Info zu diesem Release

Oct 21, 2015

Citrix Receiver für Windows bietet Benutzern sicheren Self-Service-Zugriff auf virtuelle Desktops und Anwendungen, die von XenDesktop und XenApp bereitgestellt werden.

Receiver für Windows **4.2.100** umfasst die folgenden neuen Fixes und Verbesserungen:

- Aktivieren **einzelner Apps** im Startmenü oder als Desktopverknüpfungen
- Unterstützung für TLS 1.1 und 1.2
- Passthrough-Authentifizierung mit Webinterface
- Unterstützung für Windows XP (Embedded Edition)
  Hinweis: Support für Windows XP endete zusammen mit dem erweiterten Support für Windows XP durch Microsoft am 8. April 2014.
- Verwenden von Receiver Desktop Lock auf in Domänen eingebundenen und **nicht in Domänen eingebundenen** Endpunkten
- Unterstützung für die **automatische Wiederverbindung von Clients** (Automatic Client Reconnection, ACR), wenn Benutzer eine Verbindung mit NetScaler Gateway herstellen und CloudBridge oder HDX Insight zur Bereitstellung gehören
- Vom Administrator deaktivierte Anwendungen werden ohne Benutzereingriff entfernt. Benutzern wird keine Popupmeldung mit dem Text "Einige Apps sind nicht länger verfügbar..." angezeigt.

Receiver für Windows **4.2** umfasst die folgenden neuen Features und Verbesserungen.

- **Integration in Startmenü und Verknüpfungsverwaltung**: Veröffentlichte Apps werden nahtlos in das Startmenü integriert oder in Form von Desktopverknüpfungen bereitgestellt. Dies ist eine konfigurierbare Option für den Administrator. Dieser kann auswählen, ob Apps im Startmenü, als Desktopverknüpfung oder über die Self-Service-Schnittstelle angeboten werden sollen. Weitere Informationen zum Verschieben von Anwendungen in das Startmenü finden Sie unter Konfigurieren des Nur-Verknüpfungsmodus.
- **Verbesserte Benutzererfahrung für Windows-Tablets und -Touchgeräte**
  - **Echtes Multitouchremoting**: Auf Windows 8.1-Touchgeräten können Multitouchbewegung wie etwa Auf- und Zuziehen zum Zoomen in virtuellen Apps und Desktops, die Fingereingabe unterstützen, verwendet werden.
    Hinweis: Multitouchremoting erfordert XenApp 7.0 oder höher, bzw. XenDesktop 7.0 oder höher und wird in virtualisierten Apps und Desktops unter Windows 7, Windows 8, Windows 8.1 und Windows 2012 R2 unterstützt.
  - **Touchzugriff für XenApp und XenDesktop**: Benutzer von Windows 8.1-Geräten, für die Fingereingabe aktiviert ist, können in Anwendungen grundlegende Fingerbewegungen verwenden, obwohl diese nicht nativ unterstützt werden. Einfaches Antippen wird beispielsweise in einen linken Mausklick umgesetzt, Streichen nach oben oder nach unten wird in einen Bildlauf nach oben oder unten per Maus umgesetzt. Die Gesten zum Auf- und Zuziehen werden nicht unterstützt.
  - **Aktualisierte Desktop Viewer-Symbolleiste**: Windows-Benutzer können über die Desktop Viewer-Symbolleiste auf Hilfsprogrammfunktionen wie Strg + Alt + Entf, auf eine virtuelle Tastatur und auf Verknüpfungen für Windows 8 zugreifen. Die Schaltfläche für die virtuelle Tastatur wird angezeigt, wenn keine Tastatur angeschlossen ist. Verknüpfungen auf der Desktop Viewer-Symbolleiste bieten Zugriff auf das Startmenü, Optionen zum Wechseln von Apps, App-Befehle und Charms.

- **Mobile SDK für Windows-Apps**: Citrix Receiver für Windows 4.2 unterstützt Version 2 von Citrix Mobile SDK für Windows-Apps und Version 3 von Citrix Hosted MobileMail. Weitere Informationen finden Sie unter https://www.citrix.com/go/mobile-sdk-for-windows-apps.html und https://www.citrix.com/go/hosted-mobilemail.html. Informationen zu der Liste der unterstützten Funktionen und Enumerationen von Mobile SDK für Windows-Apps finden Sie in der Features-Matrix für Receiver.
- **Verbindliche Apps**: Administratoren können einzelne Apps oder Appgruppen für Benutzer verbindlich machen. Benutzer haben keine Option zum Entfernen des Abonnements verbindlicher Apps. Im Startmenü oder als Desktopverknüpfung veröffentlichte Apps sind immer verbindlich und können vom Benutzer nicht entfernt werden. Weitere Informationen zum Konfigurieren verbindlicher Apps finden Sie unter Konfigurieren der Anwendungsbereitstellung.
- **Neues Receiver Desktop Lock**: Ein neues Receiver Desktop Lock ermöglicht die Verwendung von Receiver für Windows 4.2 auf gesperrten Thin Clients und umfunktionierten Computern für den Zugriff auf virtuelle Apps und Desktops. Installieren Sie Receiver Desktop Lock (CitrixReceiverDesktopLock.MSI), um den Client zu sperren. Nach der Installation kann der Benutzer nicht mehr auf die Optionen Home und Vollbild über die Desktop Viewer-Symbolleiste zugreifen. Weitere Informationen zu Receiver Desktop Lock finden Sie unter Receiver Desktop Lock.
- **Verbesserungen in USB**
  - **USB-Plug & Play**: Die für spezielle USB-Geräte (z. B. Diktiergeräte) verwendete generische USB-Umleitung ist in Version 7.6 USB-3.0-fähig, sodass solche Geräte per Plug & Play in Receiver für Windows verwendet werden können. Weitere Informationen zur generischen USB-Umleitung finden Sie unter Konfigurieren der USB-Unterstützung für XenDesktop- und XenApp-Verbindungen.
  - **Vereinfachter USB-Betrieb**: Das Dialogfeld Einstellungen und das Menü Geräte bieten in diesem Release mehr Transparenz und Kontrolle über verbundene Geräte.
  - **USB 3.0-Umleitung**: Receiver für Windows ermöglicht die Umleitung von Geräten, die über USB 3.0-Ports verbunden sind.
    Hinweis: USB 3.0-spezifische Features wie SuperSpeed sind bei Verwendung der Umleitung nicht verfügbar.
  - **Geräteauswahl für Seamless Apps**: Das aktualisierte Connection Center ermöglicht das Verwalten von USB-Geräteverbindungen für Seamless Apps und bietet eine native Interaktionserfahrung.
- **Verbesserte Grafikleistung**: Receiver für Windows bietet jetzt HD-Videowiedergabe mit H.264, sodass hochwertige Windows Media-Videos auf preisgünstigen Thin Clients wiedergegeben werden können. Die H.264-Decodierung wurde für Thin Clients mit Multimonitorkonfigurationen und höheren Bildschirmauflösungen verbessert.
- **Unterstützung für UDP-Audio**: In Receiver für Windows wird Audio-Remoting über NetScaler Gateway mit nativem UDP (User Datagram Protocol) unterstützt.
- **Webcamwechsel**: Unter Receiver für Windows ist beim Arbeiten mit Videokonferenz-Apps in einer XenDesktop- bzw. XenApp-Sitzung die Auswahl zwischen verschiedenen Webcams auf dem Clientcomputer möglich.
- **Öffnen des Connection Centers über den Infobereich**: Sie können jetzt mit der rechten Maustaste auf den Infobereich in Citrix Receiver klicken und direkt auf das Connection Center zugreifen. Dieses zeigt alle von Citrix Receiver aus hergestellten Verbindungen. Im Modus ohne Self-Service bzw. im Startmenüintegrationsmodus wird im Infobereich die Schaltfläche Aktualisieren angezeigt.
- **Fast Connect -Skripting-API**: Bietet Anwendungsprogrammierschnittstellen für Citrix Partner zur schnellen Authentifizierung von Benutzern bei Citrix Sitzungen oder Citrix Desktops. Die aktuelle Version von Receiver für Windows unterstützt Fast Connect 3 und frühere Versionen.
- **SSON für die bimodale Domänen-Passthrough-Authentifizierung**: Benutzer können sich bei in eine Domäne eingebundenen Clientcomputern mit ihren Domänenanmeldeinformationen oder einer Smartcard anmelden und über Receiver für Windows direkt zu Receiver für Web oder StoreFront wechseln. Zuvor mussten die Benutzer zusätzlich zunächst die Authentifizierungsmethode auswählen, bevor sie Receiver aufrufen konnten.
- **SSON per Smartcard bei domänenexternen Geräten**: Durch die Vereinfachung des Anmeldungsverfahrens müssen Benutzer mit einer Smartcard nur eine PIN-Authentifizierung durchführen. Der Administrator hat den Vorteil, dass nur ein

StoreFront-Server konfiguriert werden muss. Zuvor musste für jeden Authentifizierungstyp (Smartcard und Benutzername/Kennwort) ein StoreFront-Server konfiguriert werden.

- **Sitzungsvorabstart standardmäßig aktiviert**: Das Feature für den Sitzungsvorabstart ist standardmäßig aktiviert, wenn Sie die Single Sign-On (SSO)-Komponente installieren. Zuvor wurde dieses Feature durch Bearbeiten der Registrierungsschlüssel oder während der Installation aktiviert.
- **SSLv3 ist deaktiviert**: Zum Verhindern eines neuen Angriffs (z. B. POODLE) auf SSL 3 wurde die Verwendung dieser Protokollversion in Receiver für Windows deaktiviert. Siehe CTX200238.
  Wichtig: Sie müssen sicherstellen, dass TLS 1.0 aktiviert ist.
  Hinweis: Citrix empfiehlt, SSLv3 auf dem IIS-Server mit StoreFront ebenfalls zu deaktivieren. Weitere Informationen finden Sie im Supportartikel von Microsoft.
- **Verbesserte Installationsprotokollierung**: Die Protokollierung von Installation, Deinstallation und Upgrades erfolgt am gleichen Ort zur Vereinfachung der Problembehandlung -lösung. Das Protokoll ist für jeden Benutzer in %TEMP%\ CTXReceiverInstallLogs.
- **Veraltete Features**: Merchandising Server kann zum Aktualisieren von Receiver nicht mehr verwendet werden, da es nicht mehr gewartet wird. Außerdem wird das Konfigurieren von Receiver zum Prüfen auf Updates auf citrix.com nicht unterstützt. Weitere Informationen zum Upgrade von Receiver finden Sie unter Upgrade von Citrix Receiver 3.4 auf Receiver 4.2.100.

Wichtig: Wenn Sie XenApp oder XenDesktop 7.6 verwenden, sollten Sie die Installation des VDA-Hotfixes unter CTX142037, CTX142094 und CTX142095 erwägen. Durch diesen Hotfix werden Audioprobleme nach dem Wiederverbinden einer Sitzung gelöst sowie die Reaktionszeit bei Grafiken, die Bildqualität und Anzeigefehler verbessert.

Receiver für Windows 4.2 - Behobene Probleme

Oct 21, 2015

Verglichen mit: Citrix Receiver für Windows 4.2

Receiver für Windows 4.2.100 enthält alle Problembehebungen der Versionen Receiver für Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200 und 4.2 und darüber hinaus folgende neuen Korrekturen:

Tastatur

- Wenn Benutzer in einer veröffentlichten Receiver-Sitzung dazu aufgefordert werden, ihr Kennwort mit der Tastenkombination Strg+Alt+Ende zu ändern, funktioniert die Tastenkombination möglicherweise nicht.

  [Von RcvrForWin4.2_14.2.100][#LC0862]

Lokaler App-Zugriff

- Bei Verwendung des Features des lokalen App-Zugriffs "KEYWORDS:prefer="*pattern*"" für eine Anwendung in XenApp 7.5 und StoreFront 2.5 verwendet wird, kann es zu Problemen bei Receiver kommen. Außerdem können Probleme bei der automatischen Erstellung von Verknüpfungen für bevorzugte Anwendungen auftreten, wenn ein Verzeichnis für bevorzugte Vorlagen verwendet wird.

