesparmodus schlägt die automatische Wiederverbindung von Clients möglicherweise fehl, sodass Sitzungen nicht wiederverbunden werden. [LC7705]
- Bei aktiviertem lokalem App-Zugriff kann der Prozess wfcrun32.exe unerwartet beendet werden. [LC7946]

Smartcards

- Wenn in einer Benutzersitzung unter der Richtlinie "Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards" die lokale Sicherheitseinstellung "Arbeitsstation sperren" festgelegt ist, wird die Sitzung möglicherweise nicht gesperrt, wenn Sie den Smartcardleser aus der Sitzung entfernen. [LC7571]
- Wenn die SCardListReaderGroup-API in einer Benutzersitzung vom Server aufgerufen wird, wird die auf der Clientseite aufgerufene API möglicherweise nicht von Citrix Receiver für Windows ausgeführt. [LC7699]

Benutzererfahrung

- Das Doppeltippen auf den Touchscreen eines Gerätes funktioniert möglicherweise nicht bei allen Anwendungen in einer Benutzersitzung. [LC6698]
- Wenn Sie in einer Seamlesssitzung auf die Taskleistensymbole klicken, um zwischen den Fenstern einer Drittanbieter-Anwendung zu wechseln, wird das zugehörige Fenster der Drittanbieter-Anwendung möglicherweise nicht im Vordergrund angezeigt. [LC6709]
- Wenn Sie bei gedrückter Maustaste die Auflösung des Benutzergeräts ändern, wird das Loslassen der Maustaste in Seamless-Apps möglicherweise nicht erkannt. Das Erfassen von Mauseingaben geht dadurch verloren. [LC7419]
- Wenn Sie Verknüpfungsoptionen in der Store-Datei web.config konfigurieren, werden Verknüpfungen für veröffentlichte Anwendungen möglicherweise nicht mehr im Startmenü und auf dem Desktop angezeigt. [LC7577]

- Wenn Sie bei der Verwendung von Epic Hyperspace eine Sitzung im Seamlessmodus starten, verhindert die Anwendung möglicherweise, dass andere Anwendungen, die lokal auf einem Endpunkt ausgeführt werden, im Vordergrund erscheinen. Epic Hyperspace bleibt dann so lange im Vordergrund, bis die Anwendung minimiert wird. [LC7906]

Hinweis: Diese Version von Citrix Receiver für Windows enthält alle Problembehebungen der Versionen 4.8, 4.7, 4.6, 4.5, 4.4, 4.3, 4.2, 4.1 und 4.0.

Bekannte Probleme

June 21, 2019

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU7

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU6

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU5

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU4

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU3

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU2

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Citrix Receiver für Windows 4.9 LTSR CU1

Citrix Receiver für Windows 4.9 enthält einige der bekannten Probleme, die in Version 4.5, 4.6, 4.7 und 4.8 vorlagen, sowie das folgende bekannte Problem:

- Wenn Framehawk aktiviert ist, wird der Prozess wfica32.exe möglicherweise unerwartet beendet, wenn Sie versuchen, sich kontinuierlich an- und abzumelden. [LCMRFWIN-704]

Bekannte Probleme in Citrix Receiver für Windows 4.9

- Wenn Sie auf einem Surface Pro-Gerät eine Desktopsitzung im Fenstermodus starten, kann der Wechsel zwischen Tablet- und Desktopmodus dazu führen, dass der Desktop Viewer nicht mehr reagiert. [RFWIN-5837]

Hinweise zu Drittanbietern

November 21, 2018

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

Citrix Receiver für Windows – Third Party Notices (PDF-Download)

Systemanforderungen und Kompatibilität

June 21, 2019

Anforderungen

- Diese Version von Citrix Receiver für Windows benötigt mindestens 500 MB freien Speicherplatz und 1 GB RAM.
- Mindestanforderungen für .NET Framework
  - Für das Self-Service Plug-In ist .NET 3.5 Service Pack 1 erforderlich. Benutzer können damit über die Receiver-Benutzeroberfläche oder über eine Befehlszeile Desktops und Anwendungen abonnieren und starten. Weitere Informationen finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.

- NET 2.0 Service Pack 1 und Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package sind erforderlich.

Kompatibilitätsmatrix

Citrix Receiver für Windows Version 4.9 ist mit folgenden Windows-Betriebssystemen und Webbrowsern kompatibel. Es ist auch kompatibel mit allen derzeit unterstützten Versionen von XenApp, XenDesktop und NetScaler Gateway, die in der Citrix Product Lifecycle Matrix aufgeführt sind.

> **Hinweis**
>
> Das NetScaler Gateway-Plug-In für die Endpunktanalyse (EPA) bietet keine Unterstützung für den nativen Citrix Receiver für Windows.

Betriebssystem	Browser
Windows 10 [1]	Internet Explorer
Windows 10 IoT Enterprise [2]	
Windows 8.1, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)	Google Chrome (aktuelle Version, erfordert StoreFront)
Windows 7, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)	Mozilla Firefox (aktuelle Version)
Windows Thin PC	Microsoft Edge
Windows Server 2016	
Windows Server 2012 R2, Standard und Datacenter Edition	
Windows Server 2012, Standard und Datacenter Edition	
Windows Server 2008 R2, 64-Bit-Edition	

[1] Unterstützt Windows 10 Anniversary Update, Creators Update, Falls Creators Update, das Update von April 2018 (Version 1803) und das Update von Oktober 2018 (Version 1809).
[2] Unterstützt Windows 10 IoT Enterprise 2015 LTSB, Windows 10 IoT Enterprise 2016 LTSB, Anniversary Update, Creators Update, Falls Creators Update, April 2018 Update (Version 1803) und Oktober 2018 Update (Version 1809).

> **Hinweis**

> - Das Oktober 2018-Update (Version 1809) wird nur für Receiver für Windows Version 4.9 CU5 und höher unterstützt.
> - Das April 2018-Update wird nur für Receiver für Windows Version 4.9 CU3 und höher unterstützt.
> - Das Falls Creators Update wird nur für Receiver für Windows Version 4.9 CU1 und höher unterstützt. Receiver für Windows Version 4.9 unterstützt es nicht.

Unterstützungsmatrix

Auf Touchgeräten unterstützte Betriebssysteme	Auf VDAs unterstützte Betriebssysteme
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2
	Windows Server 2016
	Windows Server 2008 R2

Verbindungen, Zertifikate und Authentifizierung

March 26, 2019

Verbindungen

1. HTTP-Store
2. HTTPS-Store
3. NetScaler Gateway 10.5 oder höher
4. Webinterface 5.4

Citrix Receiver für Windows kann auf domänengebundenen Maschinen unter Windows, verwalteten Geräten (lokal und remote mit oder ohne VPN) und auf nicht in Domänen eingebundenen Maschinen mit dem VDA verbunden werden, oder es kann eine ICA-Sitzung eingerichtet werden.

Zertifikate

1. Privat (selbstsigniert)
2. Stamm
3. Platzhalter
4. Zwischenzertifikat

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 erfolgreich mit Citrix Receiver für Windows auf Ressourcen von Citrix zuzugreifen.

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

Installieren von Stammzertifikaten

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

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

Zertifikate mit Platzhalterzeichen

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

Citrix Receiver für Windows unterstützt Zertifikate mit Platzhalterzeichen. Diese dürfen jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden. In der Praxis kann als Alternative zu Zertifikaten mit Platzhalterzeichen ein Zertifikat erwogen werden, das eine Liste der Servernamen mit der Erweiterung “Alternativer Antragstellername” (SAN) enthält. Diese Zertifikate werden von privaten und öffentlichen Zertifizierungsstellen ausgestellt.

Zwischenzertifikate

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem NetScaler Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter Konfigurieren von Zwischenzertifikaten.

Authentifizierung

Authentifizierung bei StoreFront

	Receiver für Web mit Browsern	StoreFront Services-Site (nativ)	StoreFront XenApp Services-Site (nativ)	NetScaler bei Receiver für Web (Browser)	NetScaler bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoke				Ja*	Ja*
Zweistufig (Domäne mit Sicherheitsto-ken)				Ja*	Ja*
SMS				Ja*	Ja*
Smartcard	Ja	Ja		Ja	Ja
Benutzerzertifil				Ja (NetScaler-Plug-In)	Ja (NetScaler-Plug-In)

*Mit oder ohne NetScaler-Plug-In auf dem Gerät.

> **Hinweis**
>
> Citrix Receiver für Windows 4.8 unterstützt die zweistufige Authentifizierung (Domäne plus Sicherheitstoken) über NetScaler Gateway für den nativen StoreFront-Dienst.

Authentifizierung beim Webinterface

Citrix Receiver für Windows unterstützt die folgenden Authentifizierungsmethoden (beim Webinterface wird die Authentifizierung mit Domäne und Sicherheitstoken als **explizit** bezeichnet):

	Webinterface (Browser)	Webinterface XenApp Services-Site	NetScaler bei Web Interface (Browser)	NetScaler bei Webinterface XenApp Services-Site
Anonym	Ja			
Domäne	Ja	Ja	Ja*	
Domänen-Passthrough	Ja	Ja		
Sicherheitstoken			Ja*	
Zweistufig (Domäne mit Sicherheitstoken)			Ja*	
SMS			Ja*	
Smartcard	Ja	Ja		
Benutzerzertifikat			Ja (NetScaler-Plug-In)	

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

Informationen zur Authentifizierung finden Sie unter Konfigurieren von Authentifizierung und Autorisierung in der NetScaler Gateway-Dokumentation und unter Verwalten in der StoreFront-Dokumentation.

Weitere Informationen zu den Authentifizierungsmethoden, die das Webinterface unterstützt, finden Sie in der Webinterface-Dokumentation.

Installieren

January 7, 2019

Das Installationspaket CitrixReceiver.exe kann wie folgt installiert werden:

- Von einem Benutzer von Citrix.com oder Ihrer eigenen Downloadsite
  - Ein Erstbenutzer, der Citrix Receiver für Windows von Citrix.com oder Ihrer eigenen Downloadsite herunterlädt, kann ein Konto durch Eingabe einer E-Mail-Adresse statt einer Server-URL einrichten. Citrix Receiver für Windows ermittelt den der E-Mail-Adresse zugeordneten NetScaler Gateway oder StoreFront-Server und fordert den Benutzer zur Anmeldung und Fortsetzung der Installation auf. Dieses Feature wird als e-mail-basierte Kontenermittlung bezeichnet. Hinweis: Ein Erstbenutzer ist ein Benutzer, der Receiver nicht auf dem Gerät installiert hat.
  - Die e-mail-basierte Kontenermittlung wird für einen Erstbenutzer nicht angewendet, wenn Citrix Receiver für Windows von einem anderen Speicherort (d. h. nicht Citrix.com) heruntergeladen wird (z. B. einer Receiver für Web-Site).
  - Wenn Citrix Receiver für Windows für Ihre Site konfiguriert werden muss, verwenden Sie eine andere Bereitstellungsmethode.
- Automatisch von Receiver für Web oder von einem Webinterface-Anmeldebildschirm.
  - Ein Erstbenutzer kann ein Konto durch Eingabe einer Server-URL oder durch Download einer Provisioningdatei (CR-Datei) einrichten.
- Mit einem ESD-Tool (Electronic Software Distribution)
  - Ein Erstbenutzer muss für das Einrichten des Kontos eine Server-URL eingeben oder eine Provisioningdatei öffnen.

Bei Citrix Receiver für Windows sind Administratorrechte für die Installation nur erforderlich, wenn die Passthrough-Authentifizierung verwendet wird.

HDX RealTime Media Engine (RTME)

Ein Installer kombiniert den aktuellen Citrix Receiver für Windows mit dem HDX RTME-Installer. Beim Installieren von Citrix Receiver mit der ausführbaren Datei (.exe) wird HDX RTME ebenfalls installiert.

Wenn Sie die HDX RealTime Media Engine installiert haben, stellen Sie beim Deinstallieren und Neuinstallieren von Citrix Receiver für Windows sicher, dass Sie den gleichen Modus verwenden, den Sie bei der Installation der HDX RealTime Media Engine verwendet haben.

> **Hinweis**

> Für die Installation der aktuellen Version von Citrix Receiver mit integrierter Unterstützung für RTME sind Administratorrechte auf der Hostmaschine erforderlich.

Berücksichtigen Sie folgende HDX RTME-Probleme, wenn Sie Citrix Receiver für Windows installieren oder aktualisieren:

- Die aktuelle Version von Citrix ReceiverPlusRTME enthält HDX RTME. Für die Installation von RTME sind keine weiteren Aktionen erforderlich.
- Upgrades von einer früheren Version von Citrix Receiver für Windows auf das aktuelle Versionspaket (Citrix Receiver mit RTME) werden unterstützt. Bereits installierte Versionen von RTME werden mit der aktuellen Version überschrieben. Upgrades von derselben Version von Citrix Receiver für Windows auf das aktuelle Versionspaket (z. B. von Receiver 4.7 auf das Paket Receiver 4.7 einschließlich RTME) werden nicht unterstützt.
- Wenn eine ältere RTME-Version vorhanden ist, wird bei der Installation der aktuellen Version von Citrix Receiver für Windows RTME auf dem Clientgerät automatisch aktualisiert.
- Wenn eine aktuellere RTME-Version vorhanden ist, behält das Installationsprogramm die aktuelle Version bei.

> **Wichtig**
>
> Der HDX RealTime Connector auf Ihren XenApp-/XenDesktop-Servern muss mindestens Version 2.0.0.417 sein, damit die Kompatibilität mit dem neuen RTME-Paket gewährleistet ist. Sie können RTME 2.0 nicht mit dem 1.8 RTME-Connector verwenden.

Manuelles Upgrade auf Citrix Receiver für Windows

Bereitstellungen mit StoreFront:

- Sie sollten für BYOD-Benutzer (Bring Your Own Device) die aktuellen Versionen von NetScaler Gateway und StoreFront gemäß der zugehörigen Dokumentation auf der Website mit der Produktdokumentation konfigurieren. Senden Sie die von StoreFront erstellte Provisioningdatei als Anlage in einer E-Mail und teilen Sie den Benutzern mit, wie die Aktualisierung und das Öffnen der Provisioningdatei nach der Installation von Citrix Receiver für Windows ausgeführt wird.
- Als Alternative zum Bereitstellen einer Provisioningdatei können Benutzer die URL von NetScaler Gateway eingeben. Oder, wenn Sie die e-mail-basierte Kontenermittlung konfiguriert haben, wie in der StoreFront-Dokumentation beschrieben, fordern Sie die Benutzer zur Eingabe der E-Mail-Adresse auf.
- Eine andere Methode ist die Konfiguration einer Citrix Receiver für Web-Site, wie in der StoreFront-Dokumentation beschrieben, und der Abschluss der Konfiguration, wie unter Bereitstellen von Citrix Receiver für Windows über Citrix Receiver für Web beschrieben. Geben Sie den Benutzern die Informationen zum Upgrade von Citrix Receiver für Windows, zum Zugriff auf die Citrix Receiver für Web-Site und zum Download der Provisioningdatei von Citrix Receiver für Web (klicken Sie auf den Benutzernamen und dann auf **Aktivieren**).

Bereitstellungen mit dem Webinterface

- Aktualisieren Sie Ihre Webinterface-Site mit Citrix Receiver für Windows und schließen Sie die Konfiguration ab, wie unter Bereitstellen von Citrix Receiver für Windows über einen Webinterface-Anmeldebildschirm beschrieben. Teilen Sie den Benutzern mit, wie Citrix Receiver für Windows aktualisiert wird. Sie können z. B. eine Downloadsite erstellen, von der Benutzer den benannten Citrix Receiver-Installer herunterladen.

Überlegungen zum Upgrade

Mit Citrix Receiver für Windows 4.x kann Citrix Receiver für Windows 3.x sowie das Citrix Online Plug-In 12.x aktualisiert werden.

Wenn Citrix Receiver für Windows 3.x pro Computer installiert wurde, wird ein Pro-Benutzer-Upgrade (von einem Benutzer ohne Administratorrechte) nicht unterstützt.

Wenn Citrix Receiver für Windows 3.x pro Benutzer installiert wurde, wird ein Pro-Computer-Upgrade nicht unterstützt.

Manuelles Installieren und Deinstallieren von Citrix Receiver für Windows

November 21, 2018

Sie können Citrix Receiver für Windows vom Installationsmedium, von einer Netzwerkfreigabe und Windows Explorer oder an einer Befehlszeile durch manuelles Ausführen des Installationspakets CitrixReceiver.exe installieren. Weitere Informationen zu Parametern für die Installation an der Befehlszeile und zu den Speicherplatzanforderungen finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.

Überprüfen auf freien Speicherplatz

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

Bei einer Neuinstallation wird die Installation beendet, wenn nicht genügend Speicherplatz vorhanden ist, und das folgende Dialogfeld wird angezeigt.

Bei einem Upgrade von Citrix Receiver für Windows wird die Installation beendet, wenn nicht genügend Speicherplatz vorhanden ist, und das folgende Dialogfeld wird angezeigt.

Die folgende Tabelle enthält Informationen zum mindestens erforderlichen Speicherplatz für die Installation von Citrix Receiver für Windows.

Installationstyp	Erforderlicher Speicherplatz
Neuinstallation	320 MB
Upgrade von Citrix Receiver	206 MB

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

Deinstallieren von Citrix Receiver für Windows

Sie können Citrix Receiver für Windows mit dem Windows-Hilfsprogramm “Programme und Funktionen” (Programme hinzufügen/entfernen) deinstallieren.

> **Hinweis**
>
> Sie werden aufgefordert, das Citrix HDX RTME-Paket zu deinstallieren, bevor Sie mit der Installation von Citrix Receiver für Windows fortfahren. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX200340.

Deinstallieren von Citrix Receiver für Windows über die Befehlszeilenschnittstelle

Sie können Citrix Receiver für Windows mit dem folgenden Befehl auch über die Befehlszeile deinstallieren.

CitrixReceiver.exe /uninstall

Nach der Deinstallation von Citrix Receiver für Windows verbleiben die mit Receiver.adm/Receiver.adml oder Receiver.admx angepassten Registrierungsschlüssel für die Citrix Receiver für Windows-Einstellungen im Verzeichnis Software\Policies\Citrix\ICA Client unter HKEY_LOCAL_MACHINE und HKEY_LOCAL_USER.

Wenn Sie Citrix Receiver für Windows neu installieren, werden diese Richtlinien u. U. erzwungen und können zu unerwartetem Verhalten führen. Um diese Anpassungen zu entfernen, löschen Sie sie manuell.

Konfigurieren und Installieren mit Befehlszeilenparametern

March 26, 2019

Passen Sie das Citrix Receiver für Windows-Installationsprogramm mit Befehlszeilenoptionen an. Das Installationspaket wird automatisch vor dem Start des Setupprogramms im Temp-Verzeichnis des Benutzers extrahiert. Der benötigte Speicherplatz berücksichtigt Programmdateien, Benutzerdaten und Temp-Verzeichnisse nach dem Start mehrerer Anwendungen.

Weitere Informationen zu Speicherplatzanforderungen finden Sie unter Systemanforderungen.

Installieren Sie Citrix Receiver für Windows an einer Eingabeaufforderung mit der folgenden Syntax:

CitrixReceiver.exe [Optionen]

Automatische Updates

Option	/ AutoUpdateCheck = automatisch / manuell / deaktiviert
Beschreibung	Gibt an, dass Citrix Receiver für Windows erkennt, wenn ein Update verfügbar ist. **Auto:** Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung). **Manual:** Sie werden nicht benachrichtigt, wenn Updates zur Verfügung stehen. Suchen Sie manuell nach Updates. **Disabled:** Das Feature für automatische Updates ist deaktiviert.
Beispiel für Verwendung	CitrixReceiver.exe / AutoUpdateCheck = auto CitrixReceiver.exe / AutoUpdateCheck = manual CitrixReceiver.exe / AutoUpdateCheck = disabled

Option	/AutoUpdateStream= LTSR/Current
Beschreibung	Gibt den Versionstyp von Citrix Receiver für Windows an. **LTSR:** Release ist ein Long Term Service Release **Current:** Release ist die aktuelle Version von Citrix Receiver für Windows
Beispiel für Verwendung	CitrixReceiver.exe /AutoUpdateStream= LTSR CitrixReceiver.exe / AutoUpdateStream= Current

Option	/DeferUpdateCount
Beschreibung	Gibt an, wie oft die Option Später erinnern angezeigt wird. Gibt an, wie oft das Update verschoben werden kann. **-1:** Gibt an, dass Sie Benachrichtigungen beliebig oft verschieben können (Standardwert = -1). **0:** Gibt an, dass die Option “Später erinnern” nicht angezeigt wird. **Beliebige andere Zahl:** Gibt an, wie oft die Option “Später erinnern” angezeigt wird. Beispiel: Bei einem Wert von 10 wird die Option Später erinnern zehnmal angezeigt.
Beispiel für Verwendung	CitrixReceiver.exe /DeferUpdateCount=-1 CitrixReceiver.exe /DeferUpdateCount=-0 CitrixReceiver.exe /DeferUpdateCount=<beliebige andere Zahl>

Option	/AURolloutPriority
Beschreibung	Gibt den Zeitrahmen für die Rolloutphase an. **Fast:** Das Rollout des Updates erfolgt zu Beginn des Bereitstellungszeitraums. **Medium:** Das Rollout des Updates erfolgt in der Mitte des Bereitstellungszeitraums. **Slow:** Das Rollout des Updates erfolgt am Ende des Bereitstellungszeitraums.

Option	/AURolloutPriority
Beispiel für Verwendung	CitrixReceiver.exe /AURolloutPriority=Fast CitrixReceiver.exe /AURolloutPriority=Medium CitrixReceiver.exe /AURolloutPriority=Slow

Aktivieren der bidirektionalen Inhaltsumleitung

> **Hinweis**
>
> Standardmäßig installiert Citrix Receiver für Windows keine Komponenten der bidirektionalen Inhaltsumleitung, wenn sie bereits auf dem Server installiert sind. Bei Verwendung von XenDesktop als eine Clientmaschine müssen Sie Citrix Receiver für Windows installieren und mit der Option /FORCE_LAA die Komponenten der bidirektionalen Inhaltsumleitung installieren. Das Feature muss jedoch sowohl auf dem Server und dem Client konfiguriert werden.

Option	ALLOW_BIDIRCONTENTREDIRECTION=1
Beschreibung	Gibt an, dass die bidirektionale Inhaltsumleitung zwischen Client-zu-Host und Host-zu-Client aktiviert ist.
Beispiel für Verwendung	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

Aktivieren des lokalen App-Zugriffs

Option	FORCE_LAA=1
Beschreibung	Standardmäßig installiert Citrix Receiver für Windows nicht die Komponenten für den clientseitigen lokalen App-Zugriff, wenn die Komponenten bereits auf dem Server installiert sind. Verwenden Sie zum Erzwingen der Komponenten für den clientseitigen App-Zugriff in Citrix Receiver den Befehlszeilenschalter FORCE_LAA. Zum Ausführen dieser Schritte sind Administratorprivilegien erforderlich. Weitere Informationen zum lokalen App-Zugriff finden Sie unter Lokaler App-Zugriff in der XenApp- und XenDesktop-Dokumentation.
Beispiel für Verwendung	CitrixReceiver.exe /FORCE_LAA = 1

Anzeigen der Verwendungsinformationen

Option	/? oder /help
Beschreibung	Zeigt Informationen zur Verwendung an
Beispiel für Verwendung	CitrixReceiver.exe /? CitrixReceiver.exe /help

Unterdrücken eines Neustarts bei der Installation der Benutzeroberfläche

Option	/noreboot
Beschreibung	Unterdrückt einen Neustart bei der Installation der Benutzeroberfläche. Diese Option wird nicht bei Installationen ohne Benutzereingriffe benötigt. Wenn Sie Neustartaufforderungen unterdrücken, werden USB-Geräte, die bei der Citrix Receiver für Windows-Installation im ausgesetzten Zustand sind, erst nach dem Neustart des Benutzergeräts von Citrix Receiver für Windows erkannt.

Option	/noreboot
Beispiel für Verwendung	CitrixReceiver.exe /noreboot

Automatische Installation

Option	**/silent**
Beschreibung	Deaktiviert die Fehler- und Fortschrittsdialogfelder und führt eine automatische Installation aus.
Beispiel für Verwendung	CitrixReceiver.exe /silent

Aktivieren von Single Sign-On bei der Authentifizierung

Option	/includeSSON
Beschreibung	Gibt an, dass Citrix Receiver für Windows mit der Single Sign-On-Komponente installiert wird. Die verwandte Option ENABLE_SSON wird aktiviert wenn Sie /includeSSON an der Befehlszeile angeben. Wenn Sie Features mit ADDLOCAL= angeben und Single Sign-On installieren möchten, müssen Sie auch den Wert SSON angeben. Zum Aktivieren von Passthrough-Authentifizierung für ein Benutzergerät müssen Sie Citrix Receiver für Windows mit lokalen Administratorrechten über eine Befehlszeile installieren, die die Option /includeSSON enthält. Weitere Informationen finden Sie unter Manuelles Installieren und Konfigurieren von Citrix Receiver für die Passthrough-Authentifizierung. **Hinweis:** Die Richtlinien “Smartcard”, “Kerberos” und “Lokaler Benutzername und Kennwort” sind voneinander abhängig. Die Reihenfolge der Konfiguration ist wichtig. Wir empfehlen, unerwünschte Richtlinien zunächst zu deaktivieren und anschließend die benötigten Richtlinien zu aktivieren. Prüfen Sie das Ergebnis sorgfältig.
Beispiel für Verwendung	CitrixReceiver.exe /includeSSON

Aktivieren von Single Sign-On, wenn /includeSSON angegeben ist

Option	ENABLE_SSON={Yes | No}
Beschreibung	Aktiviert Single Sign-On, wenn /includeSSON angegeben ist. Der Standardwert ist “Yes”. Aktiviert Single Sign-On, wenn /includeSSON ebenfalls angegeben ist. Diese Eigenschaft wird für Single Sign-On per Smartcard benötigt. Hinweis: Alle Benutzer müssen sich nach der Installation mit aktivierter Single Sign-On-Authentifizierung an den Geräten ab- und erneut anmelden. Hierfür sind Administratorrechte erforderlich.
Beispiel für Verwendung	CitrixReceiver.exe ENABLE_SSON=Yes

Always-On-Ablaufverfolgung

Option	/EnableTracing={true | false}
Beschreibung	Standardmäßig ist dieses Feature auf “true” festgelegt. Mit dieser Eigenschaft aktivieren oder deaktivieren Sie das Feature “Always-On-Ablaufverfolgung” explizit. Mit dem Feature “Always-On-Ablaufverfolgung” werden wichtige Protokolle während der Verbindungszeit gesammelt. Die Protokolle können bei der Problembehandlung von zeitweiligen Verbindungsproblemen hilfreich sein. Die Richtlinie “Always-On-Ablaufverfolgung” überschreibt diese Einstellung.
Beispiel für Verwendung	CitrixReceiver.exe /EnableTracing=true

Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Option	EnableCEIP={true | false}
Beschreibung	Wenn Sie die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) aktivieren, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit Citrix die Qualität und Leistung von Produkten verbessern kann.
Beispiel für Verwendung	CitrixReceiver.exe EnableCEIP=true

Angeben des Installationsverzeichnisses

Option	INSTALLDIR=<Installationsverzeichnis>
Beschreibung	Gibt den Pfad zum Installationsverzeichnis an, wobei Installationsverzeichnis das Verzeichnis ist, in dem der Großteil der Receiver-Software installiert ist. Der Standardwert ist C:\Programme\Citrix\Receiver. Die folgenden Receiver-Komponenten werden im Pfad C:\Programme\Citrix installiert: Authentifizierungsmanager, Citrix Receiver und das Self-Service-Plug-In. Wenn Sie diese Option verwenden und ein Installationsverzeichnis angeben, müssen Sie RIInstaller.msi im Verzeichnis Installationsverzeichnis\Receiver und die anderen MSI-Dateien im Installationsverzeichnis installieren.
Beispiel für Verwendung	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identifizieren eines Benutzergerätes

Option	CLIENT_NAME=<Clientname>
Beschreibung	Gibt den Clientnamen an, wobei Clientname der Name ist, mit dem das Benutzergerät beim Server identifiziert wird. Der Standardwert ist %COMPUTERNAME%.
Beispiel für Verwendung	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

Dynamischer Clientname

Option	ENABLE_CLIENT_NAME= Yes | No
Beschreibung	Bei dynamischen Clientnamen stimmt der Clientname mit dem Computernamen überein. Wenn Benutzer den Computernamen ändern, wird der Clientname entsprechend angepasst. Der Standardwert ist Yes. Stellen Sie diese Eigenschaft auf No ein und geben Sie einen Wert für die Eigenschaft CLIENT_NAME an, wenn Sie die Unterstützung dynamischer Clientnamen deaktivieren möchten.
Beispiel für Verwendung	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

Installieren bestimmter Komponenten

Option	ADDLOCAL=<feature… ,>
Beschreibung	Installiert die angegebenen Komponenten. Wenn Sie mehrere Parameter angeben, trennen Sie die Parameter durch Kommas und ohne Leerzeichen. Bei den Namen wird Groß- und Kleinschreibung erkannt. Wenn Sie diesen Parameter nicht angeben, werden alle Komponenten standardmäßig installiert. Zu den Komponenten gehören u. a.: ReceiverInside: Installiert die Citrix Receiver Experience (für den Receiver-Betrieb benötigte Komponente). ICA_Client: Installiert die Standardversion von Citrix Receiver (für den Receiver-Betrieb benötigte Komponente). WebHelper: Installiert die WebHelper-Komponente. Diese Komponente ruft die ICA-Datei aus StoreFront ab und leitet sie an die HDX Engine weiter. Darüber hinaus verifiziert sie Umgebungsparameter und teilt sie mit StoreFront (ähnlich der ICO-Clienterkennung). [Optional] SSON: Installiert Single Sign-On. Hierfür sind Administratorrechte erforderlich. AM: Installiert den Authentifizierungsmanager. SELFSERVICE: Installiert das Self-Service-Plug-In. Der Wert AM muss an der Befehlszeile angegeben werden und .NET 3.5 Service Pack 1 muss auf dem Benutzergerät installiert sein. Das Self-Service Plug-In ist für Windows Thin PC-Geräte, die .NET 3.5 nicht unterstützen, nicht verfügbar. Informationen zum Skripting des Self-Service-Plug-Ins (SSP) und eine Liste mit in Receiver für Windows 4.2 und höheren Versionen verfügbaren Parametern finden Sie im Knowledge Center unter CTX200337. Mit dem Self-Service-Plug-In greifen Benutzer auf virtuelle Desktops und Anwendungen vom Receiver-Fenster aus oder über eine Befehlszeile zu. Dies wird nachfolgend unter “Starten eines virtuellen Desktops oder einer Anwendung an einer Befehlszeile” beschrieben. USB: Installiert die USB-Unterstützung. Hierfür sind Administratorrechte erforderlich. DesktopViewer: Installiert Desktop Viewer.

Option	ADDLOCAL=<feature… ,>
Beispiel für Verwendung	CitrixReceiver.exe ADDLO- CAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

Konfigurieren von Citrix Receiver für Windows zum manuellen Hinzufügen von Stores

Option	ALLOWADDSTORE={N | S | A}
Beschreibung	Gibt an, ob Benutzer Stores, die nicht mit Merchandising Server-Bereitstellungen konfiguriert sind, hinzufügen oder entfernen können. Benutzer können Stores, die mit Merchandising Server-Bereitstellungen konfiguriert sind, aktivieren oder deaktivieren, sie können die Stores jedoch nicht entfernen oder die Namen oder URLs ändern. Der Standardwert ist “S”. Optionen sind u. a.: N: Benutzer können nie einen eigenen Store hinzufügen. S: Benutzer können nur sichere Stores hinzufügen oder entfernen (mit HTTPS konfiguriert). A: Benutzer können sichere (HTTPS) und nicht sichere (HTTP) Stores hinzufügen oder entfernen. Gilt nicht, wenn Citrix Receiver pro Benutzer installiert wird. Sie können dieses Feature auch durch Aktualisieren des Registrierungsschlüssels “HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowAddStore steuern. **Hinweis:** Nur sichere (HTTPS) Stores sind in der Standardeinstellung zulässig; dies wird für Produktionsumgebungen empfohlen. In Testumgebungen können Sie HTTP-Storeverbindungen mit der folgenden Konfiguration verwenden: Stellen Sie HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowAddStore auf A ein, damit Benutzer nicht sichere Stores hinzufügen können. Stellen Sie HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowSavePwd auf A ein, damit Benutzer die Kennwörter für nicht sichere Stores speichern können. Damit ein Store, der in StoreFront mit einem Transporttyp von HTTP konfiguriert ist, hinzugefügt werden kann, fügen Sie für HKLM\Software[Wow6432Node]Citrix\AuthManager den Wert ConnectionSecurityMode (Typ REG_SZ) hinzu und stellen ihn auf “Any” ein. Beenden und starten Sie Citrix Receiver neu.

Option	ALLOWADDSTORE={N | S | A}
Beispiel für Verwendung	CitrixReceiver.exe ALLOWADDSTORE=N

Lokales Speichern von Anmeldeinformationen für Stores mit dem PNAgent-Protokoll

Option	ALLOWSAVEPWD={N | S | A}
Beschreibung	Der Standard ist der Wert, der vom PNAgent-Server zur Laufzeit angegeben wird. Gibt an, ob Benutzer Anmeldeinformationen für Stores lokal auf ihren Computern speichern können und gilt nur für Stores, die das PNAgent-Protokoll verwenden. Der Standardwert ist S. Folgende Optionen sind verfügbar: N: Benutzer können nie die Kennwörter speichern. S: Benutzer können nur Kennwörter für sichere Stores speichern (mit HTTPS konfiguriert). A: Benutzer können Kennwörter für sichere (HTTPS) und nicht sichere (HTTP) Stores speichern. Sie können dieses Feature auch durch Aktualisieren des Registrierungsschlüssels “HKLM\Software[Wow6432Node]\Citrix\Dazzle\AllowSavePw steuern. **Hinweis:** Der folgende Registrierungsschlüssel muss manuell hinzugefügt werden, wenn AllowSavePwd nicht funktioniert. Schlüssel für Client mit 32-Bit-Betriebssystem: HKLM\Software\Citrix\AuthManager •Schlüssel für Client mit 64-Bit-Betriebssystem: HKLM\Software\wow6432node\Citrix\AuthManager •Typ: REG_SZ •Wert: Never: Benutzer dürfen nie ihre Kennwörter speichern. Secureonly: Benutzer dürfen Kennwörter nur in sicheren Stores (mit HTTPS konfiguriert) speichern. Always: Benutzer dürfen Kennwörter in sicheren Stores (HTTPS) und nicht sicheren Stores (HTTP) speichern.