  [Von RcvrForWin4.2_14.2.100][#LC2153]

Sitzung/Verbindung

- Beim Wechseln von Benutzern mit der FastConnect-Skripting-API wird die Aufforderung zur Eingabe von Anmeldeinformationen nicht geschlossen.

  [Von RcvrForWin4.2_14.2.100] [#LC2299]

- Wird eine Desktopsitzung im Vollbildmodus gestartet und der Desktop Viewer ist deaktiviert, werden möglicherweise Bildlaufleisten eingeblendet, wenn eine zweiter Monitor angeschlossen wird.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  - *32-Bit-Windows-Systeme*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Name: ProcessWM_SETTINGCHANGE
    Typ: DWORD

Wert: 1 (Standardwert = 0) (Dieser Fix ist nur für Benutzer vorgesehen, die "CDViewer Bar" deaktivieren und den Desktop im Vollbildmodus ausführen.)

- *64-Bit-Windows-Systeme*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  Name: ProcessWM_SETTINGCHANGE
  Typ: DWORD
  Wert: 1 (Standardwert = 0) (Dieser Fix ist nur für Benutzer vorgesehen, die "CDViewer Bar" deaktivieren und den Desktop im Vollbildmodus ausführen.)

Die folgenden Registrierungsschlüssel sind optional. Der Standardwert ist 0, der Wert ist nur dann erforderlich, wenn das Problem sich mit der Standardkonfiguration nicht beheben lässt.

- *32-Bit-Windows-Systeme*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: MonitorLayoutUpdateDelay
  Typ: DWORD
  Wert: 0 bis 4 (Standardwert = 0)
- *64-Bit-Windows-Systeme*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  Name: MonitorLayoutUpdateDelay
  Typ: DWORD
  Wert: 0 bis 4 (Standardwert = 0)

[Von RcvrForWin4.2_14.2.100] [#LA5746]

- Diese Verbesserung unterstützt die automatische Wiederverbindung von Clients für Receiver für Windows mit XenApp 6.5 und Serverbetriebssystemen mit VDA-Version 7.x, wenn Benutzer eine Verbindung mit NetScaler Gateway herstellen und CloudBridge oder HDX Insight in der Bereitstellung sind.

  Hinweis: Die Sitzungszuverlässigkeit und die automatische Wiederverbindung von Clients funktionieren nicht, wenn Multistream- und Multiport-Richtlinien auf dem Server aktiviert sind und mindestens eine oder folgenden Bedingungen vorliegt:

  - Die Sitzungszuverlässigkeit ist unter NetScaler Gateway deaktiviert.
  - Ein Failover findet auf dem NetScaler-Gerät statt.
  - CloudBridge wird mit NetScaler Gateway verwendet.

  [Von RcvrForWin4.2_14.2.100] [#LC1779]

- Bei der Ausführung von Receiver, wenn mehrere USB-Geräte an das Benutzergerät angeschlossen sind, wird beim Neustart eines Geräts oder beim Anschließen eines neuen USB-Geräts die folgende Meldung angezeigt:

  USB-Hubstromverbrauch überschritten.

  [Von RcvrForWin4.2_14.2.100] [#LC1904]

- Sind bei gepoolten Desktopgruppen mehrere Desktops pro Benutzer konfiguriert, kann bei Verwendung von Receiver für Windows nur der erste Desktop gestartet werden. Wenn ein Benutzer auf die Symbole anderer Desktops klickt, wird möglicherweise ein Dialogfeld zum Verbindungsaufbau angezeigt, die Verbindung schlägt jedoch fehl. Die erste Desktopsitzung wird im Vordergrund angezeigt.

  [Von RcvrForWin4.2_14.2.100] [#LC0780]

- Wird die Registrierungsschlüsseldatei "Client Selective Trust" gemäß Anweisungen im Knowledge Center-Artikel CTX133565 importiert und werden Vertrauenszone und Intranet-Zone konfiguriert, funktioniert der Registrierungsschlüssel möglicherweise nicht, wenn der Desktop Viewer im Webinterface oder in StoreFront aktiviert wird. Wenn die URL von Webinterface oder StoreFront im Browser als vertrauenswürdige Zone konfiguriert ist, wird fälschlicherweise eine Warnung über die Dateisicherheit angezeigt, wenn auf das Verzeichnis für die Clientlaufwerkzuordnung zugegriffen wird.

  [Von RcvrForWin4.2_14.2.100] [#LC0904]

- Wenn ein Benutzer sich nach der Abmeldung von einer Sitzung beim Windows XP Embedded Thin Client abmelden möchte, wird die Fehlermeldung "End program concentr.exe" angezeigt.

  [Von RcvrForWin4.2_14.2.100] [#LC2556]

- Die Zeitzone ist nicht richtig, wenn sich Benutzer mit Receiver für Windows anmelden. Dieser Hotfix erfordert Folgendes:

  - Der gleiche Zeitzonen-Hotfix von Microsoft muss auf dem Benutzergerät und dem Server installiert werden. Wenn Sie beispielsweise Microsoft Hotfix KB2998527 auf dem Benutzergerät installieren, installieren Sie den gleichen Hotfix auch auf dem Server.
  - Wird auf dem Server Windows Server 2008 R2 Service Pack 1 ausgeführt, muss Microsoft Hotfix KB2870165 auf dem Server installiert werden.
  - Der Fix LC1061 muss auf dem XenApp-Server installiert werden.

  [Aus RcvrFürWin4.2_14.2.100][#LC1392]

- Dieser Fix ermöglicht die Unterstützung der FastConnect-Skripting-API ohne Integration des Self-Service Plug-Ins. Dies kann aktiviert werden indem die Option "Integrate Self Service plugin with FastConnect" unter **ADM** > **Citrix Components** > **Citrix Receiver** > **FastConnect API Support** > **Manage FastConnectAPI support** deaktiviert wird. Alternativ können Sie den Registrierungsschlüssel "FastConnectUsingSSP" unter HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Dazzle in "False" ändern.

  [Von RcvrForWin4.2_14.2.100] [#LC2580]

- Wenn "SelfServiceMode" auf "False" festgelegt ist, werden Startmenüverknüpfungen für Hintergrundsitzungen (z. B. die Vorabstartanwendung) erstellt.

  [Von RcvrForWin4.2_14.2.100] [#LC1760]

- Dieser Fix behebt die folgenden Probleme:

  - Beim Starten einer veröffentlichten Seamless-Anwendung wird die Anwendung möglicherweise hinter der Windows-Taskleiste geöffnet.
  - Wenn die Taskleiste verschoben wird, erfolgt keine Größenanpassung der Seamless-Sitzung und die Taskleiste überlagert möglicherweise die Anwendung.

  Zum Aktivieren dieses Fixes müssen Sie auch den serverseitigen Fix LC1342 installieren.

  [Von RcvrForWin4.2_14.2.100] [#LC1645]

- Eine Fehlermeldung wird möglicherweise angezeigt, wenn eine Sitzung in Receiver für Windows 4.2 auf einem Thin Client mit Windows XP Embedded gestartet wird.

  [Von RcvrForWin4.2_14.2.100] [#LC1929]

- Dieser Fix aktiviert die Unterstützung der FastConnect Scripting API während der Installation durch Einstellen von "FastConnectAPISupportEnabled = True". Sie können diese Einstellung auch über das Gruppenrichtlinienobjekt "Fast Connect-API-Funktionalität aktivieren" unter "API-Unterstützung für Fast Connect verwalten" aktivieren.

  [Von RcvrForWin4.2_14.2.100] [#LC2131]

- Receiver für Windows 4.2 stellt möglicherweise das Senden von Netzwerkpaketen aufgrund eines Programmdeadlocks ein. Dies kann folgende Konsequenzen haben:

  - Die Sitzung wird möglicherweise nicht hergestellt.
  - Citrix HDX Engine reagiert möglicherweise nicht mehr, wenn die Desktop-Bildschirmauflösung sich ändert.

  [Von RcvrForWin4.2_14.2.100] [#LC2105]

- Diese Erweiterung bietet Unterstützung für TLS Version 1.1 und 1.2 in Receiver für Windows 4.2 kumulatives Update 1.

  [Von RcvrForWin4.2_14.2.100] [#LC1931]

- Der Roundtripzeitwert für ICA-Sitzungen des EdgeSight-Agents kann in zufällig über die Farm verteilten Sitzungen hoch sein.

  [Von RcvrForWin4.2_14.2.100] [#LC1725]

- Mit dieser Erweiterung wird die Verarbeitung von Fast Connect-Änderungen in der Datei icaclient.adm verbessert.

  [Von RcvrForWin4.2_14.2.100] [#LC2575]

- Nach Auswahl der Größenoption "Passend skalieren" in einer Receiver-Sitzung funktionieren Maus und Tastatur in der Sitzung nicht mehr.

  [Von RcvrForWin4.2_14.2.100] [#LC2219]

- Durch diese Erweiterung werden die Citrix Diagnostic Facility-Ablaufprotokolle für das Fast Connect-Feature verbessert, sodass keine nicht vorhandenen Fehler aufgezeichnet werden.

  [Von RcvrForWin4.2_14.2.100] [#LC2573]

- Nach der Installation von Receiver über die Befehlszeile wird automatisch ein neuer Store im Self-Service Plug-In hinzugefügt, wenn Receiver beendet und neu gestartet wird.

  Das Problem tritt auf, wenn der Schlüssel "Dazzle" unter HKEY_CURRENT_USER\Software\Citrix einen Unterschlüssel unter dem Namen "Properties" hat und der Registrierungsschlüssel, der die Unterschlüssel enthält, von "RegDeleteKey" nicht gelöscht werden kann, denn dadurch werden Store-Schlüsselduplikate erstellt.

  [Von RcvrForWin4.2_14.2.100] [#LC2154]

- Wenn Benutzer sich mit Fast Connect-Skripting-APIs abmelden, bleiben Anwendungsverknüpfungen im Ordner für Desktopverknüpfungen oder im Startmenü zurück.

  [Von RcvrForWin4.2_14.2.100] [#LC2590]

- Nicht authentifizierten Benutzern werden möglicherweise mehrere Anmeldeaufforderungen angezeigt, wenn diese sich mit der FastConnect-Skripting-API abmelden.

[Von RcvrForWin4.2_14.2.100] [#LC2300]

- Wenn Registrierungseinträge, die zu Receiver gehören, vor der Installation von Receiver erstellt werden, können Standardbenutzer Receiver für Windows problemlos installieren, Anwendungen werden jedoch möglicherweise nicht gestartet.

  [Von RcvrForWin4.2_14.2.100] [#LC0410]

- Der Wechsel von Benutzern in der FastConnect-Skripting-API zur expliziten Authentifizierung funktioniert möglicherweise nicht.

  [Von RcvrForWin4.2_14.2.100] [#LC2127]

- Diese Feature-Erweiterung enthält die Option zur Verwaltung von Pro-App-Verknüpfungen. Über Anwendungseigenschaften können Sie Verknüpfungen für spezifische veröffentlichte Anwendungen auf dem Desktop und im Startmenü von Benutzern erstellen.

  Hinweis: Der Startmenüordner der Anwendungseigenschaften wird nur angewendet, wenn Benutzer eine Verbindung mit der Farm oder Bereitstellungsgruppe über das Webinterface herstellen, nicht aber über StoreFront.

  [Von RcvrForWin4.2_14.2.100] [#LC1930]

- Wenn Benutzer sich von Receiver mit Fast Connect abmelden, wird die Liste abonnierter Anwendungen weiterhin im Seitenbereich angezeigt.

  [Von RcvrForWin4.2_14.2.100] [#LC2574]

- Wenn Receiver für Windows nicht mit einem Konto konfiguriert ist, kann die Verbindung von Anwendungen nicht mit dem entsprechenden SelfService-Befehl getrennt werden.

  [Von RcvrForWin4.2_14.2.100] [#LC2128]

Systemausnahmen

- In Receiver kann eine Zugriffsverletzung auftreten, worauf Receiver unerwartet geschlossen wird. Wenn dieses Problem auftritt, können Benutzer Sitzungen nicht durch Klicken auf die Anwendungssymbole im Webinterface starten.

  [Von RcvrForWin4.2_14.2.100] [#LC0650]

- Beim Starten einer veröffentlichten Anwendung auf einem mit einem lokalen Drucker verbundenen Gerät wird Receiver für Windows möglicherweise unerwartet geschlossen und die folgende Fehlermeldung wird angezeigt:

  Citrix HDX Engine funktioniert nicht mehr.

  [Von RcvrForWin4.2_14.2.100] [#LC1170]

Benutzererfahrung

- Das Erstellen von Desktopverknüpfungen für Anwendungen kann in Receiver lange dauern, wenn Benutzer sich bei StoreFront oder dem Webinterface anmelden.

  [Von RcvrForWin4.2_14.2.100] [#LC2263]

- Durch diese Problemlösung erhalten Gruppenrichtlinienobjekt-Einstellungen beim Lesen der Konfiguration für eine

Sitzung eine höhere Priorität als der primäre Store.

[Von RcvrForWin4.2_14.2.100] [#LC2698]

Benutzeroberfläche

- Nach der Installation von Receiver über die Befehlszeile werden Storename und -beschreibung auf "vorhanden" festgelegt. Wird Receiver neu gestartet, können Storename und -beschreibung automatisch auf einen anderen Wert wechseln. Die URL bleibt jedoch dieselbe und die Verbindung funktioniert einwandfrei.

  Das Problem tritt auf, weil der Storename beim Verarbeiten der Receiver-Sites nicht aus der Registrierung abgerufen, sondern stattdessen ein neuer Name auf der Basis der Store-URL erstellt wird.

  [Von RcvrForWin4.2_14.2.100] [#LC1231]

- Durch diese Verbesserung wird die Aufforderung zum Entfernen von Anwendungen aus der Liste der Anwendungen und Verknüpfungen unterdrückt, wenn eine Anwendung nicht mehr veröffentlicht oder deaktiviert ist.

  [Von RcvrForWin4.2_14.2.100] [#LC2157]

- Der Link "Weitere Informationen" im Desktop Viewer führt zu anderen Hilfedateien als das Symbol "Hilfe" im Navigationsbereich von Receiver.

  [Von RcvrForWin4.2_14.2.100] [#LC2066]

Verglichen mit: Citrix Receiver für Windows 4.1.200

Receiver für Windows 4.2 enthält alle Problembehebungen der Versionen Receiver für Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100 und 4.1.200 und darüber hinaus folgende neuen Korrekturen:

Inhaltsumleitung	Sitzung/Verbindung
HDX MediaStream	Spiegeln
HDX MediaStream Windows Media-Umleitung	Smartcards
HDX Plug-n-Play	Systemausnahmen
Installieren, Deinstallieren und Aktualisieren	Benutzererfahrung
Anmeldung und Authentifizierung	Benutzeroberfläche
Drucken	Sonstiges
Server-/Farmverwaltung	

Inhaltsumleitung

- Beim Zugriff auf die URLs in einer veröffentlichten Anwendung funktioniert die Server-an-Client-Inhaltsumleitung möglicherweise nicht und es wird ein Browser auf dem Server aber nicht auf dem Client geöffnet.

  [#LC0150]

- Gelegentlich kann der Zugriff auf eine Website, deren URL-Header anstatt einer GET-Anforderung eine HEAD-Anforderung enthält, fehlschlagen, wenn der Webserver die HEAD-Anforderung nicht akzeptiert. Die Server-an-Client-Inhaltsumleitung funktioniert dann nicht.

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

  HKEY_CURRENT_USER_\Software\Citrix\ICA Client\Engine
  Name: SpecificSites
  Typ: REG_MULTI_SZ
  Wert: Websitenamen (eine Website pro Zeile)

  Hinweis: An jede im Wert angegebene Website wird statt einer HEAD-Anforderung eine GET-Anforderung gesendet. Bei Websitenamen wird Groß-/Kleinschreibung unterschieden, der Platzhalter "*" kann verwendet werden. Wenn beispielsweise "*.meinefirma.com" in dem Registrierungswert angegeben wird, können die Benutzer auf www.meinefirma.com und support.meinefirma.com (die "spezifischen" Websites) zugreifen.

  [#LC0326]

- Dieser Fix ist eine Erweiterung von Fix #LA0803. Beim Zugriff auf benutzerdefinierte URLs in einer veröffentlichten Anwendung auf Servern mit XenApp 6 Hotfix Rollup Pack 2 und XenApp 6.5 Hotfix Rollup Pack 3 funktioniert die Server-an-Client-Inhaltsumleitung nicht und ein Webbrowser wird statt auf dem Benutzergerät auf dem Server geöffnet.

  [#LC0428]

HDX MediaStream

- Wird auf Benutzergeräten mit zwei Monitoren ein Video in Windows Media Player in einer Receiver-Sitzung auf dem ersten Monitor wiedergegeben, wird auf dem zweiten Monitor ein zusätzliches schwarzes Fenster geöffnet.

  [#LC0552]

- Bei der Wiedergabe eines Videos in Windows Media Player in einer Receiver-Sitzung wird ein zweites schwarzes Fenster mit dem Titel "Citrix HDX Movie Window" geöffnet. Das Schließen dieses zweiten Fensters hat keine Auswirkung auf die Videowiedergabe.

  [#LC0818]

HDX MediaStream Windows Media-Umleitung

- Bei der Audiowiedergabe über Windows Media Player kann es zu Störgeräuschen kommen.

  [#LA2911]

HDX Plug-n-Play

- Wird während einer Sitzung ein USB-Gerät vom Endpunkt getrennt, reagiert Receiver für Windows möglicherweise nicht

mehr.

[#LA4827]

- In Einzelfällen werden USB-Geräte nach dem Abmelden von einer Sitzung nicht freigegeben und stehen anschließend nicht zur Verwendung in der lokalen Sitzung zur Verfügung.

  [#LC0091]

Installieren, Deinstallieren und Aktualisieren

- Nach Installation von Receiver mit der Befehlszeilenoption /includeSSON wird der SSONSVR.exe-Prozess nicht ausgeführt.

  [#LC0138]

- Versucht ein Windows-Systemadministrator die Deinstallation von Receiver mit CitrixReceiver.exe /uninstall kann eine UAC-Aufforderung angezeigt werden.

  [#LC0977]

Anmeldung und Authentifizierung

- Bei Aktivieren der Smartauthentifizierung in der Client-ADM-Vorlage werden der Benutzername und das Kennwort des lokalen Benutzers in der lokalen Richtlinie automatisch auf "Aktiviert" festgelegt, selbst wenn die Richtlinie zuvor nicht konfiguriert war.

  [#LC0713]

- Die Domänen-Passthrough-Authentifizierung kann bei Citrix Receiver für Windows 3.4 mit kumulativem Update 3 zeitweilig fehlschlagen.

  [#LC0865]

Drucken

- Wird der lokale Drucker in Internet Explorer 8 so konfiguriert, dass mehrere Seiten pro Blatt gedruckt werden, wird diese Einstellung möglicherweise nicht eingehalten und eine Seite pro Blatt gedruckt. Das Problem tritt auf, wenn eine Verbindung von einem veröffentlichten XenApp 6.5-Desktop mit einer Internet Explorer 8-Instanz hergestellt wird, die auf einem XenApp 6-Server veröffentlicht wurde.

  [#LA3379]

- Bei Klicken auf "Vorschau auf Client" im universellen XPS-Druckertreiber wird in Internet Explorer die folgende Fehlermeldung angezeigt:

  Die Webseite kann von Internet Explorer nicht angezeigt werden.

  [#LA5896]

- Die automatische Erstellung von Druckern ist auf 100 pro Sitzung limitiert.

  [#LC0031]

- Durch diese Erweiterung wird der clientseitigen Komponente der LPT-Zuordnung Unterstützung für die CDF-Ablaufverfolgung hinzugefügt.

  [#LC0823]

Server-/Farmverwaltung

- Dieser Fix behebt ein Speicherproblem in einer Hintergrundkomponente.

  [#LA5664]

- Wenn Receiver für Windows eine Verbindung mit NetScaler Gateway herstellt und die Verbindung dann an StoreFront übergibt, ist nur die Dienst-URL in der Antwort von StoreFront enthalten, nicht aber die Beacons. Wenn dieses Problem auftritt, wird ein HTTP 403-Fehler gemeldet und die Autodiscovery funktioniert möglicherweise nicht.

  [#LC0481]

- Wenn ein Benutzer die Einstellung "USB-Root-Hub" deaktiviert und dann über Device Manager auf dem Benutzergerät wieder aktiviert, während das Gerät mit einem VDA verbunden ist, funktioniert die USB-Geräteumleitung nicht.

  [#LC0541]

Sitzung/Verbindung

- Anmeldungen und Abmeldungen auf einem Windows 7-Clientgerät mit Receiver für Windows Enterprise Edition können verzögert werden. Das Problem tritt auf, wenn Anmelde-/Abmeldeskripts von einem Gruppenrichtlinienobjekt angewendet werden. Jedes Skript kann zu einer erheblichen Verzögerung führen.

  [#LA3811]

- Nach Reaktivieren eines Endpunkts aus dem Energiesparmodus oder Ruhezustand bei bestehender Verbindung mit einer XenApp- oder XenDesktop-Sitzung mit Receiver für Windows können Kopier-/Einfügevorgänge zwischen Endpunkt und Citrix Sitzung fehlschlagen.

  [#LA3973]

- Bei aktiviertem Multistream kann Receiver mit Desktop Lock möglicherweise nicht aus einem VDA-Bildschirmschoner reaktiviert werden und keine erneute Verbindung herstellen, wenn ein VDA gesperrt ist.

  [#LA4097]

- Wird versucht, eine Microsoft Word- oder Excel 2003-Datei in einem der Sitzung mit Lesezugriff zugeordneten Clientlaufwerk zu öffnen, wird die Datei möglicherweise nicht geöffnet.

  [#LA4198]

- Wenn die Richtlinie zum Ausblenden des Symbols aktiviert ist, wird das Fenster "Info zu Citrix Receiver" möglicherweise nach der Anmeldung beim Clientgerät automatisch angezeigt.

  [#LA4513]

- Das Starten einer Sitzung mit einem benutzerdefinierten virtuellen Treiber kann fehlschlagen.

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

- *32-Bit-Windows*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: VdLoadUnLoadTimeOut
  Typ: REG_DWORD
  Daten: Beliebiger Wert in Sekunden
- *64-Bit-Windows*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Name: VdLoadUnLoadTimeOut
  Typ: REG_DWORD
  Daten: Beliebiger Wert in Sekunden

[#LA4540]

- Bei VoIP-Anrufen von einem PVS-gestreamten VDA unter Verwendung von HollyCRM mit dem OpenEye-Plug-In von Huawei kann nach einem Zeitraum ab zwei Stunden möglicherweise keiner der Teilnehmer den anderen hören.

  [#LA4809]

- Wird über die Windows-Taste oder per Klick auf die Schaltfläche "Start" das clientseitige Startmenü geöffnet, während ein Seamless-Sitzungsfenster im Vordergrund ausgeführt wird, bleibt bei einem Klick auf das Taskleistensymbol in einem lokalen Fenster der Fokus auf dem Seamless-Sitzungsfenster, anstatt zum lokalen Fenster zu wechseln.

  [#LA5089]

- Ist "SSL-Relay" aktiviert, funktioniert die Sitzungszuverlässigkeit bei Anwendungen nicht, die zur Verwendung der Verschlüsselung konfiguriert sind.

  [#LA5476]

- Nach dem Ändern des Kennworts in einer über XenApp veröffentlichten Desktopsitzung schlägt die Passthrough-Authentifizierung bei veröffentlichten Anwendungen von der Desktopsitzung aus fehl und die Benutzer werden aufgefordert, Benutzernamen und Kennwort einzugeben.

  [#LA5587]

- Receiver kann keine Verbindung mit StoreFront über NetScaler Gateway von Windows Server 2012 R2 aus herstellen.

  [#LC0084]

- In Receiver für Windows 4.1 wird eine zweite Sitzung erstellt, wenn Benutzer versuchen, die Verbindung mit einer getrennten Sitzung durch Klicken auf das Desktopsymbol im Self-Service Plug-In wiederherzustellen.

  [#LC0182]

- Cleanup.exe kann während des Zurücksetzens von Receiver unerwartet beendet werden.