Option	ALLOWSAVEPWD={N | S | A}
Beispiel für Verwendung	CitrixReceiver.exe ALLOWSAVEPWD=N

Zertifikat auswählen

Option	AM_CERTIFICATESELECTIONMODE={Prompt |SmartCardDefault | LatestExpiry}
Beschreibung	Mit dieser Option wählen Sie ein Zertifikat aus. Der Standardwert ist “Prompt”, d. h. der Benutzer wird zur Auswahl eines Zertifikats aus einer Liste aufgefordert. Ändern Sie diese Eigenschaft, sodass das Standardzertifikat (gemäß des Smartcardanbieters) oder das Zertifikat mit dem spätesten Ablaufdatum ausgewählt wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden. Mit dieser Option wählen Sie ein Zertifikat aus. Der Standardwert ist “Prompt”, d. h. der Benutzer wird zur Auswahl eines Zertifikats aus einer Liste aufgefordert. Ändern Sie diese Eigenschaft, sodass das Standardzertifikat (gemäß des Smartcardanbieters) oder das Zertifikat mit dem spätesten Ablaufdatum ausgewählt wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden. Sie können dieses Feature auch durch Aktualisieren des Registrierungsschlüssels HKCU oder HKLM\Software[Wow6432Node]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry } steuern. In HKCU definierte Werte haben Priorität über Werte in HKLM, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.
Beispiel für Verwendung	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

Verwalten von Smartcard-PIN-Eingaben mit CSP-Komponenten

Option	AM_SMARTCARDPINENTRY=CSP
Beschreibung	Verwalten Sie Smartcard-PIN-Eingaben mit CSP-Komponenten. Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von Citrix Receiver und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Receiver fordert Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN den Smartcard-Kryptografiedienstanbieter. Geben Sie diese Eigenschaft an, um die PIN-Eingabe, einschließlich der Aufforderung für eine PIN, mit den Kryptografiedienstanbieter-Komponenten zu verwalten.
Beispiel für Verwendung	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Verwenden von Kerberos

Option	ENABLE_KERBEROS={Yes | No}
Beschreibung	Der Standardwert ist “No”. Gibt an, ob die HDX-Engine Kerberos-Authentifizierung verwendet und gilt nur, wenn die Authentifizierung mit Single Sign-On (Passthrough-Authentifizierung) aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren von Domänen-Passthrough-Authentifizierung mit Kerberos.
Beispiel für Verwendung	CitrixReceiver.exe ENABLE_KERBEROS=No

Anzeigen von Legacy-FTA-Symbolen

Option	LEGACYFTAICONS={False | True}
Beschreibung	Mit dieser Option zeigen Sie Legacy-FTA-Symbole an. Der Standardwert ist “False”. Gibt an, ob Anwendungssymbole für Dokumente angezeigt werden, die Dateitypzuordnungen für abonnierte Anwendungen haben. Wenn “False” angegeben ist, erstellt Windows Symbole für Dokumente, denen kein spezielles Symbol zugeordnet ist. Die von Windows erstellten Symbole bestehen aus einem generischen Dokumentsymbol mit einer kleineren Version des Anwendungssymbols darüber. Citrix empfiehlt, dass diese Option aktiviert ist, wenn Sie Microsoft Office-Anwendungen für Benutzer, die Windows 7 ausführen, bereitstellen.
Beispiel für Verwendung	CitrixReceiver.exe LEGACYFTAICONS=False

Aktivieren des Vorabstarts

Option	ENABLEPRELAUNCH={False | True}
Beschreibung	Der Standardwert ist “False”. Weitere Informationen zum Vorabstart von Sitzungen finden Sie unter Verkürzen des Anwendungsstarts.
Beispiel für Verwendung	CitrixReceiver.exe ENABLEPRELAUNCH=False

Angeben des Verzeichnisses für Startmenüverknüpfungen

Option	STARTMENUDIR={Directory Name}
Beschreibung	Standardmäßig werden Anwendungen unter Start > Alle Programme angezeigt. Sie können den relativen Pfad für die Verknüpfungen zu den abonnierten Anwendungen unter dem Ordner “Programme” angeben. Beispiel: Geben Sie STARTMENUDIR=\Receiver an, um Verknüpfungen unter Start > Alle Programme > Receiver zu platzieren. Benutzer können jederzeit den Ordnernamen ändern oder den Ordner verschieben. Sie können dieses Feature auch über einen Registrierungsschlüssel steuern: Erstellen Sie einen REG_SZ-Eintrag für StartMenuDir und geben Sie ihm einen Wert von “\RelativePath”. Speicherort: HKLM\Software[Wow6432Node]Citrix\Dazzle HKCU\Software\Citrix\Dazzle Für Anwendungen, die mit XenApp veröffentlicht wurden, für die ein Clientanwendungsordner (auch Program Neighborhood-Ordner genannt) angegeben ist, können Sie festlegen, dass der Clientanwendungsordner dem Verknüpfungspfad wie folgt angehängt wird: Erstellen Sie einen REG_SZ-Eintrag für UseCategoryAsStartMenuPath und geben Sie ihm den Wert “true”. Verwenden Sie die gleichen Registrierungsspeicherorte wie oben angegeben. **Hinweis:** In Windows 8/8.1 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht in mit XenApp definierten Unterordnern für Kategorien. Beispiele: •Bei einem Clientanwendungsordner von \Office, Einstellung von true für UseCategoryAsStartMenuPath und keiner Angabe von StartMenuDir werden Verknüpfungen unter Start > Alle Programme > Office abgelegt. •Bei einem Clientanwendungsordner von \Office, Einstellung von true für UseCategoryAsStartMenuPath und StartMenuDir von \Receiver werden Verknüpfungen unter Start > Alle Programme > Office abgelegt. Änderungen an diesen

Option	STARTMENUDIR={Directory Name}
Beispiel für Verwendung	CitrixReceiver.exe STARTMENUDIR=\Office

Angeben des Storenamens

Option	STOREx=”storename;http[s]://servername.domain/IISLocatio | Off] ; [storedescription]” [STOREy=”…”]
Beschreibung	Geben Sie mit dieser Option den Storenamen an. Geben Sie bis zu 10 Stores ein, die mit Citrix Receiver verwendet werden. Werte: x und y: Ganzzahlen 0 bis 9. Storename: Standardwert ist ”store”. Dieser Name muss mit dem auf dem StoreFront-Server konfigurierten Namen übereinstimmen. Servername.domäne: Der vollqualifizierte Domänenname des Servers, der den Store hostet. IISLocation: Der Pfad zum Store in IIS. Die Store-URL muss mit der URL in den StoreFront-Provisioningdateien übereinstimmen. Die Store-URLs haben das Format ”/Citrix/store/discovery”. Um die URL zu erhalten, exportieren Sie eine Provisioningdatei von StoreFront, öffnen Sie sie im Editor und kopieren Sie die URL aus dem Element <Address>. •On | Off: Die optionale Konfigurationseinstellung ”Off” ermöglicht die Bereitstellung deaktivierter Stores. So können Benutzer entscheiden, ob sie darauf zugreifen oder nicht. Wenn kein Storestatus angegeben ist, ist die Standardeinstellung ”On”. storedescription: Eine optionale Beschreibung des Stores, z. B. HR App Store. **Hinweis:** In diesem Release ist es für eine erfolgreiche Passthrough-Authentifizierung wichtig, dass “/discovery” in der Store-URL enthalten ist.
Beispiel für Verwendung	CitrixReceiver.exe STORE0=”Store`https://test.xx.com/Citrix/Store/Discovery`

Aktivieren der URL-Umleitung auf Benutzergeräten

Option	ALLOW_CLIENTHOSTEDAPPSURL=1
Beschreibung	Aktiviert die URL-Umleitung auf Benutzergeräten. Hierfür sind Administratorrechte erforderlich. Citrix Receiver muss für alle Benutzer installiert sein. Weitere Informationen zur URL-Umleitung finden Sie unter Lokaler App-Zugriff in der XenDesktop 7-Dokumentation.
Beispiel für Verwendung	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

Angeben des Verzeichnisses für Desktopverknüpfungen

Option	DESKTOPDIR=<Verzeichnisname>
Beschreibung	Fasst alle Verknüpfungen in einem Ordner zusammen. CategoryPath wird für Desktopverknüpfungen unterstützt. **Hinweis:** Wenn Sie die Option DESKTOPDIR verwenden, setzen Sie den Schlüssel PutShortcutsOnDesktop auf True.
Beispiel für Verwendung	CitrixReceiver.exe DESKTOPDIR=\Office

Upgrade von einer nicht unterstützten Citrix Receiver-Version

Option	/rcu
Beschreibung	Ermöglicht das Upgrade von einer nicht unterstützten Citrix Receiver-Version auf die aktuelle Version.
Beispiel für Verwendung	CitrixReceiver.exe /rcu

Problembehebung bei der Installation

Sollte ein Problem bei der Installation auftreten, suchen Sie im Verzeichnis des Benutzers %TEMP%/CTXReceiverInstallLogs nach den Protokollen mit dem Präfix CtxInstall- oder TrollyExpress-. Beispiel:

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Beispiele für eine Installation über die Befehlszeile:

Installieren aller Komponenten ohne Benutzereingriffe und Angeben von zwei Anwendungsstores:

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

Angeben von Single Sign-On (Passthrough-Authentifizierung) und Hinzufügen eines Stores, der auf eine XenApp Services-URL verweist:

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

Starten eines virtuellen Desktops oder einer virtuellen Anwendung über eine Befehlszeile

Citrix Receiver für Windows erstellt eine Stubanwendung für jeden abonnierten Desktop bzw. jede abonnierte Anwendung. Mit einer Stubanwendung können Sie einen virtuellen Desktop oder eine virtuelle Anwendung über die Befehlszeile starten. Stubanwendungen befinden sich in %appdata%\Citrix\SelfService. Der Dateiname einer Stubanwendung ist der Anzeigename der Anwendung ohne Leerstellen. Beispielsweise ist der Dateiname der Stubanwendung für Internet Explorer InternetExplorer.exe.

Bereitstellung mit Active Directory und Beispielstartskripts

November 21, 2018

Sie können Active Directory-Gruppenrichtlinienskripts verwenden, um Citrix Receiver für Windows basierend auf der Active Directory-Organisationsstruktur auf Systemen vorab bereitzustellen. Citrix empfiehlt, dass Sie die Skripts verwenden, statt die MSI-Dateien zu extrahieren, da Sie mit

Skripts die Installation, das Upgrade und die Deinstallation an einer Stelle durchführen. Durch die Skripts werden die Citrix Einträge in “Programme und Funktionen” konsolidiert und es ist leichter zu erkennen, welche Citrix Receiver-Version bereitgestellt wurde. Verwenden Sie in der Gruppenrichtlinien-Verwaltungskonsole die Einstellung Skripts unter Computerkonfiguration oder Benutzerkonfiguration. Allgemeine Informationen über Startskripts finden Sie in der Dokumentation von Microsoft.

Citrix stellt Beispiele von Pro-Computer-Startskripts für die Installation und Deinstallation von CitrixReceiver.exe bereit. Die Skripts sind auf der Downloadseite von Citrix Receiver für Windows verfügbar.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Wenn die Skripts beim Start oder Herunterfahren einer Active Directory-Gruppenrichtlinie ausgeführt werden, werden angepasste Konfigurationsdateien ggf. im Standardbenutzerprofil eines Systems erstellt. Wenn diese Konfigurationsdateien nicht entfernt werden, können einige Benutzer möglicherweise nicht auf das Verzeichnis mit den Receiver-Protokollen zugreifen. Die Beispielskripts von Citrix enthalten Funktionalität, mit der diese Konfigurationsdateien richtig entfernt werden.

Verwenden von Startskripts für die Bereitstellung von Receiver mit Active Directory:

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

Bearbeiten von Beispielskripts

Bearbeiten Sie die Skripts, indem Sie diese Parameter im Kopfbereich jeder Datei anpassen:

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

Hinzufügen von Pro-Computer-Startskripts

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Wählen Sie Computerkonfiguration > Richtlinien > Windows-Einstellungen > Skripts (Start/Herunterfahren).
3. Wählen Sie im rechten Bereich der Gruppenrichtlinien-Verwaltungskonsole Starten.
4. Klicken Sie in den Eigenschaften auf Dateien anzeigen, kopieren Sie das entsprechende Skript in den angezeigten Ordner und schließen Sie dann das Fenster.
5. Klicken Sie in den Eigenschaften auf Hinzufügen und verwenden Sie Durchsuchen, um das soeben erstellte Skript zu finden.

Bereitstellen von Citrix Receiver für Windows auf Pro-Computer-Basis

1. Verschieben Sie die Benutzergeräte, für die Sie diese Art der Bereitstellung verwenden möchten, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich mit einem beliebigen Benutzernamen an.
3. Stellen Sie sicher, dass das neu installierte Paket in “Programme und Funktionen” (Systemsteuerung “Software” in früheren Versionen des Betriebssystems) angezeigt wird.

Entfernen von Citrix Receiver für Windows auf Pro-Computer-Basis

1. Verschieben Sie die Benutzergeräte, die entfernt werden sollen, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich mit einem beliebigen Benutzernamen an.
3. Stellen Sie sicher, dass das zuvor installierte Paket aus “Programme und Funktionen” (Systemsteuerung “Software” in früheren Versionen des Betriebssystems) entfernt wurde.

Verwenden der Beispielsstartskripts auf Benutzerbasis

Citrix empfiehlt die Verwendung von Startskripts pro Computer. In Situationen, in denen Sie Bereitstellungen pro Benutzer für Citrix Receiver für Windows benötigen, sind zwei Pro-Benutzer-Skripts für Citrix Receiver für Windows auf den XenDesktop- und XenApp-Medien im Ordner Citrix Receiver for Windows and Plug-ins\Windows\Receiver\Startup_Logon_Scripts enthalten.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

Einrichten von Pro-Benutzer-Startskripten

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

Bereitstellen von Citrix Receiver für Windows auf Pro-Benutzer-Basis

1. Verschieben Sie die Benutzer, für die Sie diese Art der Bereitstellung verwenden möchten, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich mit dem jeweiligen Benutzernamen an.
3. Stellen Sie sicher, dass das neu installierte Paket in “Programme und Funktionen” (Systemsteuerung “Software” in früheren Versionen des Betriebssystems) angezeigt wird.

Entfernen von Citrix Receiver für Windows auf Pro-Benutzer-Basis

1. Verschieben Sie die Benutzer, die entfernt werden sollen, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich mit dem jeweiligen Benutzernamen an.
3. Stellen Sie sicher, dass das zuvor installierte Paket aus “Programme und Funktionen” (Systemsteuerung “Software” in früheren Versionen des Betriebssystems) entfernt wurde.

Bereitstellen von Citrix Receiver für Windows über Citrix Receiver für Web

January 7, 2019

Sie können Citrix Receiver für Windows über Citrix Receiver für Web bereitstellen, um sicherzustellen, dass Receiver auf den Benutzergeräten installiert ist, bevor Sie versuchen, über einen Browser eine Verbindung zu einer Anwendung herzustellen. Mit Citrix Receiver für Web-Sites können Sie über eine Webseite auf StoreFront-Stores zugreifen. Wenn die Citrix Receiver für Web-Site erkennt, dass ein Benutzer keine kompatible Citrix Receiver für Windows-Version hat, wird der Benutzer zum Download und zur Installation von Citrix Receiver für Windows aufgefordert.

Weitere Informationen finden Sie unter
Citrix Receiver für Web-Sites in der StoreFront-Dokumentation.

Die e-mail-basierte Kontenermittlung wird nicht unterstützt, wenn Citrix Receiver für Windows von Citrix Receiver für Web bereitgestellt wird. Wenn die e-mail-basierte Kontenermittlung konfiguriert ist und ein Erstbenutzer Citrix Receiver für Windows von Citrix.com installiert, fordert Citrix Receiver für Windows den Benutzer zur Eingabe einer E-Mail- oder Serveradresse auf. Bei der Eingabe einer E-Mail-Adresse wird eine Fehlermeldung “Sie können kein Konto mit der E-Mail-Adresse hinzufügen” angezeigt.

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

1. Laden Sie CitrixReceiver.exe auf den lokalen Computer herunter.
2. Benennen Sie CitrixReceiver.exe in CitrixReceiverWeb.exe um.
3. Stellen Sie die umbenannte ausführbare Datei mit der normalen Bereitstellungsmethode bereit. Wenn Sie StoreFront verwenden, finden Sie weitere Informationen unter Konfigurieren von Receiver für Web mit Konfigurationsdateien in der StoreFront-Dokumentation.

Bereitstellen von Citrix Receiver für Windows über einen Webinterface-Anmeldebildschirm

November 21, 2018

Dieses Feature ist nur für XenDesktop- und XenApp-Releases verfügbar, die das Webinterface unterstützen.

Sie können Citrix Receiver für Windows auf einer Webseite bereitstellen, um sicherzustellen, dass Citrix Receiver für Windows auf dem Benutzergerät installiert ist, bevor sie das Webinterface verwenden. Das Webinterface enthält einen Clienterkennungs- und -bereitstellungsprozess, der erkennt, welche Citrix Clients in der Umgebung des Benutzers bereitgestellt werden können, und der die Benutzer bei der Bereitstellung unterstützt.

Die Clienterkennung und -bereitstellung kann automatisch ausgeführt werden, wenn Benutzer auf eine XenApp-Website zugreifen. Wenn das Webinterface erkennt, dass ein Benutzer keine kompatible Citrix Receiver für Windows-Version hat, wird der Benutzer zum Download und zur Installation von Citrix Receiver für Windows aufgefordert.

Die e-mail-basierte Kontenermittlung gilt nicht, wenn Citrix Receiver für Windows vom Webinterface bereitgestellt wird. Wenn die e-mail-basierte Kontenermittlung konfiguriert ist und ein Erstbenutzer Citrix Receiver für Windows von Citrix.com installiert, fordert Citrix Receiver für Windows den Benutzer zur Eingabe einer E-Mail- oder Serveradresse auf. Bei der Eingabe einer E-Mail-Adresse wird eine

Fehlermeldung “Sie können kein Konto mit der E-Mail-Adresse hinzufügen” angezeigt. Verwenden Sie die folgende Konfiguration, um nur zur Eingabe der Serveradresse aufzufordern.

1. Laden Sie CitrixReceiver.exe auf den lokalen Computer herunter.
2. Benennen Sie CitrixReceiver.exe in CitrixReceiverWeb.exe um.
3. Geben Sie den geänderten Dateinamen im Parameter ClientIcaWin32 in den Konfigurationsdateien für die XenApp-Websites an.

   Für den Clienterkennungs- und -bereitstellungsprozess müssen die Citrix Receiver für Windows-Installationsdateien auf dem Webinterface-Server vorhanden sein. Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Citrix Receiver für Windows-Installationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind.
4. Sie müssen die Sites, von denen die Datei CitrixReceiverWeb.exe heruntergeladen wird, der Zone “Vertrauenswürdige Sites” hinzufügen.
5. Stellen Sie die umbenannte ausführbare Datei mit der normalen Bereitstellungsmethode bereit.

Bereitstellung über den System Center Configuration Manager 2012 R2

January 7, 2019

Sie können Citrix Receiver für Windows über Microsoft System Center Configuration Manager (SCCM) bereitstellen.

Hinweis: Die SCCM-Bereitstellung wird nur von Citrix Receiver für Windows ab Version 4.5 und höher unterstützt.

Die Bereitstellung von Citrix Receiver für Windows mit SCCM umfasst vier Teilschritte:

1. Hinzufügen von Citrix Receiver für Windows zur SCCM-Bereitstellung
2. Hinzufügen von Verteilungspunkten
3. Bereitstellen der Receiver-Software auf dem Softwarecenter
4. Erstellen von Gerätesammlungen

Hinzufügen von Citrix Receiver für Windows zur SCCM-Bereitstellung

1. Kopieren Sie die heruntergeladene Citrix Receiver-Software in einen Ordner auf dem Configuration Manager-Server und starten Sie die Configuration Manager-Konsole.

2. Wählen Sie **Softwarebibliothek** > **Anwendungsverwaltung**. Klicken Sie mit der rechten Maustaste auf **Anwendung** und klicken Sie auf **Anwendung erstellen**.
   Der Assistent zum Erstellen von Anwendungen wird angezeigt.
3. Aktivieren Sie im Bereich **Allgemein** die Option **Anwendungsinformationen manuell angeben** und klicken Sie auf **Weiter**.
4. Im Bereich **Allgemeine Informationen** geben Sie Informationen zur Anwendung wie Name, Hersteller und Softwareversion ein.
5. Im Assistenten zum Anwendungskatalog geben Sie zusätzliche Informationen wie Sprache, Anwendungsname und Benutzerkategorie ein. Klicken Sie dann auf **Weiter**.

   Hinweis: Die Benutzer können die hier angegebenen Informationen anzeigen.
6. Im Bereich **Bereitstellungstyp** klicken Sie auf **Hinzufügen**, um den Bereitstellungstyp für den Citrix Receiver-Setup zu konfigurieren. Der Assistent zum Erstellen von Bereitstellungstypen wird angezeigt.
7. Bereich **Allgemein**: Wählen Sie Windows Installer (*.msi-Datei) als Bereitstellungstyp. Aktivieren Sie **Informationen zum Bereitstellungstyp manuell angeben** und klicken Sie auf **Weiter**.
8. Bereich **Allgemeine Informationen**: Legen Sie den Bereitstellungstyp fest (z. B.: Receiver-Bereitstellung) und klicken Sie auf **Weiter**.
9. Bereich **Inhalt**:
   a) Geben Sie den Pfad zum Verzeichnis mit der Citrix Receiver-Setupdatei an. Beispiel: Tools auf dem SCCM-Server.
   b) Geben Sie das **Installationsprogramm** an. Zur Auswahl stehen folgende Optionen:
      - CitrixReceiver.exe /silent für eine automatische Standardinstallation.
      - CitrixReceiver.exe /silent /includeSSON zum Aktivieren des Domänen-Passthrough.
      - CitrixReceiver.exe /silent SELFSERVICEMODE=false zur Installation von Citrix Receiver im Modus ohne Self-Service.
   c) Geben Sie für **Deinstallationsprogramm** CitrixReceiver.exe /uninstall ein (zum Aktivieren der Deinstallation über SCCM).
10. Bereich **Erkennungsmethode**: Wählen Sie **Regeln konfigurieren, um zu erkennen, ob dieser Bereitstellungstyp vorhanden ist**, und klicken Sie auf **Klausel hinzufügen**. Das Dialogfeld “Erkennungsregel” wird angezeigt.
11. Wählen Sie als **Einstellungstyp** die Option “Dateisystem”.
12. Wählen Sie folgende Einstellungen unter **Geben Sie die Datei oder den Ordner an, um diese Anwendung zu erkennen**:
    - **Typ**: Wählen Sie im Dropdownmenü die Option “Datei”.

- **Pfad**: %Programme (x86)%\Citrix\ICA Client\Receiver
- **Datei- oder Ordnername** - Receiver.exe
- **Eigenschaft**: Wählen Sie im Dropdownmenü die Option **Version**.
- **Operator**: Wählen Sie im Dropdownmenü **größer oder gleich**.
- **Wert**: Geben Sie ein **4.3.0.65534**.

Hinweis: Diese Regelkombination gilt auch für Citrix Receiver für Windows-Upgrades.

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

    - **Installationsverhalten**: Option "Für System installieren"
    - **Anmeldeanforderung**: Option "Unabhängig von Benutzeranmeldung"
    - **Sichtbarkeit des Installationsprogramms**: Normal.

    Klicken Sie auf **Weiter**.

    Hinweis: Legen Sie keine Anforderungen und Abhängigkeiten für diesen Bereitstellungstyp fest.

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

    Es wird dann ein Erfolg gemeldet.

15. Im **Abschlussfenster** wird ein neuer Bereitstellungstyp (Receiver-Bereitstellung) unter den Bereitstellungstypen aufgelistet.

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

Hinzufügen von Verteilungspunkten

1. Klicken Sie mit der rechten Maustaste in der Configuration Manager-Konsole auf Receiver für Windows und wählen Sie **Inhalt verteilen**.
   Der Assistent für die Verteilung von Inhalt wird angezeigt.
2. Klicken Sie im Bereich "Inhaltsverteilung" auf **Hinzufügen > Verteilungspunkte**. Das Dialogfeld "Verteilungspunkte hinzufügen" wird angezeigt.
3. Navigieren Sie zum SCCM-Server, auf dem der Inhalt verfügbar ist, und klicken Sie auf **OK**. Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.
4. Klicken Sie auf **Schließen**.

Bereitstellen der Receiver-Software auf dem Softwarecenter

1. Klicken Sie mit der rechten Maustaste in der Configuration Manager-Konsole auf Receiver für Windows und wählen Sie **Bereitstellen**.
   Der Assistent zur Softwarebereitstellung wird angezeigt.

2. Wählen Sie **Durchsuchen** für die Sammlung (Gerätesammlung oder Benutzersammlung), wo die Anwendung bereitgestellt werden soll, und klicken Sie auf **Weiter**.
3. Wählen Sie im Bereich **Bereitstellungseinstellungen** für **Aktion** die Einstellung "Installation" und für **Zweck** die Option "Erforderlich". Dies aktiviert die unbeaufsichtigte Installation. Klicken Sie auf **Weiter**.
4. Legen Sie im Bereich **Zeitplanung** den Zeitplan für die Bereitstellung der Software auf den Zielgeräten fest.
5. Legen Sie im Bereich **Benutzererfahrung** das Verhalten für **Benutzerbenachrichtigungen** fest: Wählen Sie **Änderungen zum Stichtag oder während eines Wartungsfensters ausführen (erfordert Neustart)** und klicken Sie auf **Weiter**, um den Assistenten zur Softwarebereitstellung zu schließen. Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

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

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

Erstellen von Gerätesammlungen

1. Starten Sie die Configuration Manager-Konsole und klicken Sie auf **Bestand** und **Kompatibilität** > **Überblick** > **Geräte**.
2. Klicken Sie mit der rechten Maustaste auf **Gerätesammlungen** und wählen Sie **Gerätesammlung erstellen**. Der Assistent zum Erstellen von Gerätesammlungen wird angezeigt.
3. Geben Sie im Bereich **Allgemein** den Namen für das Gerät ein und klicken Sie auf **Durchsuchen**, um eine begrenzte Sammlung auszuwählen. Dies bestimmt den Geltungsbereich von Geräten. Es kann eine der von SCCM erstellten Standard-Gerätesammlungen verwendet werden. Klicken Sie auf **Weiter**.
4. Klicken Sie im Bereich "Mitgliedschaftsregeln" auf **Regel hinzufügen**. Diese wird dann zum Filtern der Geräte verwendet. Der Assistent für die Erstellung direkter Mitgliedschaftsregeln wird angezeigt.
   - Wählen Sie im Bereich "Ressourcen suchen" einen **Attributnamen**, der den gesuchten Geräten entspricht, und legen Sie einen Wert für den Attributnamen fest, der bei der Geräteauswahl verwendet werden soll.
5. Klicken Sie auf **Weiter**. Wählen Sie im Bereich "Ressourcen auswählen" die Geräte aus, die in der Gerätesammlung enthalten sein müssen. Im Abschlussfenster wird eine Erfolgsmeldung

angezeigt.

6. Klicken Sie auf **Schließen**.
7. Im Bereich “Mitgliedschaftsregeln” wird eine neue Regel aufgelistet. Klicken Sie auf **Weiter**.
8. Im Abschlussfenster wird eine Erfolgsmeldung angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zum Erstellen von Gerätesammlungen schließen. Die neue Gerätesammlung ist nun unter **Gerätesammlungen** aufgeführt. Beim Navigieren im Assistenten zur Softwarebereitstellung wird die neue Gerätesammlung in den Gerätesammlungen angezeigt.

> **Hinweis**
>
> Wenn Sie das Attribut **MSIRESTARTMANAGERCONTROL** auf **False** setzen, kann Citrix Receiver für Windows mit SCCM möglicherweise nicht bereitgestellt werden.
> Gemäß unserer Analyse wird dieses Problem nicht durch Citrix Receiver für Windows verursacht. Ein erneuter Versuch kann zudem zum Erfolg der Bereitstellung führen.

Konfigurieren

January 7, 2019

Wenn Sie Citrix Receiver für Windows verwenden, führen Sie die folgenden Konfigurationsschritte aus, damit Benutzer auf ihre gehosteten Anwendungen und Desktops zugreifen können:

- Konfigurieren der Anwendungsbereitstellung und Konfigurieren der XenDesktop-Umgebung: Stellen Sie sicher, dass die XenApp-Umgebung richtig konfiguriert ist. Machen Sie sich mit den Optionen vertraut und geben Sie aussagekräftige Anwendungsbeschreibungen für Benutzer an.
- Konfigurieren des Self-Service-Modus durch Hinzufügen eines StoreFront-Kontos zu Citrix Receiver für Windows. Dieser Modus ermöglicht Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Citrix Receiver für Windows.
- Konfigurieren über die administrative Gruppenrichtlinienobjektvorlage
- Stellen Sie den Benutzern Kontoinformationen bereit. Teilen Sie den Benutzern die Informationen mit, die sie zum Einrichten der Konten benötigen, unter denen die virtuellen Desktops und Anwendungen ausgeführt werden. In einigen Umgebungen müssen Benutzer den Zugriff auf diese Konten manuell einrichten.

Wenn Benutzer eine Verbindung von außerhalb des internen Netzwerks herstellen (beispielsweise Benutzer, die eine Verbindung vom Internet oder von Remotestandorten herstellen), konfigurieren Sie die Authentifizierung über NetScaler Gateway. Weitere Informationen finden Sie in der NetScaler Gateway-Dokumentation unter Authentication and Authorization.

Konfigurieren der Anwendungsbereitstellung

March 26, 2019

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit XenDesktop oder XenApp, um die Benutzererfahrung zu verbessern.

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

Hinweis: Standardmäßig können Benutzer von Citrix Receiver für Windows Anwendungen zur Anzeige im Startmenü auswählen.

- Nur-Verknüpfungsmodus: Als Administrator für Citrix Receiver für Windows können Sie Citrix Receiver für Windows so konfigurieren, dass Verknüpfungen für Anwendungen und Desktops ähnlich wie bei Citrix Receiver für Windows Enterprise direkt im Startmenü oder auf dem Desktop platziert werden. Mit dem neuen *Nur-Verknüpfungsmodus* werden die veröffentlichten Anwendungen entsprechend dem gewohnten Windows-Navigationsschema angezeigt.

Weitere Informationen zur Bereitstellung von Anwendungen mit XenApp und XenDesktop 7 finden Sie unter Erstellen einer Bereitstellungsgruppenanwendung.

Hinweis: Fügen Sie aussagekräftige Beschreibungen für Anwendungen in einer Bereitstellungsgruppe hinzu. Die Beschreibungen sind sichtbar, wenn Benutzer von Citrix Receiver für Windows den Webzugriffs- oder Self-Service-Modus verwenden.

Konfigurieren eines NetScaler Gateway-Stores

Citrix empfiehlt Regeln für das Netzwerkrouting, für die Proxyserver und für die vertrauenswürdige Serverkonfiguration, für das Benutzerrouting, für die Remoteclientgeräte und die Benutzererfahrung mit dem Gruppenrichtlinienobjekt “Administrative Vorlagen” zu konfigurieren.
Sie können die Vorlagendateien receiver.admx bzw. receiver.adml für Domänenrichtlinien und

lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Dies ist besonders nützlich, wenn Sie Citrix Receiver für Windows-Einstellungen auf mehrere verschiedene Benutzergeräte im Unternehmen anwenden möchten. Wenn Sie nur ein einziges Benutzergerät bearbeiten möchten, importieren Sie die Vorlagendatei mit dem lokalen Gruppenrichtlinien-Editor auf dem Gerät.

Hinzufügen oder Festlegen eines NetScaler Gateways mit der administrativen Gruppenrichtlinienobjektvorlage:

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
    - Wenn Sie die Richtlinie auf einen einzigen Computer anwenden, starten Sie sie vom Startmenü.
    - Wenn Sie sie auf Domänenrichtlinien anwenden, starten Sie sie mit der Gruppenrichtlinien-Verwaltungskonsole.
2. Navigieren Sie unter dem Knoten “Computerkonfiguration” zu “Administrative Vorlagen” > “Klassische administrative Vorlagen (ADM)” > “Citrix Komponenten” > “Citrix Receiver” > “StoreFront” und wählen Sie “NetScaler Gateway-URL/StoreFront-Kontenliste”.
3. Bearbeiten Sie die Einstellungen.
    - Storename: der angezeigte Name des Stores
    - Store-URL: die URL des Stores
    - #Storename: der Name des Stores hinter dem NetScaler Gateway
    - Storeaktivierungszustand: der Zustand des Stores, Ein/Aus
    - Storebeschreibung: eine Beschreibung des Stores
4. Fügen Sie die NetScaler-URL hinzu oder geben Sie sie an. Geben Sie den Namen der URL durch Semikolon getrennt ein:

> **Beispiel:**
>
> `HRStore; https://dtls.blrwinrx.com\##Store name;On; Store for HR staff`
> In diesem Beispiel ist #Store name der Name des Stores hinter NetScaler Gateway und dtls.blrwinrx.com die NetScaler-URL.
>
> Wenn Citrix Receiver für Windows nach dem Hinzufügen von NetScaler Gateway mit dem Gruppenrichtlinienobjekt gestartet wird, wird die folgende Meldung im Infobereich angezeigt.

Einschränkungen:

1. Die NetScaler-URL sollte als Erste gefolgt von der/den StoreFront-URL(s) aufgeführt werden.
2. Mehrere NetScaler-URLs werden nicht unterstützt.
3. Bei Änderungen der NetScaler-URL muss Citrix Receiver für Windows zurückgesetzt werden, damit die Änderungen wirksam werden.

4. Eine mit dieser Methode konfigurierte NetScaler Gateway-URL unterstützt keine PNA-Dienste-Site hinter NetScaler Gateway.

Konfigurieren des Self-Service-Modus

Sie konfigurieren den *Self-Service-Modus* durch Hinzufügen eines StoreFront-Kontos zu Citrix Receiver oder durch Verweisen von Citrix Receiver auf eine StoreFront-Site. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Citrix Receiver. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

Hinweis: Standardmäßig können Benutzer von Citrix Receiver für Windows Anwendungen zur Anzeige im Startmenü auswählen.

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

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

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

Konfigurieren von Speicherorten für App-Verknüpfungen mit der Gruppenrichtlinienobjektvorlage

> **Hinweis**
>
> Sie müssen Änderungen an der Gruppenrichtlinie vor dem Konfigurieren eines Stores vornehmen. Wenn Sie die Gruppenrichtlinie ändern möchten, müssen Sie Citrix Receiver zurücksetzen, die Gruppenrichtlinie konfigurieren und dann den Store neu konfigurieren.

Als Administrator können Sie Verknüpfungen mit der Gruppenrichtlinie konfigurieren.

1. Öffnen Sie den Editor für lokale Gruppenrichtlinien, indem Sie den Befehl gpedit.msc lokal über das Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.

2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner Administrative Vorlagen aus.
3. Klicken Sie im Menü “Aktion” auf “Vorlagen hinzufügen/entfernen”.
4. Wählen Sie “Hinzufügen” aus, navigieren Sie zum Konfigurationsordner von Receiver und wählen Sie dann receiver.admx (oder receiver.adml) aus.
5. Klicken Sie auf “Öffnen”, um die Vorlage hinzuzufügen, und klicken Sie dann auf “Schließen”, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor zu “Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Self-Service”.
7. Wählen Sie “Self-Service-Modus verwalten” aus, um die Receiver-Self-Service-Benutzeroberfläche zu aktivieren bzw. deaktivieren.
8. Wählen Sie “App-Verknüpfung verwalten” aus, um Folgendes zu aktivieren bzw. zu deaktivieren:
    - Verknüpfungen auf dem Desktop
    - Verknüpfungen im Startmenü
    - Desktopverzeichnis
    - Startmenüverzeichnis
    - Kategoriepfad für Verknüpfungen
    - Entfernen von Apps bei Abmeldung
    - Entfernen von Apps beim Beenden
9. Wählen Sie Allow users to Add/Remove account aus, wenn Benutzer Privilegien zum Hinzufügen oder Entfernen mehrerer Konten erhalten sollen.

Konfigurieren von Speicherorten für App-Verknüpfungen mit StoreFront-Kontoeinstellungen

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

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

Hinweis: In Windows 8/8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht

in mit XenApp definierten Unterordnern für Kategorien.

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

In der Datei web.config müssen die Änderungen im XML-Abschnitt für das Konto hinzugefügt werden. Sie finden diesen Abschnitt durch Suchen des Starttags:

< Account Id =… Name = “Store”

Der Abschnitt endet mit dem Tag </account>.

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

<properties> <clear /> </properties>

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

<property name=”PutShortcutsOnDesktop” value=”True” />

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

Ausführliches Beispiel für diesen Abschnitt:

<properties> <property name=”PutShortcutsOnDesktop” value=”True” /> <property name=”DesktopDir” value=”Citrix Applications” />

> **Wichtig**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Wenn Sie die Änderungen vorgenommen haben, übertragen Sie die Konfigurationsänderungen auf die

> Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

Konfigurieren von Speicherorten für App-Verknüpfungen mit Einstellungen pro App in XenApp und XenDesktop 7.x

Mit Citrix Receiver können Anwendungs- und Desktopverknüpfungen direkt in das Startmenü oder auf dem Desktop platziert werden. Ältere Versionen von Citrix Receiver enthielten eine ähnliche Funktionalität, ab Release 4.2.100 kann jedoch die Platzierung von App-Verknüpfungen in XenApp über Einstellungen pro App gesteuert werden. Diese Funktionalität ist in Umgebungen mit nur einer Handvoll Anwendungen nützlich, die immer am gleichen Ort angezeigt werden sollen.

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

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden…	konfigurieren Sie Receiver mit **PutShortcutsInStartMenu=false** und aktivieren Sie die Einstellungen pro App. **Hinweis:** Diese Einstellung gilt nur für die Webinterface-Site.

> **Hinweis:**
>
> Die Einstellung **PutShortcutsInStartMenu=false** gilt für XenApp 6.5 und XenDesktop 7.x.

Konfigurieren von Speicherorten für App-Verknüpfungen mit Einstellungen pro App in XenApp 7.6

Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 7.6:

1. Navigieren Sie in Citrix Studio zum Bildschirm Anwendungseinstellungen.
2. Wählen Sie im Bildschirm “Anwendungseinstellungen” die Option **Bereitstellung**. In diesem Bildschirm legen Sie fest, wie Anwendungen Benutzern bereitgestellt werden.
3. Wählen Sie das entsprechende Symbol für die Anwendung. Klicken Sie auf **Ändern**, um zum Speicherort des gewünschten Symbols zu navigieren.
4. Im Feld **Anwendungskategorie** können Sie für die Anwendung eine Kategorie in Receiver angeben. Wenn Sie beispielsweise Verknüpfungen für Microsoft Office-Anwendungen hinzufügen, geben Sie **Microsoft Office** ein.

5. Aktivieren Sie das Kontrollkästchen **Verknüpfung auf Benutzerdesktop hinzufügen**.
6. Klicken Sie auf **OK**.

Reduzieren von Enumerationsverzögerungen oder digitales Signieren von Anwendungsstubs

Wenn die App-Enumeration bei jeder Anmeldung langsam ist oder Anwendungsstubs digital signiert werden müssen, können Sie mit Receiver die .EXE-Stubs von einer Netzwerkfreigabe kopieren.

Diese Funktionalität umfasst mehrere Schritte:

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

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

1. Öffnen Sie den Registrierungs-Editor (regedit) und fügen Sie HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d mit dem Wert “true” hinzu.
2. Öffnen Sie den Registrierungs-Editor (regedit) und fügen Sie HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d mit dem Wert “true” hinzu. HKCU hat Vorrang vor HKLM.

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

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

1. Erstellen Sie auf einer Clientmaschine EXE-Stubdateien für alle Apps. Fügen Sie dazu mit Receiver alle Anwendungen der Maschine hinzu. Receiver generiert die EXE-Dateien.
2. Verwenden Sie die EXE-Stubdateien aus %APPDATA%\Citrix\SelfService. Sie benötigen nur die Dateien mit der Erweiterung .exe.
3. Kopieren Sie die EXE-Dateien in eine Netzwerkfreigabe.
4. Legen Sie für jeden Clientcomputer, der gesperrt werden soll, folgende Registrierungsschlüssel fest:

a) Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\ShareOne\ReceiverStubs” hinzu.
b) Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v
c) CopyStubsFromCommonStubDirectory /t REG\SZ /d “true”. Diese Einstellungen sind auch über HKCU möglich. HKCU hat Vorrang vor HKLM.
d) Beenden und starten Sie Receiver, um die Einstellungen zu testen.

Anwendungsfälle

In diesem Abschnitt finden Sie Anwendungsfälle für App-Verknüpfungen.

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

Wenn Sie Dutzende oder sogar Hunderte von Apps haben, ist es am Besten, wenn Benutzer ihre liebsten Apps selber auswählen und dem Startmenü hinzufügen können:

Wenn Benutzer Apps selber auswählen und dem Startmenü hinzufügen sollen…	konfigurieren Sie Citrix Receiver im Self-Service-Modus. In diesem Modus können Sie nach Bedarf Schlüsselworteinstellungen für *obligatorische* und *automatisch bereitgestellte* Apps konfigurieren.
Wenn Benutzer die Apps für das Startmenü selber auswählen aber auch bestimmte App-Verknüpfungen auf dem Desktop platziert werden sollen…	konfigurieren Sie Citrix Receiver ohne Optionen und legen Sie die Einstellungen für die wenigen Apps, die auf dem Desktop platziert werden, einzeln fest. Verwenden Sie *automatisch bereitgestellte* und *obligatorische* Apps nach Bedarf.

Keine App-Verknüpfungen im Startmenü

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

Wenn Citrix Receiver nicht automatisch Anwendungsverknüpfungen im Startmenü platzieren soll…	konfigurieren Sie Citrix Receiver mit PutShortcutsInStartMenu=False. Citrix Receiver platziert keine App-Verknüpfungen im Startmenü, selbst wenn der Self-Service-Modus aktiviert ist. Sie können App-Verknüpfungen pro App über die Einstellungen festlegen.

Alle App-Verknüpfungen im Startmenü oder auf dem Desktop

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

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

Einstellungen pro App in XenApp 6.5 oder 7.x

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

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden…	konfigurieren Sie Citrix Receiver mit **PutShortcutsInStartMenu=false** und aktivieren Sie die Einstellungen pro App. **Hinweis:** Diese Einstellung gilt nur für die Webinterface-Site.

Apps in Kategorieordnern oder in bestimmten Ordnern

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

Wenn die von Citrix Receiver im Startmenü platzierten Anwendungsverknüpfungen in den zugeordneten Kategorieordnern angezeigt werden sollen…	konfigurieren Sie Citrix Receiver mit **UseCategoryAsStartMenuPath=True**. **Hinweis:** In Windows 8/8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht in mit XenApp definierten Unterordnern für Kategorien.
Wenn die von Citrix Receiver im Startmenü platzierten Anwendungsverknüpfungen in einem bestimmten Ordner angezeigt werden sollen…	Konfigurieren Sie Citrix Receiver mit StartMenuDir=Startmenü-Ordnername.

Entfernen von Apps beim Abmelden oder Beenden

Wenn der Endpunkt von mehreren Benutzern verwendet wird und andere Benutzer die Apps nicht sehen sollen, stellen Sie sicher, dass die Apps beim Abmelden und Beenden des Benutzers entfernt werden.

Wenn Citrix Receiver alle Apps beim Abmelden entfernen soll…	konfigurieren Sie Citrix Receiver mit RemoveAppsOnLogoff=True.

Wenn Citrix Receiver alle Apps beim Beenden entfernen soll…	konfigurieren Sie Citrix Receiver mit RemoveAppsOnExit=True.