  [#LC0249]

- Während des Sitzungsvorabstarts in nicht-englischen XenApp-Umgebungen wird die Citrix Receiver-Fortschrittsanzeige möglicherweise eingeblendet und reagiert nicht. Es wird die folgende Fehlermeldung angezeigt:

  "Verbindung aufgebaut. Funktionalität wird ausgehandelt"

[#LC0306]

- Das Eingeben von Text in veröffentlichten Instanzen von Microsoft Outlook kann dazu führen, dass die Sitzung grundlos getrennt wird.

  [#LC0323]

- Wird versucht, eine Datei mit einem TWAIN-Gerät mit Drittanbieter-Anwendung zu übertragen, wird die Anwendung möglicherweise unerwartet beendet.

  [#LC0369]

- Wenn Benutzer mit einer Verbindung mit einem Windows 7-VDA unter Verwendung von Receiver für Windows ein SpeechMike mit Desktop Viewer umleiten, schlägt die Umleitung möglicherweise fehl, wenn die Mikrofontaste freigegeben wird.

  [#LC0510]

- Obwohl die Dateitypzuordnung konfiguriert ist, werden Benutzer aufgefordert, eine Anwendung zum Öffnen einer bestimmten Datei auszuwählen.

  [#LC0515]

- Versuche, eine Verbindung über einen Proxyserver mit einer PAC-Datei herzustellen, schlagen fehl.

  [#LC0529]

- Citrix Receiver für Windows 13.4 mit kumulativem Update 3 wird bei veröffentlichten SAP-Anwendungen unter Meldung des folgenden Fehlers möglicherweise unerwartet beendet:

  Citrix HDX Engine funktioniert nicht mehr.

  [#LC0712]

- Das umgeleitete COM-Portgerät funktioniert nicht in einer Receiver-Sitzung.

  [#LC0851]

- Wurde Fix #LC0031 angewendet und Benutzer trennen die Verbindung oder melden sich ab, reagiert die Sitzung über zwei Minuten lang nicht mehr, wenn andere aktive Sitzungen vorhanden sind.

  [#LC0983]

Spiegeln

- Versucht ein Administrator das Spiegeln einer Sitzung, kann eine schwarze Spiegelsitzung begonnen werden, die möglicherweise nicht automatisch neu aufgebaut wird. Das Problem tritt auf, wenn das Fenster der Originalsitzung und das der Spiegelsitzung gleich groß sind.

  [#LA2913]

Smartcards

- Citrix Receiver für Windows findet möglicherweise kein gültiges Smartcardzertifikat und die folgende Fehlermeldung wird

im Debugprotokoll von Authentifizierungsmanager angezeigt:

ERROR_WINHTTP_CLIENT_AUTH_CERT_NEEDED: Unknown error code '12044'

[#LC0783]

Systemausnahmen

- Wird ein Clientgerät aus dem Ruhezustand reaktiviert, reagiert Receiver für Windows möglicherweise nicht mehr.

  [#LA5023]

- Ein Problem mit dem CDViewer-Prozess kann zur Anzeige eines schwarzen Bildschirms und Meldung eines .NET-Ausnahmefehlers führen.

  [#LC1038]

Benutzererfahrung

- Bei manchen Konfigurationen kann die Maus in Benutzersitzungen flimmern.

  [#LA309]

- Wenn "Lokales Textecho" aktiviert ist, kann der Textcursor in veröffentlichten Instanzen von Internet Explorer bei Verbindungen mit hoher Latenz flimmern oder unsichtbar sein.

  [#LA4762]

- Unter bestimmten Umständen werden Anwendungen beim Start in den Hintergrund verschoben.

  [#LC0050]

- Wenn Benutzer mehrere Excel-Arbeitsmappen öffnen und Excelhook ist in der Registrierung aktiviert, wird bei Schließen der letzten Arbeitsmappe das Excel-Taskleistensymbol ausgeblendet, obwohl das Excel-Fenster geöffnet ist.

  [#LC0062]

- Alle Benutzer mit Ausnahme desjenigen, der Receiver installiert hat, werden zum Hinzufügen eines Kontos aufgefordert, wenn sie Receiver zum ersten Mal starten.

  [#LC0253]

- Nach Auswahl von "Bildschirm ausschalten" und Reaktivieren der Sitzung wird diese als kleines Fenster oben links auf dem Bildschirm dargestellt.

  [#LC0319]

- Versuche, das Fenster einer veröffentlichten Anwendung hinter die lokale Windows- Taskleiste zu verschieben, können fehlschlagen.

  [#LC0561]

- Anwendungsfenster werden in Konfigurationen mit mehreren Monitoren möglicherweise nicht richtig wieder aufgebaut.

  [#LC0600]

Benutzeroberfläche

- Wenn das Receiver Store-Fenster während des Anwendungsstarts geschlossen wird, bleibt die Fortschrittsanzeige möglicherweise sichtbar, nachdem die Anwendung gestartet ist.

  [#LC0464]

- Beim Starten einer Anwendung oder eines Desktops bleibt das Startdialogfeld mehrere Sekunden lang leer.

  [#LC0624]

- Dieser Fix korrigiert einen typografischen Fehler in der Standard-Admin-Vorlage.

  [#LC0848]

Sonstiges

- Diese Feature-Erweiterung für die Protokollierung des Installationsprogramms von Citrix Receiver ermöglicht Folgendes:
  - Speichern von Protokollen an einem Permanentspeicherort
  - Beibehaltung des Installationsverlaufs nach jeder Installation
  - Sammeln von Benutzerumgebungsinformationen vor der Installation
  - Mehr Debugging-Informationen in den Installationsprotokollen

  [#LA4615]

- Die Dateien CtxCredApi.dll und CtxCredApi(64).dll sind jetzt im MSI-Paket für Citrix Receiver für Windows Enterprise enthalten. Die API unterstützt jetzt 64-Bit-Plattformen. Verwenden Sie CtxCredApi64.dll für 64-Bit-Anwendungen.

  [#LA4630]

- Die CPU-Auslastung aller wfica-Prozesse auf einem Server kann um 10 Prozent steigen, wenn ein einzelner Benutzer Audio in einer Sitzung verwendet.

  [#LA5918]

- Receiver kann möglicherweise den Organisationsnamen von Zertifikaten nicht richtig lesen, wenn der Name Sonderzeichen enthält, insbesondere solche außerhalb der ersten 128 Zeichen des ASCII-Zeichensatzes.

  [#LC0801]

- Bei Verwendung des Befehls "wfica32.exe /setup" wird Internet Explorer vom ActiveX wfica.ocx-Add-On nicht registriert.

  [#LC0927]

Hinweis: Diese Version von Citrix Receiver enthält alle Problembehebungen der Versionen 4.1 und 4.0.

Receiver für Windows 4.2 - Bekannte Probleme

Nov 09, 2015

In diesem Release bestehen die folgenden Probleme:

- Die Smartcard-Autorisierung funktioniert bei XenApp Services-Sites nicht. Bei StoreFront-Sites ist die Funktion jedoch vorhanden. Sei lösen das Problem, indem Sie die Smartcard-Autorisierung an eine StoreFront-Site verweisen.

- Die Unterstützung für Windows XP (Embedded Edition) ist bei Thin Clients mit Access Gateway begrenzt.

  [#522093]

- GPO-Bereitstellungen von Receiver Desktop Lock verursachen u. U. ein Fehlschlagen der Installation [#323424]. Verwenden Sie als Workaround das Softwaretool eines Drittanbieters, z. B. **Orca** (https://msdn.microsoft.com/en-us/library/aa370557), um den Sprachcode des Sprachpakets von **1033** in **9** zu ändern. Mit Orca verfahren Sie wie folgt:
  1. Laden Sie **Orca** herunter und installieren Sie es.
  2. Klicken Sie mit der rechten Maustaste auf CitrixReceiverDesktopLock.msi > Edit with Orca > View > Summary Information.
  3. Ändern Sie unter "Languages" **1033** in **9**.
  4. Klicken Sie auf OK.

- Citrix Receiver für Windows 3.4 (13.4.400) kann nur auf Citrix Receiver für Windows 4.2 oder höher aktualisiert werden. Zum Durchführen eines Upgrade von 3.4 (13.4.400) auf andere 4.x-Versionen muss 13.4.400 zunächst deinstalliert werden.

- Verweise auf SSL werden möglicherweise in Feldnamen auf der Benutzeroberfläche noch angezeigt (z. B. **TLS/SSL data encryption and server identification**). Diese werden in einem künftigen Release aktualisiert.

- Die Sprachenleiste wird nicht im Anmeldebildschirm des Desktop Lock-Clients angezeigt. Zur Problemvermeidung verwenden Sie die unverankerte Sprachenleiste.

  [#502678]

- Die Optionen für Verknüpfung in Citrix Desktop Viewer funktionieren nicht, wenn die Sitzung im Fenstermodus geöffnet wird.

  [#510529]

- Die Desktop Viewer-Warnung beim Trennen der Verbindung gilt nicht für Sitzungen anonymer Benutzer. Dies ist beabsichtigt.

  [#481561]

- Receiver für Windows kann auf Windows 2012 R2-Computern nicht mit einem einfachen Benutzerkonto (nicht-

Administratorkonto) installiert werden.

[#492508]

- Die gleichen Einstellungen für die Webcamauswahl werden für mehrere Virtual Desktop Agents (VDA) verwendet, wenn ein Benutzer mehrere VDAs mit demselben Hostnamen in verschiedenen Domänen hat.

  [#497489]

- Bei der Installation des VDAs ignoriert CitrixReceiver.exe die Angabe eines benutzerdefinierten Pfads.

  [#487849]

- Benachrichtigungen im Infobereich werden manchmal im Desktop Lock-Modus angezeigt.

  [#488620]

- Die virtuelle Tastatur wird für den Terminalserver-VDA nicht automatisch angezeigt. Zur Problemumgehung öffnen Sie die virtuelle Tastatur über das Symbol auf der Desktop Viewer-Symbolleiste oder – bei Apps – über das Symbol für die virtuelle Tastatur auf der Taskleiste.

  [#502774]

- Wenn die Einstellung zur Webcamauswahl auf "Automatisch" und der Registrierungseintrag PreferredWebcam auf dem Clientgerät festgelegt wurde, gilt die über den Registrierungsschlüssel "PreferredWebcam" festgelegte Webcameinstellung. Dies ist beabsichtigt.

  [#494785]

- Die Audioqualität ist beim Remoting eines USB-Headsets (Logitech USB H340) über die generische USB-Umleitung niedriger als erwartet. Dies ist beabsichtigt. Bei der USB-Umleitung wird keine Audiooptimierung durchgeführt. Eine entsprechende Erweiterung wird bei einem zukünftigen Release in Erwägung gezogen.

  [#469670]

- Langsame App-Enumeration. Hierfür gibt es zwei Workarounds:
  1. Wenn der Benutzer RemoveappsOnLogoff und RemoveAppsonExit aktiviert hat und die App-Enumeration bei jeder Anmeldung langsam ist, müsste die folgende Workaround-Konfiguration die Verzögerung verringern.
     1. Fügen Sie mit dem Registrierungs-Editor HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true" hinzu.
     2. Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true" hinzu.

     HKCU hat Vorrang vor HKLM.

  2. Ermöglichen Sie die Verwendung zuvor erstellter und in einer Netzwerkfreigabe gespeicherter EXE-Stubdateien durch den Computer:
     1. Erstellen Sie auf einem Computer EXE-Stubdateien für alle Apps. Am einfachsten ist es, dem Computer alle Anwendungen über Windows Receiver hinzuzufügen, denn dabei werden die EXE-Dateien erstellt.
     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. Beispiel: \\ShareOne\ReceiverStubs
4. Legen Sie nun für jeden Clientcomputer, der gesperrt werden soll, folgende Registrierungsschlüssel fest:
   - Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs" hinzu.
   - Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v CopyStubsFromCommonStubDirectory /t REG_SZ /d "true" hinzu.

   Diese Einstellungen sind auch über HKCU möglich. HKCU hat Vorrang vor HKLM.
5. Beenden und starten Sie Receiver für einen Test.

Hinweis: HKLM-Pfade auf 32-Bit-Computern: HKLM\Software\Citrix\Dazzle. HKLM-Pfade auf 64-Bit-Computern: HKLM\Software**Wow6432Node**\Citrix\Dazzle.

[#492154]

- Die Gesten zum Aufziehen und Zuziehen funktionieren nicht beim Anwendungsremoting über XenApp- bzw. XenDesktop-Versionen vor 7.0 und über XenApp und XenDesktop ab Version 7.0 unter Windows 2008 R2.

  [#517877]

Systemanforderungen

Oct 19, 2016

Betriebssystem

- Windows 8.1, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows 7, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows 7, 32-Bit- und 64-Bit-Editionen (inkl. Embedded Edition)
- Windows Vista, 32-Bit- und 64-Bit-Editionen
- Windows Thin PC
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2, 64-Bit-Edition
- Windows Server 2008, 32-Bit- und 64-Bit-Edition
- Windows Server 2008, 32-Bit- und 64-Bit-Edition
- Unterstützung für Windows XP (Embedded Edition)

Hinweis: Support für Windows XP endete zusammen mit dem erweiterten Support für Windows XP durch Microsoft am 8. April 2014.

Hardware:

- VGA- oder SVGA-Grafikkarte mit Farbmonitor.
- Windows-kompatible Soundkarte für die Audiounterstützung (optional).
- Für Netzwerkverbindungen mit der Serverfarm werden eine Netzwerkkarte und die entsprechende Netzwerkprotokoll-Software benötigt.

Touchfähige Geräte

Receiver für Windows 4.2.x kann auf touchfähigen Laptops, Tablets und Monitoren unter Windows 7 und Windows 8.1 mit XenApp und XenDesktop 7 oder höher und auf Virtual Desktop Agents unter Windows 7, Windows 8 und Windows 2012 verwendet werden.

- XenApp (eines der folgenden Produkte):
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5, Feature Pack 2 für Windows Server 2008 R2
  - Citrix XenApp 6.5 Feature Pack 1 für Windows Server 2008 R2
  - Citrix XenApp 6.5 für Windows Server 2008 R2
  - Citrix XenApp 4, Feature Pack 2, für Unix-Betriebssysteme
- XenDesktop (eines der folgenden Produkte):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1

    - XenDesktop 7.0
    - XenDesktop 5.6 Feature Pack 1
    - XenDesktop 5.6
    - XenDesktop 5.5
    - XenDesktop 5
- Citrix VDI-in-a-Box
    - VDI-in-a-Box 5.3
    - VDI-in-a-Box 5.2
- Sie können den browserbasierten Zugriff auf Receiver für Windows 4.2.x (mit oder ohne NetScaler Gateway-Plug-In) in Kombination mit StoreFront Receiver für Web und dem Webinterface verwenden.
  StoreFront:
    - StoreFront 2.6 (empfohlen), 2.5 und 2.1
      Bietet direkten Zugriff auf StoreFront-Stores.

    - StoreFront konfiguriert mit einer Receiver für Web-Site
      Bietet Zugriff auf StoreFront-Stores über einen Webbrowser. Informationen zu den Beschränkungen dieser Bereitstellung finden Sie im Abschnitt "Wichtige Überlegungen" unter Receiver für Web-Sites.

  Webinterface mit dem NetScaler VPN-Client:
    - Webinterface 5.4 für Windows mit Webinterface-Sites
      Bietet Zugriff auf virtuelle Desktops und Apps über einen Webbrowser.

    - Webinterface 5.4 für Windows mit XenApp Services- oder XenDesktop Services-Sites
- Methoden der Bereitstellung von Receiver für Benutzer:
    - Download durch die Benutzer von receiver.citrix.com und Konfiguration unter Verwendung einer E-Mail- oder Dienstadresse in Kombination mit StoreFront
    - Angebot der Installation von Citrix Receiver für Web-Site (mit StoreFront konfiguriert)
    - Angebot der Installation von Receiver von Citrix Webinterface 5.4
    - Bereitstellen über Active Directory-Gruppenrichtlinienobjekte
    - Bereitstellen über Microsoft System Center 2012 Configuration Manager

- Internet Explorer
  Verbindungen mit Receiver für Web oder dem Webinterface unterstützen den 32-Bit-Modus von Internet Explorer. Weitere Informationen zu den unterstützten Internet Explorer-Versionen finden Sie unter StoreFront-Systemanforderungen und Webinterface-Systemanforderungen.

- Mozilla Firefox 18.x (unterstützte Mindestversion)
- Google Chrome 21 oder 20 (erfordert StoreFront)
  Hinweis: Weitere Informationen über Änderungen an der Google Chrome NPAPI-Unterstützung finden Sie im Citrix Blog-Artikel unter Preparing for NPAPI being disabled by Google Chrome .

Citrix Receiver für Windows unterstützt HTTPS- und ICA-über-TLS-Verbindungen über folgende Konfigurationen:

- LAN-Verbindungen:
    - StoreFront mit StoreFront Services- oder Receiver für Web-Sites.
    - Webinterface 5.4 für Windows mit Webinterface oder XenApp Services-Sites.

Weitere Informationen zu in Domänen eingebundenen und nicht in Domänen eingebundenen Geräten finden Sie in der XenDesktop 7-Dokumentation .

- Für sichere Remote- oder lokale Verbindungen:
  - Citrix NetScaler Gateway 10.5
  - Citrix NetScaler Gateway 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX

  Verwaltete Windows-Geräte, die zu einer Domäne gehören (lokal und remote, mit oder ohne VPN), und Geräte, die nicht zu einer Domäne gehören (mit oder ohne VPN) werden unterstützt.

  Weitere Informationen zu den von StoreFront unterstützten NetScaler Gateway- und Access Gateway-Versionen finden Sie unter StoreFront-Systemanforderungen .

Hinweis: Verweise auf NetScaler Gateway in diesem Abschnitt gelten auch für Access Gateway, soweit nicht anders angegeben.

Info zu sicheren Verbindungen und Zertifikaten

Hinweis: Weitere Informationen zu Sicherheitszertifikaten finden Sie in den Abschnitten unter Sichere Verbindungen und Sichere Kommunikation.

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 Receiver auf Citrix Ressourcen zuzugreifen.

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

Installieren von Stammzertifikaten auf Benutzergeräten

Weitere Informationen zur Installation von Stammzertifikaten auf Benutzergeräten und zur Webinterface-Konfiguration für die Verwendung von Zertifikaten finden Sie unter Sichern der Receiver-Kommunikation.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Receiver für Windows unterstützt Zertifikate mit Platzhalterzeichen. Diese sollten jedoch nur gemäß den jeweils gültigen Sicherheitsrichtlinien verwendet werden. In der Praxis kann die Verwendung von Alternativen, z. B. von Zertifikaten mit einer Liste der Servernamen in der Subject Alternative Name-Erweiterung, in Betracht gezogen werden. Solche Zertifikate können von privaten und öffentlichen Zertifizierungsstellen ausgestellt werden.

Zwischenzertifikate und NetScaler Gateway

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

Für Verbindungen mit StoreFront unterstützt Receiver die folgenden Authentifizierungsmethoden:

	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		
Sicherheitstoken				Ja*	Ja*
Zweistufig (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Ja*
Smartcard	Ja	Ja	Nein		
Benutzerzertifikat				Ja (NetScaler-Plug-In)	Ja (NetScaler-Plug-In)

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

Hinweis: Receiver für Windows 4.2.x unterstützt Zweifaktorauthentifizierung (Domäne plus Sicherheitstoken) über NetScaler Gateway für den nativen StoreFront-Dienst.
Für Verbindungen mit Webinterface 5.4 unterstützt Receiver die folgenden Authentifizierungsmethoden (bei 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) SMS	Webinterface (Browser)	Webinterface XenApp Services-Site	Ja* NetScaler bei Web Interface (Browser) Ja*	NetScaler bei Webinterface XenApp Services-Site
Smartcard	Ja	Nein		
Benutzerzertifikat			Ja (NetScaler-Plug-In)	

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

Weitere Informationen zur Authentifizierung finden Sie unter Configuring Authentication and Authorization in der NetScaler Gateway-Dokumentation und unter Verwaltung in der StoreFront-Dokumentation. Weitere Informationen zu den Authentifizierungsmethoden, die das Webinterface unterstützt, finden Sie unter Konfigurieren der Authentifizierung für das Webinterface.

Mit Receiver für Windows 4.x kann Receiver für Windows 3.x sowie das Citrix Online Plug-In 12.x aktualisiert werden. Weitere Informationen zum Upgrade finden Sie unter Überlegungen zum Upgrade.

Wichtig: Receiver für Windows 4.2.100 ist ein großes Upgrade für Receiver 3.4 Enterprise für Windows. Direkte Upgrades durch Endbenutzer werden nicht unterstützt. Vollständige schrittweise Upgradeanleitungen finden Sie unter Upgrade von Citrix Receiver 3.4 auf Receiver 4.2.100 . Das Dokument enthält Best Practices und zahlreiche Bildschirmaufnahmen, um ein unproblematisches Upgrade zu gewährleisten. Weitere Upgradeinformationen finden Sie unter Installieren von Receiver für Windows .

- **Anforderungen für .NET Framework**
  - Für das Self-Service Plug-In ist .NET 3.5 Service Pack 1 erforderlich. Benutzer können damit über das Receiver-Fenster 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++ 2005 Service Pack 1 Redistributable Package sind erforderlich, um sicherzustellen, dass das Receiver-Symbol richtig angezeigt wird. Microsoft Visual C++ 2005 Service Pack 1 ist Teil von .NET 2.0 Service Pack 1, .NET 3.5 und .NET 3.5 Service Pack 1 und ist auch separat verfügbar.
  - Für XenDesktop-Verbindungen: Für Desktop Viewer wird .NET 2.0 Service Pack 1 oder höher benötigt. Diese Version ist erforderlich, weil die Überprüfung von Zertifikatsperrlisten den Verbindungsstart verlangsamt, wenn kein Internetzugang verfügbar ist. Die Überprüfungen können in dieser Version des Frameworks deaktiviert werden, um die Startzeiten zu verbessern, aber nicht in Version .NET 2.0.
- Weitere Informationen zur Verwendung von Receiver mit Microsoft Lync Server 2013 und dem Microsoft Lync 2013 VDI Plug-In für Windows finden Sie unter XenDesktop, XenApp and Citrix Receiver Support for Microsoft Lync 2013 VDI Plug-in.

- **Unterstützte Verbindungsmethoden und Netzwerkprotokolle:**
  - TCP/IP+HTTP
    Wichtig: Wenn Stores in StoreFront mit einem Transporttyp von HTTP konfiguriert sind, müssen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKLM\Software\[Wow6432Node\]Citrix\AuthManager:

ConnectionSecurityMode=Any hinzufügen.
Informationen zu ggf. erforderlichen zusätzlichen Werten finden Sie unter CTX 134341.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

- TLS+HTTPS

Installieren von Receiver für Windows

Sep 22, 2016

Das Installationspaket CitrixReceiver.exe kann wie folgt installiert werden:

- Von einem Benutzer von Citrix.com oder Ihrer eigenen Downloadsite
  - Ein Erstbenutzer von Receiver, der Receiver von Citrix.com oder Ihrer eigenen Downloadsite herunterlädt, kann ein Konto durch Eingabe einer E-Mail-Adresse statt einer Server-URL einrichten. Receiver ermittelt den NetScaler Gateway-/Access Gateway- oder StoreFront-Server, der der E-Mail-Adresse zugeordnet ist, und fordert den Benutzer dann 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 für einen Erstbenutzer gilt nicht, wenn Receiver von einem anderen Speicherort (d. h. nicht Citrix.com) heruntergeladen wird (z. B. einer Receiver für Web-Site).
  - Wenn Receiver für Ihre Site konfiguriert werden muss, verwenden Sie eine andere Bereitstellungsmethode.
- Automatisch von Receiver für Web oder von einem Webinterface-Anmeldebildschirm .
  - Ein Erstbenutzer von Receiver 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 von Receiver muss eine für das Einrichten des Kontos eine Server-URL eingeben oder eine Provisioningdatei öffnen.

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

Wichtig: Fordern Sie Erstbenutzer von Receiver auf, Receiver nach der Installation neu zu starten. Der Neustart von Receiver stellt sicher, dass Benutzer Konten hinzufügen können, und dass Receiver USB-Geräte erkennen kann, die bei der Installation von Receiver im ausgesetzten Zustand waren.