Konfigurieren von lokalem App-Zugriff für Anwendungen

Konfigurieren von lokalem App-Zugriff für Anwendungen:

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

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

  Wenn ein Benutzer eine bevorzugte Anwendung außerhalb von Citrix Receiver deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Receiver-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung vom Citrix Receiver-Fenster deinstalliert, kündigt Citrix Receiver das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

> **Hinweis:** Das Schlüsselwort “prefer” wird angewendet, wenn Citrix Receiver eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.
>
> Sie können das Schlüsselwort “prefer” mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

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

  Bevor Citrix Receiver eine Anwendung auf dem Computer des Benutzers installiert, erfolgt eine Suche nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert Citrix Receiver die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Citrix Receiver-Fenster aus startet, startet Receiver die lokal installierte (bevorzugte) Anwendung.
  Wenn ein Benutzer eine bevorzugte Anwendung außerhalb von Citrix Receiver deinstalliert,

wird das Abonnement für die Anwendung bei der nächsten Citrix Receiver-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung vom Citrix Receiver-Fenster deinstalliert, kündigt Citrix Receiver das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

> **Hinweis:** Das Schlüsselwort "prefer" wird angewendet, wenn Citrix Receiver eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

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

- prefer="Anwendungsname"

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

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

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

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

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

- prefer=”\Folder1\Folder2…\ApplicationName”

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

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

Informationen zu anderen Schlüsselwörtern finden Sie unter “Zusätzliche Empfehlungen” unter Optimieren der Benutzererfahrung in der StoreFront-Dokumentation.

Konfigurieren der XenDesktop-Umgebung

November 21, 2018

Nach der Installation von Citrix Receiver für Windows können die Benutzer mit den folgenden Konfigurationsschritten auf ihre gehosteten Anwendungen und Desktops zugreifen:

- Adaptiver Transport: Der adaptive Transport optimiert den Datentransport durch Anwenden des neuen Citrix Protokolls Enlightened Data Transport (EDT) statt TCP, sofern möglich. Weitere Informationen zur Konfiguration des adaptiven Transports finden Sie unter Konfigurieren des adaptiven Transports.
- Automatische Updates: Durch dieses Feature werden Updates für Citrix Receiver für Windows und für das HDX RealTime Optimization Pack automatisch bereitgestellt, ohne dass ein manueller Download erforderlich ist. Weitere Informationen zum Konfigurieren von automatischen Updates finden Sie unter Konfigurieren von automatischen Updates.
- Bidirektionale Inhaltsumleitung: Die bidirektionale Inhaltsumleitung ermöglicht das Aktivieren und Deaktivieren der Client-zu-Host- und der Host-zu-Client-URL-Umleitung. Weitere Informationen zum Konfigurieren der bidirektionalen Inhaltsumleitung finden Sie unter Konfigurieren der bidirektionalen Inhaltsumleitung.
- Bloomberg-Tastaturen: USB-Spezialgeräte (beispielsweise Bloomberg Tastaturen und 3-D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unterKonfigurieren von Bloomberg-Tastaturen.
- USB-Verbundgerät: USB-Verbundgeräte sind in der Lage, mehrere Funktionen auszuführen. Dies wird erreicht, indem jede Funktion über eine andere Schnittstelle verfügbar gemacht wird. Weitere Informationen zum Konfigurieren von USB-Verbundgeräten finden Sie unter Konfigurieren von USB-Verbundgeräten.
- USB-Unterstützung: Mit der USB-Unterstützung können Benutzer mit zahlreichen USB-Geräten interagieren, wenn sie mit einem virtuellen Desktop verbunden sind. Weitere Informationen zum Konfigurieren der USB-Unterstützung finden Sie unter Konfigurieren der USB-Unterstützung.

Konfigurieren des adaptiven Transports

November 21, 2018

> **Anforderungen**

- XenApp und XenDesktop 7.12 und höher (erforderlich, um das Feature mit Citrix Studio zu aktivieren).
- StoreFront 3.8.
- Nur IPv4 VDAs; IPv6- und heterogene Konfigurationen mit IPv6 und IPv4 werden nicht unterstützt.
- Firewallregel zum Zulassen von eingehendem Datenverkehr an den UDP-Ports 1494 und 2598 des VDAs

> **Hinweis**
>
> TCP-Ports 1494 und 2598 sind auch erforderlich und werden automatisch geöffnet, wenn Sie den VDA installieren. Die UDP-Ports 1494 und 2598 werden jedoch nicht automatisch geöffnet. Sie müssen sie aktivieren.

Adaptiver Transport muss auf dem VDA konfiguriert werden, indem Sie die Richtlinie anwenden, bevor sie für die Kommunikation zwischen VDA und Citrix Receiver verfügbar ist.

In der Standardeinstellung ist der adaptive Transport in Citrix Receiver für Windows zugelassen. Jedoch versucht der Client auch standardmäßig nur die Verwendung von adaptivem Transport, wenn der VDA in der Citrix Studio-Richtlinie **Bevorzugt** konfiguriert ist, und die Einstellung auf dem VDA angewendet wurde.

Sie können den adaptiven Transport mit der Einstellung **Adaptiver HDX-Transport** aktivieren. Legen Sie diese neue Richtlinieneinstellung auf **Bevorzugt** fest, damit der adaptive Transport verwendet wird, sofern dies möglich ist. Wo dies nicht möglich ist, wird TCP verwendet.

Wenn Sie den adaptiven Transport auf einem bestimmten Client deaktivieren möchten, stellen Sie die EDT-Optionen mit der administrativen Gruppenrichtlinienobjektvorlage von Citrix Receiver entsprechend ein.

Konfigurieren des adaptiven Transports mit der administrativen Gruppenrichtlinienobjektvorlage von Citrix Receiver (optional)

Die folgenden Konfigurationsschritte sind optional und dienen zum Anpassen der Umgebung. Sie können das Feature beispielsweise aus Sicherheitsgründen für einen bestimmten Client deaktivieren.

> **Hinweis**
>
> Standardmäßig ist adaptiver Transport deaktiviert und TCP wird immer verwendet.

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
    - Wenn Sie die Richtlinie auf einem einzigen Computer anwenden, starten Sie sie vom Startmenü.

- Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie sie mit der Gruppenrichtlinien-Verwaltungskonsole.

Weitere Informationen zum Importieren der administrativen Citrix Receiver für Windows-Vorlagendateien in den Gruppenrichtlinien-Editor finden Sie unter Konfigurieren von Citrix Receiver für Windows mit der Gruppenrichtlinienobjektvorlage.

2. Navigieren Sie unter dem Knoten "Computerkonfiguration" zu **Administrative Vorlagen** > **Citrix Receiver** > **Netzwerkrouting**.
3. Legen Sie die Richtlinie **Transportprotokoll für Receiver** auf **Aktiviert** fest.
4. Wählen Sie das erforderliche **Kommunikationsprotokoll für Citrix Receiver**.
   - **Aus**: Gibt an, dass TCP zur Datenübertragung verwendet wird.
   - **Bevorzugt**: Gibt an, dass Citrix Receiver versucht, eine Verbindung mit dem Server zuerst über UDP herzustellen und dann ein Fallback auf TCP durchführt.
   - **Ein**: Gibt an, dass Citrix Receiver ausschließlich über UDP eine Verbindung mit dem Server herstellt. Bei dieser Option erfolgt kein Fallback auf TCP.
5. Klicken Sie auf **Anwenden** und auf **OK**.
6. Führen Sie an einer Befehlszeile den Befehl gpupdate /force aus.

Damit die Konfiguration für den adaptiven Transport wirksam wird, muss der Benutzer die Citrix Receiver für Windows-Vorlagendateien dem Ordner mit den Richtliniendefinitionen hinzufügen. Weitere Informationen über das Hinzufügen von ADMX/ADML-Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter Konfigurieren von Citrix Receiver für Windows mit der Gruppenrichtlinienobjektvorlage.

Prüfen, ob die Richtlinieneinstellung in Kraft gesetzt wurde

Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT und stellen Sie sicher, dass der Schlüssel **HDXOverUDP** eingeschlossen ist.

Konfigurieren von automatischen Updates

March 26, 2019

Wenn Sie automatische Updates von Citrix Receiver für Windows konfigurieren, nutzen Sie die folgenden Verfahren in der Reihenfolge ihrer Priorität:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Befehlszeilenschnittstelle
3. Erweiterte Einstellungen (pro Benutzer)

Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
    - Wenn Sie die Richtlinie auf einen einzigen Computer anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
    - Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver mit der Gruppenrichtlinien-Verwaltungskonsole.
2. Navigieren Sie unter dem Knoten "Computerkonfiguration" zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Receiver** > **Automatische Updates**.
3. Wählen Sie die Richtlinie **Verzögerung für Prüfung auf Updates festlegen**. Mit dieser Richtlinie können Sie ein zeitlich gestaffeltes Rollout durchführen.
4. Wählen Sie **Aktiviert** und anschließend im Dropdownmenü neben **Für Gruppe aufschieben** eine der folgenden Optionen:
    - **Fast** – Das Rollout des Updates erfolgt zu Beginn des Bereitstellungszeitraums.
    - **Medium** – Das Rollout des Updates erfolgt in der Mitte des Bereitstellungszeitraums.
    - **Slow** – Das Rollout des Updates erfolgt am Ende des Bereitstellungszeitraums.
5. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.
6. Klicken Sie im AutoUpdate-Bereich auf **AutoUpdate-Richtlinie aktivieren oder deaktivieren**.
7. Wählen Sie **Aktiviert** und legen Sie die Werte nach Bedarf fest:
    - Wählen Sie im Dropdownmenü neben **AutoUpdate-Richtlinie aktivieren** eine der folgenden Optionen:
        - **Auto** – Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).
        - **Manual** – Sie werden nicht benachrichtigt, wenn Updates zur Verfügung stehen. Suchen Sie manuell nach Updates.
    - Aktivieren Sie **Nur LTSR**, um Updates nur für LTSR zu erhalten.
    - Wählen Sie im Dropdownmenü **Auto-Update-DeferUpdate-Count** einen Wert zwischen **-1** und **30**.
        - **-1:** Gibt an, dass Sie Benachrichtigungen beliebig oft verschieben können (Standardwert = -1).
        - **0:** Gibt an, dass die Option **Später erinnern** nicht angezeigt wird.
        - Beliebige andere Zahl: Gibt an, wie oft die Option **Später erinnern** angezeigt wird. Beispiel: Bei einem Wert von 10 wird die Option **Später erinnern** zehnmal angezeigt.
8. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.

Konfiguration über die Befehlszeilenschnittstelle

Während der Installation von Citrix Receiver für Windows

Konfigurieren der Einstellungen für automatische Updates als Administrator über die Befehlszeileneinstellungen während der Installation von Citrix Receiver:

- **/AutoUpdateCheck =** auto/manual/disabled
- **/AutoUpdateStream=** LTSR/Current. Hier bezieht sich "LTSR" auf Long Term Service Release und "Current" auf das aktuelle Release.
- **/DeferUpdateCount=** beliebiger Wert zwischen-1 und 30
- **/AURolloutPriority=** auto/fast/medium/slow

Beispiel: *CitrixReceiver.exe /AutoUpdateCheck=auto /AutoUpdateStream= Current /DeferUpdateCount=-1 / AURolloutPriority= fast*

- Konfigurieren der Einstellungen für automatische Updates als Benutzer über die Befehlszeileneinstellungen während der Installation von Citrix Receiver:
  - **/AutoUpdateCheck=**auto/manua**l**

Beispiel: *CitrixReceiver.exe / AutoUpdateCheck=auto*

Werden die Einstellungen für automatische Updates mit der administrativen Gruppenrichtlinienobjektvorlage bearbeitet, werden dadurch die Einstellungen überschrieben, die bei der Installation von Citrix Receiver für Windows für alle Benutzer angewendet wurden.

Nach der Installation von Citrix Receiver für Windows

Automatische Updates können nach der Installation von Citrix Receiver für Windows konfiguriert werden.

Verwenden der Befehlszeile

Öffnen Sie eine Windows-Eingabeaufforderung und ändern Sie das Verzeichnis zum Speicherort von **CitrixReceiverUpdater.exe**. Normalerweise befindet sich CitrixReceiverUpdater.exe unter *CitrixReceiverInstallLocation*\Citrix\Ica Client\Receiver.

Sie können auch die Richtlinie für automatische Updates über die Befehlszeile mit dieser Binärdatei festlegen.

Beispiel: Administratoren können alle vier Optionen verwenden:

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

Konfiguration über die grafische Benutzeroberfläche

Ein Benutzer kann die Einstellung für automatische Updates im Dialogfeld **Erweiterte Einstellungen** überschreiben. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet.

1. Klicken Sie im Infobereich mit der rechten Maustaste auf Citrix Receiver für Windows.
2. Wählen Sie **Erweiterte Einstellungen** und klicken Sie auf **Automatische Updates**.

   Das Dialogfeld für automatische Updates wird angezeigt.
3. Wählen Sie eine der folgenden Optionen:
   - Ja, benachrichtigen Sie mich
   - Nein, nicht benachrichtigen
   - Vom Administrator festgelegte Einstellungen verwenden
4. Klicken Sie auf **Speichern**.

Konfigurieren von automatischen Updates mit StoreFront

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

   Beispiel: <account id=… name=”Store”>

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

   <properties>

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

   <account>

   <clear />

   <account id=”d1197d2c-ac82-4f13-9346-2ee14d4b0202” name=”F84Store”

   description=”” published=”true” updaterType=”Citrix” remoteAccessType=”None”>

   <annotatedServices>

   <clear />

   <annotatedServiceRecord serviceRef=”1__Citrix_F84Store”>


```
    <metadata>
     <plugins>
      <clear />
     </plugins>
     <trustSettings>
      <clear />
     </trustSettings>
     <properties>
      <property name=”Auto-Update-Check” value=”auto” />
      <property name=”Auto-Update-DeferUpdate-Count” value=”1” />
            <property name=”Auto-Update-LTSR-Only” value=”FALSE” />
      <property name=”Auto-Update-Rollout-Priority” value=”fast” />
          </properties>
    </metadata>
   </annotatedServiceRecord>
  </annotatedServices>
  <metadata>
   <plugins>
    <clear />
   </plugins>
   <trustSettings>
    <clear />
   </trustSettings>
   <properties>
    <clear />
   </properties>
  </metadata>
 </account>
```


auto-update-Check

Dies gibt an, dass Citrix Receiver für Windows erkennt, wenn ein Update verfügbar ist.

Gültige Werte:

- Auto – Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).
- Manual – Sie werden nicht benachrichtigt, wenn Updates zur Verfügung stehen. Suchen Sie manuell nach Updates.
- Disabled: Das Feature für automatische Updates ist deaktiviert.

auto-update-LTSR-Only

Dies gibt an, dass Citrix Receiver für Windows nur Updates für LTSR akzeptieren muss.

Gültige Werte:

- True: Die automatische Updatefunktion sucht nur LTSR-Updates von Citrix Receiver für Windows.
- False: Die automatische Updatefunktion sucht auch LTSR-fremde Updates von Citrix Receiver für Windows.

auto-update-DeferUpdate-Count

Dies gibt an, wie oft Benachrichtigungen zurückgestellt werden können. Die Option Später erinnern wird gemäß der hier festgelegten Zahl angezeigt.

Gültige Werte:

- -1: Gibt an, dass Sie Benachrichtigungen beliebig oft verschieben können (Standardwert = -1).
- 0: Gibt an, dass die Option “Später erinnern” nicht angezeigt wird.
- Beliebige andere Zahl: Gibt an, wie oft die Option “Später erinnern” angezeigt wird. Beispiel: Bei einem Wert von 10 wird die Option Später erinnern zehnmal angezeigt.

auto-update-Rollout-Priority:

Dies gibt den Zeitrahmen für die Rolloutphase an.

Gültige Werte:

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

Einschränkungen:

1. Das System muss Zugriff auf das Internet haben.

2. Receiver für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
3. Wenn Sie einen Outbound-Proxy mit SSL-Interception konfiguriert haben, müssen Sie eine Ausnahme zum Receiver-Signaturdienst für automatische Updates (https://citrixupdates.cloud.com) und zum Downloadspeicherort (https://downloadplugins.citrix.com) hinzufügen.
4. Standardmäßig sind automatische Updates auf dem VDA deaktiviert. Dies umfasst RDS-Server mit mehreren Benutzern, VDI- und Remote-PC-Maschinen.
5. Automatische Updates sind auf Maschinen deaktiviert, auf denen Desktop Lock installiert ist.

Konfigurieren der bidirektionalen Inhaltsumleitung

January 7, 2019

Sie können die bidirektionale Inhaltsumleitung mit Folgendem aktivieren:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Registrierung

> **Hinweis**
>
> - Die bidirektionale Inhaltsumleitung funktioniert nicht in einer Sitzung, in der **Lokaler App-Zugriff** aktiviert ist.
> - Die bidirektionale Inhaltsumleitung muss auf dem Server und dem Client aktiviert sein. Wenn sie auf dem Server oder auf dem Client deaktiviert ist, ist die Funktion deaktiviert.

Aktivieren der bidirektionalen Inhaltsumleitung mit der administrativen Gruppenrichtlinienobjektvorlage

Verwenden Sie die Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage für die Erstinstallation von Citrix Receiver für Windows.

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
   - Wenn Sie die Richtlinie auf einem einzigen Computer anwenden, starten Sie sie vom Startmenü.
   - Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie sie mit der Gruppenrichtlinien-Verwaltungskonsole.
2. Navigieren Sie unter dem Knoten "Benutzerkonfiguration" zu **Administrative Vorlagen** > **Klassische administrative Vorlage (ADM)** > **Citrix Komponenten** > **Citrix Receiver** > **Benutzererfahrung**.

3. Wählen Sie die Richtlinie **Bidirektionale Inhaltsumleitung**.
4. Bearbeiten Sie die Einstellungen.

   Hinweis:
   Wenn Sie URLs einschließen, können Sie eine URL oder eine durch Strichpunkt getrennte Liste der URLs angeben. Sie können ein Sternchen (*) als Platzhalter verwenden.
5. Klicken Sie auf **Anwenden** und auf **OK**.
6. Führen Sie an einer Befehlszeile den Befehl gpupdate /force aus.

Aktivieren der bidirektionalen Inhaltsumleitung mit der Registrierung

Zum Aktivieren der bidirektionalen Inhaltsumleitung führen Sie den Befehl **redirector.exe/RegIE** vom Installationsordner für Citrix Receiver für Windows aus (C:\Programme (x86)\Citrix\ICA Client).

Einschränkungen:

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

Wichtig:

- Stellen Sie sicher, dass Umleitungsregeln keine Schleifenkonfiguration ergeben. Eine Schleifenkonfiguration entsteht zum Beispiel, wenn VDA-Regeln so festgelegt sind, dass eine URL wie `https://www.my_company.com` an den Client umgeleitet wird und dieselbe URL auch für die Umleitung an den VDA konfiguriert ist.
- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder die mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Wenn zwei Anwendungen mit demselben Anzeigenamen mehrere StoreFront-Konten verwenden, wird der Anzeigename im primären StoreFront-Konto für den Start der Anwendung oder einer Desktopsitzung verwendet.
- Ein neues Browserfenster wird nur geöffnet, wenn die URL zum Client umgeleitet wird. Wenn die URL zum VDA umgeleitet wird, und der Browser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet.
- Eingebettete Links in Dateien wie Dokumente, E-Mails, PDFs werden unterstützt.

Konfigurieren von Bloomberg-Tastaturen

January 7, 2019

Citrix Receiver für Windows unterstützt die Verwendung einer Bloomberg-Tastatur in einer XenApp- und XenDesktop-Sitzung. Die erforderlichen Komponenten werden mit dem Plug-In installiert. Sie können das Feature für Bloomberg-Tastaturen während der Installation von Citrix Receiver für Windows oder über die Registrierung aktivieren.

Mehrere Sitzungen zu Bloomberg-Tastaturen sind nicht empfehlenswert. Die Tastatur funktioniert nur in Umgebungen mit einer Sitzung richtig.

Aktivieren oder Deaktivieren der Unterstützung für Bloomberg-Tastaturen:

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

1. Gehen Sie zu folgendem Schlüssel in der Registrierung:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Führen Sie einen der folgenden Schritte aus:

   - Zum Aktivieren dieses Features müssen Sie den Eintrag mit Typ DWORD und dem Namen EnableBloombergHID auf den Wert 1 setzen.
   - Zum Deaktivieren dieses Features setzen Sie den Wert auf 0.

Weitere Informationen zum Konfigurieren von Bloomberg-Tastaturen finden Sie im Knowledge Center-Artikel CTX122615.

Verhindern des Abblendens des Desktop Viewer-Fensters

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

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

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

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

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

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

   Die Verwendung der Registrierungsschlüssel ist optional, da XenDesktop-Administratoren und nicht Plug-in-Administratoren oder Benutzern normalerweise die Richtlinieneinstellungen mit der Gruppenrichtlinie steuern. Vor der Verwendung dieser Registrierungsschlüssel sollten Sie beim XenDesktop-Administrator nachfragen, ob eine Richtlinie für dieses Feature festgelegt wurde.

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

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

   a) HKEY_CURRENT_USER\Software\Policies\Citrix\…
   b) HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
   c) HKEY_CURRENT_USER\Software\Citrix\…
   d) HKEY_LOCAL_MACHINE\Software\Citrix\…

Konfigurieren der Umleitung von USB-Verbundgeräten

November 21, 2018

Konfigurieren der Umleitung von USB-Verbundgeräten mit der administrativen Gruppenrichtlinienobjektvorlage

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie **gpedit.msc** ausführen.

a) Wenn Sie die Richtlinie auf einen einzigen Computer anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
b) Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver mit der Gruppenrichtlinien-Verwaltungskonsole.

2. Navigieren Sie unter dem Knoten "Benutzerkonfiguration" zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Receiver** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices**.
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Übernehmen**.
6. Klicken Sie auf **OK**, um die Richtlinie zu speichern.

Zulassen oder Ablehnen einer Schnittstelle mit der administrativen Gruppenrichtlinienobjektvorlage

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.

   a) Wenn Sie die Richtlinie auf einen einzigen Computer anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
   b) Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver mit der Gruppenrichtlinien-Verwaltungskonsole.

2. Navigieren Sie unter dem Knoten "Benutzerkonfiguration" zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Receiver** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-Geräteregeln**.
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-Geräteregeln** das USB-Gerät hinzu, das zugelassen oder abgelehnt werden soll.
   Beispiel: *ALLOW: vid=047F pid= C039 split=01 intf=00,03 //Schnittstellen 00 und 03 sind zugelassen, andere werden beschränkt.*
6. Klicken Sie auf **Anwenden** und auf **OK**.

   In einer Desktopsitzung werden per Splitting aufgeteilte USB-Geräte im Desktop Viewer unter **Geräte** angezeigt. Darüber hinaus werden aufgeteilte USB-Geräte unter **Einstellungen** > **Geräte** angezeigt.

In einer Anwendungssitzung werden per Splitting aufgeteilte USB-Geräte im **Connection Center** angezeigt.

In der folgenden Tabelle werden Verhaltensszenarien erläutert, wenn eine USB-Schnittstelle zugelassen oder abgelehnt wird.

Zulassen einer Schnittstelle:

Aufteilen	Schnittstelle	Aktion
TRUE	Gültige Zahl 0 -n	Angegebene Schnittstelle zulassen
TRUE	Ungültige Zahl	Alle Schnittstellen zulassen
FALSE	Beliebiger Wert	Generisches USB von übergeordnetem Gerät zulassen
Nicht angegeben	Beliebiger Wert	Generisches USB von übergeordnetem Gerät zulassen

Beispielsweise gibt SplitDevices - *true* an, dass alle Geräte durch Splitting aufgeteilt sind.

Ablehnen einer Schnittstelle:

Split	Schnittstelle	Aktion
TRUE	Gültige Zahl 0 - n	Angegebene Schnittstelle ablehnen
TRUE	Ungültige Zahl	Alle Schnittstellen ablehnen
FALSE	Beliebiger Wert	Generisches USB von übergeordnetem Gerät ablehnen
Nicht angegeben	Beliebiger Wert	Generisches USB von übergeordnetem Gerät ablehnen

Beispielsweise gibt SplitDevices - *false* an, dass Geräte nicht mit der angegebenen Schnittstellenzahl aufgeteilt sind.

Beispiel: Mein_<*plantronics*>-Headset

Schnittstellenzahl:

- Schnittstellenklasse für Audio - 0
- Schnittstellenklasse für HID - 3

Beispielregeln für Mein_<*plantronics*>-Headset:

- ALLOW: vid=047F pid= C039 split=01 intf=00,03 // Schnittstellen 00 und 03 sind zugelassen, andere werden beschränkt
- DENY: Vid = 047F pid = C039 split = 01 intf = 00,03 // Schnittstellen 00 und 03 ablehnen

Einschränkungen:

Citrix empfiehlt, Schnittstellen für eine Webcam nicht per Splitting aufzuteilen. Als Workaround können Sie das Gerät als einzelnes Gerät über die generische USB-Umleitung weiterleiten. Verwenden Sie zur Leistungsverbesserung den optimierten virtuellen Kanal.

Konfigurieren der USB-Unterstützung

March 26, 2019

Mit der USB-Unterstützung können Sie mit zahlreichen USB-Geräten interagieren, wenn sie mit einem virtuellen Desktop verbunden sind. Sie können USB-Geräte an die Geräte anschließen und mit Remoting der Geräte stehen sie auf dem virtuellen Desktop zur Verfügung. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets. Benutzer von Desktop Viewer können mit einer Einstellung auf der Symbolleiste steuern, ob USB-Geräte auf dem virtuellen Desktop verfügbar sind.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz und hoher Geschwindigkeit unterstützt. Dadurch können diese Geräte mit Programmpaketen wie Microsoft Office Communicator und Skype verwendet werden.

Die folgenden Gerätetypen werden direkt in einer XenApp- bzw. XenDesktop-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

Hinweis: USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unter

Konfigurieren von Bloomberg-Tastaturen. Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie im Knowledge Center-Artikel CTX122615.

Standardmäßig werden bestimmte Arten von USB-Geräten nicht für das Remoting über XenDesktop und XenApp unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre bei einem solchen Gerät nicht angebracht. Die folgenden Typen von USB-Geräten können standardmäßig nicht in einer XenDesktop-Sitzung verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs
- USB-Grafikadapter

Remoting ist möglich für USB-Geräte, die mit einem Hub verbunden sind, jedoch nicht für den Hub selbst.

Die folgenden USB-Gerätetypen können standardmäßig nicht in einer XenApp-Sitzung verwendet werden:

- Bluetooth-Dongle
- Integrierte Netzwerkkarten
- USB-Hubs
- USB-Grafikadapter
- Audiogeräte
- Massenspeichergeräte

Anweisungen zum automatischen Umleiten spezifischer USB-Geräte finden Sie im Knowledge Center-Artikel CTX123015.

Funktionsweise der USB-Unterstützung

Wenn ein Benutzer ein USB-Gerät anschließt, wird es mit der USB-Richtlinie überprüft, und wenn das Gerät zulässig ist, erfolgt ein Remoting zum virtuellen Desktop. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Wenn ein Benutzer ein USB-Gerät anschließt, wird eine Meldung über den Anschluss eines neuen Geräts angezeigt. Der Benutzer wählt die Geräte, für die ein Remoting zum virtuellen Desktop erfolgen soll, bei jeder Verbindung in der Liste aus. Der Benutzer kann die USB-Unterstützung auch so konfigurieren, dass für alle USB-Geräte, die vor oder während einer Sitzung angeschlossen werden, ein Remoting zum virtuellen Desktop erfolgt, der den Fokus hat.

Massenspeichergeräte

Ausschließlich für Massenspeichergeräte ist nicht nur die USB-Unterstützung sondern auch der Remotezugriff über die Clientlaufwerkzuordnung verfügbar, die Sie in der Citrix Receiver-Richtlinie "Remoting von Clientgeräten > Clientlaufwerkzuordnung" konfigurieren. Wenn diese Richtlinie angewendet wird, werden die Laufwerke auf dem Benutzergerät automatisch Laufwerkbuchstaben auf dem virtuellen Desktop zugeordnet, wenn sich Benutzer anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

Feature	Clientlaufwerkzuordnung	USB-Unterstützung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein
Sicheres Entfernen des Geräts in einer Sitzung	Nein	Ja, wenn der Benutzer im Infobereich auf Hardware sicher entfernen klickt.

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor dem Sitzungsstart angeschlossen wird, wird es zuerst mit der Clientlaufwerkzuordnung umgeleitet, bevor eine Umleitung mit der USB-Unterstützung erwägt wird. Wenn das Gerät nach dem Sitzungsstart angeschlossen wird, wird die Umleitung mit der USB-Unterstützung vor der Clientlaufwerkzuordnung erwogen.

In der Standardeinstellung zulässige USB-Geräteklassen

Verschiedene Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln in der Standardeinstellung zugelassen.

Auch wenn sie in dieser Liste sind, stehen manche Klassen nur nach zusätzlicher Konfiguration für das Remoting in XenDesktop- bzw. XenApp-Sitzungen zur Verfügung. Es wird im Folgenden darauf hingewiesen.

- **Audio (Geräteklasse 01)**: Umfasst Audioeingabegeräte (Mikrofone), Audioausgabegeräte und MIDI-Controller. Moderne Audiogeräte verwenden im Allgemeinen isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Audio (Geräteklasse01) ist für XenApp nicht relevant, da Geräte dieser Klasse für das Remoting in XenApp mit USB-Unterstützung nicht verfügbar sind.

Hinweis: Für manche Spezialgeräte (z. B. VOIP-Telefone) ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123015.

- **PID (Physical Interface Devices) (Geräteklasse 05)**: Diese Geräte ähneln HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Exoskelette.
- **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 und eine Kamera kann möglicherweise über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

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

- **Drucker (Geräteklasse 07)**: Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. 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.

> **Hinweis:** Für diese Klasse von Geräten (vor allem Drucker mit Scanfunktion) ist eine zusätzliche Konfiguration erforderlich. Anweisungen hierzu finden Sie im Knowledge Center-Artikel CTX123015.

- **Massenspeicher (Geräteklasse 08)**: Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke sowie über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, der auch eine Massenspeicherschnittstelle darstellt, u. a. Media Player, digitale Kameras und Mobiltelefone. Massenspeicher (Geräteklasse 08) ist für XenApp nicht relevant, da Geräte dieser Klasse für das Remoting in XenApp mit USB-Unterstützung nicht verfügbar sind. Bekannte Unterklassen:
  - 01: Begrenzte Flashlaufwerke
  - 02: Normalerweise CD- bzw. DVD-Geräte (ATAPI/MMC-2)
  - 03: Normalerweise Bandgeräte (QIC-157)
  - 04: Normalerweise Diskettenlaufwerke (UFI)
  - 05: Normalerweise Diskettenlaufwerke (SFF-8070i)
  - 06: Die meisten Massenspeichergeräte verwenden diese SCSI-Variante

  Der Zugriff auf Massenspeichergeräte erfolgt oft über die Clientlaufwerkzuordnung und USB-Unterstützung wird daher nicht benötigt.

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.

- **Content Security (Geräteklasse 0d)**: Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.
- **Video (Geräteklasse 0e)**: Die Videoklasse umfasst Geräte, mit denen Videos und mit Video zusammenhängendes Material manipuliert werden, u. a. Webcams, digitale Camcorder, analoge Videokonverter, einige Fernsehtuner und einige digitale Kameras, die Videostreaming unterstützen.

> **Hinweis:** Die meisten Videostreaminggeräte verwenden isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Für manche Videogeräte (z. B. Webcams mit Bewegungserkennung) ist eine zusätzliche Konfiguration erforderlich. Anweisungen hierzu finden Sie im Knowledge Center-Artikel CTX123015.

- **Personal Healthcare (Geräteklasse 0f)**: Hierzu gehören Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.
- **Anwendungs- und herstellerspezifisch (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 USB-Geräteklassen werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a): Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein solches Gerät möglicherweise selbst die Verbindung zum virtuellen Desktop bereitstellt.
- HID (Human Interface Devices, Geräteklasse 03): Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktabletts, Sensoren, Game Controller, Tasten und Steuerfunktionen.

  Die Unterklasse 01 wird “Boot Interface”-Klasse genannt und für Tastaturen und Maus verwendet.

  USB-Tastaturen (Klasse 03, Unterklasse 01, Protokoll 1) oder USB-Mäuse (Klasse 03, Unterklasse 01, Protokoll 2) werden von der USB-Standardrichtlinie nicht zugelassen. Begründung: Die meisten Tastaturen und Mäuse werden ohne USB-Unterstützung ausreichend gehandhabt und werden sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.

- USB-Hubs (Geräteklasse 09): Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.
- Smartcard (Geräteklasse 0b): Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.

  Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.
- Kabellose Controller (Geräteklasse e0): Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang oder die Verbindung mit Peripheriegeräten wie Bluetooth-Tastaturen oder -Mäuse.

  Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit USB-Unterstützung gegeben werden sollte.
- **Verschiedene Netzwerkgeräte (Geräteklasse ef, Unterklasse 04)**: Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang. Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit USB-Unterstützung gegeben werden sollte.

Aktualisieren der für Remoting verfügbaren USB-Geräteliste

Sie können die USB-Geräte aktualisieren, die für das Remoting zu Desktops verfügbar sind, indem Sie die Vorlagendatei für Citrix Receiver für Windows bearbeiten. Sie können so Citrix Receiver für Windows über eine Gruppenrichtlinie ändern. Die Datei ist in folgendem Installationsordner:

<Stammlaufwerk>:\Programme\Citrix\ICA Client\Configuration\<Sprache>

Sie können auch die Registrierung auf jedem Benutzergerät ändern und den folgenden Registrierungsschlüssel hinzufügen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name=”DeviceRules” Wert=

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

Die Standardregeln für das Produkt sind an folgendem Speicherort gespeichert:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name=“DeviceRules” Value=

Ändern Sie nicht die Produktstandardregeln.

Informationen über die Regeln und deren Syntax finden Sie im Knowledge Center-Artikel CTX119722.

Konfigurieren von USB-Audio pro Benutzer

Citrix empfiehlt, Regeln für das Netzwerkrouting, für die Proxyserver und für die vertrauenswürdige Serverkonfiguration, für das Benutzerrouting, für die Remoteclientgeräte und die Benutzererfahrung mit der Gruppenrichtlinienobjektvorlage receiver.admx/receiver.adml zu konfigurieren.
Sie können die Vorlagendatei receiver.admx für Domänenrichtlinien und lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Dies ist besonders nützlich, wenn Sie Citrix Receiver für Windows-Einstellungen auf mehrere verschiedene Benutzergeräte im Unternehmen anwenden möchten. Wenn Sie nur ein einziges Benutzergerät bearbeiten möchten, importieren Sie die Vorlagendatei mit dem lokalen Gruppenrichtlinien-Editor auf dem Gerät.

Hinweis: Dieses Feature ist nur für XenApp-Server verfügbar.

Konfigurieren von USB-Audiogeräten pro Benutzer

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vomStartmenü ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.

   Hinweis: Wenn Sie die Receiver-Vorlage bereits dem Gruppenrichtlinien-Editor hinzugefügt haben, können Sie die Schritte 2 bis 5 überspringen.

2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner Administrative Vorlagen aus.
3. Klicken Sie im Menü **Aktion** auf **Vorlagen hinzufügen/entfernen**.
4. Klicken Sie auf **Hinzufügen**, navigieren Sie zum Konfigurationsordner für Receiver (für 32-Bit-Maschinen üblicherweise C:\Programme\Citrix\ICA Client\Configuration, für 64-Bit-Maschinen üblicherweise C:\Programme (x86)\Citrix\ICA Client\Configuration), und wählen Sie receiver.admx aus.
5. Klicken Sie auf **Öffnen**, um die Vorlage hinzuzufügen, und klicken Sie dann auf **Schließen**, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie unter dem Knoten “Computerkonfiguration” zu **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzererfahrung** und wählen Sie **Audio über generische USB-Umleitung**.
7. Bearbeiten Sie die Einstellungen.

8. Klicken Sie auf **Anwenden** und auf **OK**.
9. Öffnen Sie eine Eingabeaufforderung im Administratormodus.
10. Führen Sie den Befehl unten aus
    gpupdate /force

Hinweis: Bei Änderungen an der Richtlinie muss der XenApp-Server neu gestartet werden, damit die Änderungen wirksam werden.

Konfigurieren von StoreFront

March 26, 2019

Citrix StoreFront authentifiziert Benutzer an XenDesktop, XenApp und VDI-in-a-Box. Verfügbare Desktops und Anwendungen werden in Stores aufgelistet und zusammengefasst, auf die Benutzer über Citrix Receiver für Windows zugreifen.

Zusätzlich zu der Konfiguration, die in diesem Abschnitt zusammengefasst ist, müssen Sie außerdem NetScaler Gateway konfigurieren, sodass Benutzer sich von außerhalb mit dem internen Netzwerk verbinden können (z. B. Benutzer, die über das Internet oder von Remotestandorten eine Verbindung herstellen).

> **Tipp**
>
> Citrix Receiver für Windows zeigt gelegentlich ältere StoreFront UI statt der aktualisierten StoreFront UI nachdem Sie die Option zum Anzeigen aller Stores wählen.

Konfigurieren von StoreFront

Installieren und konfigurieren Sie StoreFront, wie in der StoreFront-Dokumentation beschrieben. Citrix Receiver für Windows benötigt eine HTTPS-Verbindung. Wenn der StoreFront-Server für HTTP konfiguriert ist, muss ein Registrierungsschlüssel auf dem Benutzergerät eingestellt werden. Eine Anleitung finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern in der Beschreibung der Eigenschaft ALLOWADDSTORE.

> **Hinweis:**
>
> Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für Citrix Receiver für Windows erstellen.

Wiederverbindung über Workspace Control verwalten

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

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

Erstellen Sie WSCReconnectModeUser und ändern Sie den vorhandenen Registrierungsschlüssel WSCReconnectMode im Masterdesktopimage oder auf dem XenApp-Server. Der veröffentlichte Desktop kann das Verhalten von Citrix Receiver für Windows ändern.

WSCReconnectMode-Schlüsseleinstellungen für Citrix Receiver für Windows:

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

Deaktivieren von Workspace Control für Citrix Receiver für Windows

Erstellen Sie den folgenden Schlüssel, um Workspace Control für Citrix Receiver für Windows zu deaktivieren:

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

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectModeUser**

Typ: REG_SZ

Wert: 0

Ändern Sie den folgenden Schlüssel vom Standardwert 3 auf 0

HKEY_CURRENT\USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 Bit)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectMode**

Typ: REG_SZ

Wert: 0

Hinweis: Wenn Sie keinen neuen Schlüssel erstellen möchten, können Sie den REG_SZ-Wert WSCReconnectAll auf “false” festlegen.

Ändern des Timeouts der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird. Zum Ändern des Timeoutzeitraums erstellen Sie einen REG_DWORD-Wert SI INACTIVE MS in HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine. Sie können den REG_DWORD-Wert auf 4 festlegen, wenn die Statusanzeige eher ausgeblendet werden soll.