Wichtig: Wenn das Citrix Lync Optimization Pack auf dem Endpunktgerät installiert ist, muss es zuerst deinstalliert und nach dem Upgrade von Citrix Receiver für Windows neu installiert werden. Weitere Informationen finden Sie unter CTX200340.
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 Citrix 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 Receiver ausgeführt wird.
- Als Alternative zum Bereitstellen einer Provisioningdatei können Sie den Benutzern die URL von NetScaler Gateway (oder Access Gateway Enterprise Edition) mitteilen. 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 Receiver für Web-Site, wie in der StoreFront-Dokumentation beschrieben, und der Abschluss der Konfiguration, wie unter Bereitstellen von Receiver für Windows von Receiver für Web beschrieben. Geben Sie den Benutzern die Informationen zum Upgrade von Receiver, zum Zugriff auf die Receiver für Web-Site und zum Download der Provisioningdatei von Receiver für Web (klicken Sie auf den Benutzernamen und dann auf Aktivieren).

Bereitstellungen mit dem Webinterface

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

Wichtig: Die Konfiguration der Passthrough-Authentifizierung (Single Sign-On) hat sich für Receiver für Windows 4.x geändert. Weitere Informationen finden Sie in der Beschreibung des Parameters /includeSSON unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern .
Mit Receiver für Windows 4.x kann Receiver für Windows 3.x sowie das Citrix Online Plug-In 12.x aktualisiert werden.

Für das Upgrade des Online Plug-Ins (vollständige Version), das für PNA oder Citrix Receiver (Enterprise) konfiguriert ist, auf Receiver für Windows 4.x (CitrixReceiver.exe), müssen Sie zuerst die alte Version deinstallieren und dann die neue Version installieren.

Wenn CitrixReceiver.exe bereits ohne das Online Plug-In oder mit dem Online Plug-In (Web) installiert ist, stellt ein Upgrade auf Receiver für Windows 4.x den webbasierten Zugriff auf Citrix Receiver bereit.

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

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

Receiver für Windows 4.2.100 ist ein großes Upgrade für Receiver 3.4 Enterprise für Windows. Direkte Upgrades durch Endbenutzer werden nicht unterstützt. Der IT-Administrator muss die Umgebung für das Upgrade vorbereiten, damit alle Benutzer im Netzwerk das Upgrade auf Receiver 4.2.100 erfolgreich abschließen können. Dieser Vorgang findet normalerweise im Hintergrund statt, wenn die Benutzer ihre Clients neu starten, nachdem das Receiver-Upgrade verteilt wurde.

Für das ordnungsgemäße Upgrade von Version 3.4 auf 4.2100 sind verschiedene Schritte nötig, die die gewohnte Benutzeroberfläche von Receiver 3.4 während des Upgrades gewährleisten. Der Upgradepfad hängt von den Clients ab, die für die Verwendung von Citrix StoreFront oder des älteren Webinterface konfiguriert sind. In beiden Fällen gibt es Anleitungen zum Upgrade von IMA-basierten XenApp 6.5-Umgebungen und FMA-basierten 7.6-Umgebungen.

Das Upgrade umfasst im Allgemeinen die folgenden Schritte:

1. Deinstallieren Sie Receiver 3.4 mit Gruppenrichtlinienobjekten (GPO).
2. Stellen Sie Receiver 4.2.100 mit Passthrough-Authentifizierung durch Installation per Skript bereit.
3. Konfigurieren Sie globale Anwendungsverknüpfungen im Startmenü und auf Desktops mit Gruppenrichtlinienobjekten.
4. Alternativ können Sie auch Einstellungen pro App für Startmenü- und Desktopverknüpfungen konfigurieren.
5. Führen Sie Gruppenrichtlinien aus, um Receiver zu aktualisieren und die Einstellungen per Push auf Endpunkten bereitzustellen.

Nächste Schritte

Wenn sich die Endbenutzer bei ihren Clients anmelden, werden die Gruppenrichtlinien angewendet. Es dauert einige Minuten, bis das Upgrade abgeschlossen ist. Dann müssen Benutzer sich abmelden und sich einmal an ihrer Windows-Sitzung anmelden. Der Single Sign-On-Dienst speichert die Anmeldeinformationen und bei nachfolgenden Anmeldungen werden Benutzer durch Windows Passthrough-Authentifizierung bis zu ihren veröffentlichte Apps und Desktops authentifiziert. Im

Nur-Verknüpfungsmodus müssen Benutzer nie selber Apps abonnieren. Ihre mobilen Workspace-Apps werden nach Wunsch im gewohnten Startmenü oder in Desktopordnern bereitgestellt, genau wie die lokal installierten Apps.

Hinweis: Vollständige schrittweise Upgradeanleitungen finden Sie in Upgrading from Citrix Receiver 3.4 to Receiver 4.2.100 . Das Dokument enthält Best Practices und zahlreiche Bildschirmaufnahmen, um ein unproblematisches Upgrade zu gewährleisten.

Manuelles Installieren und Deinstallieren von Receiver für Windows

May 08, 2015

Sie können Receiver 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.

Wenn Sie die Receiver-Installation vorzeitig abbrechen, wurden einige Komponenten ggf. installiert. Entfernen Sie in dieser Situation Receiver mit dem Windows-Hilfsprogramm "Programme und Funktionen" (Programme hinzufügen/entfernen).

Wichtig: Die Konfiguration der Passthrough-Authentifizierung (Single Sign-On) hat sich für Receiver für Windows 4.x geändert. Weitere Informationen finden Sie in der Beschreibung des Parameters /includeSSON unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern .
Wenn Unternehmensrichtlinien die Verwendung von EXE -Dateien verhindern, lesen Sie How to Manually Extract, Install, and Remove Individual .msi Files.

Sie können Receiver mit dem Windows-Hilfsprogramm "Programme und Funktionen" (Programme hinzufügen/entfernen) deinstallieren.
Hinweis: Verwenden Sie diese Methode nicht, wenn Receiver mit Citrix Receiver Updater installiert wurde.
Manchmal werden bei der Deinstallation von Receiver für Windows nicht alle Komponenten oder Registrierungseinträge entfernt. Wenn Sie nach der Deinstallation einer älteren Version Receiver nicht installieren können, entfernen Sie alte Dateien und Registrierungseinträge mit dem Hilfsprogramm Receiver Clean-Up .

Wenn Sie Dateien oder Registrierungseinträge, die zu Receiver gehören, vor der Deinstallation von Receiver mit "Programme und Funktionen" löschen, schlägt die Deinstallation möglicherweise fehl. Der Microsoft Windows Installer (MSI) versucht gleichzeitig eine Reparatur und eine Deinstallation. Starten Sie in diesen Situationen eine automatische Reparatur mit Receiver. Nach dem Abschluss der automatischen Reparatur können Sie Receiver sauber mit "Programme und Funktionen" deinstallieren.

Die automatische Reparatur wird bei einem Problem mit Receiver ausgeführt; es gibt jedoch keine Option "Reparieren" in "Programme und Funktionen" für Receiver. Wenn Sie in der Option "Reparieren" für Receiver den Speicherort der MSI-Datei angeben müssen, navigieren Sie zu einem dieser Speicherorte:

- Bei einer Installation pro Computer:
  - Betriebssystem: Windows Server 2012/2008, Windows 8, Windows 7, Windows Vista
    C:\Programme\Citrix\Citrix Receiver\
  - Betriebssystem: Windows 2003 und Windows XP
    C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Citrix\Citrix Receiver\
- Bei einer Installation pro Benutzer:
  - Betriebssystem: Windows Server 2012/2008, Windows 8, Windows 7, Windows Vista
    %USERPROFILE%\Appdata\local\Citrix\Citrix Receiver\

- Betriebssystem: Windows 2003 und Windows XP
  %USERPROFILE%\Lokale Einstellungen\Anwendungsdaten\Citrix\Citrix Receiver\

Entfernen von Receiver über die Befehlszeile

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

CitrixReceiver.exe /uninstall

Nach der Deinstallation von Receiver von einem Benutzergerät verbleiben die mit icaclient.adm angepassten Registrierungsschlüssel für die Receiver-Einstellungen im Verzeichnis Software\Policies\Citrix\ICA Client unter HKEY_LOCAL_MACHINE und HKEY_LOCAL_USER. Wenn Sie Receiver neu installieren, werden diese Richtlinien u. U. wirksam und können zu unerwartetem Verhalten führen. Um diese Anpassungen zu entfernen, löschen Sie sie manuell.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern

Oct 26, 2015

Passen Sie das Receiver-Installationsprogramm mit Befehlszeilenoptionen an. Das Installationspaket wird automatisch vor dem Start des Setupprogramms im Temp-Verzeichnis des Benutzers extrahiert und benötigt 78,8 MB freien Speicherplatz im Verzeichnis %temp%. Der benötigte Speicherplatz berücksichtigt Programmdateien, Benutzerdaten und Temp-Verzeichnisse nach dem Start mehrerer Anwendungen.

Citrix Receiver 4.2 für Windows herunterladen.

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.
Installieren sie Receiver für Windows an einer Eingabeaufforderung mit der folgenden Syntax:

CitrixReceiver.exe [**Options**]

Es gibt folgende Optionen:

- /? oder /help zeigen Syntaxinformationen an.
- /noreboot unterdrückt einen Neustart bei Installationen der Benutzeroberfläche. Diese Option wird nicht bei Installationen ohne Benutzereingriffe benötigt. Wenn Sie Neustartaufforderungen unterdrücken, werden USB-Geräte, die bei der Receiver-Installation im ausgesetzten Zustand sind, erst nach dem Neustart des Benutzergeräts von Receiver erkannt.
- /silent deaktiviert die Fehler- und Fortschrittsdialogfelder und führt eine unbeaufsichtigte Installation durch. Siehe auch: /noreboot.
- /includeSSON installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Diese Option wird für Smartcard-Single Sign-On benötigt.
  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 Receiver mit lokalen Administratorrechten über eine Befehlszeile installieren, die die Option /includeSSON enthält. Auf dem Benutzergerät müssen Sie zudem die folgenden Richtlinien aktivieren, die Sie hier finden: Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung:

  Lokaler Benutzername und Kennwort

  Passthrough-Authentifizierung aktivieren

  Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen (abhängig von der Konfiguration des Webinterface und der Sicherheitseinstellungen möglicherweise notwendig)

  Starten Sie nach dem Ausführen der Änderungen das Benutzergerät neu. Weitere Informationen finden Sie unter How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication.

Hinweis: Die Richtlinien "Smartcard", "Kerberos" und "Local user name and password" 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.

- PROPERTY=Value
  Wobei PROPERTY eine der folgenden in Großbuchstaben geschriebenen Variablen (Schlüssel) ist, die mit einem Valueangegeben wird.

  - INSTALLDIR=Installation directory, wobei Installation directory 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, Receiver und das Self-Service Plug-In. Wenn Sie diese Option verwenden und ein Installation directoryangeben, müssen Sie RIInstaller.msi im Verzeichnis Installation directory\Receiver und die anderen MSI-Dateien im Installation directory installieren.

  - CLIENT_NAME=ClientName, wobei ClientName der Name ist, mit dem das Benutzergerät für die Serverfarm identifiziert wird. Der Standardwert ist %COMPUTERNAME%.
  - ENABLE_DYNAMIC_CLIENT_NAME={Yes | No}. 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.
  - featureADDLOCAL=[,...] 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.
    Hinweis: ReceiverInside und ICA_Client sind Voraussetzungen für alle anderen Komponenten und müssen installiert werden.
    ReceiverInside: Installiert die Receiver-Oberfläche. (Erforderliche Komponente für die Funktion von Receiver.)

    ICA_Client: Installiert den Standard-Receiver. (Erforderliche Komponente für die Funktion von Receiver.)

    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 unter http://support.citrix.com/article/CTX200337.

    Das Self-Service Plug-In ermöglicht Benutzern den Zugriff auf virtuelle Desktops und Anwendungen vom Receiver-Fenster aus oder über eine Befehlszeile. Dies wird nachfolgend unter
    — Starten eines virtuellen Desktops oder einer Anwendung an einer Befehlszeile
    erläutert.

    USB: Installiert die USB-Unterstützung. Hierfür sind Administratorrechte erforderlich.

    DesktopViewer: Installiert Desktop Viewer.

    Flash: Installiert HDX MediaStream für Flash.

    Vd3d: Aktiviert die Windows Aero-Oberfläche (für Betriebssysteme, die sie unterstützen)

- ALLOWADDSTORE={N | S | A}: Gibt an, ob Benutzer Stores, die nicht in Merchandising Server-Bereitstellungen konfiguriert sind, hinzufügen und entfernen können. (Benutzer können Stores, die in Merchandising Server-Bereitstellungen konfiguriert sind, aktivieren oder deaktivieren. Sie können sie aber nicht entfernen oder Namen oder URLs ändern.) Der Standard ist S.
  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 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:
  1. Stellen Sie HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore auf A ein, damit Benutzer nicht sichere Stores hinzufügen können.
  2. Stellen Sie HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd auf A ein, damit Benutzer die Kennwörter für nicht sichere Stores speichern können.
  3. Damit ein Store, der in StoreFront mit einem Transporttyp von HTTP konfiguriert ist, hinzugefügt werden kann, fügen Sie HKLM\Software\[Wow6432Node\]Citrix\AuthManager den Wert ConnectionSecurityMode (Typ REG_SZ) hinzu und stellen ihn auf Any ein.
  4. Beenden und starten Sie Receiver neu.
- ALLOWSAVEPWD={N | S | A}: 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.
  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\AllowSavePwd steuern.

  Hinweis: Der folgenden Registrierungsschlüssel muss manuell hinzugefügt werden, wenn AllowSavePwd nicht funktioniert.
  Schlüssel für 32-Bit-Client: HKLM\Software\Citrix\AuthManager

  Schlüssel für Client mit 64-Bit-Betriebssystem: HKLM\Software\wow6432node\Citrix\AuthManager

  Name: SavePasswordMode

  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.
- ENABLE_SSON={Yes | No}: Der Standardwert ist Yes. Aktiviert Single Sign-On, wenn /includeSSON ebenfalls angegeben ist. Diese Eigenschaft wird für Smartcard-Single Sign-On 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.
Wichtig: Wenn Sie die Single Sign-On-Authentifizierung deaktivieren, müssen Benutzer Receiver neu installieren, wenn Sie sie später aktivieren.

- AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry } : 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.

- AM_SMARTCARDPINENTRY=CSP: Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von 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.
  Sie können dieses Feature auch mit dem Registrierungsschlüssel HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP steuern.

- ENABLE_KERBEROS={Yes | No}: 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 der Domänen-Passthrough-Authentifizierung mit Kerberos.
- LEGACYFTAICONS={False | True}: 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.
- ENABLEPRELAUNCH={False | True}: Der Standardwert ist False. Weitere Informationen zum Vorabstart von Sitzungen finden Sie unter Verkürzen des Anwendungsstarts.
- STARTMENUDIR=Text stringTextzeichenfolge: Anwendungen werden in der Standardeinstellung 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 angeben, dass der Clientanwendungsordner dem Verknüpfungspfad wie folgt angehängt wird: Erstellen Sie einen REG_SZ-Eintrag für UseCategoryAsStartMenuPath

und geben Sie ihm einen Wert von "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, UseCategoryAsStartMenuPath von true und keiner Angabe von StartMenuDir werden Verknüpfungen unter Start > Alle Programme > Office abgelegt. Bei einem Clientanwendungsordner von \Office, UseCategoryAsStartMenuPath von true und StartMenuDir von \Receiver werden Verknüpfungen unter Start > Alle Programme > Office abgelegt.

Änderungen an diesen Einstellungen wirken sich nicht auf bereits erstellte Verknüpfungen aus. Zum Verschieben von Verknüpfungen müssen Sie die Anwendungen deinstallieren und dann neu installieren.

- STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On | Off];[storedescription]"[STOREy="..."] – Gibt bis zu 10 Stores für die Verwendung mit Receiver an.. 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.domain : Der vollqualifizierte Domänenname des Servers, der den Store hostet.
  - IISLocation : Der Pfad zum Store in IIS. Die Store-URL muss mit der URL in 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 .
  - 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.
  - ALLOW_CLIENTHOSTEDAPPSURL=1: Aktiviert die URL-Umleitung auf Benutzergeräten. Hierfür sind Administratorrechte erforderlich. Receiver muss für alle Benutzer installiert sein. Weitere Informationen zur URL-Umleitung finden Sie in den Abschnitten Lokaler App-Zugriff in der XenDesktop 7-Dokumentation.
  - SELFSERVICEMODE={False | True}: Der Standardwert ist "True". Wenn der Administrator das SelfServiceMode-Flag auf "false" festlegt, hat der Benutzer keinen Zugriff mehr auf die Self-Service-Benutzeroberfläche von Receiver. Der Zugriff auf abonnierte Apps ist stattdessen über das Startmenü und über Desktopverknüpfungen möglich. Dies wird als "Nur-Verknüpfungsmodus" bezeichnet. Weitere Informationen hierzu finden Sie unter Konfigurieren des Nur-Verknüpfungsmodus.
  - DESKTOPDIR=Dir_Name: fasst alle Verknüpfungen in einem Ordner zusammen. CategoryPath wird für Desktopverknüpfungen unterstützt.
    Hinweis: Für DESKTOPDIR muss der Schlüssel PutShortcutsOnDesktop auf "True" festgelegt werden. Weitere Informationen hierzu finden Sie unter Konfigurieren des Nur-Verknüpfungsmodus.

Anzeigen eines Dialogfelds "Installation abgeschlossen" während unbeaufsichtigten Installationen

Bei unbeaufsichtigten Installationen von CitrixReceiver.exe wird einem Erstbenutzer ein Dialogfeld für die Kontoeinrichtung vor dem Abschluss der Installation angezeigt. Der Benutzer muss eine E-Mail-Adresse oder eine Serveradresse in das Dialogfeld "Konto hinzufügen" eingeben, um die Installation abzuschließen. Sie können das Dialogfeld "Konto hinzufügen" durch ein Dialogfeld zum Einrichten eines Kontos ersetzen, das dem Benutzer nach dem Abschluss der Installation angezeigt wird, indem Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKCU\Software\Citrix\Receiver and HKCU\Software\Policies\Citrix: **EnableFTU**=0 hinzufügen.

Fügen Sie den gleichen Registrierungsschlüssel den maschinenweiten Richtlinien hinzu, wenn sich mehrere Benutzer an derselben Maschine anmelden.

Hinweis: Wenn durch das STOREx-Argument oder ein Gruppenrichtlinienobjekt kein gemeinsamer Speicher definiert wurde, wird für Benutzer, die sich zuvor noch nicht bei einem Computer, auf dem Receiver installiert ist, angemeldet haben, möglicherweise das Dialogfeld zum Hinzufügen eines Kontos angezeigt. Zum Unterdrücken dieses Dialogfelds erstellen Sie einen REG_DWORD-Wert **EnableFTU** in einem der folgenden Registrierungsschlüssel HKCU\Software\Citrix\Receiver oder HKCU\Software\Policies\Citrix und setzen den Wert 0.

Behandlung von Installationsproblemen

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;Apps on HR"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Backup Store Apps on HR"
```

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"
```

Receiver erstellt eine Stubanwendung für jede 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.

Bereitstellen von Receiver für Windows mit Active Directory und Beispielstartskripts

May 19, 2015

Sie können Active Directory-Gruppenrichtlinienskripts verwenden, um Receiver basierend auf der Active Directory-Organisationsstruktur auf Systemen vorab bereit zu stellen. Citrix empfiehlt, dass Sie die Skripts verwenden, statt die MSI-Dateien zu extrahieren, da Sie mit Skripts die Installation, Upgrade und Deinstallation an einer Stelle durchführen. Durch die Skripts werden die Citrix Einträge in "Programme und Funktionen" konsolidiert und es ist leichter zu erkennen, welche 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 Skripte sind auf den aktuellen XenApp-Medien im Ordner "Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts".

- 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 ein Gruppenrichtlinienobjekt (GPO) für die neu erstellte OU.

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

- **Current Version of package**: Die angegebene Versionsnummer wird validiert und es wird mit der Bereitstellung fortgefahren, 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.

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.

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.

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.

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

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Wählen Sie Benutzerkonfiguration > 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.

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.

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 Receiver für Windows über Receiver für Web

May 08, 2015

Sie können Receiver über Receiver für Web bereitstellen, um sicherzustellen, dass Receiver auf dem Benutzergerät installiert ist, bevor der Benutzer versucht, über einen Browser eine Verbindung zu einer Anwendung herzustellen. Mit Receiver für Web-Sites können Benutzer über eine Webseite auf StoreFront-Stores zugreifen. Wenn die Receiver für Web-Site erkennt, dass ein Benutzer keine kompatible Receiver-Version hat, wird der Benutzer zum Download und zur Installation von Receiver aufgefordert. Weitere Informationen finden Sie unter Receiver für Web-Sites in der StoreFront-Dokumentation.

Die e-mail-basierte Kontenermittlung gilt nicht, wenn Receiver von Receiver für Web bereitgestellt wird. Wenn die e-mail-basierte Kontenermittlung konfiguriert ist und ein Erstbenutzer Receiver von Citrix.com installiert, fordert Receiver 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.
   Wichtig: Beim Namen CitrixReceiverWeb.exe wird die Groß-/Kleinschreibung beachtet.
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-Sites mit Konfigurationsdateien in der StoreFront-Dokumentation.

Bereitstellen von Citrix Receiver für Windows über einen Webinterface-Anmeldebildschirm

May 08, 2015

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

Sie können Receiver auf einer Webseite bereitstellen, um sicherzustellen, dass Receiver 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 Receiver-Version hat, wird der Benutzer zum Download und zur Installation von Receiver aufgefordert.

Weitere Informationen finden Sie unter Konfigurieren der Clientbereitstellung in der Webinterface-Dokumentation.

Die e-mail-basierte Kontenermittlung gilt nicht, wenn Receiver vom Webinterface bereitgestellt wird. Wenn die e-mail-basierte Kontenermittlung konfiguriert ist und ein Erstbenutzer Receiver von Citrix.com installiert, fordert Receiver 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.
   Wichtig: Beim Namen CitrixReceiverWeb.exe wird die Groß-/Kleinschreibung beachtet.
3. Geben Sie den geänderten Dateinamen im Parameter ClientIcaWin32 in den Konfigurationsdateien für die XenApp-Websites an.
   Für den Clienterkennungs- und -bereitstellungsprozess müssen die Receiver-Installationsdateien auf dem Webinterface-Server vorhanden sein. Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Receiver-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.

Konfigurieren von Receiver für Windows

May 18, 2015

Wenn Sie 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 Receiver. Dieser Modus ermöglicht Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Receiver.
- Konfigurieren des Nur-Verknüpfungsmodus einschließlich:
  - Konfigurieren von Verknüpfungen mit einer Gruppenrichtlinienobjektvorlage :
  - Konfigurieren von Verknüpfungen mit Registrierungsschlüsseln
  - Konfigurieren von Verknüpfungen basierend auf StoreFront-Kontoeinstellungen
- Bereitstellen der Kontoinformationen für Benutzer 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.

Konfigurieren der Anwendungsbereitstellung

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit XenDesktop oder XenApp, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen zu erhöhen:

Webzugriffsmodus

Ohne jegliche Konfiguration bietet Receiver für Mac im Webzugriffsmodus browserbasierten Zugriff auf Anwendungen und Desktops. Benutzer greifen einfach über einen Browser auf eine Receiver für Web- oder Webinterface-Site zu und wählen die gewünschten Anwendungen zur Verwendung aus. Im Webzugriffsmodus werden keine Appverknüpfungen im App-Ordner auf den Benutzergeräten platziert.

Self-Service-Modus

Sie konfigurieren den Self-Service-Modus durch Hinzufügen eines Kontos für StoreFront oder für eine Webinterface Services-Site zu Receiver für Windows. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über Receiver. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores. Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren. Wenn ein Benutzer eine Anwendung auswählt, wird eine Verknüpfung für die Anwendung im App-Ordner auf dem Benutzergerät platziert.

Beim Zugreifen auf eine StoreFront 3.0-Site erleben Benutzer die Receiver-Benutzererfahrung. Weitere Informationen zur Receiver-Benutzererfahrung finden Sie unter StoreFront 3.0 Technology Preview.