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

Anpassen des Speicherorts für Anwendungsverknüpfungen über die Befehlszeilenschnittstelle (CLI)

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

Als Citrix Receiver-Administrator können Sie Befehlszeilen-Installationsflags, Gruppenrichtlinienobjekte, Kontodienste oder Registrierungseinstellungen zum Deaktivieren der normalen Self-Service-Schnittstelle von Citrix Receiver verwenden und diese mit einem vorkonfigurierten Startmenü ersetzen. Das Flag heißt SelfServiceMode und ist standardmäßig auf “true” festgelegt. Wenn der Administrator das SelfServiceMode-Flag auf “false” festlegt, hat der Benutzer keinen Zugriff mehr auf die Self-Service-Benutzeroberfläche von Citrix Receiver. Der Zugriff auf abonnierte Apps ist stattdessen über

das Startmenü und über Desktopverknüpfungen möglich. Dies wird hier als Nur-Verknüpfungsmodus bezeichnet.

Benutzer und Administratoren können eine Reihe von Registrierungseinstellungen zur Einrichtung der Verknüpfungen verwenden.

Arbeiten mit Verknüpfungen

- Benutzer können Apps nicht entfernen. Alle Apps sind verbindlich, wenn das Flag SelfServiceMode auf “false” festgelegt ist (= Nur-Verknüpfungsmodus). Wenn ein Benutzer ein Verknüpfungssymbol vom Desktop entfernt, wird das Symbol wieder angezeigt, wenn er über das Citrix Receiver für Windows-Infobereichsymbol “Aktualisieren” auswählt.
- Benutzer können nur einen Store konfigurieren. Die Optionen Konto und Einstellungen sind nicht verfügbar. Auf diese Weise wird verhindert, dass Benutzer zusätzliche Stores konfigurieren. Der Administrator kann einem Benutzer besondere Privilegien zum Hinzufügen mehrerer Konten erteilen, indem er die Gruppenrichtlinienobjektvorlage verwendet oder den Registrierungsschlüssel HideEditStoresDialog auf dem Clientcomputer manuell hinzufügt. Wenn der Administrator einem Benutzer dieses Privileg erteilt, steht diesem die Option “Einstellungen” über das Infobereichsymbol zur Verfügung, mit der er Konten hinzufügen und entfernen kann.
- Benutzer können Apps nicht über die Windows-Systemsteuerung entfernen.
- Sie können Desktopverknüpfungen über eine anpassbare Registrierungseinstellung hinzufügen. Desktopverknüpfungen werden nicht standardmäßig hinzugefügt. Nach jeglichen Änderungen an Registrierungseinstellungen muss Citrix Receiver für Windows neu gestartet werden.
- Verknüpfungen werden im Startmenü standardmäßig mit einem Kategoriepfad erstellt: UseCategoryAsStartMenuPath.

Hinweis: In Windows 8/8.1 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden einzeln oder im Stammordner angezeigt, jedoch nicht in mit XenApp definierten Unterordnern für Kategorien.

- Sie können während der Installation das Flag [DESKTOPDIR=”Dir_name”] hinzufügen, um alle Verknüpfungen in einem Ordner zusammenzufassen. CategoryPath wird für Desktopverknüpfungen unterstützt.
- Die automatische Neuinstallation geänderter Apps ist ein Feature, das über den Registrierungsschlüssel “AutoReInstallModifiedApps” aktiviert werden kann. Wenn AutoReInstallModifiedApps aktiviert ist, werden alle auf dem Server durchgeführten Änderungen an Attributen veröffentlichter Anwendungen und Desktops auf dem Clientcomputer übernommen. Wenn AutoReInstallModifiedApps deaktiviert ist, werden Attribute von Anwendungen und Desktops nicht aktualisiert und Verknüpfungen werden nach dem Löschen bei einer Aktualisierung

auf dem Client nicht wieder aufgeführt. Standardmäßig ist AutoReInstallModifiedApps aktiviert. Weitere Informationen finden Sie unter “Konfigurieren von Speicherorten für App-Verknüpfungen mit Registrierungsschlüsseln”.

Anpassen des Speicherorts für Anwendungsverknüpfungen über die Registrierung

> **Hinweis**
>
> Standardmäßig verwenden Registrierungsschlüssel ein Zeichenfolgeformat.

Sie können Einstellungen von Registrierungsschlüsseln zum Anpassen von Verknüpfungen verwenden. Sie können Registrierungsschlüssel an den nachfolgend aufgeführten Orten festlegen. Diese werden in der Reihenfolge, in der sie aufgeführt sind, angewendet.

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

> **Hinweis:**
>
> Sie müssen Änderungen an Registrierungsschlüsseln vor dem Konfigurieren eines Stores vornehmen. Möchten Sie oder ein Benutzer die Registrierungsschlüssel ändern, müssen er oder Sie Receiver zurücksetzen, die Registrierungsschlüssel konfigurieren und dann den Store neu konfigurieren.

Registrierungsschlüssel für 32-Bit-Maschinen

Name	Standardwert	Orte in der Reihenfolge der Priorität
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

Name	Standardwert	Orte in der Reihenfolge der Priorität
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
StartMenuDir	"" (leer)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	"" (leer)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	True bei SelfServiceMode, False bei NonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle;HKL

Name	Standardwert	Orte in der Reihenfolge der Priorität
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registrierung während der Installation nicht erstellt.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE \Citrix\Dazzle

Registrierungsschlüssel für 64-Bit-Maschinen

Name	**Standardwert**	**Orte in der Reihenfolge der Priorität**
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties

Name	Standardwert	Orte in der Reihenfolge der Priorität
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	”” (leer)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
DesktopDir	"" (leer)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
HideEditStoresDialog	True bei SelfServiceMode, False bei NonSelfServiceMode	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz

Name	Standardwert	Orte in der Reihenfolge der Priorität
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
WSCReconnectModeUser	Registrierung während der Installation nicht erstellt.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID+\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz

Konfigurieren der Anwendungsanzeige über die grafische Benutzeroberfläche

Hinweis: Verknüpfungen können nur für die abonnierten Anwendungen und Desktops festgelegt werden.

1. Melden Sie sich an Citrix Receiver für Windows an.
2. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol für Citrix Receiver für Windows und dann auf **Erweiterte Einstellungen**.
   Das Dialogfeld "Erweiterte Einstellungen" wird angezeigt.
3. Klicken Sie auf **Einstellungsoption**.

   Hinweis: Standardmäßig ist die Option "Anwendungen im Startmenü anzeigen" ausgewählt.
4. Geben Sie den Namen des Ordners an. Alle abonnierten Apps werden dann in den angegebenen Ordner im Startmenü verschoben. Anwendungen können einem neuen oder vorhandenen Ordner im Startmenü hinzugefügt werden. Beim Aktivieren dieses Features werden vorhandene und neu hinzugefügte Anwendungen dem angegebenen Ordner hinzugefügt.
5. Aktivieren Sie das Kontrollkästchen **Anwendungen auf dem Desktop anzeigen** im Bereich **Desktopoptionen**.
6. Geben Sie den Namen des Ordners an. Alle abonnierten Apps werden dann in den angegebenen Ordner auf dem lokalen Desktop verschoben.
7. Aktivieren Sie unter **Kategorieoptionen** das Kontrollkästchen **Unterschiedliche Pfade für Startmenü und Desktop aktivieren**. Die Verknüpfungen und Kategorieordner für Anwendungen werden dann erstellt, wie es in den Anwendungseigenschaften definiert wurde. Beispiel: IT-Apps, Finanz-Apps

Hinweis: Standardmäßig ist die Option “Kategorie als Startmenüpfad” ausgewählt.

a) Wählen Sie **Kategorie als Startmenüpfad**, damit die abonnierten Apps und der Kategorieordner wie in den Anwendungseigenschaften definiert im Windows-Startmenü angezeigt werden.
b) Wählen Sie **Kategorie als Desktoppfad**, damit die abonnierten Apps und der Kategorieordner wie im Anwendungseigenschaftenserver definiert auf dem lokalen Desktop angezeigt werden.

8. Klicken Sie auf **OK**.

Konfigurieren von Wiederverbindungsoptionen über die grafische Benutzeroberfläche

Nach der Anmeldung beim Server können Benutzer eine Verbindung zu all ihren Desktops oder Anwendungen jederzeit wiederherstellen. Standardmäßig werden mit den Wiederverbindungsoptionen sowohl getrennte Desktops oder Anwendungen geöffnet als auch alle aktiven Anwendungen, die derzeit auf einem anderen Clientgerät ausgeführt werden. Sie können die Wiederverbindungsoptionen so konfigurieren, dass nur die Desktops oder Anwendungen wiederverbunden werden, deren Verbindung der Benutzer zuvor getrennt hat.

1. Melden Sie sich an Citrix Receiver für Windows an.
2. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol für Citrix Receiver für Windows und dann auf **Erweiterte Einstellungen**. Das Dialogfeld “Erweiterte Einstellungen” wird angezeigt.
3. Klicken Sie auf **Einstellungsoption**.
4. Klicken Sie auf **Wiederverbindungsoptionen**.
5. Wählen Sie **Für Workspace Control Support aktivieren**, damit Benutzer jederzeit die Verbindung zu ihren Desktops und Anwendungen wiederherstellen können.

   a) Wählen Sie **Mit allen aktiven und getrennte Sitzungen wiederverbinden**, damit Benutzer die Verbindung mit den aktiven und getrennten Sitzungen wiederherstellen können.

   b) Wählen Sie **Nur getrennte Sitzungen wiederverbinden**, damit Benutzer die Verbindung zu getrennten Sitzungen wiederherstellen können.

   Hinweis: Unterstützter Wiederverbindungsmodus übernimmt den im Gruppenrichtlinienobjekt festgelegten Wert. Benutzer können diese Option ändern: **Administrative Vorlagen > Citrix Komponenten > Citrix Receiver > Self-Service > Steuern, wann Receiver versucht, Verbindungen zu vorhandenen Sitzungen wiederherzustellen**.

   Informationen zum Ändern dieser Option in der Registrierung finden Sie im Knowledge Center-Artikel CTX136339.

6. Klicken Sie auf **OK**.

Ausblenden der Einstellungsoption über die Befehlszeilenschnittstelle

Option	/DisableSetting
Beschreibung	Unterdrückt die Anzeige der Einstellungsoption im Dialogfeld “Erweiterte Einstellungen”.
Beispiel für Verwendung	CitrixReceiver.exe /DisableSetting=3

Anzeigen von “Anwendungsanzeige” und “Wiederverbindungsoptionen” in der Einstellungsoption:	Geben Sie CitrixReceiver.exe /DisableSetting=0 ein
Ausblenden von Einstellungsoption im Dialogfeld “Erweiterte Einstellungen”	Geben Sie CitrixReceiver.exe /DisableSetting=3 ein
Einstellungsoption zeigt nur “Anwendungsanzeige” an:	Geben Sie CitrixReceiver.exe /DisableSetting=2 ein
Einstellungsoption zeigt nur “Wiederverbindungsoptionen” an:	Geben Sie CitrixReceiver.exe /DisableSetting=1 ein

Konfigurieren der administrativen Gruppenrichtlinienobjektvorlage

March 26, 2019

Citrix empfiehlt, für die Konfiguration von Citrix Receiver für Windows den Windows Gruppenrichtlinienobjekt-Editor zu verwenden. Im Installationsverzeichnis von Citrix Receiver für Windows befinden sich administrative Vorlagendateien (receiver.adm oder receiver.admx\receiver.adml, je nach Betriebssystem).

Hinweis:

- Ab Citrix Receiver für Windows-Version 4.6 enthält das Installationsverzeichnis die Dateien CitrixBase.admx und CitrixBase.adml. Citrix empfiehlt die Verwendung von CitrixBase.admx

und CitrixBase.adml um sicherzustellen, dass die Optionen im Gruppenrichtlinienobjekt-Editor richtig sortiert angezeigt werden.

- Die ADM-Datei ist nur zur Verwendung mit Windows XP Embedded-Plattformen. Die ADMX/ADML-Dateien sind zur Verwendung mit Windows Vista/Windows Server 2008 und allen höheren Versionen von Windows.
- Wenn Citrix Receiver für Windows per VDA installiert wird, sind die ADMX/ADML-Dateien im Citrix Receiver für Windows-Installationsverzeichnis. Beispiel: <Installationsverzeichnis>\Online Plugin\Configuration.
- Wenn Citrix Receiver für Windows ohne VDA installiert wird, sind die ADMX/ADML-Dateien normalerweise im Verzeichnis C:\Programme\Citrix\ICA Client\Configuration.

In der Tabelle unten finden Sie Informationen zu Citrix Receiver für Windows-Vorlagendateien und die entsprechenden Speicherorte.

Hinweis:

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

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

Hinweis:

- Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, geht möglicherweise die Richtlinie ICA-Dateisignierung aktivieren verloren.
- Beim Upgrade von Citrix Receiver für Windows müssen Sie die aktuellen Vorlagendateien wie im Folgenden beschrieben zum lokalen Gruppenrichtlinienobjekt hinzufügen. Beim Import der aktuellen Dateien werden die vorherigen Einstellungen beibehalten.

Hinzufügen der Vorlagendatei receiver.adm zum lokalen Gruppenrichtlinienobjekt (nur für Win-

dows XP Embedded-Betriebssysteme):

Hinweis: Sie können ADM-Vorlagendateien zum Konfigurieren von lokalen und domänenbasierten Gruppenrichtlinienobjekten verwenden.

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vomStartmenü ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden. **Hinweis**: Wenn Sie die Citrix Receiver für Windows-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner **Administrative Vorlagen** aus.
3. Klicken Sie im Menü "Aktion" auf **Vorlagen hinzufügen/entfernen**.
4. Wählen Sie "Hinzufügen" und navigieren Sie zum Speicherort der Vorlagendatei: <Installationsverzeichnis>\I Client\Configuration\receiver.adm.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.

Die Citrix Receiver für Windows-Vorlagendatei ist im lokalen Gruppenrichtlinienobjekt in folgendem Pfad verfügbar: **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver.**

Nachdem die ADM-Vorlagendateien dem lokalen Gruppenrichtlinienobjekt hinzugefügt wurden, wird die folgende Meldung angezeigt:
"Der folgende Eintrag im Abschnitt [strings] ist zu lang und wurde abgeschnitten:
Klicken Sie auf **OK**, um diese Meldung ignorieren.

Hinzufügen der Vorlagendateien receiver.admx/adml zum lokalen Gruppenrichtlinienobjekt (höhere Versionen des Windows-Betriebssystems):

Hinweis: Sie können ADMX/ADML-Vorlagendateien zum Konfigurieren von lokalen GPO und domänenbasierten GPO verwenden. Weitere Informationen zum Verwalten von ADMX-Dateien finden Sie im Microsoft MSDN-Artikel.

1. Kopieren Sie nach der Installation von Citrix Receiver für Windows die Vorlagendateien.

   ADMX:

   Von: <Installationsverzeichnis>\ICA Client\Configuration\receiver.admx

   Nach: %systemroot%\policyDefinitions\

   Von: <Installationsverzeichnis>\ICA Client\Configuration\CitrixBase.admx

   Nach: %systemroot%\policyDefinitions\

   ADML:

Von: <Installationsverzeichnis>\ICA Client\Configuration\[MUIculture]receiver.adml

Nach: %systemroot%\policyDefinitions\[MUIculture]

Von: <Installationsverzeichnis>\ICA Client\Configuration\[MUIculture]\CitrixBase.adml

Nach: %systemroot%\policyDefinitions\[MUIculture]

Hinweis:
Citrix Receiver für Windows-Vorlagendateien sind im lokalen Gruppenrichtlinienobjekt unter "Administrative Vorlagen > Citrix Komponenten > Citrix Receiver" nur verfügbar, wenn der Benutzer die Dateien CitrixBase.admx/CitrixBase.adml dem Ordner \policyDefinitions hinzufügt.

Bereitstellen der Kontoinformationen für Benutzer

March 26, 2019

Teilen Sie den Benutzern die Kontoinformationen mit, die sie zum Zugriff auf die virtuellen Anwendungen und Desktops benötigen. Sie können diese Informationen folgendermaßen bereitstellen:

- Konfigurieren der e-mail-basierten Kontenermittlung
- Bereitstellen einer Provisioningdatei für Benutzer
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

> **Wichtig**
>
> Citrix empfiehlt, Citrix Receiver für Windows nach der Installation neu zu starten. Damit wird sichergestellt, dass Benutzer Konten hinzufügen können, und dass Citrix Receiver für Windows USB-Geräte erkennt, die während der Installation im ausgesetzten Zustand waren.

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

Unterdrücken des Dialogfelds "Konto hinzufügen"

Das Dialogfeld Konto hinzufügen wird angezeigt, wenn der Store nicht konfiguriert ist. Benutzer können in diesem Dialogfeld ein Citrix Receiver-Konto durch Eingabe einer E-Mail-Adresse oder einer Server-URL einrichten.

Citrix Receiver für Windows ermittelt den NetScaler Gateway, StoreFront-Server oder das virtuelle App Controller-Gerät, der bzw. das der E-Mail-Adresse zugeordnet ist, und fordert den Benutzer dann zur Anmeldung auf, damit die Enumeration erfolgen kann.

Das Dialogfeld "Konto hinzufügen" kann wie folgt unterdrückt werden:

1. **Bei der Systemanmeldung**

   Wählen Sie **Dieses Fenster bei der Anmeldung nicht automatisch anzeigen**, damit das Fenster "Konto hinzufügen" bei nachfolgenden Anmeldungen nicht angezeigt wird.

   Diese Einstellung wird pro Benutzer festgelegt und wird beim Zurücksetzen von Citrix Receiver für Windows zurückgesetzt.

2. **Installation über die Befehlszeile**

   Installieren Sie Citrix Receiver für Windows als Administrator an der Befehlszeilenschnittstelle mit dem folgenden Parameter:
   CitrixReceiver.exe /ALLOWADDSTORE=N.
   Diese Einstellung gilt pro Maschine, daher ist das Verhalten für alle Benutzer gleich.

   Die folgende Meldung wird angezeigt, wenn kein Store konfiguriert ist.

   Darüber hinaus kann das Dialogfeld "Konto hinzufügen" auf folgende Weise unterdrückt werden.

Hinweis: Citrix empfiehlt, dass Benutzer das Dialogfeld "Konto hinzufügen" bei der Systemanmeldung oder über die Befehlszeilenschnittstelle unterdrücken.

- **Umbenennen der ausführbaren Citrix Datei**:
  Benennen Sie die Datei **CitrixReceiver.exe** in **CitrixReceiverWeb.exe** um, um das Verhalten des Dialogfelds "Konto hinzufügen" zu ändern. Durch Umbenennen der Datei wird das Dialogfeld "Konto hinzufügen" nicht vom Startmenü angezeigt.
  Weitere Informationen zu Citrix Receiver für Web finden Sie unter Bereitstellen von Receiver für Windows über Receiver für Web.

- **Gruppenrichtlinienobjekt:**
  Zum Ausblenden der Schaltfläche "Konto hinzufügen" im Installationsassistenten von Citrix Receiver für Windows deaktivieren Sie **EnableFTUpolicy** im Knoten "Self-Service" im Editor für lokale Gruppenrichtlinien wie unten dargestellt.
  Diese Einstellung gilt pro Maschine, daher ist das Verhalten für alle Benutzer gleich.
  Informationen zum Laden der Vorlagendatei finden Sie unter Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage.

Konfigurieren der e-mail-basierten Kontenermittlung

Wenn Sie Citrix Receiver für Windows für die e-mail-basierte Kontenermittlung konfigurieren, geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration von Citrix Receiver für Windows ein. Citrix Receiver für Windows ermittelt den NetScaler Gateway- oder StoreFront-Server, der der E-Mail-Adresse auf der Basis von DNS-Dienstdatensätzen zugeordnet

ist, und fordert den Benutzer dann zur Anmeldung auf, um auf virtuelle Desktops und Anwendungen zuzugreifen.

Hinweis:

> Die e-mail-basierte Kontenermittlung wird nicht für die Bereitstellungen mit dem Webinterface unterstützt.

Weitere Informationen zur Konfiguration von NetScaler Gateway finden Sie unter Verbinden mit StoreFront über die e-mail-basierte Kontoermittlung in der NetScaler Gateway-Dokumentation.

Bereitstellen von Provisioningdateien für Benutzer

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

Sie können mit StoreFront ein Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, damit sie Citrix Receiver für Windows automatisch konfigurieren können. Nach der Installation von Citrix Receiver für Windows öffnen Benutzer die Datei, um Citrix Receiver für Windows zu konfigurieren. Wenn Sie Citrix Receiver für Web-Sites konfigurieren, können Benutzer Citrix Receiver für Windows-Provisioningdateien auch von diesen Seiten abrufen.

- Weitere Informationen finden Sie unter Exportieren von Store-Provisioningdateien für Benutzer in der StoreFront-Dokumentation.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

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

- Für Verbindungen mit einem StoreFront-Store teilen Sie den Benutzern die URL für den betreffenden Server mit. Beispiel: `https://servername.company.com`

  Für Webinterface-Bereitstellungen teilen Sie den Benutzern die URL für die XenApp Services-Site mit.

- Für Verbindungen über NetScaler Gateway legen Sie fest, ob Benutzer alle konfigurierten Stores sehen oder nur den Store, für den der Remotezugriff auf einen bestimmten NetScaler Gateway aktiviert ist.
  - Anzeigen aller konfigurierten Stores: Teilen Sie den Benutzern den FQDN für NetScaler Gateway mit.
  - Beschränken des Zugriffs auf einen bestimmten Store: Teilen Sie den Benutzern den FQDN für NetScaler Gateway und den Storenamen wie folgt mit:

NetScalerGatewayFQDN?MyStoreName

Wenn z. B. für Store “SalesApps” der Remotezugriff auf server1.com aktiviert ist und für Store “HRApps” Remotezugriff auf server2.com, muss ein Benutzer server1.com?SalesApps für den Zugriff auf SalesApps eingeben bzw. server2.com?HRApps für den Zugriff auf HRApps. Für dieses Feature muss ein Erstbenutzer ein Konto erstellen, indem er eine URL eingibt, und die e-mail-basierte Kontenermittlung ist nicht verfügbar.

Wenn ein Benutzer Informationen für ein neues Konto eingibt, versucht Citrix Receiver für Windows, die Verbindung zu überprüfen. Wenn die Verbindung hergestellt werden kann, fordert Citrix Receiver für Windows den Benutzer auf, sich an dem Konto anzumelden.

Zum Verwalten von Konten öffnet ein Citrix Receiver für Windows-Benutzer die Homepage von Citrix Receiver für Windows, klickt auf und dann auf **Konten**.

Automatisches Freigeben von mehreren Store-Konten

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

Wenn Sie mehr als ein Store-Konto haben, können Sie Citrix Receiver für Windows so konfigurieren, dass beim Erstellen einer Sitzung automatisch Verbindungen zu allen Konten hergestellt werden. Automatisches Anzeigen aller Konten beim Öffnen von Citrix Receiver für Windows:

Bei 32-Bit-Systemen: Erstellen Sie den Schlüssel “CurrentAccount”:

Speicherort: HKLM\Software\Citrix\Dazzle

Schlüsselname: CurrentAccount

Wert: AllAccount

Typ: REG_SZ

Bei 64-Bit-Systemen: Erstellen Sie den Schlüssel “CurrentAccount”:

Speicherort: HKLM\Software\Wow6432Node\Citrix\Dazzle

Schlüsselname: CurrentAccount

Wert: AllAccount

Typ: REG_SZ

Konfigurieren von automatischen Updates

February 20, 2019

Wenn Sie automatische Updates von Citrix Receiver für Windows konfigurieren, nutzen Sie die folgenden Verfahren in der Reihenfolge ihrer Priorität:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Befehlszeilenschnittstelle
3. Erweiterte Einstellungen (pro Benutzer)

Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
    - Wenn Sie die Richtlinie auf einen einzigen Computer anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
    - Wenn Sie die Richtlinie auf eine Domäne anwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver mit der Gruppenrichtlinien-Verwaltungskonsole.
2. Navigieren Sie unter dem Knoten “Computerkonfiguration” zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Receiver** > **Automatische Updates**.
3. Wählen Sie die Richtlinie **Verzögerung für Prüfung auf Updates festlegen**. Mit dieser Richtlinie können Sie ein zeitlich gestaffeltes Rollout durchführen.
4. Wählen Sie **Aktiviert** und anschließend im Dropdownmenü neben **Für Gruppe aufschieben** eine der folgenden Optionen:
    - **Fast** – Das Rollout des Updates erfolgt zu Beginn des Bereitstellungszeitraums.
    - **Medium** – Das Rollout des Updates erfolgt in der Mitte des Bereitstellungszeitraums.
    - **Slow** – Das Rollout des Updates erfolgt am Ende des Bereitstellungszeitraums.
5. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.
6. Klicken Sie im AutoUpdate-Bereich auf **AutoUpdate-Richtlinie aktivieren oder deaktivieren**.
7. Wählen Sie **Aktiviert** und legen Sie die Werte nach Bedarf fest:
    - Wählen Sie im Dropdownmenü neben **AutoUpdate-Richtlinie aktivieren** eine der folgenden Optionen:
        - **Auto** – Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).

  - **Manual** – Sie werden nicht benachrichtigt, wenn Updates zur Verfügung stehen. Suchen Sie manuell nach Updates.
- Aktivieren Sie **Nur LTSR**, um Updates nur für LTSR zu erhalten.
- Wählen Sie im Dropdownmenü **Auto-Update-DeferUpdate-Count** einen Wert zwischen **-1** und **30**.
  - **-1:** Gibt an, dass Sie Benachrichtigungen beliebig oft verschieben können (Standardwert = -1).
  - **0:** Gibt an, dass die Option **Später erinnern** nicht angezeigt wird.
  - Beliebige andere Zahl: Gibt an, wie oft die Option **Später erinnern** angezeigt wird. Beispiel: Bei einem Wert von 10 wird die Option **Später erinnern** zehnmal angezeigt.

8. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.

Konfiguration über die Befehlszeilenschnittstelle

Während der Installation von Citrix Receiver für Windows

Konfigurieren der Einstellungen für automatische Updates als Administrator über die Befehlszeileneinstellungen während der Installation von Citrix Receiver:

- **/AutoUpdateCheck=** auto/manual/disabled
- **/AutoUpdateStream=** LTSR/Current. Hier bezieht sich “LTSR” auf Long Term Service Release und “Current” auf das aktuelle Release.
- **/DeferUpdateCount=** beliebiger Wert zwischen-1 und 30
- **/AURolloutPriority=** auto/fast/medium/slow

Beispiel: *CitrixReceiver.exe /AutoUpdateCheck=auto /AutoUpdateStream= Current /DeferUpdateCount=-1 / AURolloutPriority= fast*

- Konfigurieren der Einstellungen für automatische Updates als Benutzer über die Befehlszeileneinstellungen während der Installation von Citrix Receiver:
  - **/AutoUpdateCheck=auto/manual**

Beispiel: *CitrixReceiver.exe / AutoUpdateCheck=auto*

Werden die Einstellungen für automatische Updates mit der administrativen Gruppenrichtlinienobjektvorlage bearbeitet, werden dadurch die Einstellungen überschrieben, die bei der Installation von Citrix Receiver für Windows für alle Benutzer angewendet wurden.

Nach der Installation von Citrix Receiver für Windows

Automatische Updates können nach der Installation von Citrix Receiver für Windows konfiguriert werden.

Verwenden der Befehlszeile

Öffnen Sie eine Windows-Eingabeaufforderung und ändern Sie das Verzeichnis zum Speicherort von **CitrixReceiverUpdater.exe**. Normalerweise befindet sich CitrixReceiverUpdater.exe unter *CitrixReceiverInstallLocation*\Citrix\Ica Client\Receiver.

Sie können auch die Richtlinie für automatische Updates über die Befehlszeile mit dieser Binärdatei festlegen.

Beispiel: Administratoren können alle vier Optionen verwenden:

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

Konfiguration über die grafische Benutzeroberfläche

Ein Benutzer kann die Einstellung für automatische Updates im Dialogfeld **Erweiterte Einstellungen** überschreiben. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet.

1. Klicken Sie im Infobereich mit der rechten Maustaste auf Citrix Receiver für Windows.
2. Wählen Sie **Erweiterte Einstellungen** und klicken Sie auf **Automatische Updates**.

   Das Dialogfeld für automatische Updates wird angezeigt.
3. Wählen Sie eine der folgenden Optionen:
   - Ja, benachrichtigen Sie mich
   - Nein, nicht benachrichtigen
   - Vom Administrator festgelegte Einstellungen verwenden
4. Klicken Sie auf **Speichern**.

Konfigurieren von automatischen Updates mit StoreFront

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

   Beispiel: <account id=… name=”Store”>

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

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


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

```
<account>

    <clear />

    <account id=”d1197d2c-ac82-4f13-9346-2ee14d4b0202” name=”F84Store”

      description=”” published=”true” updaterType=”Citrix”
         remoteAccessType=”None”>

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef=”1__Citrix_F84Store”>

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>

            <properties>

              <property name=”Auto-Update-Check” value=”auto” />

              <property name=”Auto-Update-DeferUpdate-Count” value=”1”
                 />

                    <property name=”Auto-Update-LTSR-Only” value=”
                       FALSE” />

              <property name=”Auto-Update-Rollout-Priority” value=”fast
                 ” />

                  </properties>
```



```
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

Dies gibt an, dass Citrix Receiver für Windows erkennt, wenn ein Update verfügbar ist.

Gültige Werte:

- Auto – Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung).
- Manual – Sie werden nicht benachrichtigt, wenn Updates zur Verfügung stehen. Suchen Sie manuell nach Updates.
- Disabled: Das Feature für automatische Updates ist deaktiviert.

auto-update-LTSR-Only

Dies gibt an, dass Citrix Receiver für Windows nur Updates für LTSR akzeptieren muss.

Gültige Werte:

- True: Die automatische Updatefunktion sucht nur LTSR-Updates von Citrix Receiver für Windows.
- False: Die automatische Updatefunktion sucht auch LTSR-fremde Updates von Citrix Receiver für Windows.

auto-update-DeferUpdate-Count

Dies gibt an, wie oft Benachrichtigungen zurückgestellt werden können. Die Option Später erinnern wird gemäß der hier festgelegten Zahl angezeigt.

Gültige Werte:

- -1: Gibt an, dass Sie Benachrichtigungen beliebig oft verschieben können (Standardwert = -1).
- 0: Gibt an, dass die Option "Später erinnern" nicht angezeigt wird.
- Beliebige andere Zahl: Gibt an, wie oft die Option "Später erinnern" angezeigt wird. Beispiel: Bei einem Wert von 10 wird die Option Später erinnern zehnmal angezeigt.

auto-update-Rollout-Priority:

Dies gibt den Zeitrahmen für die Rolloutphase an.

Gültige Werte:

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

Einschränkungen:

1. Das System muss Zugriff auf das Internet haben.
2. Receiver für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
3. Wenn Sie einen Outbound-Proxy mit SSL-Interception konfiguriert haben, müssen Sie eine Ausnahme zum Receiver-Signaturdienst für automatische Updates `https://citrixupdates.cloud.com` und zum Downloadspeicherort `https://downloadplugins.citrix.com` hinzufügen.
4. Standardmäßig sind automatische Updates auf dem VDA deaktiviert. Dies umfasst RDS-Server mit mehreren Benutzern, VDI- und Remote-PC-Maschinen.
5. Automatische Updates sind auf Maschinen deaktiviert, auf denen Desktop Lock installiert ist.

Optimieren der Umgebung

November 21, 2018

Sie können die Umgebung optimieren:

- Verkürzen des Anwendungsstarts
- Vereinfachen der Verbindung von Geräten mit veröffentlichten Ressourcen
- Unterstützen der DNS-Namensauflösung
- Verwenden von Proxyservern für XenDesktop-Verbindungen
- Aktivieren des Zugriffs auf anonyme Anwendungen
- Prüfen der Konfiguration für Single Sign-On

Verkürzen des Anwendungsstarts

January 7, 2019

Verwenden Sie das Feature zum Sitzungsvorabstart, um den Anwendungsstart in Zeiten mit normalem oder hohem Netzwerkverkehr zu verkürzen und die Benutzererfahrung dadurch zu verbessern. Mit dem Vorabstart-Feature kann eine Vorabstartsitzung bei der Benutzeranmeldung an Citrix Receiver für Windows oder zu einem bestimmten Zeitpunkt, wenn der Benutzer bereits angemeldet ist, erstellt werden.

Diese Vorabstartsitzung verkürzt die Startzeit der ersten Anwendung. Wenn ein Benutzer eine neue Kontoverbindung in Citrix Receiver für Windows hinzufügt, findet der Sitzungsvorabstart erst in der nächsten Sitzung statt. Die Standardanwendung ctxprelaunch.exe wird in der Sitzung ausgeführt, ist jedoch für den Benutzer unsichtbar.

Sitzungsvorabstart wird für StoreFront-Bereitstellungen ab dem StoreFront 2.0-Release unterstützt. Stellen Sie bei Webinterfacebereitstellungen sicher, dass die Option “Kennwort speichern” aktiviert ist, um Anmeldeaufforderungen zu vermeiden. Sitzungsvorabstart wird nicht für XenDesktop 7-Bereitstellungen unterstützt.

Vorabstartsitzungen sind in der Standardeinstellung deaktiviert. Geben Sie zum Aktivieren vom Vorabstart von Sitzungen den Parameter ENABLEPRELAUNCH=true an der Receiver-Befehlszeile an oder stellen Sie den Registrierungsschlüssel EnablePreLaunch auf true. Die Standardeinstellung “Null” bedeutet, dass der Vorabstart deaktiviert ist.

Hinweis: Wenn der Client zur Unterstützung der Domänen-Passthrough-Authentifizierung (SSON) konfiguriert wurde, ist Vorabstart automatisch aktiviert. Wenn Sie die Domänen-Passthrough-Authentifizierung ohne Vorabstart verwenden möchten, legen Sie den

Registrierungsschlüssel “EnablePreLaunch”
auf “false” fest.

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

Die Registrierungsverzeichnisse sind:

HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazzle

HKEY_CURRENT_USER\Software\Citrix\Dazzle

Es gibt zwei Arten von Vorabstart:

- **Just-In-Time-Vorabstart**: Der Vorabstart wird direkt nach dem Authentifizieren der Anmeldeinformationen des Benutzers gestartet, unabhängig davon, ob es sich um einem Zeit mit hohem Netzwerkverkehr handelt. Normalerweise für Zeiten mit normalen Datenverkehr verwendet. Ein Benutzer kann den Just-In-Time-Vorabstart durch einen Neustart von Citrix Receiver für Windows auslösen.
- **Geplanter Vorabstart**: Der Vorabstart wird nach einem Zeitplan gestartet. Geplanter Vorabstart startet nur, wenn das Benutzergerät bereits ausgeführt wird und authentifiziert wurde. Wenn diese beiden Bedingungen zur geplanten Vorabstartzeit nicht erfüllt, wird keine Sitzung gestartet. Um Netzwerk- und Serverlast zu verteilen, wird die geplante Sitzung innerhalb eines Zeitfensters gestartet. Wenn beispielsweise Vorabstart für 13:45 geplant ist, wird die Sitzung tatsächlich irgendwann zwischen 13:15 und 13:45 gestartet. Normalerweise für Zeiten mit hohem Datenverkehr verwendet.

Zur Vorabstart-Konfiguration auf dem XenApp-Server gehört das Erstellen, Bearbeiten oder Löschen von Vorabstartanwendungen sowie das Aktualisieren der Benutzerrichtlinien, die die Vorabstartanwendung steuern. Weitere Informationen zur Konfiguration von Vorabstart von Sitzungen auf dem XenApp-Server finden Sie in der XenApp-Dokumentation.

Anpassen der Vorabstartfunktion mit der Datei receiver.admx wird nicht unterstützt. Sie können aber die Vorabstartkonfiguration ändern, indem Sie während oder nach der Citrix Receiver für Windows-Installation die Registrierungswerte ändern. Es gibt drei HKLM-Werte und zwei HKCU-Werte:

- Die HKLM-Werte werden während der Clientinstallation geschrieben.
- Mit den HKCU-Werten können Sie verschiedenen Benutzern auf derselben Maschine unterschiedliche Einstellungen bereitstellen. Benutzer können die HKCU-Werte ohne Administratorrechte ändern. Sie können Skripte bereitstellen, mit denen die Benutzer diese Konfigurationsänderungen erreichen können.

Registrierungswerte für HKEY_LOCAL_MACHINE

Für Windows 7 und 8 (64 Bit): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Für alle anderen unterstützten Windows-Betriebssysteme (32 Bit): HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Name: UserOverride

Werte:

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

1 - Werte unter HKEY_CURRENT_USER verwenden, wenn vorhanden, sonst den Wert unter HKEY_LOCAL_MACHINE.

Name: State

Werte:

0 - Vorabstart deaktivieren.

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

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

Name: Schedule

Wert:

Uhrzeit (24-Stunden-Format) und Wochentage für geplanten Vorabstart in folgendem Format:

HH:MM	Mo:Di:Mi:Do:Fr:Sa:So, wobei HH und MM Stunden und Minuten sind. Mo:Di:Mi:Do:Fr:Sa:So sind die Wochentage. Um beispielsweise den Vorabstart montags, mittwochs und freitags um 13:45 zu aktivieren, stellen Sie Folgendes ein: Schedule=13:45	1:0:1:0:1:0:0 . Tatsächlich wird die Sitzung irgendwann zwischen 13:15 und 13.45 gestartet.

Registrierungswerte für HKEY_CURRENT_USER

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

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

Zuweisen von Clientgeräten

January 7, 2019

Citrix Receiver für Windows unterstützt das Zuordnen von Geräten auf Benutzergeräten, sodass sie in einer Sitzung zur Verfügung stehen. Benutzer haben folgende Möglichkeiten:

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

Während der Anmeldung informiert Citrix Receiver für Windows den Server über die verfügbaren Clientlaufwerke, COM- und LPT-Ports. Standardmäßig werden Clientlaufwerke Serverlaufwerksbuchstaben zugeordnet. Für Clientdrucker werden Druckerwarteschlangen erstellt, sodass die Clientdrucker direkt mit der Sitzung verbunden zu sein scheinen. Diese Zuordnungen stehen nur dem aktuellen Benutzer während der aktuellen Sitzung zur Verfügung. Sie werden bei der Abmeldung des Benutzers gelöscht und bei seiner nächsten Anmeldung neu erstellt.

Mit den Einstellungen der Richtlinie für die Umleitung können Sie Benutzergeräte zuordnen, die nicht automatisch bei der Anmeldung zugeordnet werden. Weitere Informationen finden Sie in der XenDesktop- oder XenApp-Dokumentation.

Deaktivieren von Benutzergerätzuordnungen

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

Umleiten von Clientordnern

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf

dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner statt des kompletten Dateisystems auf dem Benutzergerät werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt. Weitere Informationen, u. a. die Konfiguration der Umleitung von Clientordnern für Benutzergeräte, finden Sie in der XenDesktop 7-Dokumentation.

Zuordnen von Clientlaufwerken zu serverseitigen Laufwerksbuchstaben

Die Clientlaufwerkzuordnung ermöglicht das Umleiten von Laufwerksbuchstaben auf der Hostseite auf Laufwerke, die auf dem Benutzergerät vorhanden sind. Beispiel: In einer Citrix Benutzersitzung kann das Laufwerk H dem Laufwerk C auf dem Benutzergerät, auf dem Citrix Receiver für Windows ausgeführt wird, zugeordnet werden.

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

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

Clientlaufwerksbuchstabe	Der Server greift darauf wie folgt zu:
A	A
B	B
C	V
D	U

Der Server kann so konfiguriert werden, dass zwischen den Laufwerksbuchstaben des Servers und des Clients keine Konflikte entstehen. Dazu werden die Laufwerksbuchstaben des Servers in höhere Laufwerksbuchstaben geändert. Werden beispielsweise die Serverlaufwerke C und D in M und N geändert, können die Clientgeräte direkt auf ihre Laufwerke C und D zugreifen. Diese Methode führt zu den folgenden Laufwerkszuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Der Server greift darauf wie folgt zu:
A	A
B	B
C	C
D	D

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

Wenn ein Benutzergerät eine Verbindung mit einem Server herstellt, werden die Clientzuordnungen wiederhergestellt, wenn die automatische Clientgerätzuordnung nicht deaktiviert ist. Die Clientlaufwerkzuordnung ist standardmäßig aktiviert. Sie können die Einstellungen mit dem Konfigurationstool der Remotedesktopdienste (Terminaldienste) ändern. Außerdem können Sie mit Richtlinien genauer steuern, wie die Clientgerätzuordnung angewendet wird. Weitere Informationen zu Richtlinien finden Sie in der XenDesktop- oder XenApp-Dokumentation in der Produktdokumentation von Citrix.

HDX Plug-n-Play-USB-Geräteumleitung

Aktualisiert: 27.01-2015

HDX Plug-n-Play USB-Geräteumleitung ermöglicht die dynamische Umleitung von Mediengeräten, einschließlich Kameras, Scannern, Medienplayern und POS-Geräten, zum Server. Sie oder der Benutzer können die Umleitung auf einige oder alle Geräte beschränken. Bearbeiten Sie die Richtlinien auf dem Server oder wenden Sie Gruppenrichtlinien auf dem Benutzergerät an, um die Einstellungen für die Umleitung zu konfigurieren. Weitere Informationen finden Sie unter Überlegungen zu USB und Clientlaufwerk in der Dokumentation zu XenApp und XenDesktop.

Wichtig: Wenn Sie die Plug-n-Play-USB-Geräteumleitung in einer Serverrichtlinie nicht zulassen, kann der Benutzer diese Richtlinieneinstellung nicht überschreiben.

Ein Benutzer kann Berechtigungen in Citrix Receiver für Windows festlegen und die Geräteumleitung immer zulassen oder ablehnen oder bei jeder Verbindung eines Geräts gefragt werden. Diese Einstellung wirkt sich nur auf Geräte aus, die eingesteckt werden, nach dem der Benutzer die Einstellung geändert hat.

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

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

Sie können Client-COM-Ports von der Befehlszeile aus zuordnen. Sie können auch die Client-COM-Portzuordnung vom Remotedesktop-Konfigurationstool (Terminaldienste) oder mit Richtlinien steuern. Weitere Informationen zu Richtlinien finden Sie in der XenDesktop- oder XenApp-Dokumentation.

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

1. Aktivieren Sie für XenDesktop 7-Bereitstellungen die Richtlinieneinstellung Client-COM-Portumleitung.
2. Melden Sie sich an Citrix Receiver für Windows an.
3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   net use comx: \\client\comz:

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

   net use

   an der Eingabeaufforderung ein. Die angezeigte Liste enthält zugeordnete Laufwerke, LPT- und zugeordnete COM-Ports.

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

Unterstützen der DNS-Namensauflösung

January 7, 2019

Wenn Citrix Receiver für Windows den Citrix XML-Dienst verwendet, kann er einen DNS-Namen anstatt der IP-Adresse eines Servers anfordern.

Wichtig: Wenn Ihre DNS-Umgebung nicht speziell für die Verwendung dieser Funktion konfiguriert ist, empfiehlt Citrix, die DNS-Namensauflösung in der Serverfarm nicht zu aktivieren.

Beim Herstellen einer Verbindung zu veröffentlichten Anwendungen über das Webinterface kann Citrix Receiver für Windows ebenfalls den Citrix XML-Dienst verwenden. Damit Citrix Receiver für Windows Verbindungen über das Webinterface herstellen kann, löst der Webserver den DNS-Namen für Citrix Receiver für Windows auf.

Die DNS-Namensauflösung ist in der Serverfarm standardmäßig deaktiviert und in Citrix Receiver für Windows standardmäßig aktiviert. Wenn die DNS-Namensauflösung in der Serverfarm deaktiviert ist, wird bei jeder Citrix Receiver für Windows-Anfrage nach einem DNS-Namen eine IP-Adresse ausgegeben. Die DNS-Namensauflösung muss nicht auf Citrix Receiver für Windows deaktiviert werden.

Deaktivieren der DNS-Namensauflösung für bestimmte Benutzergeräte

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

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

1. Fügen Sie eine Registrierungsschlüssel-Zeichenfolge xmlAddressResolutionType zu HKEY_LOCAL_MACHINE\Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing hinzu.
2. Setzen Sie den Wert auf “IPv4-Port”.
3. Wiederholen Sie diesen Vorgang für alle Benutzer der Benutzergeräte.

Verwenden von Proxyservern für XenDesktop

February 20, 2019

Wenn Sie keine Proxyserver in der Umgebung verwenden, berichtigen Sie die Proxyeinstellungen von Internet Explorer auf allen Benutzergeräten, auf denen Internet Explorer 7.0 unter Windows XP ausgeführt wird. In der Standardeinstellung werden bei dieser Konfiguration die Proxyeinstellungen automatisch erkannt. Wenn Proxyserver nicht verwendet werden, stellen Benutzer unnötige Verzögerungen bei der Erkennung fest. Weitere Informationen zur Änderung der Proxyeinstellungen finden Sie in der Internet Explorer-Dokumentation. Sie können die Proxyeinstellungen auch mit dem Webinterface ändern. Weitere Informationen finden Sie in der Webinterface-Dokumentation.

Überprüfen der Konfiguration von Single Sign-On mit der Konfigurationsprüfung

January 7, 2019

Ab Release 4.5 von Citrix Receiver für Windows können Benutzer mit der Konfigurationsprüfung einen Test ausführen, um sicherzustellen, dass Single Sign-On richtig konfiguriert ist. Der Test wird für verschiedene Prüfpunkte der Single Sign-On-Konfiguration ausgeführt und die Konfigurationsergebnisse werden angezeigt.

1. Melden Sie sich an Citrix Receiver für Windows an.
2. Klicken Sie im Infobereich mit der rechten Maustaste auf Citrix Receiver für Windows und wählen Sie **Erweiterte Einstellungen**. Das Dialogfeld "Erweiterte Einstellungen" wird angezeigt.
3. Wählen Sie **Konfigurationsprüfung**. Das Fenster der Citrix Konfigurationsprüfung wird angezeigt.
4. Wählen Sie **SSONChecker** im Bereich **Auswählen** aus.
5. Klicken Sie auf **Ausführen**. Eine Fortschrittsanzeige mit dem Status des Tests wird angezeigt.

Das Fenster der Konfigurationsprüfung enthält die folgenden Spalten:

1. **Status**: zeigt das Ergebnis eines Tests auf einem bestimmten Prüfpunkt an.
    - Ein grünes Häkchen bedeutet, dass der Prüfpunkt ordnungsgemäß konfiguriert ist.
    - Ein blaues I bedeutet, dass zu dem Prüfpunkt Informationen vorhanden sind.
    - Ein rotes X bedeutet, dass der Prüfpunkt nicht ordnungsgemäß konfiguriert ist.
2. **Anbieter**: zeigt den Namen des Moduls an, auf dem der Test ausgeführt wird. In diesem Fall Single Sign-On.
3. **Suite**: die Kategorie des Tests. Beispiel: Installation.
4. **Test**: der Name des Tests, der ausgeführt wird.
5. **Details**: zusätzlichen Informationen über den Test, ungeachtet des Erfolgs oder Fehlschlagens. Der Benutzer erhält weitere Informationen zu den einzelnen Prüfpunkten und den entsprechenden Ergebnissen.

Die folgenden Tests werden ausgeführt:

1. Mit Single Sign-On installiert
2. Anmeldeinformationen erfassen
3. Registrierung von Netzwerkanbieter: Das Testergebnis für "Registrierung von Netzwerkanbieter" hat nur ein grünes Häkchen, wenn "Citrix Single Sign-On" als erster Netzwerkanbieter festgelegt ist. Wenn "Citrix Single Sign-On" an einer weiteren Stelle in der Liste steht, werden neben

dem Testergebnis für “Registrierung von Netzwerkanbieter” ein blaues I und zusätzliche Informationen angezeigt.

4. Single Sign-On-Prozess wird ausgeführt
5. Gruppenrichtlinie: Diese Richtlinie ist standardmäßig auf dem Client konfiguriert.
6. Interneteinstellungen für Sicherheitszonen: Stellen Sie sicher, dass Sie die Store-/XenApp-Dienst-URL der Liste der Sicherheitszonen in den Internetoptionen hinzufügen. Wenn die Sicherheitszonen per Gruppenrichtlinie konfiguriert sind, erfordern Änderungen in der Richtlinie das erneute Öffnen des Fensters “Erweiterte Einstellungen”, damit die Änderungen wirksam werden und der richtige Teststatus angezeigt wird.
7. Authentifizierungsmethode für das Webinterface oder StoreFront.

Hinweis: Wenn der Benutzer auf Receiver für Web zugreift, sind die Testergebnisse nicht gültig.
Wenn Citrix Receiver für Windows mit mehreren Stores konfiguriert ist, wird der Test für die Authentifizierungsmethode für alle konfigurierten Stores ausgeführt.

Hinweis: Die Testergebnisse können in Berichten gespeichert werden. Das Standardformat für Berichte ist TXT.

Ausblenden der Konfigurationsprüfung im Dialogfeld “Erweiterte Einstellungen”:

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vomStartmenü ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
2. Navigieren Sie im Gruppenrichtlinien-Editor zu **Citrix Komponenten** > **Citrix Receiver** > **Self-Service** > **DisableConfigChecker**.
3. Wählen Sie **Aktiviert**.
   Dadurch wird Konfigurationsprüfungsoption im Fenster **Erweiterte Einstellungen** ausgeblendet.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Öffnen Sie eine Eingabeaufforderung.
6. Führen Sie den Befehl gpupdate /force aus.

Um die Änderungen zu übernehmen, müssen Sie das Dialogfeld “Erweiterte Einstellungen” schließen und erneut öffnen.

Einschränkungen:

Die Konfigurationsprüfung enthält nicht den Prüfpunkt für die Konfiguration von “An XML-Dienst gesendeten Anfragen vertrauen” auf XenApp- oder XenDesktop-Servern.

Verbessern der Benutzererfahrung

March 26, 2019

Sie können die Benutzererfahrung mit den folgenden Features verbessern:

Konfigurieren generischer Client-IMEs (Eingabemethoden-Editor)

Konfigurieren eines generischen Client-IME über die Befehlszeilenschnittstelle

Zum Aktivieren des generischen Client-IME führen Sie den Befehl **wfica32.exe /localime:on** vom Installationsordner für Citrix Receiver für Windows (C:\Programme (x86)\Citrix\ICA Client) aus.

> **Hinweis**
>
> Sie können mit der Befehlszeilenoption **wfica32.exe /localime:on**den generischen Client-IME und die Tastaturlayoutsynchronisierung aktivieren.

Zum Deaktivieren des generischen Client-IME führen Sie den Befehl **wfica32.exe /localgenericime:off** vom Installationsordner für Citrix Receiver für Windows (C:\Programme (x86)\Citrix\ICA Client) aus. Dieser Befehl hat keine Auswirkungen auf die Einstellungen für die Tastaturlayoutsynchronisierung.

Wenn Sie den generischen Client-IME über die Befehlszeilenschnittstelle deaktiviert haben, können Sie das Feature durch Ausführen des Befehls **wfica32.exe /localgenericime:on** wieder aktivieren.

Ein-/Ausschalten:

Citrix Receiver für Windows unterstützt das Ein- und Ausschalten für dieses Feature. Sie können das Feature durch Ausführen des Befehls **wfica32.exe /localgenericime:on** ein- oder ausschalten. Die Einstellungen für die Tastaturlayoutsynchronisierung haben jedoch Vorrang vor der Ein-/Ausschaltfunktion. Wenn die Tastaturlayoutsynchronisierung auf **Aus** festgelegt ist, kann der generische Client-IME nicht durch Ein-/Ausschalten aktiviert werden.

Konfigurieren eines generischen Client-IME über die grafische Benutzeroberfläche

Der generische Client-IME erfordert VDA-Version 7.13 oder höher.

Das generische Client-IME-Feature kann durch Aktivieren der Tastaturlayoutsynchronisierung aktiviert werden. Weitere Informationen finden Sie unter Tastaturlayoutsynchronisierung.

Citrix Receiver für Windows ermöglicht das Konfigurieren verschiedener Optionen für den generischen Client-IME. Entsprechend Ihrer Anforderungen und der Nutzung können Sie eine der Optionen auswählen.

1. Klicken Sie in einer aktiven Anwendungssitzung mit der rechten Maustaste auf das Citrix Receiver-Symbol im Infobereich und wählen Sie **Connection Center**.
2. Wählen Sie **Einstellungen** und klicken Sie auf **Lokaler IME**.

Für die Unterstützung verschiedener IME-Modi sind die folgenden Optionen verfügbar:

1. **Server-IME aktivieren**: Wählen Sie diese Option, um den lokalen IME zu deaktivieren. Mit dieser Option können nur die auf dem Server festgelegten Sprachen verwendet werden.
2. **Lokalen IME-Modus für hohe Leistung einstellen**: Wählen Sie diese Option, um den lokalen IME mit beschränkter Bandbreite zu verwenden. Diese Option schränkt die Funktionalität des Kandidatenfensters ein.
3. **Lokalen IME-Modus für beste Erfahrung einstellen**: Wählen Sie diese Option, um den lokalen IME mit optimaler Benutzerfreundlichkeit zu verwenden. Diese Option verbraucht hohe Bandbreite. Diese Option ist standardmäßig ausgewählt, wenn der generische Client-IME aktiviert ist.

Die Einstellungsänderung wird nur in der aktuellen Sitzung angewendet.

Konfigurieren von Tastenkombinationen mit einem Registrierungs-Editor

Wenn der generische Client-IME aktiviert ist, können Sie mit der Tastenkombination **Umschalt+F4** verschiedene IME-Modi auswählen. Die verschiedenen Optionen für die IME-Modi werden oben rechts in der Sitzung angezeigt.

Standardmäßig ist die Tastenkombination für den generischen Client-IME deaktiviert.

Navigieren Sie im Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys.

Wählen Sie **AllowHotKey** und ändern Sie den Standardwert in 1.

> **Hinweis**
>
> Die Tastenkombination wird in Desktop- und Anwendungssitzungen unterstützt.

Einschränkungen:

1. Der generische Client-IME unterstützt keine UWP-Apps (Universelle Windows-Plattform-Anwendungen) wie Suchbenutzeroberfläche und Edge-Browser des Windows 10-Betriebssystems. Verwenden Sie als Workaround den Server-IME.
2. Der generische Client-IME wird für Internet Explorer Version 11 im geschützten Modus nicht unterstützt. Als Workaround können Sie den geschützten Modus unter **Internetoptionen** deaktivieren. Klicken Sie hierfür auf **Sicherheit** und deaktivieren Sie das Kontrollkästchen **Geschützten Modus aktivieren**.

Tastaturlayout

Die Tastaturlayoutsynchronisierung ermöglicht es Benutzern, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist in der Standardeinstellung deaktiviert.

Aktivieren der Tastaturlayoutsynchronisierung:

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol für Citrix Receiver für Windows und dann auf **Erweiterte Einstellungen** > **Einstellung des lokalen Tastaturlayouts** > **Ja**.
2. Klicken Sie auf **Speichern**.

Sie können dieses Feature deaktivieren, indem Sie **Nein** auswählen.

Sie können die Tastaturlayoutsynchronisierung auch über die Befehlszeile aktivieren und deaktivieren, indem Sie den Befehl **wfica32:exe/localime:on** oder **wfica32:exe /localime:off** vom Citrix Receiver für Windows-Installationsordner (C:\Programme (x86)\Citrix\ICA Client) aus ausführen.

Hinweis: Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Benutzer, die Japanisch, Chinesisch und Koreanisch verwenden, den Server-IME bevorzugen, müssen sie die Option für das lokale Tastaturlayout durch Auswählen von **Nein** deaktivieren oder den Befehl **wfica32:exe /localime:off** ausführen. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.

Gelegentlich wird der Wechsel des Clienttastaturlayouts nicht in einer aktiven Sitzung wirksam. Sie beheben das Problem, indem Sie sich von Citrix Receiver für Windows abmelden und dann wieder anmelden.

Einschränkungen:

- Für Remoteanwendungen, die mit erhöhten Rechten ausgeführt werden (z. B. wenn Sie mit der rechten Maustaste auf ein Anwendungssymbol klicken und “Als Administrator ausführen” wählen), kann keine Tastaturlayoutsynchronisierung erfolgen. Um dieses Problem zu umgehen, ändern Sie das Tastaturlayout manuell auf der Serverseite (VDA) oder deaktivieren Sie die Benutzerkontensteuerung (UAC).
- Wenn der Benutzer für das Tastaturlayout auf dem Client ein Layout wählt, das nicht auf dem Server unterstützt wird, dann wird das Feature für die Tastaturlayoutsynchronisierung aus Sicherheitsgründen deaktiviert, da ein unbekanntes Tastaturlayout als mögliches Sicherheitsrisiko behandelt wird. Um das Feature für die Tastaturlayoutsynchronisierung wiederherzustellen, muss der Benutzer sich von der Sitzung abmelden und wieder anmelden.
- Wenn RDP als Anwendung bereitgestellt wird und der Benutzer in einer RDP-Sitzung arbeitet, kann das Tastaturlayout nicht mit Alt+Umschalt-Tastenkombinationen geändert werden. Zum Umgehen dieses Problems können Benutzer das Tastaturlayout mit der Sprachenleiste in der RDP-Sitzung ändern.
- Dieses Feature ist in Windows Server 2016 aufgrund eines Drittanbieterproblems deaktiviert, was u. U. ein Risiko für die Leistung ist. Das Feature kann mit einer Registrierungseinstellung auf

dem VDA aktiviert werden: in HKLM\Software\Citrix\ICA\IcaIme. Fügen Sie einen neuen Schlüssel namens DisableKeyboardSync hinzu und legen Sie den Wert auf 0 fest.

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

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 kann nur in einer veröffentlichten Desktopsitzung angewendet werden.

Aktivieren der Unterstützung für relative Mausbewegungen

1. Anmelden an Citrix Receiver für Windows
2. Starten Sie eine veröffentlichte Desktopsitzung.
3. Klicken Sie auf der Desktop Viewer-Symbolleiste auf **Einstellungen**.
   Das Fenster für die Einstellungen in Citrix Receiver wird angezeigt.
4. Wählen Sie Verbindungen.
5. Aktivieren Sie unter “Relative Mauseinstellungen” die Option **Relative Maus verwenden**.
6. Klicken Sie auf **Anwenden** und auf **OK**.

Hinweis: Dieses Feature wird pro Sitzung angewendet. Wenn Sie die Verbindung mit einer getrennten Sitzung wiederherstellen, ist die Einstellung deaktiviert. Die Benutzer müssen das Feature jedes Mal erneut aktivieren, wenn sie eine Verbindung mit dem veröffentlichten Desktop (wieder)herstellen.

Hardwaredecodierung

Wenn Sie Citrix Receiver für Windows (mit HDX Engine 14.4) verwenden, kann die GPU für H.264-Decodierung verwendet werden, wenn sie auf dem Client verfügbar ist. Die für GPU-Decodierung verwendete API-Ebene ist DXVA (DirectX Video Acceleration).

Weitere Informationen finden Sie unter Improved User Experience: Hardware Decoding for Citrix Windows Receiver.

> **Hinweis**
>
> Dieses Feature ist nicht standardmäßig für eingebettete GPUs aktiviert.

Aktivieren der Hardwaredecodierung:

1. Kopieren Sie die Datei “receiver.adml” aus “root\Citrix\ICA Client\Configuration\en” nach “C:\Windows\PolicyDefinitions\”.
2. Kopieren Sie die Datei “receiver.admx” aus “root\Citrix\ICA Client\Configuration” nach “C:\Windows\PolicyDefinitions\”.
3. Navigieren Sie zum **Editor für lokale Gruppenrichtlinien**.
4. Öffnen Sie unter “Computerkonfiguration” -> “Administrative Vorlagen” -> “Citrix Receiver” -> “Benutzererfahrung” die Option **Hardwarebeschleunigung für Grafiken**.
5. Wählen Sie **Aktiviert** und klicken Sie auf **OK**.

Anhand der folgenden Registrierungseinträge sehen Sie, ob die Richtlinie angewendet wird und die Hardwarebeschleunigung in einer aktiven ICA-Sitzung verwendet wird:

Registrierungspfad: HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\<Sitzungs-ID>

> **Tipp**
>
> Der Wert für **Graphics_GfxRender_Decoder** und **Graphics_GfxRender_Renderer** sollte 2 sein. Wenn der Wert 1 ist, wird auf der CPU basierende Decodierung verwendet.

Wenn Sie das Hardwaredecodierungsfeature verwenden, berücksichtigen Sie folgende Einschränkungen:

- Wenn der Client zwei GPUs hat und wenn einer der Bildschirme auf der zweiten GPU aktiv ist, wird CPU-Decodierung verwendet.
- Bei einer Verbindung mit einem XenApp 7.x-Server, der unter Windows Server 2008 R2 ausgeführt wird, empfiehlt Citrix, auf dem Windows-Gerät des Benutzers keine Hardwaredecodierung zu verwenden. Ist die Hardwaredecodierung aktiviert, treten Probleme auf, wie geringe Leistung beim Markieren von Text und Flackern.

Clientseitige Mikrofoneingabe

Citrix Receiver für Windows unterstützt die mehrfache clientseitige Mikrofoneingabe. Lokal installierte Mikrofone können für Folgendes verwendet werden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Benutzer von Citrix Receiver für Windows können am Gerät angeschlossene Mikrofone verwenden, wenn sie eine Einstellung in Connection Center ändern. XenDesktop-Benutzer können außerdem in XenDesktop Viewer unter Einstellungen ihre Mikrofone und Webcams deaktivieren.

Multimonitorunterstützung

Sie können maximal acht Monitore mit Citrix Receiver für Windows verwenden.

Jeder Monitor in einer Multimonitorumgebung hat eine eigene, vom Hersteller festgelegte Auflösung. Monitore können in Sitzungen verschiedene Auflösungen und Ausrichtungen haben.

Sitzungen können auf zwei Arten auf mehrere Monitore übergreifend ausgeführt werden:

- Vollbildmodus: Mehrere Monitore werden in der Sitzung angezeigt; Anwendungen werden genauso wie beim lokalen Desktop an Monitore angedockt.

  XenDesktop: Sie können das Desktop Viewer-Fenster über jede rechteckige Untergruppe von Monitoren anzeigen, wenn Sie die Größe des Fensters über einen Monitorbereich ändern und auf **Maximieren** klicken.

- Im Fenstermodus mit einem Monitorbild für die Sitzung werden Anwendungen nicht an einzelne Monitore angedockt.

XenDesktop: Wenn ein Desktop in derselben Zuordnung (früher Desktopgruppe) anschließend gestartet wird, wird die Fenstereinstellung gespeichert, und der Desktop wird auf denselben Monitoren angezeigt. Mehrere virtuelle Desktops können auf einem Gerät angezeigt werden, wenn die Monitoranordnung rechteckig ist. Wenn der primäre Monitor auf dem Gerät von der XenDesktop-Sitzung verwendet wird, wird er der primäre Monitor in der Sitzung. Sonst wird der zahlenmäßig niedrigste Monitor in der Sitzung zum primären Monitor.

Für die Multimonitorunterstützung müssen Sie Folgendes sicherstellen:

- Das Benutzergerät ist für die Unterstützung von mehreren Monitoren konfiguriert.
- Das Betriebssystem auf dem Benutzergerät muss auch jeden Monitor erkennen können. Auf Windows-Plattformen können Sie auf dem Benutzergerät im Dialogfeld Anzeigeeigenschaften die Registerkarte Einstellungen anzeigen und bestätigen, dass jeder Monitor einzeln angezeigt wird.
- Nach dem Erkennen der Monitore:
  - **XenDesktop:** Konfigurieren Sie das Grafikspeicherlimit mit der Citrix Maschinenrichtlinieneinstellung “Anzeigespeicherlimit”.
  - **XenApp:** Abhängig von der installierten XenApp-Serverversion:
    * Konfigurieren Sie das Limit für den Grafikspeicher mit der Citrix Computerrichtlinieneinstellung Anzeigespeicherlimit.
    * Wählen Sie im linken Bereich der Citrix Verwaltungskonsole für den XenApp-Server die Farm aus. Wählen Sie im Aufgabenbereich Servereigenschaften ändern > Alle

Eigenschaften ändern > Serverstandard > HDX Broadcast > Anzeige (oder Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > ICA > Anzeige) und stellen Sie Maximaler Speicher für Grafiken pro Sitzung ein.

Stellen Sie sicher, dass die Einstellung hoch genug (in Kilobytes) ist, damit ausreichend Grafikspeicher bereitgestellt wird. Wenn der Wert dieser Einstellung nicht hoch genug ist, wird die veröffentlichte Ressource auf einen Teilbereich der Monitore beschränkt, der in die angegebene Größe passt.

Weitere Informationen zum Berechnen der Größe des Grafikspeichers in Sitzungen für XenApp und XenDesktop finden Sie im Knowledge Center-Artikel CTX115637.

Überschreibung von Druckereinstellungen auf Geräten

Wenn die Richtlinieneinstellung Universal Printing-Optimierungsstandards für Nicht-Administratoren können diese Einstellungen anpassen aktiviert ist, können Benutzer die in dieser Richtlinieneinstellung angegebenen Optionen Bildkomprimierung und Zwischenspeichern von Bildern und Schriftarten überschreiben.

Überschreiben der Druckereinstellungen auf dem Benutzergerät

1. Klicken Sie im Menü Drucken, das in einer Anwendung auf dem Benutzergerät zur Verfügung steht, auf Eigenschaften.
2. Klicken Sie auf der Registerkarte Clienteinstellungen auf Erweiterte Optimierungen und ändern Sie die Optionen Bildkomprimierung und Bild- und Schriftartcaching.

Steuerung der Bildschirmtastatur

Damit über Windows-Tablets der Touchzugriff auf virtuelle Anwendungen und Desktops möglich ist, zeigt Citrix Receiver für Windows automatisch eine Bildschirmtastatur an, wenn Sie ein Texteingabefeld aktivieren und das Gerät im Falt- oder Tabletmodus ist.

Auf einigen Geräten und unter bestimmten Umständen kann Citrix Receiver für Windows den Modus des Geräts nicht genau bestimmen und die Bildschirmtastatur wird u. U. angezeigt, wenn sie nicht benötigt wird.

Bei einem konvertierbaren Gerät kann die Anzeige der Bildschirmtastatur unterdrückt werden, indem Sie einen “REG_DWORD”-Wert unter DisableKeyboardPopup in HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver erstellen und den Wert auf 1 festlegen.

Hinweis: Erstellen Sie den Wert auf einer 64-Bit-Maschine in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\C Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Die Tasten können, wie nachfolgend erläutert, auf 3 verschiedene Modi festgelegt werden:

- **Automatisch**: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- **Immer anzeigen** (Bildschirmtastatur): AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- **Nie anzeigen** (Bildschirmtastatur): AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

Tastenkombinationen

Sie können Tastenkombinationen konfigurieren, die Receiver als Sonderfunktionen interpretiert. Wenn die Richtlinie für Tastenkombinationen aktiviert ist, können Sie Zuordnungen von Citrix Tastenkombinationen, das Verhalten von Windows-Tastenkombinationen und das Tastaturlayout für Sitzungen festlegen.

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.

   Hinweis: Wenn Sie die Citrix Receiver für Windows-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.

2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner Administrative Vorlagen aus.
3. Klicken Sie im Menü “Aktion” auf “Vorlagen hinzufügen/entfernen”.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie die Citrix Receiver für Windows-Vorlagendatei aus.
   Hinweis: Wählen Sie die Citrix Receiver für Windows-Vorlagendatei (receiver.adm oder receiver.admx/receiver.adml) entsprechend der Version des Windows-Betriebssystems aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor zu Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzererfahrung > Tastenkombinationen.
7. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert und die gewünschten Optionen.

Citrix Receiver für Windows-Unterstützung für Symbole in 32-Bit-Farben

Citrix Receiver für Windows unterstützt jetzt Symbole in 32 Bit High Color und die Farbtiefe wird automatisch für Anwendungen ausgewählt, die im Citrix Connection Center, im Startmenü und auf der Taskleiste angezeigt werden, um Anwendungen im Seamlessmodus darzustellen.

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

Sie können eine bevorzugte Farbtiefe einstellen, indem Sie der Registrierung unter HKEY_LOCAL_MACHINE\SOFTW Client\Engine\Lockdown Profiles\All Regions\Preferences einen neuen Zeichenfolgenschlüssel "TWIDesiredIconColor" hinzufügen und den gewünschten Wert angeben. Die möglichen Werte für die Farbtiefe von Symbolen sind 4, 8, 16, 24 und 32 Bits pro Pixel. Benutzer können eine geringere Farbtiefe für die Symbole wählen, wenn die Netzwerkverbindung langsam ist.

Aktivieren von 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 Citrix Receiver für Windows einrichten.

Verwenden Sie **Desktop Viewer**, wenn Benutzer mit dem virtuellen Desktop interagieren müssen. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario kann der Benutzer mit der Funktionalität der Desktop Viewer-Symbolleiste einen virtuellen Desktop in einem Fenster öffnen und den Desktop im lokalen Desktop ziehen und skalieren. Benutzer können Einstellungen festlegen und mit mehreren Desktops über mehrere XenDesktop-Verbindungen an demselben Benutzergerät arbeiten.

Hinweis: Benutzer müssen Citrix Receiver für Windows zum Ändern der Bildschirmauflösung auf ihren virtuellen Desktops verwenden. Die Bildschirmauflösung kann nicht in der Windows-Systemsteuerung geändert werden.

Tastatureingabe in Desktop Viewer-Sitzungen

In Desktop Viewer-Sitzungen wird die Windows-Logo-Taste+L an den lokalen Computer gesendet.

Strg+Alt+Entf wird an den lokalen Computer gesendet.

Tastatureingaben, die die Einrastfunktion, die Anschlagverzögerung und Statusanzeige (Eingabehilfen von Microsoft) aktivieren, werden normalerweise an den lokalen Computer gesendet.

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

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

Hinweis: Wenn Desktop Viewer maximiert ist, können Sie mit Alt+Tab standardmäßig zwischen Fenstern in der Sitzung wechseln. Wenn Desktop Viewer in einem Fenster angezeigt wird, wechseln Sie mit Alt+Tab zwischen Fenstern außerhalb der Sitzung.

Citrix hat bestimmte Tastenkombinationen entwickelt. Beispiel: Mit Strg+F1 reproduzieren Sie Strg+Alt+Entf und mit Umschalt+F2 wechseln Sie Anwendungen vom Vollbild- in den Fenstermodus und umgekehrt. Sie können Tastenkombinationen nicht mit virtuellen Desktops verwenden, die in Desktop Viewer angezeigt werden (d. h. mit XenDesktop-Sitzungen). Sie können sie aber mit veröffentlichten Anwendungen verwenden (d. h. mit XenApp-Sitzungen).

Verbinden mit virtuellen Desktops

In einer Desktopsitzung können Benutzer keine Verbindung zu demselben Desktop herstellen. Bei einem Versuch wird die bestehende Desktopsitzung getrennt. Aus diesem Grund empfiehlt Citrix Folgendes:

- Administratoren sollten die Clients auf dem Desktop nicht so konfigurieren, dass sie auf eine Site verweisen, die denselben Desktop veröffentlicht.
- Benutzer sollten keine Site besuchen, die denselben Desktop hostet, wenn die Site für die automatische Wiederverbindung der Benutzer mit vorhandenen Sitzungen konfiguriert ist.
- Benutzer sollten keine Site besuchen, die denselben Desktop hostet und versuchen, ihn zu starten.

Vergessen Sie nicht, dass ein Benutzer, der sich lokal an einem Computer anmeldet, der als virtueller Desktop fungiert, Verbindungen zu diesem Desktop blockiert.

Wenn Benutzer eine Verbindung mit virtuellen Anwendungen (die mit XenApp veröffentlicht wurden) von einem virtuellen Desktop aus herstellen, und das Unternehmen einen separaten XenApp-Administrator hat, sollten Sie mit ihm die Gerätezuordnung festlegen, sodass Desktopgeräte konsistent in Desktop- und Anwendungssitzungen zugeordnet werden. Da lokale Laufwerke in Desktopsitzungen als Netzwerklaufwerke angezeigt werden, muss der XenApp-Administrator die Richtlinie für die Laufwerkzuordnung ändern und Netzwerklaufwerke einschließen.

Ändern des Timeouts der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird. Zum Ändern des Timeoutzeitraums erstellen Sie einen REG_DWORD-Wert SI INACTIVE MS in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine. Sie können den REG_DWORD-Wert auf 4 festlegen, wenn die Statusanzeige eher ausgeblendet werden soll.

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

Sichere Verbindungen

January 7, 2019

Zur maximalen Sicherung der Umgebung müssen die Verbindungen zwischen Citrix Receiver für Windows und den veröffentlichten Ressourcen gesichert sein. Sie können verschiedene Authentifizierungsmethoden für die Citrix Receiver für Windows-Software konfigurieren, u. a. Smartcardauthentifizierung, Überprüfen der Zertifikatsperrliste und Kerberos-Passthrough-Authentifizierung.

NTLM-Authentifizierung (Windows NT Challenge/Response) wird standardmäßig für Computer unter Windows unterstützt.

Konfigurieren von Domänen-Passthrough-Authentifizierung

March 26, 2019

Weitere Informationen zum Konfigurieren von Domänen-Passthrough-Authentifizierung finden Sie im Knowledge Center-Artikel CTX133982.

Citrix Receiver für Windows-Installation mit Single Sign-On

Es gibt zwei Möglichkeiten, um bei der Installation von Citrix Receiver für Windows Domänen-Passthrough (SSON) zu aktivieren:

- Aktivieren über die Befehlszeile
- Aktivieren über die grafische Benutzeroberfläche

Aktivieren von Domänen-Passthrough über die Befehlszeilenschnittstelle

Aktivieren von Domänen-Passthrough (SSON) über die Befehlszeilenschnittstelle:

1. Installieren Sie Citrix Receiver 4.x mit dem Schalter **/includeSSON**.
   - Installieren Sie mindestens einen StoreFront-Store (Sie können diesen Schritt auch später ausführen). Das Installieren von StoreFront-Stores ist keine Voraussetzung für das Einrichten von Domänen-Passthrough-Authentifizierung.
   - Überprüfen Sie nach dem Neustart des Endpunkts, auf dem Citrix Receiver installiert ist, ob die Passthrough-Authentifizierung aktiviert ist, indem Sie Citrix Receiver starten und dann im Task-Manager prüfen, ob der Prozess ssonsvr.exe ausgeführt wird.

> **Hinweis**
>
> Informationen zur Syntax zum Hinzufügen von StoreFront-Stores finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.

Aktivieren von Domänen-Passthrough über die grafische Benutzeroberfläche

Aktivieren von Domänen-Passthrough über die grafische Benutzeroberfläche

1. Navigieren Sie zur Installationsdatei von Citrix Receiver für Windows (CitrixReceiver.exe).
2. Doppelklicken Sie auf **CitrixReceiver.exe**, um das Installationsprogramm zu starten.
3. Aktivieren Sie im Installationsassistenten zum Aktivieren von Single Sign-On das Kontrollkästchen “Single Sign-On aktivieren”, sodass Citrix Receiver für Windows mit aktiviertem SSON-Feature installiert wird. Diese Methode entspricht der Installation von Citrix Receiver für Windows mit der Befehlszeilenoption **/includeSSON**.

In der Abbildung unten ist das Aktivieren von Single Sign-On dargestellt:

> **Hinweis**
>
> Der Installationsassistent zum Aktivieren von Single Sign-On ist nur bei der Neuinstallation auf in Domänen eingebundenen Maschinen verfügbar.

Überprüfen Sie nach dem Neustart des Endpunkts, auf dem Citrix Receiver für Windows installiert ist, ob die Passthrough-Authentifizierung aktiviert ist, indem Sie Citrix Receiver für Windows neu starten und dann im Task-Manager prüfen, ob der Prozess **ssonsvr.exe** ausgeführt wird.

Gruppenrichtlinieneinstellungen für SSON

Mit den Informationen in diesem Abschnitt können Sie Gruppenrichtlinieneinstellungen für die SSON-Authentifizierung konfigurieren.

> **Hinweis**
>
> Der Standardwert der GPO-Richtlinieneinstellung für SSON ist **Passthrough-Authentifizierung aktivieren**.

Konfigurieren von SSON über die administrative Gruppenrichtlinienobjektvorlage

1. Öffnen Sie **gpedit.msc** und klicken Sie mit der rechten Maustaste auf **Computerkonfiguration > Administrative Vorlagen > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung**.
2. Aktivieren Sie die GPO-Einstellungen des lokalen Computers (auf der lokalen Maschine des Benutzers und/oder im "Golden Image" des VDA-Desktops):
   - Wählen Sie den lokalen Benutzernamen und das Kennwort.
   - Wählen Sie **Aktiviert**.
   - Wählen Sie **Passthrough-Authentifizierung aktivieren**.
3. Führen Sie einen Neustart des Endpunkts (auf dem Citrix Receiver für Windows installiert ist) oder des Golden Image des VDA-Desktops aus.

Verwenden einer ADM-Datei für die SSON-Gruppenrichtlinie

Verwenden Sie das folgende Verfahren zum Konfigurieren von Gruppenrichtlinieneinstellungen mit einer ADM-Datei:

1. Öffnen Sie den Editor für lokale Gruppenrichtlinien, indem Sie Folgendes auswählen: **Computerkonfiguration > Rechtsklick auf Administrative Vorlagen > Vorlagen hinzufügen/entfernen**.
2. Klicken Sie auf **Hinzufügen**, um eine ADM-Vorlage hinzuzufügen.
3. Wenn Sie die Vorlage **receiver.adm** hinzugefügt haben, erweitern Sie **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Components > Citrix Receiver > User Authentication**.
4. Öffnen Sie Internet Explorer auf der lokalen Maschine und/oder im Golden Image des VDA-Desktops.
5. Fügen Sie die vollqualifizierten Domänennamen der StoreFront-Server (ohne den Storepfad) unter **Internetoptionen > Sicherheit > Vertrauenswürdige Sites** der Liste hinzu. Beispiel: `https://storefront.example.com`

   Hinweis: Sie können den StoreFront-Server auch mit einem Microsoft-Gruppenrichtlinienobjekt den vertrauenswürdigen Sites hinzufügen. Das Gruppenrichtlinienobjekt nennt sich **Liste der Site zu Zonenzuweisungen** und ist unter **Computerkonfiguration > Administrative Vorlagen**

> Windows-Komponenten > Internet Explorer > Internetsystemsteuerung > Sicherheitsseite zu finden.

6. Melden Sie sich vom Citrix Receiver-Endpunkt ab und wieder an.

Wenn Citrix Receiver geöffnet wird und der aktuelle Benutzer an der Domäne angemeldet ist, werden die Anmeldeinformationen des Benutzers sowie die enumerierten Apps und Desktops und die Startmenüeinstellungen des Benutzers an StoreFront weitergeleitet. Wenn der Benutzer auf ein Symbol klickt, leitet Citrix Receiver die Domänenanmeldeinformationen des Benutzers an den Delivery Controller weiter und die App oder der Desktop wird geöffnet.

Vertrauen zu XML für Delivery Controller aktivieren

Verwenden Sie das folgende Verfahren zum Konfigurieren von SSON für StoreFront und das Webinterface:

1. Melden Sie sich am Delivery Controller als Administrator an.
2. Öffnen Sie Windows PowerShell (mit Administratorrechten). In PowerShell geben Sie Befehle, damit der Delivery Controller den von StoreFront gesendeten XML-Anfragen vertraut.
3. Laden Sie ggf. die Citrix Cmdlets, indem Sie **Add-PSSnapin Citrix** eingeben und die **Eingabetaste** drücken.
4. Drücken Sie die Eingabetaste.
5. Geben Sie dann **Add-PSSnapin citrix.broker.admin.v2** ein und drücken Sie die **Eingabetaste**.
6. Geben Sie **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True** ein und drücken Sie die **Eingabetaste**.
7. Schließen Sie die PowerShell.

Konfigurieren von SSON für StoreFront und das Webinterface

Konfigurieren in StoreFront

Sie konfigurieren SSON für StoreFront und das Webinterface, indem Sie Citrix Studio auf dem StoreFront-Server öffnen und **Authentifizierung -> Methoden hinzufügen/entfernen** auswählen. Wählen Sie dann **Domänen-Passthrough**.

Konfiguration des Webinterface

Sie konfigurieren SSON auf dem Webinterface, indem Sie **Citrix Webinterface-Verwaltung > XenApp Services-Sites > Authentifizierungsmethoden** auswählen und die Option **Passthrough** aktivieren.

Konfigurieren von Domänen-Passthrough-Authentifizierung mit Kerberos

January 7, 2019

Dieser Abschnitt gilt nur für Verbindungen zwischen Citrix Receiver für Windows und StoreFront, XenDesktop oder XenApp.

Citrix Receiver für Windows unterstützt Kerberos für Domänen-Passthrough-Authentifizierung in Bereitstellungen mit Smartcardverwendung. Kerberos ist eine der in der integrierten Windows-Authentifizierung (IWA) enthaltenen Authentifizierungsmethoden.

Bei aktivierter Kerberos-Authentifizierung handhabt Kerberos die Authentifizierung ohne Kennwörter für Citrix Receiver für Windows und verhindert trojaner-artige Angriffe auf das Benutzergerät, um auf die Kennwörter zuzugreifen. Benutzer melden sich mit einer beliebigen Authentifizierungsmethode am Benutzergerät an, z. B. biometrische Authentifizierungsmethoden wie ein Fingerabdrucklesegerät, und greifen ohne weitere Authentifizierung auf veröffentlichte Ressourcen zu.

Wenn Citrix Receiver für Windows, StoreFront, XenDesktop und XenApp für Smartcardauthentifizierung konfiguriert sind und ein Benutzer sich mit einer Smartcard anmeldet, handhabt Citrix Receiver für Windows die Passthrough-Authentifizierung mit Kerberos wie folgt:

1. Der Single Sign-On-Dienst von Citrix Receiver für Windows erfasst die Smartcard-PIN.
2. Citrix Receiver für Windows verwendet IWA (Kerberos) für die Authentifizierung des Benutzers bei StoreFront. StoreFront stellt Citrix Receiver für Windows Informationen zu den verfügbaren virtuellen Desktops und Apps bereit.
   Hinweis: Für diesen Schritt ist die Verwendung von Kerberos nicht erforderlich. Durch die Aktivierung von Kerberos auf Citrix Receiver für Windows wird lediglich eine weitere PIN-Eingabe vermieden. Wenn Sie die Kerberos-Authentifizierung nicht verwenden, führt Citrix Receiver für Windows mit den Smartcard-Anmeldeinformationen eine Authentifizierung bei StoreFront durch.
3. Die HDX Engine (früher als ICA-Client bezeichnet) übergibt die Smartcard-PIN an XenDesktop oder XenApp, um den Benutzer an der Windows-Sitzung anzumelden. XenDesktop oder XenApp stellen dann die angeforderten Ressourcen bereit.

Stellen Sie zur Verwendung der Kerberos-Authentifizierung bei Citrix Receiver für Windows sicher, dass für die Kerberos-Konfiguration Folgendes gilt.

- Kerberos funktioniert nur zwischen Citrix Receiver für Windows und Servern, die zu denselben oder vertrauenswürdigen Windows Server-Domänen gehören. Den Servern muss außerdem für Delegierungszwecke vertraut werden, eine Option, die Sie über das Verwaltungstool Active Directory-Benutzer und -Computer konfigurieren können.

- Kerberos muss in der Domäne und in XenDesktop und XenApp aktiviert sein. Um hohe Sicherheit und die Verwendung von Kerberos zu gewährleisten, deaktivieren Sie alle IWA-Optionen außer Kerberos.
- Kerberos-Anmeldung ist nicht verfügbar für Remotedesktopdienste-Verbindungen, die eine Standardauthentifizierung oder immer bestimmte Anmeldeinformationen verwenden oder die immer zur Eingabe des Kennworts auffordern.

Im Folgenden wird beschrieben, wie Sie Domänen-Passthrough-Authentifizierung für die häufigsten Szenarien konfigurieren. Wenn Sie von Webinterface auf StoreFront migrieren und zuvor eine benutzerdefinierte Authentifizierungslösung verwendet haben, erhalten Sie weitere Informationen von dem für Sie zuständigen Mitarbeiter des Citrix Support.

> **Warnung**
>
> Für einige der in diesem Abschnitt beschriebenen Konfigurationen muss die Registrierung bearbeitet werden. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Konfigurieren der Domänen-Passthrough-Authentifizierung mit Kerberos für die Verwendung mit Smartcards

Wenn Sie mit Smartcard-Bereitstellungen in einer XenDesktop-Umgebung nicht vertraut sind, sollten Sie die Informationen zu Smartcards unter Sichern der Bereitstellung in der XenDesktop-Dokumentation lesen, bevor Sie fortfahren.

Wenn Sie Citrix Receiver für Windows installieren, fügen Sie die folgende Befehlszeilenoption hinzu:

- /includeSSON

  Mit dieser Option wird die Single Sign-On-Komponente auf dem in die Domäne eingebundenen Computer installiert, sodass Citrix Receiver für Windows mit IWA (Kerberos) die Authentifizierung bei StoreFront durchführen kann. Die Single Sign-On-Komponente speichert die Smartcard-PIN, die dann von der HDX Engine verwendet wird, wenn sie eine Remoteverbindung zwischen Smartcard-Hardware und -Anmeldeinformationen und XenDesktop herstellt. XenDesktop wählt automatisch ein Zertifikat von der Smartcard aus und ruft die PIN von der HDX Engine ab.

  Eine verwandte Option, ENABLE_SSON, ist standardmäßig aktiviert und sollte unverändert bleiben.

Wenn eine Sicherheitsrichtlinie die Aktivierung von Single Sign-On auf einem Gerät verhindert, konfigurieren Sie Citrix Receiver für Windows mit der folgenden Richtlinie:

Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort

Hinweis: In diesem Szenario lassen Sie zu, dass die HDX Engine anstelle von Kerberos die Smartcardauthentifizierung verwendet. Verwenden Sie daher nicht die Option ENABLE_KERBEROS=Yes, mit der die HDX Engine zur Verwendung von Kerberos gezwungen wird.

Starten Sie Citrix Receiver für Windows auf dem Benutzergerät neu, um die Einstellungen zu übernehmen.

Konfigurieren von StoreFront:

- Legen Sie in der Datei default.ica auf dem StoreFront-Server DisableCtrlAltDel auf false fest. **Hinweis**: Dieser Schritt ist nicht erforderlich, wenn auf allen Clientmaschinen Citrix Receiver für Windows 4.2 oder höher ausgeführt wird.
- Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie das Kontrollkästchen Domänen-Passthrough. Mit dieser Einstellung wird die integrierte Windows-Authentifizierung aktiviert. Das Kontrollkästchen Smartcard muss nur aktiviert werden, wenn Sie auch Clients haben, die nicht in Domänen eingebunden sind und mit Smartcards eine Verbindung zu StoreFront herstellen.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

Info über FastConnect-API und HTTP Basic-Authentifizierung

Die FastConnect-API verwendet die HTTP Basic-Authentifizierungsmethode, die oft mit den für Domänenpassthrough verwendeten Authentifizierungsmethoden Kerberos und IWA verwechselt wird. Citrix empfiehlt, dass Sie IWA auf StoreFront und in der ICA-Gruppenrichtlinie deaktivieren.

Konfigurieren der Smartcardauthentifizierung

March 26, 2019

Citrix Receiver für Windows unterstützt die folgenden Features der Smartcardauthentifizierung. Weitere Informationen zur XenDesktop- und StoreFront-Konfiguration finden Sie in der Dokumentation für diese Komponenten. In diesem Abschnitt wird die Konfiguration von Citrix Receiver für Windows für Smartcards beschrieben.

- **Passthrough-Authentifizierung (Single Sign-On):** Die Passthrough-Authentifizierung erfasst Smartcard-Anmeldeinformationen, wenn sich Benutzer an Citrix Receiver für Windows anmelden. Citrix Receiver für Windows verwendet die erfassten Anmeldeinformationen wie folgt:
  - Benutzer von in Domänen eingebundenen Geräten, die sich mit Smartcard-Anmeldeinformationen an Citrix Receiver für Windows anmelden, starten virtuelle Desktops und Anwendungen ohne erneute Authentifizierung.
  - Benutzer von nicht in Domänen eingebundenen Geräten, die sich mit Smartcard-Anmeldeinformationen an Citrix Receiver für Windows anmelden, müssen zum Starten eines virtuellen Desktops oder einer Anwendung die Anmeldeinformationen erneut eingeben.

  StoreFront und Citrix Receiver für Windows müssen für die Passthrough-Authentifizierung konfiguriert werden.
- **Bimodale Authentifizierung:** Bei der bimodalen Authentifizierung können Benutzer zwischen einer Smartcard und der Eingabe des Benutzernamens und des Kennworts wählen. Dieses Feature ist nützlich, wenn die Smartcard nicht verwendet werden kann (z. B. wenn sie vom Benutzer zu Hause vergessen wurde oder das Zertifikat abgelaufen ist). Hierfür müssen dedizierte Stores pro Site eingerichtet werden, damit die Methode DisableCtrlAltDel zur Smartcardverwendung auf False festgelegt werden kann. Die bimodale Authentifizierung erfordert eine StoreFront-Konfiguration. Umfasst die Lösung NetScaler Gateway, muss auch dies konfiguriert werden.

  Die bimodale Authentifizierung ermöglicht dem StoreFront-Administrator nun außerdem das Anbieten der Authentifizierung über Benutzernamen/Kennwort und per Smartcard bei dem gleichen Store, indem er diese in der StoreFront Management Console auswählt. Weitere Informationen finden Sie in der StoreFront-Dokumentation.
- **Mehrere Zertifikate:** Mehrere Zertifikate können für eine Smartcard verfügbar sein, wenn mehrere Smartcards verwendet werden. Wenn ein Benutzer eine Smartcard in einen Kartenleser einsteckt, stehen die Zertifikate für alle Anwendungen zur Verfügung, die auf dem Benutzergerät ausgeführt werden, einschließlich Citrix Receiver für Windows. Konfigurieren Sie Citrix Receiver für Windows, um die Auswahl von Zertifikaten zu ändern.
- **Clientzertifikatauthentifizierung:** NetScaler Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
  - Für den Zugriff auf StoreFront-Ressourcen über NetScaler Gateway müssen Benutzer sich ggf. nach dem Entfernen der Smartcard neu authentifizieren.
  - Wenn die SSL-Konfiguration von NetScaler Gateway auf die verbindliche Clientzertifikatauthentifizierung eingestellt ist, ist der Betrieb sicherer. Die verbindliche Clientzertifikatauthentifizierung ist jedoch nicht mit der bimodalen Authentifizierung kompatibel.

- **Double-Hop-Sitzungen:** Wenn ein Double Hop benötigt wird, wird eine weitere Verbindung zwischen Receiver und dem virtuellen Desktop des Benutzers hergestellt. Bereitstellungen, die Double Hop unterstützen, werden in der XenDesktop-Dokumentation beschrieben.
- **Smartcard-aktivierte Anwendungen:** In smartcard-aktivierten Anwendungen, wie Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in virtuellen Desktop- oder Anwendungssitzungen verfügbar sind, digital signieren oder verschlüsseln.

Voraussetzungen:

In diesem Abschnitt wird davon ausgegangen, dass Sie mit den Smartcardabschnitten in der XenDesktop- und StoreFront-Dokumentation vertraut sind.

Einschränkungen:

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Zertifikatauswahl wird in Citrix Receiver für Windows nicht speichert, es kann jedoch die PIN gespeichert werden, wenn sie konfiguriert ist. Die PIN wird nur im nicht ausgelagerten Speicher für die Dauer der Benutzersitzung zwischengespeichert. Sie wird zu keinem Zeitpunkt auf der Festplatte gespeichert.
- Citrix Receiver für Windows verbindet keine Sitzungen wieder, wenn eine Smartcard eingesteckt wird.
- Wenn Citrix Receiver für Windows für die Smartcardauthentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung von VPN-Tunneln mit der Smartcardauthentifizierung müssen Benutzer das NetScaler Gateway Plug-In installieren und sich über eine Webseite anmelden und sich mit den Smartcards und PINs an jedem Schritt authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem NetScaler Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Die Kommunikation von Citrix Receiver für Windows Updater mit citrix.com und Merchandising Server ist nicht mit der Smartcardauthentifizierung an NetScaler Gateway kompatibel.

> **Warnung**
>
> Für einige der in diesem Abschnitt beschriebenen Konfigurationen muss die Registrierung bearbeitet werden. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Aktivieren von Single Sign-On für die Smartcardauthentifizierung

Fügen Sie zum Konfigurieren von Citrix Receiver für Windows bei der Installation die folgende Befehlszeilenoption hinzu:

- ENABLE_SSON=Yes

  Single Sign-On ist ein anderer Begriff für Passthrough-Authentifizierung. Wenn diese Einstellung aktiviert ist, zeigt Citrix Receiver für Windows keine zweite PIN-Eingabeaufforderung an.

Alternativ können Sie die Konfiguration über die folgenden Richtlinien- und Registrierungsänderungen ausführen:

- Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort
- Wenn die Single Sign-On-Komponente nicht installiert ist, legen Sie in einem der folgenden Registrierungsschlüssel die Option SSONCheckEnabled auf false fest. Der Schlüssel verhindert, dass der Authentifizierungsmanager von Citrix Receiver für Windows nach der Single Sign-On-Komponente sucht, sodass Citrix Receiver für Windows die Authentifizierung bei StoreFront durchführen kann.

  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

Alternativ können Sie die Smartcardauthentifizierung bei StoreFront anstelle von Kerberos aktivieren. Zum Aktivieren der Smartcardauthentifizierung bei StoreFront anstelle von Kerberos installieren Sie Citrix Receiver für Windows mit den unten aufgeführten Befehlszeilenoptionen. Hierfür sind Administratorprivilegien erforderlich. Der Computer muss nicht in eine Domäne eingebunden sein.

- /includeSSON installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Aktiviert das Zwischenspeichern der Anmeldeinformationen und die Verwendung der domänenbasierten Passthrough-Authentifizierung.
- Meldet sich der Benutzer beim Endpunkt mit einer anderen Authentifizierungsmethode an (z. B. über den Benutzernamen und das Kennwort), verwenden Sie folgende Befehlszeile:

  ```
  1  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  ```

  Hierdurch wird verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden, und ermöglicht, dass die PIN durch Citrix Receiver für Windows bei der Anmeldung bei Citrix Receiver für Windows gespeichert wird.
- Wechseln Sie zu Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort.

Passthrough-Authentifizierung aktivieren. Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise die Option Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen aktivieren, damit die Passthrough-Authentifizierung funktioniert.

Konfigurieren von StoreFront:

- Wenn Sie den Authentifizierungsdienst konfigurieren, aktivieren Sie das Kontrollkästchen Smartcard.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

Aktivieren der Benutzergeräte für die Smartcardverwendung

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
2. Installieren Sie die kryptografische Middleware.
3. Installieren und konfigurieren Sie Citrix Receiver für Windows.

Ändern der Zertifikatauswahl

Wenn mehrere Zertifikate gültig sind, fordert Citrix Receiver für Windows den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können Citrix Receiver für Windows auch so konfigurieren, dass das Standardzertifikat (gemäß des Smartcard-Anbieters) oder das Zertifikat mit dem spätesten Ablaufdatum verwendet wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden.

Ein gültiges Zertifikat muss die drei folgenden Merkmale haben:

- Die aktuelle Uhrzeit auf dem lokalen Computer liegt im Gültigkeitszeitraum des Zertifikats.
- Der öffentliche Schlüssel des Subjekts muss den RSA-Algorithmus verwenden und eine Schlüssellänge von 1024, 2048 oder 4096 Bits haben.
- Die Schlüsselverwendung muss digitale Signatur enthalten.
- Der alternative Name des Subjekts muss den UPN enthalten.
- Die erweiterte Schlüsselverwendung muss Smartcard-Anmeldung und Clientauthentifizierung oder alle Schlüsselverwendungen enthalten.
- Eine der Zertifizierungsstellen in der Ausstellerkette des Zertifikats muss mit einem der Distinguished Names übereinstimmen, den der Server im TLS-Handshake sendet.

Ändern Sie mit einer der folgenden Methoden, wie Zertifikate ausgewählt werden:

- Geben Sie an der Citrix Receiver für Windows-Befehlszeile die Option `AM\CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` an.

Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Citrix Receiver für Windows für SmartCardDefault oder LatestExpiry den Benutzer zur Auswahl eines Zertifikats auf.

- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKCU oder HKLM\Software\[Wow6432N hinzu: `CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }` .

  In HKCU definierte Werte haben Priorität über Werte in HKLM, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

Verwenden von CSP-PIN-Aufforderungen

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von Citrix Receiver für Windows und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Citrix Receiver für Windows fordert Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN an den Smartcard-Kryptografiedienstanbieter. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung, können Sie in Citrix Receiver für Windows konfigurieren, dass die PIN-Eingabe, einschließlich der Aufforderung für eine PIN von den CSP-Komponenten verwaltet wird.

Ändern Sie mit einer der folgenden Methoden, wie die PIN-Eingabe gehandhabt wird:

- Geben Sie an der Citrix Receiver für Windows-Befehlszeile die Option AM_SMARTCARDPINENTRY=CSP an.
- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKLM\Software\[Wow6432Node]\Citrix SmartCardPINEntry=CSP hinzu.

Überprüfen von Zertifikatsperrlisten für gesteigerte Sicherheit

November 21, 2018

Wenn die Überprüfung von Zertifikatsperrlisten (CRL) aktiviert ist, überprüft Citrix Receiver, ob das Zertifikat des Servers widerrufen wurde. Da Citrix Receiver zu einer Überprüfung gezwungen wird, wird die kryptografische Authentifizierung für den Server sowie die allgemeine Sicherheit der TLS-Verbindung zwischen einem Benutzergerät und einem Server verbessert.

Sie können für die Überprüfung der Zertifikatsperrlisten mehrere Stufen einstellen. Sie können beispielsweise Citrix Receiver so konfigurieren, dass nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft werden. Außerdem können Sie die Überprüfung der

Zertifikate so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Wenn Sie diese Änderung auf einem lokalen Computer durchführen, beenden Sie Citrix Receiver, wenn er ausgeführt wird. Vergewissern Sie sich, dass alle Citrix Receiver-Komponenten, einschließlich Connection Center, geschlossen sind.

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
   Hinweis: Wenn Sie die Citrix Receiver für Windows-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner Administrative Vorlagen aus.
3. Klicken Sie im Menü “Aktion” auf “Vorlagen hinzufügen/entfernen”.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Receiver-Konfigurationsordner (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie die Citrix Receiver für Windows-Vorlagendatei aus.
   Hinweis: Wählen Sie die Citrix Receiver für Windows-Vorlagendatei (receiver.adm oder receiver.admx/receiver.adml) entsprechend der Version des Windows-Betriebssystems aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert.
8. Wählen Sie im Dropdownmenü CRL verification eine der Optionen aus.
   - Deaktiviert: Es wird keine Überprüfung von Zertifikatsperrlisten durchgeführt.
   - Nur lokal gespeicherte CRLs prüfen: Es werden vorher heruntergeladene oder installierte Zertifikatsperrlisten für die Zertifikatüberprüfung verwendet. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen wurde.
   - CRLs für Verbindung erforderlich: Es werden lokale Zertifikatsperrlisten von relevanten Zertifikatausgabestellen im Netzwerk überprüft. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen oder nicht gefunden wurde.
   - CRLs vom Netzwerk abrufen: Zertifikatsperrlisten von relevanten Zertifikatausgabestellen werden überprüft. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen wurde. Wenn Sie “CRL verification” nicht einstellen, ist die Standardeinstellung “Nur lokal gespeicherte CRLs prüfen”.

Sichere Kommunikation

July 30, 2018

Zum Sichern der Kommunikation zwischen XenDesktop-Sites oder XenApp-Serverfarmen und Citrix Receiver für Windows können Sie Citrix Receiver für Windows-Verbindungen mit Sicherheitstechnologien wie den folgenden integrieren:

- Citrix NetScaler Gateway: Weitere Informationen finden Sie in den Themen in diesem Abschnitt und in der Dokumentation zu NetScaler Gateway und StoreFront.
  Hinweis: Citrix empfiehlt, die Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit NetScaler Gateway zu sichern.
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie Citrix Receiver für Windows 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.
- Konfiguration vertrauenswürdiger Server.
- Nur für XenApp- oder Webinterface-Bereitstellungen, gilt nicht für XenDesktop 7: Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, bzw. HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das und vom Netzwerk ein und verarbeiten Verbindungen zwischen Receiver und Servern. Receiver unterstützt die Protokolle SOCKS und Secure Proxy.
- Nur für XenApp- oder Webinterface-Bereitstellungen, gilt nicht für XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 und XenApp 7.5: SSL-Relay-Lösungen mit TLS-Protokollen (Transport Layer Security).
- Für XenApp 7.6 und XenDesktop 7.6 können Sie eine SSL-Verbindung direkt zwischen Benutzern und VDAs aktivieren.

Citrix Receiver für Windows ist kompatibel mit und funktioniert in Umgebungen, in denen die Microsoft SSLF-Desktopsicherheitsvorlagen (Specialized Security - Limited Functionality) verwendet werden. Diese Vorlagen werden auf verschiedenen Windows-Plattformen unterstützt. Informationen über die Vorlagen und dazugehörige Einstellungen finden Sie in der Microsoft-Dokumentation in den Sicherheitshinweisen für Windows.

Konfigurieren und Aktivieren von TLS

March 26, 2019

Dieses Thema gilt für XenApp- und XenDesktop-Version 7.6 und höher.

Wenn Sie ausschließlich TLS-Verschlüsselung für die Citrix Receiver für Windows-Kommunikation verwenden möchten, konfigurieren Sie das Benutzergerät, Citrix Receiver für Windows und, wenn Sie das Webinterface verwenden, den Webinterface-Server. Informationen zum Sichern der StoreFront-Kommunikation finden Sie unter Sichern in der StoreFront-Dokumentation. Weitere Informationen finden Sie in der Dokumentation zum Webinterface.

Voraussetzungen:

Benutzergeräte müssen die in den Systemanforderungen angegebenen Anforderungen erfüllen.

Diese Richtlinie ermöglicht das Konfigurieren der TLS-Optionen, sodass Citrix Receiver für Windows den Server für die Verbindung sicher identifizieren kann, und sie ermöglicht die Verschlüsselung der gesamten Kommunikation mit dem Server.

Diese Optionen ermöglichen Folgendes:

- Erzwingen der Verwendung von TLS. Citrix empfiehlt, für alle Verbindungen über nicht vertrauenswürdige Netzwerke, einschließlich für das Internet, TLS zu verwenden.
- Erzwingen der Verwendung der für FIPS (Federal Information Processing Standards) genehmigten Kryptografie und Einhalten der Empfehlungen im Dokument NIST SP 800-52. Diese Optionen sind standardmäßig deaktiviert.
- Erzwingen der Verwendung einer bestimmten Version von TLS und bestimmter TLS-Verschlüsselungssammlungen. Citrix unterstützt die Protokolle TLS 1.0, TLS 1.1 und TLS 1.2 zwischen Citrix Receiver für Windows und XenApp oder XenDesktop.
- Herstellen von Verbindungen mit bestimmten Servern.
- Überprüfen, ob das Serverzertifikat widerrufen wurde.
- Überprüfen auf eine bestimmte Serverzertifikatausstellungsrichtlinie.
- Auswählen eines bestimmten Clientzertifikats, wenn der Server für die Anforderung konfiguriert ist.

Konfigurieren der TLS-Unterstützung über die administrative Gruppenrichtlinienobjektvorlage

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
    - Um die Richtlinie auf einen einzigen Computer anzuwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
    - Um die Richtlinie auf eine Domäne anzuwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver in der Gruppenrichtlinien-Verwaltungskonsole.

2. Navigieren Sie unter dem Knoten “Computerkonfiguration” zu **Administrative Vorlagen** > **Citrix Receiver** > **Netzwerkrouting**. Wählen Sie dann die Richtlinie **Konfiguration von TLS und Konformitätsmodus**.
3. Wählen Sie **Aktiviert**, um sichere Verbindungen zu aktivieren und die Kommunikation auf dem Server zu verschlüsseln. Legen Sie folgende Optionen fest:

   > **Hinweis:** Citrix empfiehlt TLS für sichere Verbindungen.

4. Aktivieren Sie **TLS für alle Verbindungen verwenden**. Damit erzwingen Sie, dass Citrix Receiver für Windows TLS für alle Verbindungen mit veröffentlichten Anwendungen und Desktops verwendet.
5. Wählen Sie im Dropdownmenü zum **Sicherheitskonformitätsmodus** die geeignete Option aus:
   - **Ohne:** Es wird kein Konformitätsmodus erzwungen.
   - **SP800-52:** Wählen Sie **SP800-52** für Konformität mit NIST SP 800-52. Wählen Sie diese Option nur, wenn Server oder Gateway den Empfehlungen von NIST SP 800-52 entsprechen.

     Hinweis:

     Bei Auswahl von SP800-52 wird automatisch FIPS-validierte Kryptografie verwendet, selbst wenn **FIPS aktivieren** nicht ausgewählt ist. Sie müssen auch die Windows-Sicherheitsoption **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden aktivieren**. Andernfalls kann Citrix Receiver für Windows u. U. keine Verbindung zu veröffentlichten Anwendungen und Desktops herstellen.

     Wenn Sie SP800-52 auswählen, müssen Sie für die Richtlinie **Zertifikatsperrüberprüfung** die Einstellung **Volle Zugriffsprüfung** oder **Volle Zugriffsprüfung und CRL erforderlich** auswählen.

     Wenn Sie SP800-52 auswählen, überprüft Citrix Receiver für Windows, ob das Serverzertifikat den Empfehlungen in NIST SP 800-52 entspricht. Wenn dies nicht der Fall ist, kann Citrix Receiver für Windows möglicherweise keine Verbindung herstellen.
6. **FIPS aktivieren**: Wählen Sie diese Option, um die Verwendung von FIPS-validierter Kryptografie zu erzwingen. Sie müssen auch die Windows-Sicherheitsoption aus der Gruppenrichtlinie des Betriebssystems **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden** aktivieren. Andernfalls kann Citrix Receiver für Windows u. U. keine Verbindung zu veröffentlichten Anwendungen und Desktops herstellen.
7. Wählen Sie im Dropdownmenü neben **Zulässige TLS-Server** die Portnummer aus. Sie können festlegen, dass Citrix Receiver nur eine Verbindung zu den Servern herstellt, die in einer

durch Trennzeichen getrennten Liste aufgeführt sind. Sie können Platzhalter und Portnummern angeben. Beispielsweise ermöglicht *.citrix.com:4433 die Verbindung mit allen Servern auf Port 4433, deren allgemeiner Name mit .citrix.com endet. Die Genauigkeit der Informationen in einem Sicherheitszertifikat wird durch den Aussteller des Zertifikats bestätigt. Wenn Citrix Receiver den Aussteller nicht erkennt und ihm nicht traut, wird die Verbindung abgelehnt.

8. Wählen Sie im Dropdownmenü neben **TLS-Version** eine der folgenden Optionen:

   - **TLS 1.0, TLS 1.1 oder TLS 1.2**: Dies ist die Standardeinstellung. Diese Option wird nur empfohlen, wenn die Kompatibilität mit TLS 1.0 eine Geschäftsanforderung ist.
   - **TLS 1.1, TLS 1.2**: Mit dieser Option stellen Sie sicher, dass TLS 1.1 oder TLS 1.2 für ICA-Verbindungen verwendet wird.
   - **TLS 1.2**: Diese Option wird empfohlen, wenn TLS 1.2 eine Geschäftsanforderung ist.

9. **TLS-Verschlüsselungssammlung**: Um die Verwendung von bestimmten TLS-Verschlüsselungssammlungen zu erzwingen, wählen Sie “Behörden” (GOV), “Kommerziell” (COM) oder “Alle” (ALLE). Bei bestimmten NetScaler Gateway-Konfigurationen müssen Sie u. U. die Option “Kommerziell (KOM)” wählen.

   Citrix Receiver für Windows unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

   > **Hinweis:** RSA-Schlüssel mit einer Länge von 1024 Bits werden von Citrix nicht empfohlen.

   In der folgenden Tabelle sind alle unterstützten Verschlüsselungssammlungen aufgelistet.

   - **Beliebig**: Bei Verwendung der Einstellung “Beliebig” wird die Richtlinie nicht konfiguriert und jede der folgenden Verschlüsselungssammlungen ist zulässig.
     - TLS_RSA_WITH_RC4_128_MD5
     - TLS_RSA_WITH_RC4_128_SHA
     - TLS_RSA_WITH_3DES_EDE_CBC_SHA
     - TLS_RSA_WITH_AES_128_CBC_SHA
     - TLS_RSA_WITH_AES_256_CBC_SHA
     - TLS_RSA_WITH_AES_128_GCM_SHA256
     - TLS_RSA_WITH_AES_256_GCM_SHA384
   - **Kommerziell**: Bei Verwendung der Einstellung “Kommerziell’ sind nur die folgenden Verschlüsselungssammlungen zulässig:
     - TLS_RSA_WITH_RC4_128_MD5
     - TLS_RSA_WITH_RC4_128_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256

- **Behörden**: Bei Verwendung der Einstellung “Behörden” sind nur die folgenden Verschlüsselungssammlungen zulässig:
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

10. Wählen Sie im Dropdownmenü zur Richtlinie **Zertifikatsperrüberprüfung** eine der folgenden Optionen aus:
    - **Prüfung ohne Netzwerkzugriff**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Es werden nur lokale Zertifikatsperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Secure Gateway-Server vorgelegt wird, nicht obligatorisch.
    - **Volle Zugriffsprüfung**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Zielserver vorgelegt wird, nicht wichtig.
    - **Volle Zugriffsprüfung und CRL erforderlich**: Die Zertifikatsperrliste wird ohne Stamm-Zertifizierungsstelle überprüft. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
    - **Volle Zugriffsprüfung und alle CRL erforderlich**: Die Zertifikatsperrliste und die Stamm-Zertifizierungsstelle werden überprüft. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
    - **Keine Prüfung**: Es wird keine Überprüfung der Zertifikatsperrliste durchgeführt.
11. Mit der **Richtlinienerweiterungs-OID** können Sie Citrix Receiver für Windows auf Verbindungen mit Servern beschränken, auf denen eine bestimmte Zertifikatausstellungsrichtlinie festgelegt ist. Wenn Sie **Richtlinienerweiterungs-OID** auswählen, akzeptiert Citrix Receiver für Windows nur Serverzertifikate mit Richtlinienerweiterungs-OID.

12. Wählen Sie im Dropdownmenü zur **Clientauthentifizierung** eine der folgenden Optionen aus:
    - **Deaktiviert**: Die Clientauthentifizierung ist deaktiviert.
    - **Zertifikatauswähler anzeigen**: Der Benutzer wird immer aufgefordert, ein Zertifikat auszuwählen.
    - **Wenn möglich automatisch auswählen**: Die Aufforderung wird nur angezeigt, wenn mehrere Zertifikate zur Identifizierung ausgewählt werden können.
    - **Nicht konfiguriert**: Gibt an, dass die Clientauthentifizierung nicht konfiguriert ist.
    - **Angegebenes Zertifikat verwenden**: Verwenden Sie das unter “Clientzertifikat” festgelegte Clientzertifikat.
13. Geben Sie mit der Einstellung **Clientzertifikat** den Fingerabdruck des identifizierenden Zertifikats an, damit Benutzer nicht unnötig aufgefordert werden.
14. Klicken Sie auf **Anwenden** und auf **OK**, um die Richtlinie zu speichern.

Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

TLS-Verschli	**GOV**	**COM**	**ALLE**	**GOV**	**COM**	**ALLE**	**GOV**	**COM**	**ALLE**
FIPS aktivieren	Aus	Aus	Aus	Ein	Ein	Ein	Ein	Ein	Ein
Sicherh SP800-52	Aus	Aus	Aus	Aus	Aus	Aus	Ein	Ein	Ein
TLS_ECDH	XE_RSA_WITH_AES_	X256_GCM	X_SHA384			X			
TLS_ECI	X		X	X		X			
TLS_RSA_	XWITH_AES_256_GC	M_SHA384	X			X	X		X
TLS_RSA	X	X	X	X	X	X	X	X	X
TLS_RSA_	XWITH_AES_256_CB	C_SHA256	X			X			
TLS_RSA	X		X	X		X	X		X
TLS_RSA_WITH_AES	_128_CB	C_SHA		X	X		X	X	
TLS_RSA		X	X						
TLS_RSA_WITH_RC	4_128_MD	5							
TLS_RSA	X		X	X		X	X		X

Konfigurieren der Smartcardauthentifizierung für das Webinterface 5.4

November 21, 2018

Wenn Citrix Receiver für Windows mit einer SSON-Komponente installiert wurde, ist die Passthrough-Authentifizierung standardmäßig aktiviert, selbst wenn die Passthrough-Authentifizierung mit PIN für Smartcards nicht in der XenApp PNAgent-Site aktiviert ist. Die Passthrough-Einstellung für Authentifizierungsmethoden ist nicht mehr gültig. In der Abbildung unten ist dargestellt, wie Smartcard als Authentifizierungsmethode aktiviert wird, wenn Citrix Receiver für Windows ordnungsgemäß mit SSON konfiguriert ist.

Weitere Informationen finden Sie unter How to Manually install and configure Citrix Receiver for Pass-through Authentication.

Verwenden Sie die Richtlinie für das Entfernen von Smartcards, um das Verhalten beim Entfernen einer Smartcard zu steuern, wenn sich ein Benutzer bei der Citrix Webinterface 5.4 PNAgent-Site authentifiziert.

Wenn diese Richtlinie aktiviert ist, wird der Benutzer von der XenApp-Sitzung abgemeldet, wenn die Smartcard aus dem Clientgerät entfernt wird. Der Benutzer ist jedoch weiterhin bei Citrix Receiver für Windows angemeldet.

Damit diese Richtlinie wirksam wird, muss die Richtlinie für das Entfernen von Smartcards in der Webinterface XenApp Services-Site festgelegt werden. Die Einstellungen sind auf Webinterface 5.4 unter **XenApp Services Site > Pass-through with smart card > Enable Roaming > Logoff the sessions when smart card removed**.
Wenn die Richtlinie für das Entfernen der Smartcard deaktiviert ist, wird die XenApp-Sitzung des Benutzers getrennt, wenn der Benutzer die Smartcard aus dem Clientgerät entfernt. Das Entfernen der Smartcard aus der Webinterface XenApp Services-Site hat keine Auswirkungen.
Hinweis: Es gibt unterschiedliche Richtlinien für 32-Bit- und 64-Bit-Clients. Der Richtlinienname für 32-Bit-Geräte ist **Smartcard-Entfernungsrichtlinie (32-Bit-Maschine)**, und der Richtlinienname für 64-Bit-Geräte ist **Smartcard-Entfernungsrichtlinie (64-Bit-Maschine)**.

Änderungen bei der Unterstützung und Entfernung von Smartcards

Berücksichtigen Sie Folgendes, wenn Sie eine Verbindung mit einer XenApp 6.5 PNAgent-Site herstellen:

- Ab Citrix Receiver für Windows 4.5 wird die Anmeldung per Smartcard für Anmeldungen an PNAgent-Sites unterstützt.
- Die Smartcard-Entfernungsrichtlinie hat sich auf der PNAgent-Site geändert:
  Eine XenApp-Sitzung wird abgemeldet, wenn die Smartcard entfernt wird. Wenn Smartcard

als Authentifizierungsmethode für die PNAgent-Site konfiguriert ist, muss die entsprechende Richtlinie in Citrix Receiver für Windows konfiguriert sein, damit das Abmelden der XenApp-Sitzung erzwungen werden kann. Aktivieren Sie das Roaming für die Smartcardauthentifizierung in der XenApp PNAgent-Site und aktivieren Sie die Richtlinie für das Entfernen von Smartcards, durch die XenApp von der Receiver-Sitzung abgemeldet wird. Der Benutzer bleibt an der Receiver-Sitzung angemeldet.

Bekanntes Problem

Wenn ein Benutzer sich an der PNAgent-Site per Smartcardauthentifizierung anmeldet, wird der Benutzername als **Angemeldet** angezeigt.

Verbinden mit Secure Gateway

July 30, 2018

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Secure Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen Citrix Receiver für Windows und dem Server bereitzustellen. Eine Citrix Receiver für Windows-Konfiguration ist nicht erforderlich, wenn Sie Secure Gateway im Normalmodus verwenden und Benutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Secure Gateway-Servern verwendet Citrix Receiver für Windows Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Weitere Informationen zur Konfiguration der Einstellungen für den Proxyserver für Citrix Receiver für Windows finden Sie in den Abschnitten über das Webinterface.

Informationen zum Konfigurieren der Proxyservereinstellungen finden Sie in der Dokumentation für das Webinterface.

Wenn Secure Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Secure Gateway Proxy im Relaymodus verwenden.

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

- Vollqualifizierter Domänenname (FQDN) des Secure Gateway-Servers.
- Portnummer des Secure Gateway-Servers. Der Relaymodus wird von Secure 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 im Allgemeinen als Domänenname bezeichnet.

Herstellen einer Verbindung durch eine Firewall

March 26, 2019

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss Citrix Receiver für Windows über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können.

Allgemeine Citrix Kommunikationsports

Quelle	Typ	Port	Details
Citrix Receiver	TCP	80/443	Kommunikation mit StoreFront
ICA/HDX	TCP	1494	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX mit Sitzungszuverlässigkeit	TCP	2598	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX über SSL	TCP	443	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX von HTML5 Receiver	TCP	8008	Zugriff auf Anwendungen und virtuelle Desktops
ICA/HDX Audio über UDP	TCP	16500-16509	Portbereich für ICA/HDX Audio

Quelle	Typ	Port	Details
IMA	TCP	2512	Independent Management Architecture (IMA)
Managementkonsole	TCP	2513	Hinweis für Citrix Managementkonsolen und *WCF-Dienste: Für FMA-basierte Plattformen ab Version 7.5 und höher wird Port 2513 NICHT verwendet.
Anwendungs-/Desktopanforderung	TCP	80/8080/443	XML-Dienst
STA	TCP	80/8080/443	Secure Ticketing Authority (im XML-Dienst eingebettet)

> **Hinweis**
>
> In XenApp 6.5 wird Port 2513 vom XenApp Command Remoting Dienst über WCF verwendet.

Wenn die Firewall für die Netzwerkadressenübersetzung konfiguriert ist, verwenden, können Sie im Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports definieren. Beispiel: Wenn XenApp Server oder XenDesktop Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface Receiver eine alternative Adresse bereitstellen. Citrix Receiver für Windows stellt dann über die externe Adresse und die Portnummer eine Verbindung mit dem Server her. Weitere Informationen finden Sie in der Dokumentation unter Webinterface.

Herstellen von Verbindungen über Proxyserver

July 30, 2018

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und Verbindungen zwischen Citrix Receiver für Windows und Servern gehandhabt. Citrix Receiver für Windows unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit der Serverfarm verwendet Receiver die Einstellungen für den Proxyserver, die remote auf dem Receiver für Web- oder Webinterface-Server konfiguriert wurden. Informationen zur Proxyserverkonfiguration finden Sie in der StoreFront- oder Webinterface-Dokumentation.

Für die Kommunikation mit dem Webserver verwendet Receiver die Einstellungen für den Proxyserver, die über die Internetoptionen des Standardwebbrowsers auf dem Benutzergerät konfiguriert wurden. Sie müssen die Internetoptionen des Standardwebbrowsers auf dem Benutzergerät entsprechend konfigurieren.

Konfigurieren Sie die Proxyeinstellungen mit dem Registrierungs-Editor, um zu erzwingen, dass Citrix Receiver für Windows den Proxyserver für Verbindungen verwendet oder ihn ignoriert.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können.

1. Navigieren Sie zu HKLM\Software\Citrix\AuthManager.\
2. Definieren Sie **ProxyEnabled** (REG_SZ).
    a) True: Gibt an, dass Citrix Receiver für Windows den Proxyserver bei Verbindungen berücksichtigt.
    b) False: Gibt an, dass Citrix Receiver für Windows den Proxyserver bei Verbindungen ignoriert.
3. Schließen Sie den Registrierungs-Editor.
4. Starten Sie die Citrix Receiver für Windows-Sitzung neu, um die Änderungen zu übernehmen.

Durchsetzen von Vertrauensbeziehungen

November 21, 2018

Die Konfiguration mit vertrauenswürdigen Servern dient dazu, Vertrauensbeziehungen bei Citrix Receiver für Windows-Verbindungen zu identifizieren und durchzusetzen.

Wenn Sie dieses Feature aktivieren, legt Citrix Receiver für Windows die Anforderungen für vertrauenswürdige Server fest und entscheidet, ob die Verbindung zum Server als vertrauenswürdig angesehen werden kann. Beispiel: Ein Citrix Receiver für Windows, der eine Verbindung zu einer bestimmten Adresse herstellt (wie `https://*.citrix.com`) und dabei einen bestimmten Verbindungstyp verwendet (wie TLS), wird an eine vertrauenswürdige Zone auf dem Server weitergeleitet.

Wenn Sie dieses Feature aktivieren, befindet sich der verbundene Server in der Zone vertrauenswürdiger Sites von Windows. Eine Anleitung, wie Sie Server der Zone vertrauenswürdiger Sites von Windows hinzufügen, finden Sie in der Onlinehilfe von Internet Explorer.

Aktivieren der vertrauenswürdigen Serverkonfiguration über die administrative Gruppenrichtlinienobjektvorlage

Voraussetzung:

Beenden Sie alle Citrix Receiver für Windows-Komponenten, einschließlich des Connection Centers.

1. Öffnen Sie als Administrator die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver, indem Sie gpedit.msc ausführen.
   a) Um die Richtlinie auf einen einzigen Computer anzuwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver im Startmenü.
   b) Um die Richtlinie auf eine Domäne anzuwenden, starten Sie die administrative Gruppenrichtlinienobjektvorlage von Citrix Receiver in der Gruppenrichtlinien-Verwaltungskonsole.
2. Erweitern Sie den Knoten "Computerkonfiguration" und navigieren Sie zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Receiver** > **Netzwerkrouting** > **Vertrauenswürdige Serverkonfiguration konfigurieren**.
3. Wählen Sie **Aktiviert**, um das Durchführen einer Regionsidentifizierung in Citrix Receiver für Windows durchzusetzen.
4. Wählen Sie **Vertrauenswürdige Serverkonfiguration erzwingen**. Der Client muss dann die Identifizierung mit einem vertrauenswürdigen Server durchführen.
5. Wählen Sie im Dropdownmenü zu **Windows-Internetzone** die Client-Serveradresse aus. Diese Einstellung gilt nur für die Zone vertrauenswürdiger Sites von Windows.
6. Legen Sie im Feld **Adresse** die Client-Serveradresse für die Zone vertrauenswürdiger Sites außer Windows fest. Sie können eine durch Trennzeichen getrennte Liste verwenden.
7. Klicken Sie auf **OK** und **Übernehmen**.

Erhöhte Rechte und wfcrun32.exe

November 21, 2018

Wenn die Benutzerkontensteuerung auf Geräten unter Windows 10, Windows 8 oder Windows 7 aktiviert ist, können nur Prozesse, die dieselben erhöhten Rechte bzw. Integritätsebene wie wfcrun32.exe haben, virtuelle Anwendungen starten.

Beispiel 1:

Wenn wfcrun32.exe als Standardbenutzer (keine Rechteanhebung) ausgeführt wird, müssen andere Prozesse, u. a. Receiver, als Standardbenutzer ausgeführt werden, um Anwendungen über wfcrun32.exe zu starten.

Beispiel 2:

Wenn wfcrun32.exe mit erhöhten Rechten ausgeführt wird, können andere Prozesse, u. a. Receiver, Connection Center und Anwendungen von Drittherstellern, die das ICA-Clientobjekt verwenden, die ohne erhöhte Rechte ausgeführt werden, nicht mit wfcrun32.exe kommunizieren.

ICA-Dateisignierung: Schutz vor dem Starten von Anwendungen oder Desktops von nicht vertrauenswürdigen Servern

November 21, 2018

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface und Verwendung von administrativen Vorlagen.

Die ICA-Dateisignierung hilft, Benutzer vor unautorisierten Anwendungs- oder Desktopstarts zu schützen. Citrix Receiver für Windows prüft, ob eine vertrauenswürdige Quelle die Anwendung oder den Desktop gestartet hat und verhindert basierend auf administrativen Richtlinien das Starten von Ressourcen auf nicht vertrauenswürdigen Servern. Sie können die Citrix Receiver für Windows-Sicherheitsrichtlinie für die Prüfung der Signatur beim Anwendungs- oder Desktopstart mit Gruppenrichtlinienobjekten, StoreFront oder Citrix Merchandising Server konfigurieren. Die ICA-Dateisignierung ist in der Standardeinstellung nicht aktiviert. Informationen zum Aktivieren der ICA-Dateisignierung für StoreFront finden Sie in der StoreFront-Dokumentation.

In Webinterface-Bereitstellungen ermöglicht und konfiguriert das Webinterface mit dem Citrix ICA-Dateisignierungsdienst, dass beim Start von Anwendungen und Desktops eine Signatur eingeschlossen wird. Der Dienst kann ICA-Dateien mit einem Zertifikat des lokalen Zertifikatspeichers des Computers signieren.

Citrix Merchandising Server mit Citrix Receiver für Windows aktiviert und konfiguriert das Prüfen der Signatur beim Start mit dem Assistenten Citrix Merchandising Server Administrator Console > Deliveries und fügt vertrauenswürdige Zertifikatfingerabdrücke hinzu.

Aktivieren und Konfigurieren der Prüfung der Signatur beim Anwendungs- oder Desktopstart mit Gruppenrichtlinienobjekten:

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.

Hinweis: Wenn Sie die Vorlage ica-file-signing.adm bereits dem Gruppenrichtlinien-Editor hinzugefügt haben, können Sie die Schritte 2 bis 5 überspringen.

2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner Administrative Vorlagen aus.
3. Klicken Sie im Menü “Aktion” auf “Vorlagen hinzufügen/entfernen”.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Citrix Receiver für Windows-Konfigurationsordner (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie ica-file-signing.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Components > Citrix Receiver und dann auf Enable ICA File Signing.
7. Wenn Sie Enabled wählen, können Sie Fingerabdrücke von Signaturzertifikaten der Positivliste der vertrauenswürdigen Zertifikatfingerabdrücke hinzufügen, oder Sie können auf Show klicken und auf dem Bildschirm Show Contents Fingerabdrücke von Signaturzertifikaten aus der Positivliste entfernen. Sie können die Fingerabdrücke von Signaturzertifikaten von den Eigenschaften des Signaturzertifikats kopieren und einfügen. Klicken Sie in der Dropdownliste Policy auf Only allow signed launches (more secure) oder Prompt user on unsigned launches (less secure).

Option	Beschreibung
Nur signierte Starts zulassen (sicherer)	Nur richtig signierte Anwendungs- oder Desktopstarts von einem vertrauenswürdigen Server sind zulässig. Dem Benutzer wird eine Sicherheitswarnung im Citrix Receiver für Windows angezeigt, wenn eine gestartete Anwendung oder ein Desktop eine ungültige Signatur haben. Der Benutzer kann nicht weiterarbeiten, und der nicht autorisierte Start wird blockiert.
Benutzer bei nicht signierten Starts auffordern (weniger sicher)	Bei jedem versuchten Start einer nicht signierten oder falsch signierten Anwendung oder eines Desktops wird dem Benutzer eine Aufforderung angezeigt. Der Benutzer kann den Anwendungsstart fortsetzen oder ihn abbrechen (Standardeinstellung).

Auswählen und Verteilen eines digitalen Signaturzertifikats

Bei der Auswahl eines digitalen Signaturzertifikats empfiehlt Citrix eine Auswahl aus dieser Prioritätsliste:

1. Erwerben Sie ein codesigniertes Zertifikat oder ein SSL-Signaturzertifikat einer öffentlichen Zertifizierungsstelle.
2. Wenn Ihr Unternehmen eine private Zertifizierungsstelle hat, erstellen Sie ein codesigniertes oder SSL-Signaturzertifikat mit der privaten Zertifizierungsstelle.
3. Verwenden Sie ein vorhandenes SSL-Zertifikat, z. B. das Webinterface-Serverzertifikat.
4. Erstellen Sie ein neues Stammzertifikat der Zertifizierungsstelle und verteilen es mit einem Gruppenrichtlinienobjekt oder einer manuellen Installation auf die Benutzergeräte.

Citrix Receiver für Windows - Hilfe

July 30, 2018

Info über Citrix Receiver

July 30, 2018

Citrix Receiver bietet Zugriff auf virtuelle Desktops und Apps von einem beliebigen Gerät, damit Sie an jedem beliebigen Ort arbeiten können. Receiver ist sicher, leicht zu bedienen und geräteübergreifend konsistent.

Hinweis: Der Administrator gibt Ihnen möglicherweise nicht den Zugriff auf alle Features, die in diesen Abschnitten beschrieben werden.

Hinzufügen von Konten oder Wechseln von Servern

July 30, 2018

Wenn Ihr Helpdesk Sie bittet, ein Konto hinzuzufügen oder ein anderes NetScaler Gateway zu verwenden, führen Sie diese Schritte aus.

Hinzufügen eines Citrix Receiver für Windows-Kontos

1. Klicken Sie auf der Citrix Receiver für Windows-Homepage auf das Pfeil-nach-unten-Symbol und klicken Sie dann auf **Konten**.
2. Klicken Sie im Fenster “Konto hinzufügen” auf **Hinzufügen** und geben Sie die Informationen ein, die Ihnen der Helpdesk gegeben hat.

Verwenden eines anderen NetScaler Gateways

Ihr Unternehmen verwendet möglicherweise einen NetScaler Gateway zum Überprüfen Ihrer Identität.

1. Klicken Sie mit der rechten Maustaste auf das Symbol für Citrix Receiver für Windows und klicken Sie dann auf **Info**.
2. Wählen Sie im Menü **NetScaler Gateway** einen Server aus.

Ändern von Aussehen und Funktionsweise von Desktops

January 7, 2019

Ihr virtueller Desktop wird in einem Fenster angezeigt. Verwenden Sie die Schaltflächen auf der Symbolleiste des Fensters, um den Desktop zu verschieben und die Größe anzupassen und um zu steuern, wie Sie auf Dateien und Geräte zugreifen. Oben im Fenster oder auf dem Bildschirm (wenn das Fenster maximiert ist), wird ein kleiner Ziehpunkt angezeigt. Klicken Sie auf den Ziehpunkt, um die Symbolleiste anzuzeigen.

Verschieben der Symbolleiste auf dem Bildschirm

Sie können die Symbolleiste an eine geeignete Stelle verschieben, sodass der Inhalt anderer Fenster oder Steuerelemente nicht verdeckt wird.

- Klicken Sie auf den Ziehpunkt der Symbolleiste, der oben auf dem Bildschirm oder am Fenster angezeigt wird, und verschieben Sie sie nach links oder rechts.

Steuern des Zugriffs auf lokale Dateien

Ein virtueller Desktop muss ggf. Dateien auf dem lokalen Computer zugreifen. Sie können diesen Zugriff steuern.

- Klicken Sie auf der Symbolleiste auf **Einstellungen** > **Dateizugriff**, wählen Sie eine der folgenden Optionen und klicken Sie dann auf OK:

Option	Beschreibung
Lese-/Schreibrechte	Virtueller Desktop hat Lese- und Schreibrechte für die lokalen Dateien.
Leserechte	Virtueller Desktop hat nur Leserechte für die lokalen Dateien.
Kein Zugriff	Virtueller Desktop hat keinen Zugriff auf lokale Dateien.
Immer fragen	Bei jedem Zugriff des virtuellen Desktops auf lokale Dateien wird eine Aufforderung angezeigt.

Einrichten eines Mikrofons oder einer Webcam

Führen Sie diese Schritte aus, wenn Sie ändern möchten, wie Ihr virtueller Desktop auf ein lokales Mikrofon oder eine Webcam zugreift.

- Klicken Sie auf der Symbolleiste auf **Einstellungen** > **Verbindungen** und wählen Sie eine der folgenden Optionen:

Option	Beschreibung
Automatisch verbinden	Mikrofon oder Webcam können auf dem virtuellen Desktop verwendet werden.
Nicht verbinden	Mikrofon oder Webcam können auf dem virtuellen Desktop nicht verwendet werden.
Fragen	Bei jedem Zugriff des virtuellen Desktops auf das Mikrofon oder die Webcam wird eine Aufforderung angezeigt.

1. Wählen Sie in **Globale Einstellungen** die **Bevorzugte Webcam**.
2. Klicken Sie auf OK.

Einschränkung:

- Das Dialogfeld “Bevorzugte Webcam” wird im Citrix Connection Center angezeigt, auch wenn die Windows Media-Umleitungsrichtlinie im Desktop Delivery Controller auf **Deaktiviert** fest-

gelegt ist.

Anzeigen Ihrer Geräte in Desktop Viewer

January 7, 2019

Citrix Receiver für Windows erkennt die an Ihren Computer angeschlossenen Geräte und ermöglicht Ihnen die Auswahl der Geräte zur Verwendung mit dem gehosteten Desktop und den gehosteten Anwendungen.

Mit den Einstellungen in **Einstellungen > Verbindungen** können Sie anpassen, welche Geräte, z. B. Mikrofone und Webcams, mit der virtuellen Sitzung verbunden werden.

- Mit der lokalen Maschine verbundene Geräte werden in der Geräteliste unter Einstellungen > Geräte angezeigt.
- Wenn Sie eine Verbindung mit einem Gerät hergestellt haben und es wird nicht in der Liste angezeigt, klicken Sie auf Aktualisieren.
- Verbundene Geräte werden als **Optimiert**, **Von Richtlinie eingeschränkt** oder **Allgemein** angezeigt.

Geräte	Beschreibung
Optimiert	Das Gerät hat einen virtuellen Citrix Kanal und ist automatisch in der Remotesitzung und auf der lokalen Maschine gleichzeitig verfügbar. In der Spalte “Aktuelle Verbindung” für optimierte Geräte wird angezeigt, dass das Gerät auf der lokalen Maschine und in der Remotesitzung verbunden ist. Das Kontrollkästchen “Umleiten” ist aktiviert und kann nicht bearbeitet werden. Mit der Schaltfläche zum Wechseln in der Spalte “Virtueller Kanal” können Sie zwischen “Optimiert” und “Allgemein” wechseln. Wählen Sie beispielsweise “Zu allgemein wechseln”, wenn der virtuelle Kanal nicht die volle Funktionalität des Geräts unterstützt.

Geräte	Beschreibung
Generisch	Das Gerät hat keinen virtuellen Citrix Kanal und kann nicht auf der lokalen Maschine und in der Remotesitzung gleichzeitig verwendet werden. Mit dem Kontrollkästchen “Umleiten” können Sie die Verfügbarkeit des Geräts in der Remotesitzung oder auf der lokalen Maschine aktivieren und dazwischen wechseln. Der aktuelle Verbindungsstatus wird in der Spalte “Aktuelle Verbindung”angezeigt.
Von Richtlinie eingeschränkt	Der Administrator hat eine Richtlinie festgelegt, um diesen Gerätetyp einzuschränken. Beispielsweise sind USB-Mäuse und -Tastaturen in der Regel durch Richtlinien eingeschränkt, da ihr Verhalten in der Remotesitzung automatisch ohne USB-Unterstützung gehandhabt wird. Andere Geräte, wie Netzwerkgeräte, können aus Sicherheitsgründen eingeschränkt sein. In der Spalte “Aktuelle Verbindung” für von Richtlinien eingeschränkte Geräte wird nur Lokale Maschine angezeigt. Sie können das Kontrollkästchen “Umleiten” nicht für von Richtlinien eingeschränkte Geräte aktivieren.

Verwalten von Kennwörtern

November 21, 2018

Citrix Single Sign-On verwaltet die Informationen, die Sie zum Anmelden an kennwortgeschützten Programmen und Websites benötigen. Die Benutzerinformationen werden auf einem Server gespeichert, auf den Sie von jedem Computer im Unternehmen zugreifen können, auf dem Single Sign-On ausgeführt wird. Das heißt, Sie können auf eigene Programme und Einstellungen zugreifen und von verschiedenen Standorten aus arbeiten.

Single Sign-On automatisiert nicht nur die Anmeldung sondern spart auch Zeit, da Sie sich für das Zurücksetzen der Kennwörter oder für das Entsperren des Kontos nicht mehr an den Helpdesk wen-

den müssen. Single Sign-On kann sogar sehr sichere Kennwörter für Sie erstellen.

Abhängig von der Single Sign-On-Konfiguration im Unternehmen wird das Programm gestartet, wenn Sie sich am Computer anmelden oder das erste kennwortgeschützte Programm oder die kennwortgeschützte Website öffnen. Zu diesem Zeitpunkt stellt Single Sign-On eine Verbindung mit dem Server her, auf dem die Benutzerinformationen gespeichert sind, und bestätigt Ihre Identität. Sie werden dann an allen Programmen oder Websites angemeldet, für für die Anmeldeinformationen gespeichert sind. Sie werden auch aufgefordert, die Anmeldeinformationen hinzuzufügen, wenn Sie Programme oder Websites öffnen, für die momentan keine Anmeldeinformationen gespeichert sind.

Abhängig von der Single Sign-On-Konfiguration im Unternehmen können Sie das Programm vom **Startmenü** aus öffnen.

- Klicken Sie im **Startmenü** auf **Alle Programme > Citrix > Citrix Single Sign-On**.

Single Sign-On nur wird heruntergefahren, wenn Sie Citrix Receiver für Windows beenden. Sie können Single Sign-On jedoch anhalten, ohne das Programm zu beenden.

Wichtig: Single Sign-On ist ein flexibles Programm, das genau für die speziellen Bedürfnisse von Unternehmen konfiguriert werden kann. Nicht alle beschriebenen Features stehen allen Benutzern zur Verfügung. Die Verfügbarkeit von Features wird vom Unternehmen festgelegt. Manchmal stehen ganze Aufgaben, wie z. B. das Anzeigen der Kennwörter, nicht zur Verfügung. Auch die für eine Aufgabe beschriebenen Schritte können sich leicht unterscheiden. Es wurde versucht, auf diese Unterschiede hinzuweisen, Sie werden möglicherweise noch andere finden. In diesen Situationen finden Sie weitere Informationen in der Citrix-Dokumentation.

Verwenden des Konto-Self-Service

July 30, 2018

Wenn das Feature im Unternehmen verwendet wird, können Sie mit dem Konto-Self-Service-Feature in Single Sign-On Folgendes ausführen:

- Entsperren des Windows-Kontos, wenn Sie eine Meldung erhalten, dass das Konto gesperrt ist.
- Zurücksetzen des Kennworts für das Windows-Konto, wenn Sie das Kennwort vergessen haben und sich nicht am Computer anmelden können.

Die Schaltfläche “Konto-Self-Service” steht auf dem Bildschirm **Benutzer wechseln** (für Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2) oder in den Dialogfeldern **Anmeldung an Windows** und **Computer entsperren** (für andere unterstützte Windows-Betriebssysteme). Wenn Sie auf diese Schaltfläche klicken, wird der Assistent für den Konto-Self-Service gestartet.

Mit dem Konto-Self-Service können Sie jetzt diese Probleme selbst beheben und müssen sich nicht an den Helpdesk wenden.

Wichtig: Bei der Verwendung des Konto-Self-Service müssen Sie Ihre Identität bestätigen und die Antworten auf Ihre Single Sign-On-Sicherheitsfragen eingeben. Wenden Sie sich an den Helpdesk, wenn Sie die Antworten auf die Sicherheitsfragen nicht wissen. Der Helpdesk kann das Windows-Konto entsperren oder setzt Ihr Windows-Kennwort zurück.

Entsperren des Kontos (Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2)

1. Drücken Sie Strg+Alt+Entf.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf der Willkommenseite auf **Benutzer wechseln**.
     Das Dialogfeld "Benutzer wechseln" wird angezeigt.
   - Klicken Sie auf der Willkommenseite auf **Andere Anmeldeinformationen**.
     Das Dialogfeld "Benutzer wechseln" wird angezeigt.
3. Klicken Sie auf **Konto-Self-Service**. Das Dialogfeld "Konto-Self-Service" wird angezeigt.
4. Klicken Sie unter dem Konto-Self-Service-Titel auf **Klicken Sie hier, um das Kennwort zurückzusetzen oder die Kontosperrung aufzuheben**, um den Assistenten für den Konto-Self-Service zu starten.
5. Klicken Sie auf der Seite **Willkommen beim Assistenten für den Konto-Self-Service** auf **Sperrung des Kontos aufheben** und klicken Sie dann auf **Weiter**.
6. Stellen Sie auf der Seite **Konto angeben** sicher, dass der Benutzername und die Domäne richtig sind, und klicken Sie auf **Weiter**. Die Seite **Sperrung des Kontos aufheben** wird angezeigt.
7. Klicken Sie auf der Seite **Sperrung des Kontos aufheben** auf **Weiter**, um die erste Sicherheitsfrage anzuzeigen.
8. Geben Sie im Feld **Antwort** die Antwort auf die erste Frage ein und klicken Sie auf **Weiter**. Wenn weitere Sicherheitsfragen erstellt wurden, wird die nächste Frage angezeigt.
9. Wiederholen Sie Schritt 8, bis die Seite **Sperrung des Kontos aufheben** angezeigt wird.
10. Klicken Sie auf der Seite **Sperrung des Kontos** auf **Weiter**.
11. Klicken Sie auf der Seite **Kontosperrung wurde aufgehoben** auf **Fertig stellen**.

Zurücksetzen des Kennworts für das Windows-Konto (Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2)

1. Drücken Sie Strg+Alt+Entf.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf der Willkommenseite auf **Benutzer wechseln**.
     Das Dialogfeld "Benutzer wechseln" wird angezeigt.

- Klicken Sie auf der Willkommenseite auf **Andere Anmeldeinformationen**.
  Das Dialogfeld "Benutzer wechseln" wird angezeigt.

3. Klicken Sie auf **Konto-Self-Service**. Das Dialogfeld "Konto-Self-Service" wird angezeigt.
4. Klicken Sie unter dem Konto-Self-Service-Titel auf **Klicken Sie hier, um das Kennwort zurückzusetzen oder die Kontosperrung aufzuheben**, um den Assistenten für den Konto-Self-Service zu starten.
5. Klicken Sie auf der Seite **Willkommen beim Assistenten für den Konto-Self-Service** auf **Kennwort zurücksetzen** und klicken Sie dann auf **Weiter**.
6. Stellen Sie auf der Seite **Konto angeben** sicher, dass der Benutzername und die Domäne richtig sind, und klicken Sie auf **Weiter**. Die Seite **Konto zurücksetzen** wird angezeigt.
7. Klicken Sie auf der Seite **Konto zurücksetzen** auf **Weiter**, um die erste Sicherheitsfrage anzuzeigen.
8. Geben Sie im Feld **Antwort** die Antwort auf die erste Frage ein und klicken Sie auf **Weiter**.
9. Wiederholen Sie Schritt 8, bis die Seite **Neues Kennwort eingeben** angezeigt wird.
10. Geben Sie auf der Seite **Neues Kennwort eingeben** das Kennwort ein, bestätigen Sie die Eingabe und klicken Sie dann auf **Weiter**.
11. Klicken Sie auf der Seite **Die Kennwortänderung war erfolgreich** auf **Fertig stellen**. Die Seite "Konto-Self-Service" wird angezeigt, auf der Sie das Konto auswählen und sich anmelden können.

Entsperren des Kontos (gilt nicht für Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2)

1. Führen Sie einen der folgenden Schritte aus:
   - Drücken Sie im Dialogfeld **Willkommen bei Windows** STRG+ALT+ENTF und klicken Sie ggf. auf **Optionen**.
   - Drücken Sie im Dialogfeld **Computer ist gesperrt** STRG+ALT+ENTF und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Konto-Self-Service**, um den Assistenten für den Konto-Self-Service zu starten.
3. Klicken Sie auf der Seite **Willkommen beim Assistenten für den Konto-Self-Service** auf **Sperrung des Kontos aufheben** und klicken Sie dann auf **Weiter**.
4. Stellen Sie auf der Seite **Konto angeben** sicher, dass der Benutzername und die Domäne richtig sind, und klicken Sie auf **Weiter**. Die Seite **Sperrung des Kontos aufheben** wird angezeigt.
5. Klicken Sie auf der Seite **Sperrung des Kontos aufheben** auf **Weiter**, um die erste Sicherheitsfrage anzuzeigen.
6. Geben Sie im Feld **Antwort** die Antwort auf die erste Frage ein und klicken Sie auf **Weiter**. Wenn weitere Sicherheitsfragen erstellt wurden, wird die nächste Frage angezeigt.
7. Wiederholen Sie Schritt 6, bis die Seite **Sperrung des Kontos aufheben** angezeigt wird.
8. Klicken Sie auf der Seite **Sperrung des Kontos** auf **Weiter**.

9. Klicken Sie auf der Seite **Kontosperrung wurde aufgehoben** auf **Fertig stellen**.

Zurücksetzen des Kennworts für das Windows-Konto (gilt nicht für Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2)

1. Führen Sie einen der folgenden Schritte aus:
   - Drücken Sie im Dialogfeld **Willkommen bei Windows** STRG+ALT+ENTF und klicken Sie ggf. auf **Optionen**.
   - Drücken Sie im Dialogfeld **Computer ist gesperrt** STRG+ALT+ENTF und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Konto-Self-Service**, um den Assistenten für den Konto-Self-Service zu starten.
3. Klicken Sie auf der Seite **Willkommen beim Assistenten für den Konto-Self-Service** auf **Kennwort zurücksetzen** und klicken Sie dann auf **Weiter**.
4. Stellen Sie auf der Seite **Konto angeben** sicher, dass der Benutzername und die Domäne richtig sind, und klicken Sie auf **Weiter**. Die Seite **Konto zurücksetzen** wird angezeigt.
5. Klicken Sie auf der Seite **Konto zurücksetzen** auf **Weiter**, um die erste Sicherheitsfrage anzuzeigen.
6. Geben Sie im Feld **Antwort** die Antwort auf die erste Frage ein und klicken Sie auf **Weiter**.
7. Wiederholen Sie Schritt 6, bis die Seite **Neues Kennwort eingeben** angezeigt wird.
8. Geben Sie auf der Seite **Neues Kennwort eingeben** das Kennwort ein, bestätigen Sie die Eingabe und klicken Sie dann auf **Weiter**.
9. Klicken Sie auf der Seite **Die Kennwortänderung war erfolgreich** auf **Fertig stellen**.

Manuelles Ändern des Kennworts

July 30, 2018

1. Folgen Sie den Anweisungen für das Programm oder für die Website und ändern Sie das Kennwort.
2. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
3. Wählen Sie im Fenster “Kennwörter verwalten” das gewünschte Programm oder die Website aus und klicken Sie auf **Bearbeiten**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein,

wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

4. Wählen Sie im Feld **Kennwort** den aktuellen Inhalt aus und geben Sie dasselbe Kennwort wie in Schritt 1 ein.
5. Klicken Sie auf **OK**. Das neue Kennwort wird in Single Sign-On gespeichert.

Häufig gestellte Fragen und Probleme

July 30, 2018

Im Anschluss finden Sie eine Liste von Fragen und Problemen, auf die Sie möglicherweise beim Arbeiten mit Single Sign-On stoßen.

Ich wurde in einer Fehlermeldung über den baldigen Ablauf des Kennworts benachrichtigt

Informationen werden am besten gesichert, wenn Sie das Kennwort regelmäßig ändern. Abhängig von der Konfiguration im Unternehmen erinnert Sie Single Sign-On, wenn die Kennwörter zu lange verwendet wurden.

Sie erhalten diese Meldungen, bis Sie das Kennwort ändern.

Ich möchte Single Sign-On vorübergehend anhalten

Manchmal möchten Sie Single Sign-On ggf. nicht ausführen. Sie müssen z. B. an einer Anmeldeseite arbeiten, ohne dass Sie von Single Sign-On am Programm angemeldet werden.

Verwenden Sie in diesen Situationen das Feature “Anhalten” von Single Sign-On. Mit “Anhalten” beenden Sie die automatische Anmeldung, Single Sign-On bleibt jedoch geöffnet und kann von Ihnen verwendet werden.

Das Programm hat mein neues Kennwort abgelehnt

Sie haben das Kennwort für ein bestimmtes Programm mit dem Assistenten für Kennwortänderungen geändert, wenn Sie sich jedoch am Programm anmelden, wird das neue Kennwort vom Programm als ungültig abgelehnt.

Wahrscheinlich wurde das neue Kennwort in Single Sign-On gespeichert, jedoch nicht vom Programm akzeptiert. Daher sendet Single Sign-On ein falsches Kennwort.

Beheben Sie das Problem mit dem Feature “Altes Kennwort wiederherstellen”, wenn dieses Feature im Unternehmen den Benutzern zur Verfügung gestellt wird.

Hinweis: Sollte dieses Feature nicht verfügbar sein, wenden Sie sich an den Helpdesk.

Wiederherstellen des alten Kennworts für ein Programm

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster “Kennwörter verwalten” das gewünschte Programm oder die Website aus und klicken Sie auf **Bearbeiten**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

   Ein Dialogfeld mit den Eigenschaften des ausgewählten Programms wird angezeigt.
3. Klicken Sie auf **Altes Kennwort wiederherstellen** und bestätigen Sie die Aktion durch Klicken auf **Ja**.

Ich habe keinen Zugriff auf meine Benutzerdaten

Bei der Anmeldung am Computer stellt Single Sign-On eine Verbindung mit dem Server her, auf dem das Unternehmen die Single Sign-On-Benutzerinformationen speichert. Wenn die Verbindung erfolgreich hergestellt und Ihre Identität bestätigt wird, startet Single Sign-On.

Wenn das Herstellen der Verbindung oder das Prüfen der Identität nicht erfolgreich ist, wird Single Sign-On nicht gestartet und Sie erhalten eine Fehlermeldung, dass der Zugriff auf die Benutzerdaten nicht möglich war. Wenden Sie sich in diesen Situationen an den Helpdesk.

Mein Webbrowser funktioniert nicht mit Single Sign-On

Single Sign-On unterstützt nur die Verwendung von Microsoft Internet Explorer. Wenn Sie andere Webbrowser verwenden, erhalten Sie möglicherweise nicht die gewünschten Ergebnisse.

Nach dem Abmelden meldet Single Sign-On mich erneut an

Wenn Sie sich manchmal von einem kennwortgeschützten Programm oder einer Website abmelden, geht das Programm auf das Anmeldedialogfeld zurück. Abhängig von der Single Sign-On-Konfiguration im Unternehmen reagiert das Programm auf die Anmeldeseite und meldet Sie wieder am Programm an.

Sie umgehen das Problem wie folgt:

- Verwenden Sie das Feature “Anhalten” von Single Sign-On (falls im Unternehmen verfügbar), bevor Sie sich abmelden.
- Wenn “Anhalten” nicht verfügbar ist, melden Sie sich vom Programm ab und schließen Sie schnell das Programmfenster, bevor Single Sign-On Sie erneut anmelden kann.

Hinweis: Wenden Sie sich an den Helpdesk und erklären Sie das Problem. Schlagen Sie vor, dass der Single Sign-On-Administrator in den erweiterten Einstellungen der Anwendungsdefinition **Nur die erste Anmeldung für diese Anwendung verarbeiten** aktiviert.

Welche vorbereitenden Aufgaben muss ich für die Offlinearbeit ausführen?

Wenn Single Sign-On auf dem Computer installiert ist und nicht auf einem Server im Unternehmensnetzwerk ausgeführt wird, sollten Sie die Lizenz aktualisieren, bevor Sie offline arbeiten. Dies stellt sicher, dass Sie den ganzen Zeitraum für die Lizenzgültigkeit zur Verfügung haben, bevor Sie wieder eine Verbindung mit dem Unternehmensnetzwerk herstellen.

Aktualisieren der Single Sign-On-Lizenz

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

2. Klicken Sie auf **Info**.

   Das Dialogfeld **Info über Citrix Single Sign-On** wird angezeigt.

3. Klicken Sie auf **Lizenz aktualisieren**.

4. Klicken Sie auf **OK**.

Das Dialogfeld **Info über Citrix Single Sign-On** wird geschlossen.

Warum sperrt Single Sign-On die Arbeitsstation?

Single Sign-On sperrt die Arbeitsstation, wenn Sie eine Aufgabe ausführen, die ein höheres Sicherheitsniveau erfordert. Zu diesen Aufgaben kann das Ändern oder Anzeigen von Kennwörtern gehören.

Nach der Sperrung der Arbeitsstation prüft Single Sign-On ihre Identität mit dem eingegebenen Kennwort für das Konto. Manchmal müssen Sie sogar die Sicherheitsfragen beantworten. Mit dieser Verifizierung verhindert Single Sign-On, dass andere Personen auf vertrauliche Daten zugreifen.

Dies ist manchmal ärgerlich, dient aber dem Schutz der persönlichen und Unternehmensdaten.

Automatisches Ändern des Kennworts

July 30, 2018

Der Assistent für Kennwortänderungen automatisiert das Ändern der Kennwörter für angegebene Programme. Abhängig von der Single Sign-On-Konfiguration im Unternehmen können Sie ein eigenes Kennwort erstellen oder Single Sign-On erstellt ein Kennwort für Sie.

Hinweis: Da die vom Assistenten für Kennwortänderungen erstellten Kennwörter aus einer willkürlichen Anordnung von Buchstaben, Ziffern und anderen Zeichen bestehen, ist die Sicherheit dieser Kennwörter sehr hoch. Da die Kennwörter von Single Sign-On verwaltet werden, und Sie sich die Kennwörter nicht merken müssen, sollten Sie die Verwendung dieses Features erwägen.

Abhängig von der Konfiguration im Unternehmen wird der Assistent für Kennwortänderungen folgendermaßen gestartet:

- Wenn das Programm angibt, dass das Kennwort geändert werden muss.
- Wenn Sie das Verfahren zur Kennwortänderung des Programms starten.

Manchmal erkennt Single Sign-On die Kennwortänderung nicht, und der Assistent für Kennwortänderungen wird nicht gestartet. In diesen Situationen müssen Sie das Kennwort sowohl auf der Website oder im Programm als auch in Single Sign-On manuell ändern, um sicherzustellen, dass die Kennwörter übereinstimmen.

Auswählen der Erstellungsmethode für das neue Kennwort

Wenn das Unternehmen das Feature zur Verfügung stellt, können Sie im Assistenten für Kennwortänderungen auf der Seite **Erstellungsmethode für das neue Kennwort** wählen, wie das neue Kennwort erstellt wird. Es gibt folgende Optionen:

- **Systemgeneriertes Kennwort auswählen**

  Wenn Sie diese Option auswählen und auf **Weiter** klicken, erstellt der Assistent für Kennwortänderungen ein sehr sicheres Kennwort. Dieses Kennwort wird Ihnen nicht beim Erstellen angezeigt, da es in Single Sign-On gespeichert ist und Sie das Kennwort nicht kennen müssen. Wenn das Unternehmen die Option in Single Sign-On aktiviert hat, können Sie das Kennwort anzeigen, wenn Sie den Assistenten beendet haben.

  Hinweis: Da die vom Assistenten für Kennwortänderungen erstellten Kennwörter aus einer willkürlichen Anordnung von Buchstaben, Ziffern und anderen Zeichen bestehen, ist die Sicherheit dieser Kennwörter sehr hoch. Da die Kennwörter von Single Sign-On verwaltet werden, und Sie sich die Kennwörter nicht merken müssen, sollten Sie die Verwendung dieses Features erwägen.

- **Erstellen eines eigenen Kennworts**

  Wenn Sie diese Option auswählen und auf **Weiter** klicken, können Sie im Assistenten für Kennwortänderungen ein eigenes Kennwort erstellen und senden. Dieses Kennwort muss die im Unternehmen geltenden Kennwortrichtlinien hinsichtlich Länge, Komplexität und anderen Faktoren einhalten, die sich auf die Sicherheit auswirken können.

Warten auf Bestätigung

Die Seite **Warten auf Bestätigung** im Assistenten für Kennwortänderungen wird angezeigt, während der Assistent ermittelt, ob die Kennwortänderung erfolgreich war oder fehlgeschlagen ist.

Wenn Sie erkennen, dass die Kennwortänderung erfolgreich war, bevor der Assistent für Kennwortänderungen die Seite **Warten auf Bestätigung** schließt, klicken Sie auf **Überspringen**, um auf die Seite **Kennwortänderung bestätigen** zu gehen.

Bestätigen eines geänderten Kennworts

Abhängig von der Konfiguration im Unternehmen wird die Seite **Kennwortänderung bestätigen** im Assistenten für Kennwortänderungen angezeigt. Wenn die Seite angezeigt wird, müssen Sie feststellen, ob die Kennwortänderung erfolgreich war. Drei Optionen stehen zur Verfügung.

Ja:

Wenn das Dialogfeld zum Zurücksetzen des Programmkennworts nicht oder eine Erfolgsmeldung angezeigt wird, war die Kennwortänderung erfolgreich.

Wählen Sie **Ja** und klicken Sie auf **Weiter**, um dem Assistenten für Kennwortänderungen anzugeben, dass die Kennwortänderung erfolgreich war. Der Assistent wird beendet.

Nein:

Wenn das Dialogfeld zum Zurücksetzen des Programmkennworts oder eine Fehlermeldung angezeigt wird, war die Kennwortänderung nicht erfolgreich.

Wählen Sie **Nein** und klicken Sie auf **Weiter**, um dem Assistenten für Kennwortänderungen anzugeben, dass das Programm das neue Kennwort nicht akzeptiert hat. Der Assistent wird ohne Ändern des Kennwortes beendet.

Unbekannt:

Bei Auswahl von **Unbekannt** und Klicken auf **Weiter** wird eine Seite angezeigt, auf der beschrieben wird, wie Sie ermitteln, ob das Kennwort erfolgreich geändert wurde.

Wenn Sie ein eigenes Kennwort erstellt haben, können Sie feststellen, ob der Assistent erfolgreich war, wenn Sie Single Sign-On anhalten und sich mit dem neuen Kennwort am Programm anmelden.

Hinweis: Sie müssen das Dialogfeld des Assistenten für Kennwortänderungen ggf. verschieben, um zu sehen, ob das Dialogfeld zum Zurücksetzen des Programmkennworts oder anderes kennwortbezogenes Feedback angezeigt wird.

Bestätigen eines nicht geänderten Kennworts

Die Seite **Kennwort wurde nicht geändert** wird angezeigt, wenn der Assistent für Kennwortänderungen erkennt, dass die Kennwortänderung nicht erfolgreich war, oder Sie **Nein** auf der Seite **Kennwortänderung bestätigen** gewählt haben.

Auf der Seite **Kennwort wurde nicht geändert** stehen zwei Optionen zur Verfügung:

- Anderes Kennwort versuchen

  Verwenden Sie diese Option, wenn das Kennwortänderungsformular des Programms noch geöffnet ist. Wenn Sie die Option nach dem Schließen des Formulars verwenden, stimmen die Kennwörter im Programm und in Single Sign-On ggf. nicht überein.

  Wenn Sie **Anderes Kennwort versuchen** wählen und auf **Weiter** klicken, können Sie ein anderes Kennwort an das Programm senden. Abhängig von der Einrichtung des Assistenten für Kennwortänderungen im Unternehmen geschieht Folgendes:

  - Die Seite **Auswählen der Erstellungsmethode für das neue Kennwort** wird angezeigt. Sie können zwischen einem systemgenerierten oder einem eigenen Kennwort wählen.
  - Die Seite **Eigenes Kennwort erstellen** wird angezeigt.
  - Ein systemgeneriertes Kennwort wird erstellt und gesendet. Der Assistent für Kennwortänderungen versucht dann zu bestätigen, dass die Kennwortänderung erfolgreich war.

- Assistenten ohne weitere Aktion beenden

  Bei der Auswahl von **Assistenten ohne weitere Aktion beenden** wird nicht länger versucht, das Kennwort des Programms zu ändern. Sie können den Assistenten für Kennwortänderungen neu starten und es zu einem späteren Zeitpunkt erneut versuchen.

Assistenten ohne weitere Aktion beenden

Die Seite **Kennwort wurde nicht geändert** des Assistenten für Kennwortänderungen wird angezeigt, wenn das Ändern des Kennworts fehlgeschlagen ist, oder Sie auf der Seite **Kennwortänderung bestätigen** auf **Nein** geklickt haben.

Wenn der Assistent für Kennwortänderungen fehlgeschlagen ist, versuchen Sie das Kennwort folgendermaßen zu ändern:

- Klicken Sie auf der Seite **Kennwort wurde nicht geändert** auf **Fertig stellen**, um den Assistenten zu beenden. Starten Sie den Assistenten dann neu.
- Ändern Sie das Kennwort manuell im Programm und in Single Sign-On.
- Wenden Sie sich an den Helpdesk.

Beenden des Assistenten nach einer erfolgreichen Kennwortänderung

Die Seite **Kennwort wurde geändert** wird angezeigt, wenn der Assistent für Kennwortänderungen erkennt, dass die Kennwortänderung erfolgreich war, oder Sie auf der Seite **Kennwortänderung bestätigen** auf **Ja** geklickt haben.

Das neue Kennwort ist jetzt vom Programm akzeptiert und wird in Single Sign-On gespeichert.

Prüfen der Akzeptanz des neuen Kennworts vom Programm

Bei Auswahl von **Unbekannt** und Klicken auf **Weiter** auf der Seite **Kennwortänderung bestätigen** wird eine Seite angezeigt, auf der beschrieben wird, wie Sie ermitteln, ob das Kennwort erfolgreich geändert wurde.

Sie können feststellen, ob der Assistent erfolgreich war, wenn Sie Single Sign-On anhalten und sich mit dem neuen Kennwort am Programm anmelden.

Wenn Sie auf dieser Seite auf **Weiter** klicken, wird die Seite **Kennwortänderung bestätigen** erneut angezeigt.

Erstellen eines eigenen Kennworts

Im Assistenten für Kennwortänderungen wird die Seite **Eigenes Kennwort erstellen** angezeigt, wenn Sie auf der Seite **Auswählen der Erstellungsmethode für das neue Kennwort** die Option **Eigenes Kennwort erstellen** wählen. Diese Seite wird nur angezeigt, wenn Sie eigene Kennwörter erstellen können.

Um einen Schreibfehler beim Kennwort zu vermeiden, müssen Sie das Kennwort in die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** eingeben. Der Assistent für Kennwortänderungen sagt

Ihnen, wenn die Kennwörter nicht übereinstimmen. Wenn die Kennwörter übereinstimmen, steht die Schaltfläche **Weiter** zur Verfügung.

Der Assistent für Kennwortänderungen stellt sicher, dass Sie die Kennwortrichtlinien des Unternehmens einhalten. Beispiele für Unternehmensrichtlinien sind:

- Altes Kennwort darf nicht wiederholt werden.
- Kennwörter müssen aus Ziffern und Buchstaben bestehen.
- Kennwörter dürfen bestimmte Zeichen nicht enthalten.
- Kennwörter müssen eine bestimmte Länge haben.

Anhalten und Fortsetzen von Single Sign-On

July 30, 2018

Manchmal möchten Sie Single Sign-On ggf. vorübergehend anhalten. Gründe für das Anhalten können u. a. sein:

- Arbeiten an Anmeldeseiten ohne Anmeldung am Programm oder an der Website
- Arbeiten im Internet ohne Aufforderung zum Speichern der Anmeldeinformationen, wenn Single Sign-On ein Anmeldeformular erkennt

“Anhalten” unterscheidet sich von “Beenden”, da Single Sign-On und die Features weiterhin ausgeführt werden und verfügbar sind. Sie werden jedoch nicht automatisch an kennwortgeschützten Programmen oder Websites angemeldet und Sie werden nicht zum Speichern neuer Anmeldeinformationen aufgefordert. Sie können Single Sign-On schnell fortsetzen, wenn Sie das Programm wieder verwenden möchten.

Anhalten von Single Sign-On

- Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Single Sign-On anhalten**.

Überprüfen, ob Single Sign-On angehalten wurde

- Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Einstellungen**, um den Status des Citrix Single Sign-On Plug-ins im Fenster “Citrix Receiver - Einstellungen” anzuzeigen.

Fortsetzen von Single Sign-On

- Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Single Sign-On fortsetzen**.

Gruppieren von Programmen in einer Kennwortgruppe

July 30, 2018

Der Administrator erstellt Kennwortgruppen. Wenn ein Programm zu einer Kennwortgruppe gehört, entspricht das Kennwort für dieses Programm dem Kennwort für alle anderen Programme in der Gruppe. Sie können dann das Kennwort für alle Programme in der Gruppe auf einmal aktualisieren.

Beispiel: Wenn der Administrator eine Kennwortgruppe erstellt hat, zu der die E-Mail-, Buchhaltungs-, Textverarbeitungs-, Datenerfassungs- und Personalverwaltungsanwendungen gehören, können Sie das Kennwort einmal ändern, und dieses Kennwort wird dann für die ganze Gruppe aktualisiert.

Wenn Sie zwei verschiedene Benutzernamen für ein Programm in einer Kennwortgruppe verwenden, benötigen Sie ggf. auch zwei unterschiedliche Kennwörter. Sie können die Anmeldeinformationen mit dem unterschiedlichen Kennwort aus der Kennwortgruppe entfernen. Aktualisierungen der Anmeldeinformationen haben dann keine Auswirkung mehr auf die anderen für Programme in der Gruppe gespeicherten Kennwörter.

Ändern des Kennworts einer Kennwortgruppe

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster “Kennwörter verwalten” das gewünschte Programm oder die Website aus und klicken Sie auf **Bearbeiten**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

   Wenn das Programm zu einer Kennwortgruppe gehört, enthält das Eigenschaften-Dialogfeld den Link **Kennwort für diese Kennwortgruppe ändern**.
3. Klicken Sie auf **Kennwort für diese Kennwortgruppe ändern** und folgen Sie den Anweisungen im Assistenten.

So heben Sie die Zuordnung eines Programms zu einer Kennwortgruppe auf

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster "Kennwörter verwalten" das gewünschte Programm oder die Website aus und klicken Sie auf **Bearbeiten**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

   Wenn das Programm zu einer Kennwortgruppe gehört, enthält das angezeigte Dialogfeld den Link **Zuordnung dieser Anmeldeinformationen zur Kennwortgruppe aufheben**.
3. Klicken Sie auf **Die Zuordnung dieser Anmeldeinfo zur Kennwortgruppe aufheben** und folgen Sie den Anweisungen im Assistenten.

Speichern von Benutzernamen und Kennwörtern

July 30, 2018

Wenn das Unternehmen das Feature aktiviert hat, erkennt Single Sign-On automatisch, wenn Sie kennwortgeschützte Websites oder Programme öffnen. Single Sign-On meldet Sie automatisch am Programm an, wenn Sie den Benutzernamen, das Kennwort oder andere Anmeldeinformationen gespeichert haben.

Wenn Sie eine kennwortgeschützte Website öffnen oder ein kennwortgeschütztes Programm starten, für die noch keine Anmeldeinformationen gespeichert sind, können Sie die Anmeldeinformationen mit den folgenden Methoden in Single Sign-On speichern, abhängig von den Features, die das Unternehmen bereitgestellt hat:

- Wenn Single Sign-On erkennt, dass Sie eine kennwortgeschützte Website geöffnet oder ein kennwortgeschütztes Programm gestartet haben, wird automatisch ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie diese Informationen speichern möchten.
- Wenn Single Sign-On das Programm nicht erkennt, können Sie die Anmeldeinformationen manuell hinzufügen.

Single Sign-On speichert Anmeldeinformationen von folgenden Programmen:

- **Windows-basierte Programme**: Diese Programme werden normalerweise vom Startmenü oder vom Desktop aus gestartet. Lotus Notes ist ein Beispiel.
- **Webbasierte Programme oder Sites**: Dies sind Programme oder Sites, die Sie mit einem Webbrowser anzeigen oder starten. Beispiele sind Internetläden und webbasierte Schulungsprogramme.

  Wichtig: Single Sign-On unterstützt nur Microsoft Internet Explorer (32-Bit-Version) als Webbrowser.
- **Terminalemulator-basierte Programme:** Dies sind die textbasierten Programme, die normalerweise für einen Terminalemulator-Computer gelten. Diese Programmfenster haben oft eine dunkle Hintergrundfarbe, z. B. Grün, und eine hellere Schattierung der Farbe wird für den Text verwendet.

Hinweis: Die erforderlichen Anmeldeinformationen hängen vom Programm ab. Meistens müssen Sie einen Benutzernamen oder eine ID und ein Kennwort eingeben. Wenn Sie nach Angaben gefragt werden, die Sie nicht wissen, wenden Sie sich an den Helpdesk des Unternehmens.

Automatisches Speichern von Anmeldeinformationen

1. Öffnen Sie eine kennwortgeschützte Website oder starten Sie ein kennwortgeschütztes Programm. Das Anmeldedialogfeld der Website oder des Programms wird angezeigt.
2. Klicken Sie im Dialogfeld, in dem Sie gefragt werden, ob Single Sign-On die Anmeldeinformationen für die Website oder das Programm speichern soll, auf **Speichern**.
3. Wenn Sie Ihre Anmeldeinformationen für eine Website oder ein webbasiertes Programm speichern, werden die Felder und Schaltflächen im Anmeldefenster der Website markiert, mit denen die Anmeldeinformationen gesendet werden. Klicken Sie angezeigten im Dialogfeld auf **Ja**, wenn die richtigen Felder und Schaltflächen markiert sind.
4. Geben Sie im Dialogfeld **Neue Anmeldung** die Anmeldeinformationen ein und klicken Sie auf **Fertig stellen**. Das Dialogfeld **Neue Anmeldung** wird geschlossen, die Anmeldeinformationen werden von Single Sign-On gespeichert, und Sie werden am Programm angemeldet.

Manuelles Speichern von Anmeldeinformationen

1. Öffnen Sie eine kennwortgeschützte Website oder starten Sie ein kennwortgeschütztes Programm. Das Anmeldedialogfeld der Website oder des Programms wird angezeigt.
2. Wenn kein Dialogfeld angezeigt wird, in dem Sie gefragt werden, ob Single Sign-On Ihr Kennwort für diese Website oder dieses Programm speichern soll, fordern Sie Single Sign-On auf, das manuelle Speichern der Anmeldeinformationen zu ermöglichen. Klicken Sie im Microsoft

Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und wählen Sie **Kennwörter > Kennwort senden**.

Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

3. Klicken Sie im Dialogfeld, in dem Sie gefragt werden, ob Single Sign-On die Anmeldeinformationen für die Website oder das Programm speichern soll, auf **Speichern**.
4. Wenn Sie Ihre Anmeldeinformationen für eine Website oder ein webbasiertes Programm speichern, werden die Felder und Schaltflächen im Anmeldefenster der Website markiert, mit denen die Anmeldeinformationen gesendet werden. Klicken Sie angezeigten im Dialogfeld auf **Ja**, wenn die richtigen Felder und Schaltflächen markiert sind.
5. Geben Sie im Dialogfeld **Neue Anmeldung** die Anmeldeinformationen ein und klicken Sie auf **Fertig stellen**. Das Dialogfeld **Neue Anmeldung** wird geschlossen, die Anmeldeinformationen werden von Single Sign-On gespeichert, und Sie werden am Programm angemeldet.

Speichern mehrerer Benutzernamen und Kennwörter für eine Anwendung

Manchmal haben Sie mehrere Konten für ein Programm oder eine Website. Beispiel:

- Sie haben Zugriffsrechte auf das allgemeine E-Mail-Konto Ihres Unternehmens, das Zugriffsrechte genannt wird, und auf Ihr eigenes E-Mail-Konto.
- Sie müssen Materialien für zwei Projekte kaufen und haben auf der Website des Lieferanten getrennte Konten für jedes Projekt.

Wenn das Mehrkontenfeature von Single Sign-On im Unternehmen verwendet wird, können Sie mehrere Kontoinformationen für dasselbe Programm oder dieselbe Website speichern. Nach dem Speichern der Informationen für diese Konten können Sie in der Anmeldungsauswahl von Single Sign-On auswählen, welche Anmeldeinformationen Sie für die Anmeldung verwenden möchten.

Hinzufügen weiterer Kennwörter für bereits in Single Sign-On gespeicherte Programme und Websites

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster “Kennwörter verwalten” das Programm oder die Website aus, für das bzw. die Sie weitere Anmeldeinformationen hinzufügen möchten.

3. Klicken Sie auf **Kopieren**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

   Ein weiterer Eintrag für das Programm oder die Website wird in der Liste angezeigt.

4. Markieren Sie den neuen Eintrag und klicken auf **Bearbeiten**. Ein Dialogfeld mit den Anmeldeinformationen für das Programm oder die Website wird angezeigt.
5. Ändern Sie die Anmeldeinformationen entsprechend.
6. Ändern Sie im Feld **Anwendungsname** den Namen des Programms oder der Website, damit Sie diesen Eintrag von dem anderen Eintrag für das Programm unterscheiden können.
7. Klicken Sie auf **OK**.

Anmelden mit mehreren Konten

Wenn Sie mehrere Konten für ein Programm oder eine Website haben, startet Single Sign-On die Anmeldungsauswahl, damit Sie das Konto für die Anmeldung auswählen können.

Anmelden an einem Programm oder einer Website, für das bzw. für die mehrere Konten in Single Sign-On gespeichert sind

1. Starten Sie das Programm oder die Website. Das Dialogfeld **Anmeldungsauswahl** und die Anmeldeseite des Programms werden angezeigt.
2. Klicken Sie im Dialogfeld **Anmeldungsauswahl** auf das entsprechende Anmeldekonto und klicken Sie dann auf **OK**. Das Dialogfeld **Anmeldungsauswahl** wird geschlossen, und Single Sign-On meldet Sie am Programm oder der Website an.

Registrieren von Antworten auf Sicherheitsfragen

July 30, 2018

1. Klicken Sie auf der Seite **Willkommen bei der Registrierung der Sicherheitsfragen** auf **Weiter**, um die erste Sicherheitsfrage anzuzeigen.
2. Geben Sie im Feld **Antwort** die Antwort auf die erste Sicherheitsfrage ein. Abhängig von den Einstellungen im Unternehmen wird die Antwort bei der Eingabe möglicherweise als Punkte angezeigt. Sie müssen die Antwort dann erneut im Feld **Antwort bestätigen** eingeben.

Hinweis: Bei den Antworten auf die Fragen wird die Groß- und Kleinschreibung erkannt. Wenn Sie bei der Registrierung der Antworten Großbuchstaben verwenden, müssen Sie auch bei der Prüfung der Identität Großbuchstaben verwenden. Wenn Sie einen Punkt bei der Registrierung verwenden, z. B. wenn Sie als Lieblingslehrer Ms. Shestack angeben, müssen Sie den Punkt auch bei der Identitätsprüfung verwenden.

3. Klicken Sie auf **Weiter**. Wenn weitere Sicherheitsfragen erstellt wurden, wird die nächste Frage angezeigt.
4. Wiederholen Sie die Schritte 2 und 3, bis die Seite **Antworten senden** angezeigt wird.
5. Klicken Sie auf der Seite **Antworten senden** auf **Weiter**.
6. Klicken Sie auf der Seite **Registrierung der Sicherheitsfragen erfolgreich** auf **Fertig stellen**. Die Antworten auf die Sicherheitsfragen werden gespeichert.

Entfernen von Benutzernamen und Kennwörtern

July 30, 2018

In diesem Abschnitt wird beschrieben, wie Sie von Single Sign-On gespeicherte Kennwörter entfernen. Receiver kann die Kennwörter auch speichern, wenn Sie bei der Anmeldung **Kennwort speichern** wählen. Wen Sie das Kennwort von Receiver entfernen möchten, klicken Sie mit der rechten Maustaste auf das Receiver-Symbol und klicken Sie dann auf **Info** aus; erweitern Sie **Erweitert** und klicken Sie auf **Kennwörter löschen**.

Gelegentlich möchten Sie sicherlich Anmeldeinformationen von Single Sign-On entfernen. Beispiel:

- Sie haben mehrere Konten für ein Programm oder eine Website gespeichert, benötigen jedoch nicht mehr alle Konten.
- Sie haben Informationen für Programme oder Websites gespeichert, die Sie nicht mehr verwenden.

Wichtig: Wenn Sie Anmeldeinformationen entfernen, die Sie noch verwenden, werden Sie nicht automatisch von Single Sign-On an diesem Programm oder dieser Website angemeldet. Sie werden zur Speicherung dieser Informationen aufgefordert, wenn Sie das Programm das nächste Mal starten.

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster “Kennwörter verwalten” das gewünschte Programm oder die Website aus und klicken Sie auf **Entfernen**.

Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

In einem Dialogfeld müssen Sie die Löschung der Anmeldeinformationen für das ausgewählte Programm bestätigen.

3. Klicken Sie auf **Ja**. Die Anmeldeinformationen werden von Single Sign-On entfernt und nicht mehr im Fenster "Kennwörter verwalten" angezeigt.

   Hinweis: Wenn Sie das Programm oder die Website wieder öffnen, werden Sie gefragt, ob Sie die Anmeldeinformationen speichern möchten.

Anzeigen des Kennworts

July 30, 2018

Wenn das Unternehmen dieses Feature zur Verfügung stellt, können Sie in Single Sign-On Ihre Kennwörter anzeigen.

Hinweis: Vom Unternehmen wurden möglicherweise bestimmte Kennwörter angegeben, die nicht angezeigt werden können.

Achtung: Stellen Sie sicher, dass keine andere Person die Kennwörter kennt. Sonst sind Ihre Konten und die Unternehmenssysteme gefährdet.

1. Klicken Sie im Microsoft Windows-Infobereich (normalerweise ganz rechts auf der Taskleiste) mit der rechten Maustaste auf das Citrix Receiver-Symbol und klicken Sie dann auf **Kennwörter > Kennwörter verwalten**.
2. Wählen Sie im Fenster "Kennwörter verwalten" das gewünschte Programm oder die Website aus und klicken Sie auf **Kennwort anzeigen**.

   Hinweis: Möglicherweise hat das Unternehmen an dieser Stelle eine Identitätsüberprüfung festgelegt. Geben Sie in diesem Fall Ihren Windows-Benutzernamen und das Kennwort ein, wenn Sie dazu aufgefordert werden. (Wenn Sie sich mit einer Smartcard oder anderen Authentifizierungsmethode anmelden, für die kein Benutzername und Kennwort benötigt wird, prüfen Sie hiermit Ihre Identität, wenn Sie dazu aufgefordert werden.)

   In einem neuen Dialogfeld wird das Kennwort für das ausgewählte Programm angezeigt.
3. Klicken Sie auf **OK**, um das Dialogfeld mit dem Programmkennwort zu schließen.

Ersteinrichtung von Citrix Single Sign-On

July 30, 2018

Abhängig von der Citrix Single Sign-On-Konfiguration im Unternehmen wird das Programm automatisch gestartet, wenn Sie sich am Computer anmelden oder das erste kennwortgeschützte Programm oder die kennwortgeschützte Website öffnen.

Wenn Single Sign-On so konfiguriert ist, dass Sie bei der Erstausführung Informationen eingeben müssen, werden Sie ggf. zum Beantworten der Sicherheitsfragen aufgefordert, z. B. “Wie hieß Ihr Lieblingslehrer?”. Mit Ihren Antworten auf diese Fragen kann ggf. Ihre Identität verifiziert werden.

Verwenden von Anwendungen, wenn keine Verbindung zum Internet vorhanden ist

July 30, 2018

Sie müssen eine Verbindung zum Internet haben, um eine Anwendung zum ersten Mal zu öffnen. Citrix Receiver für Windows installiert manche Anwendungen auf Ihrem Gerät, sodass sie ausgeführt werden können, wenn Sie keine Verbindung mit dem Internet haben. Diese Installation kann mehrere Minuten dauern.

Hinweis: Offlinezugriff steht nicht für alle Benutzer oder Anwendungen zur Verfügung. Ihr Administrator legt fest, wie lange Sie eine Anwendung offline verwenden können, bevor Sie wieder eine Verbindung mit dem Internet herstellen müssen.

Suchen von Desktops und Apps

July 30, 2018

Ihre virtuellen Desktops und Apps stehen auf allen Geräten auf der Citrix Receiver für Windows-Homepage zur Verfügung.

Klicken Sie zuerst mit der rechten Maustaste auf das Citrix Receiver für Windows-Symbol und klicken Sie dann auf **Öffnen**.

Anwendungen und Desktops können außerdem an einem oder mehreren dieser Speicherorte sein:

- Windows-Startmenü: Von Citrix Receiver für Windows hinzugefügte Desktops und Apps werden dem Windows-Startmenü in einem Ordner unter “Alle Programme” hinzugefügt.

- Desktop: Der Administrator kann Verknüpfungen auf dem Computerdesktop zur Verfügung stellen. Die Verknüpfung ist möglicherweise in einem Ordner auf dem Desktop.
- Webseite: Der Administrator kann Links zu Desktops und Apps auf einer Webseite zur Verfügung stellen. Öffnen Sie Internet Explorer, Firefox oder Google Chrome und geben Sie die URL ein, die Ihnen der Administrator mitgeteilt hat.

Verwalten von Sitzungen

July 30, 2018

Im Citrix Connection Center werden alle aktiven Verbindungen angezeigt, die mit Receiver hergestellt wurden.

Öffnen von Connection Center

- Klicken Sie mit der rechten Maustaste auf das Receiver-Symbol und klicken Sie dann auf **Connection Center**.

Beenden einer eingefrorenen virtuellen Anwendung

Wählen Sie die Anwendung im Connection Center aus und klicken Sie dann auf **Beenden**.

Schließen aller aktiven virtuellen Apps gleichzeitig

Wählen Sie den Server im Connection Center aus und klicken Sie dann auf **Abmelden**.

Ändern der Anzeige Ihrer Desktops und Apps

Sie können zwischen dem Seamless- und Vollbildmodus wechseln.

- **Seamless-Modus**: Desktops und Apps werden nicht in einem Sitzungsfenster angezeigt. Jeder Desktop und jede App wird in einem Fenster angezeigt, dessen Größe geändert werden kann, so als ob sie auf dem Benutzergerät installiert wären. Sie können zwischen Apps und dem lokalen Desktop wechseln.
- **Vollbildmodus**: Anwendungen werden in einem Desktopfenster angezeigt.

Wechseln zum Vollbildmodus: Wählen Sie den Server im Connection Center aus, klicken Sie auf **Vollbild** und dann auf **OK**.

Um zum Seamlessmodus zurückzukehren drücken Sie Umschalt+F2.

Aktualisieren oder Entfernen von Apps

July 30, 2018

Beim Abmelden oder Beenden von Citrix Receiver für Windows werden alle Apps getrennt. Sie können die Verbindung zur Sitzung wiederherstellen, indem Sie im Dropdownmenü die Option **Apps aktualisieren** auswählen oder auf das App-Symbol klicken.

Um bei deaktiviertem Self-Service-Modus Apps zu aktualisieren, auf die Sie ausschließlich über das Startmenü oder über Desktopverknüpfungen zugreifen, klicken Sie im Infobereich mit der rechten Maustaste auf Citrix Receiver für Windows und dann auf **Aktualisieren**.

Wählen Sie die Option **Apps aktualisieren**, um aktuelle veröffentlichte Apps und Desktops von StoreFront abzurufen.

Um eine App aus der App-Ansicht zu entfernen, klicken Sie mit der rechten Maustaste auf die App und wählen dann **App entfernen**.

Citrix Receiver für Windows Desktop Lock

March 26, 2019

Sie können Citrix Receiver für Windows Desktop Lock verwenden, wenn Benutzer nicht mit dem lokalen Desktop arbeiten müssen. Sie können weiterhin den Desktop Viewer (falls aktiviert) verwenden, es sind jedoch nur die erforderlichen Optionen auf der Symbolleiste: Strg + Alt + Entf, Einstellungen, Geräte und Trennen.

Citrix Receiver für Windows Desktop Lock funktioniert auf in Domänen eingebundenen Maschinen, die für SSON (Single Sign-On) und mit einem Store konfiguriert sind. Es kann auch auf nicht in Domänen eingebundenen Maschinen ohne SSON verwendet werden. PNA-Sites werden nicht unterstützt. Vorherige Versionen von Desktop Lock werden beim Upgrade auf Citrix Receiver für Windows 4.2 oder höher nicht unterstützt.

Sie müssen Citrix Receiver für Windows mit dem Flag /includeSSON installieren. Konfigurieren Sie den Store und Single Sign-On mit der ADM/ADMX-Datei oder über die Befehlszeilenoption. Weitere Informationen finden Sie unter Installieren und Konfigurieren von Citrix Receiver an der Befehlszeile.

Installieren Sie dann Citrix Receiver für Windows Desktop Lock als Administrator mit dem Installationspaket CitrixReceiverDesktopLock.MSI, das unter Citrix Downloads verfügbar ist.

Systemanforderungen für Citrix Receiver Desktop Lock

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Weitere Informationen finden Sie unter Microsoft Download.
- Unterstützung für Windows 7 (einschließlich Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 und Windows 10 (einschließlich Anniversary Update).
- Verbindung mit StoreFront nur über native Protokolle.
- In Domänen eingebundene und nicht in Domänen eingebundene Endpunkte.
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

Lokaler App-Zugriff

> **Wichtig**
>
> Aktivieren des lokalen App-Zugriffs kann den lokalen Desktopzugriff ermöglichen, es sei denn, es wurde eine vollständige Sperrung über die Gruppenrichtlinienobjektvorlage oder eine ähnliche Richtlinie angewendet. Weitere Informationen finden Sie in der Dokumentation von XenApp und XenDesktop unter Konfigurieren von lokalem App-Zugriff und URL-Umleitung.

Arbeiten mit Citrix Receiver für Windows Desktop Lock

- Citrix Receiver für Windows Desktop Lock kann mit den folgenden Features von Citrix Receiver für Windows verwendet werden:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013-Plug-In und lokaler App-Zugriff.
  - Nur Domänen-, Smartcard- oder zweistufige Authentifizierung.
- Trennen der Citrix Receiver für Windows Desktop Lock-Sitzung führt zur Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Citrix Receiver für Windows Desktop Lock ohne die Eigenschaften Home, Restore, Maximize und Display optimiert.
- Strg+Alt+Entf steht über die Viewer-Symbolleiste zur Verfügung.
- Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben, Ausnahme bildet Windows+L. Einzelheiten finden Sie unter Weitergeben von Windows-Tastenkombinationen an die Remotesitzung.
- Strg+F1 löst Strg+Alt+Entf aus, wenn Sie die Verbindung oder Desktop Viewer für Desktopverbindungen deaktivieren.

Installieren von Citrix Receiver für Windows Desktop Lock

Mit diesen Schritten installieren Sie Citrix Receiver für Windows, sodass virtuelle Desktops mit Citrix Receiver für Windows Desktop Lock angezeigt werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter
Konfigurieren von Smartcards für die Verwendung mit Geräten mit Receiver Desktop Lock.

1. Melden Sie sich mit einem lokalen Administratorkonto an.
2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus (befindet sich im Ordner “Citrix Receiver and Plug-ins > Windows > Citrix Receiver for Windows” auf dem Installationsmedium).

   Beispiel:

   ```
   CitrixReceiver.exe
        /includeSSON
   STORE0=”DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store”
   ```

   Informationen zu dem Befehl finden Sie in der Installationsdokumentation zu Citrix Receiver für Windows unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.
3. Doppelklicken Sie im selben Ordner auf dem Installationsmedium auf CitrixReceiverDesktopLock.msi. Der Assistent “Citrix Desktop Lock” wird geöffnet. Folgen Sie den Anweisungen.
4. Wenn die Installation abgeschlossen ist, starten Sie das Benutzergerät neu. Wenn Sie Zugriffsrechte für einen Desktop haben und sich als Domänenbenutzer anmelden, zeigt das neu gestartete Gerät Receiver Desktop Lock an.

Um die Verwaltung des Benutzergeräts nach der Installation zu ermöglichen, wird das Konto, das für die Installation von CitrixReceiverDesktopLock.msi verwendet wurde, bei der Ersatz-Shell ausgeschlossen. Wenn das Konto später gelöscht wird, können Sie sich nicht bei dem Gerät anmelden und es verwalten.

Verwenden Sie zum Installieren von Receiver Desktop Lock **ohne Benutzereingriff** die folgende Befehlszeile: msiexec /i CitrixReceiverDesktopLock.msi /qn

Konfigurieren von Citrix Receiver für Windows Desktop Lock

Gewähren Sie pro Benutzer nur Zugriff auf einen virtuellen Desktop mit Citrix Receiver für Windows Desktop Lock.

Verhindern Sie mit Active Directory-Richtlinien, dass Benutzer virtuelle Desktops in den Ruhezustand versetzen.

Verwenden Sie das Administratorkonto zum Konfigurieren von Citrix Receiver für Windows Desktop Lock, das Sie für die Installation verwendet haben.

- Stellen Sie sicher, dass die Dateien receiver.admx (oder receiver.adml) und receiver_usb.admx (.adml) in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter "Computerkonfiguration" bzw. "Benutzerkonfiguration" > "Administrative Vorlagen" > "Klassische administrative Vorlagen (ADMX)" > "Citrix Komponenten" angezeigt werden). Die ADMX-Dateien sind in %Programme%\Citrix\ICA Client\Configuration.
- USB-Einstellungen: Wenn ein Benutzer ein USB-Gerät anschließt, erfolgt ein automatisches Remoting des Geräts zum virtuellen Desktop. Es ist kein Benutzereingriff erforderlich. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.
  - Aktivieren Sie die USB-Richtlinienregel.
  - Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" > "Generisches USB-Remoting" die Richtlinien Vorhandene USB-Geräte und Neue USB-Geräte.
- Laufwerkszuordnung: Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" die Richtlinie "Clientlaufwerkzuordnung".
- Mikrofon: Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" die Richtlinie "Clientmikrofon".

Konfigurieren von Smartcards für die Verwendung mit Geräten mit Citrix Receiver für Windows Desktop Lock

1. Konfigurieren Sie StoreFront
   a) Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
   b) Konfigurieren Sie StoreFront-Sites für HTTPS-Zugriff, erstellen Sie ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde und fügen Sie HTTPS-Bindung zur Standardwebsite hinzu.
   c) Stellen Sie sicher, dass Passthrough mit Smartcard aktiviert ist (standardmäßig aktiviert).
   d) Aktivieren Sie Kerberos.
   e) Aktivieren Sie Kerberos und Passthrough mit Smartcard.
   f) Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
   g) Stellen Sie sicher, dass für die IIS-Standardwebsite kein SSL erforderlich ist, und dass Clientzertifikate ignoriert werden.
2. Verwenden Sie die Gruppenrichtlinien-Verwaltungskonsole zum Konfigurieren lokaler Computerrichtlinien auf dem Benutzergerät.
   a) Importieren Sie die Vorlage Receiver.admx aus %Programme%\Citrix\ICA Client\Configuration.
   b) Erweitern Sie "Administrative Vorlagen" > "Klassische administrative Vorlagen (ADMX)" >

“Citrix Komponenten” > “Citrix Receiver” > “Benutzerauthentifizierung”.

c) Aktivieren Sie “Smartcardauthentifizierung”.

d) Aktivieren Sie “Lokaler Benutzername und Kennwort”.

3. Konfigurieren Sie das Benutzergerät vor der Installation von Citrix Receiver für Windows Desktop Lock.

a) Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste “Vertrauenswürdige Sites” hinzu.

b) Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste “Vertrauenswürdige Sites” im Format “desktop:// delivery-group-name” hinzu.

c) Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Citrix Receiver für Windows Desktop Lock auf dem Benutzergerät installiert ist, wird eine konsistente Richtlinie für das Entfernen der Smartcard zwingend angewendet. Wird die Richtlinie für das Entfernen der Smartcard beispielsweise für den Desktop auf Abmelden erzwingen festgelegt, muss der Benutzer sich auch vom Benutzergerät abmelden, unabhängig davon, wie die Richtlinie dort eingestellt ist. Dadurch wird sichergestellt, dass das Benutzergerät sich nicht in einem inkonsistenten Zustand befindet. Dies gilt nur für Benutzergeräte mit Citrix Receiver für Windows Desktop Lock.

Entfernen von Citrix Receiver für Windows Desktop Lock

Stellen Sie sicher, dass beide der unten aufgeführten Komponenten entfernt werden.

1. Melden Sie sich mit demselben lokalen Administratorkonto an, das bei der Installation und Konfiguration von Citrix Receiver für Windows Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:
   - Entfernen Sie Citrix Receiver für Windows Desktop Lock.
   - Entfernen Sie Citrix Receiver für Windows.

Weitergeben von Windows-Tastenkombinationen an die Remotesitzung

Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. In diesem Abschnitt finden Sie einige der gebräuchlichsten Tastenkombinationen.

Windows

- Win+D - Minimieren aller Fenster auf dem Desktop.
- Alt+Tab - Wechseln des aktiven Fensters.
- Strg+Alt+Entf - über Strg+F1 und die Desktop Viewer-Symbolleiste.

- Alt+Umschalt+Tab
- Windows+Tab
- Windows+Umschalt+Tab
- Windows+Alle Zeichentasten

Windows 8

- Win+C - Charms öffnen.
- Win+Q - Charm “Suche”.
- Win+H - Charm “Teilen”.
- Win+K - Charm “Geräte”.
- Win+I - Charm “Einstellungen”.
- Win+Q - Apps durchsuchen.
- Win+W - Einstellungen durchsuchen.
- Win+F - Dateien durchsuchen.

Windows 8 Apps

- Win+Z - App-Optionen anzeigen.
- Win+. - App links andocken.
- Win+Umschalt+. - App rechts andocken.
- Strg+Tab - Zum App-Verlauf wechseln.
- Alt+F4 - App schließen.

Desktop

- Win+D - Desktop öffnen.
- Win+, - Desktop kurz anzeigen.
- Win+B - Zurück zum Desktop.

Sonstiges

- Win+U - Center für erleichterte Bedienung öffnen.
- Strg+Esc - Startbildschirm.
- Win+Eingabetaste - Windows Sprachausgabe öffnen.
- Win+X - Menü für Systemprogrammeinstellungen öffnen.
- Win+Druck - Bildschirmfoto erstellen und unter “Bilder” speichern.
- Win+Tab - Liste zum Wechseln öffnen.
- Win+T - Vorschau offener Fenster in Taskleiste anzeigen.

SDK und API

November 21, 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 XenApp- oder XenDesktop-Servern. Diese Version des SDK bietet Unterstützung zum Schreiben neuer virtueller Kanäle für Receiver für Windows. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an den technischen Support von Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Die Windows Monitoring API, die die visuelle Darstellung verbessert und Unterstützung für Anwendungen von Drittanbietern bietet, die in ICA integriert sind.
- Funktionierender Quellcode für Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen zum SDK finden Sie unter Citrix Virtual Channel SDK for Citrix Receiver for Windows.

Fast Connect 3 Credential Insertion API

Die Fast Connect 3 Credential Insertion API bietet eine Schnittstelle zum Bereitstellen von Benutzeranmeldeinformationen für Single Sign-On (SSON). Dieses Feature ist für Citrix Receiver für Windows 4.2 und höher verfügbar. Mit dieser API können Citrix Partner Authentifizierungs- und SSO-Produkte bereitstellen, die StoreFront oder das Webinterface verwenden, um Benutzer an virtuellen Anwendungen oder Desktops anzumelden und die Verbindungen zu diesen Sitzungen auch wieder zu trennen.

Weitere Informationen zur Dokumentation für Fast Connect API finden Sie unter Fast Connect 3 Credential Insertion API for Citrix Receiver for Windows.

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