Wenn Sie Anwendungen auf einer XenApp-Farm veröffentlichen, können Sie die Erfahrung für Benutzer verbessern, die auf diese Anwendungen über StoreFront-Stores zugreifen, indem Sie aussagekräftige Beschreibungen für die veröffentlichten Anwendungen hinzufügen. In Citrix Receiver sind diese Beschreibungen für Benutzer sichtbar.

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

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

- Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge KEYWORDS:Auto an die Beschreibung anhängen, die Sie beim Veröffentlichen der Anwendung in XenApp angeben. 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.

Weitere Informationen finden Sie in der Dokumentation für StoreFront .

Wenn das Webinterface in der XenApp-Bereitstellung keine XenApp Services-Site hat, erstellen Sie eine Site. Der Name und die Erstellung der Site hängen von der installierten Webinterface-Version ab. Weitere Informationen finden Sie in der Dokumentation zum Webinterface.

Mit Receiver StoreFront bestehen die erstellten Stores aus Diensten, die eine Authentifizierungs- und Ressourcenbereitstellungsinfrastruktur für Citrix Receiver bereitstellen. Erstellen Sie Stores, die Desktops und Anwendungen von XenDesktop-Sites und XenApp-Farmen auflisten und aggregieren und diese Ressourcen Benutzern zur Verfügung stellen.

1. Installieren und konfigurieren Sie StoreFront. Weitere Informationen finden Sie in der StoreFront-Dokumentation .

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

Konfigurieren der Anwendungsbereitstellung

Apr 21, 2015

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit XenDesktop oder XenApp, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen zu erhöhen.

- Webzugriffsmodus: Ohne jegliche Konfiguration ermöglicht Receiver für Windows 4.2.100 browserbasierten Zugriff auf Anwendungen und Desktops. Benutzer 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 Receiver oder durch Verweisen von Receiver auf eine StoreFront-Site und ermöglichen Benutzern auf diese Weise das Abonnieren von Anwendungen über die Benutzeroberfläche von Receiver. 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 Receiver für Windows 4.2.100 Anwendungen zur Anzeige im Startmenü auswählen.

- Nur-Verknüpfungsmodus: Als Administrator für Receiver können Sie Receiver für Windows 4.2.100 so konfigurieren, dass Verknüpfungen für Anwendungen und Desktops ähnlich wie bei Receiver für Windows 3.4 Enterprise direkt im Startmenü oder auf dem Desktop platziert werden. Mit dem neuen *Nur-Verknüpfungsmodus* werden Benutzern 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 Receiver den Webzugriffs- oder Self-Service-Modus verwenden.
Weitere Informationen zum Konfigurieren von Verknüpfungen im Startmenü oder auf dem Desktop finden Sie unter Konfigurieren des Nur-Verknüpfungsmodus in der Citrix Produktdokumentation.

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

Hinweis: Standardmäßig können Benutzer von Receiver für Windows 4.2.100 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 obligatorisch zu machen, sodass sie nicht aus 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 Highlightliste von Receiver aufzulisten.

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. Die Benutzer müssen Anwendungen dann nicht über die 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 Receiver-Administrator können Sie Befehlszeilen-Installationsflags, Gruppenrichtlinienobjekte, Kontodienste oder Registrierungseinstellungen zum Deaktivieren der normalen Self-Service-Schnittstelle von Receiver verwenden und diese mit einem vorkonfigurierten Startmenü ersetzen. Das Flag heißt SelfServiceMode und ist standardmäßig auf true festgelegt. Wenn der Administrator das Flag SelfServiceMode auf false festlegt, hat der Benutzer keinen Zugriff mehr auf die Self-Service-Benutzeroberfläche von 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. Weitere Informationen finden Sie unter Konfigurieren von Speicherorten für App-Verknüpfungen mit Registrierungsschlüsseln.

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 Receiver-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 Receiver 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.

Hinweis: Sie müssen Änderungen an der Gruppenrichtlinie vor dem Konfigurieren eines Stores vornehmen. Möchten Sie oder ein Benutzer die Gruppenrichtlinie ändern, müssen Sie oder der Benutzer 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 icaclient.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 zu Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Components > Citrix Receiver > User Experience > Self-Service. **Hinweis** Die Vorlage icaclient.adm ist auch in der Benutzerkonfiguration verfügbar, nachdem sie zur Computerkonfiguration hinzugefügt wurde.
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.

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 eine Sicherungskopie 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	Falsch	HKLM\SOFTWARE\Policies\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
		HKLM\Software\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	Falsch	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\Software\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	Falsch	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	Wahr	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\Software\Citrix\Dazzle
SelfServiceMode	Wahr	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\Software\Citrix\Dazzle
UseCategoryAsStartMenuPath	Wahr	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
		HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
StartMenuDir	"" (leer)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\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\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\Software\Citrix\Dazzle
AutoReinstallModifiedApps	Wahr	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\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	Wahr	HKCU\Software\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
		HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\Software\Citrix\Dazzle
WSCReconnectAll	Wahr	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	Falsch	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	Falsch	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

Name	Standardwert	Orte in der Reihenfolge der Priorität
		HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	Falsch	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	Wahr	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	Wahr	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	Wahr	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	"" (leer)	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKCU\Software\Citrix\Dazzle

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

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

Sie können Verknüpfungen im Startmenü und auf dem Desktop von der StoreFront-Site aus einrichten. Die folgenden Einstellungen können im Abschnitt 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 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:

Der Abschnitt endet mit dem Tag .
Vor dem Ende des Abschnitts "account" ist der Abschnitt "properties" mit den Eigenschaften:

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

Hinweis: Wenn Eigenschaftenelemente vor dem Tag hinzugefügt werden, sind sie u. U. ungültig. Sie können das Tag entfernen, wenn Sie einen Eigenschaftsnamen und -wert hinzufügen.
Ausführliches Beispiel für diesen Abschnitt:

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.

Mit Receiver können Anwendungs- und Desktopverknüpfungen direkt in das Startmenü oder auf dem Desktop platziert werden. Ältere Versionen von 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 Einstellungen pro App in XenApp 6.5

Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 6.5:

1. Öffnen Sie in XenApp im Bildschirm Anwendungseigenschaften das Eigenschaftendialogfeld Grundlagen.
2. Wählen Sie die Option Verknüpfungsdarstellung.
3. Aktivieren Sie im Bildschirm " Verknüpfungsdarstellung" im Bereich Anwendungsverknüpfung festlegen das Kontrollkästchen Zu Startmenü von Client hinzufügen . Geben Sie anschließend den Namen des Ordners ein, in dem die Verknüpfung platziert werden soll. Wenn Sie keinen Ordnernamen angeben, platziert XenApp die Verknüpfung im Startmenü und nicht in einem Ordner des Startmenüs.
4. Aktivieren Sie Verknüpfung dem Clientdesktop hinzufügen , damit eine Verknüpfung auch auf dem Desktop der Clientmaschine erstellt wird.
5. Klicken Sie auf Anwenden.
6. Klicken Sie auf OK.

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.

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 eine Sicherungskopie 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:

1. Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs" hinzu.
2. Fügen Sie mit dem Registrierungs-Editor HKLM\Software\Citrix\Dazzle /v
3. CopyStubsFromCommonStubDirectory /t REG_SZ /d "true" hinzu. Diese Einstellungen sind auch über HKCU möglich. HKCU hat Vorrang vor HKLM.
4. Beenden und starten Sie Receiver, um die Einstellungen zu testen.

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 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 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 Receiver dazu ohne Konfiguration und navigieren Sie zu Receiver für Web und Webinterface. Sie können für Receiver auch Self-Service-Zugriff konfigurieren, ohne Verknüpfungen zu erstellen.

Wenn Receiver nicht automatisch Anwendungsverknüpfungen im Startmenü platzieren soll...	konfigurieren Sie Receiver mit PutShortcutsInStartMenu=False. 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 Receiver automatisch alle Anwendungsverknüpfungen im Startmenü platzieren soll...	konfigurieren Sie Receiver mit SelfServiceMode=False. Alle verfügbaren Apps werden dann im Startmenü angezeigt.
Wenn alle Anwendungsverknüpfungen auf dem Desktop platziert werden sollen...	konfigurieren Sie 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 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 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 Receiver im Startmenü platzierten Anwendungsverknüpfungen in den zugeordneten Kategorieordnern angezeigt werden sollen...	konfigurieren Sie Receiver mit UseCategoryAsStartMenuPath=True. 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.
Wenn die von Receiver im Startmenü platzierten Anwendungsverknüpfungen in einem bestimmten Ordner angezeigt werden sollen...	konfigurieren Sie 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 Receiver alle Apps beim Abmelden entfernen soll...	konfigurieren Sie Receiver mit RemoveAppsOnLogoff=True.
Wenn Receiver alle Apps beim Beenden entfernen soll...	konfigurieren Sie Receiver mit RemoveAppsOnExit=True.

Konfigurieren von lokalem App-Zugriff für Anwendungen:

- Wenn eine lokal installierte Anwendung statt einer in Receiver verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge KEYWORDS:prefer="pattern" an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.
  Bevor 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 Receiver die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Receiver-Fenster aus startet, startet Receiver die lokal installierte (bevorzugte) Anwendung.

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

Hinweis: Das Schlüsselwort prefer wird angewendet, wenn 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 Receiver verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge KEYWORDS:prefer=" pattern" an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.
  Bevor 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 Receiver die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Receiver-Fenster aus startet, startet Receiver die lokal installierte (bevorzugte) Anwendung.

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

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

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Word	\Microsoft Office\Microsoft **Word** 2010	Ja
"Microsoft Word"	\Microsoft Office**Microsoft Word** 2010	Ja
Konsole	\McAfee\VirusScan **Console**	Ja
Virus	\McAfee\VirusScan Console	Nein
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 im Abschnitt "Zusätzliche Empfehlungen" unter Optimieren der Benutzererfahrung in der StoreFront-Dokumentation.

Konfigurieren der XenDesktop-Umgebung

May 29, 2013

In diesen Abschnitten wird beschrieben, wie Sie die USB-Unterstützung konfigurieren, verhindern, dass das Desktop Viewer-Fenster abgeblendet wird, und Einstellungen für mehrere Benutzer und Geräte konfigurieren.

Mit der USB-Unterstützung können Benutzer mit zahlreichen USB-Geräten interagieren, wenn sie mit einem virtuellen Desktop verbunden sind. Benutzer 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 Webkameras, 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 XenDesktop- bzw. XenApp-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

Hinweis: 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 unter Konfigurieren von Bloomberg-Tastaturen. Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie unter CTX119722.
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-Grafikkarten

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

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

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

Weitere Informationen zum Ändern des Bereichs der USB-Geräte, die Benutzern zur Verfügung stehen, finden Sie unter Aktualisieren der für Remoting verfügbaren USB-Geräte-Liste.

Anleitungen, wie Sie bestimmte USB-Geräte automatisch umleiten, finden Sie unter 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.

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.

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. Anleitungen hierzu finden Sie unter 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 Clientlaufwerkszuordnung 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. Anleitungen hierzu finden Sie unter 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. Webkameras, digitale Camcorder, analoge Videokonverter, einige Fernsehtuner und einige digitale Kameras, die Videostreaming unterstützen.
  Hinweis: Moderne Videostreaminggeräte verwenden meistens isochrone Transfers, die von XenDesktop 4 oder höher

unterstützt werden. Für manche Videogeräte (z. B. Webcams mit Bewegungserkennung) ist eine zusätzliche Konfiguration erforderlich. Anleitungen hierzu finden Sie unter 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): Viele Geräte verwenden herstellerspezifische Protokolle oder Protokolle, die nicht vom USB-Konsortium genormt sind; sie werden normalerweise als herstellerspezifisch (Geräteklasse ff) angezeigt.

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 Mäuse verwendet.

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

- USB-Hub (Geräteklasse 09): Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.
- Chipkarte (Smartcard) (Geräteklasse 0b): Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.
  Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.

- Kabelloser 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.

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

:\Programme\Citrix\ICA Client\Configuration\

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 eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.
Die Standardregeln für das Produkt sind an folgendem Speicherort gespeichert:

HKLM\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules" Value=

Ändern Sie nicht die Produktstandardregeln.

Weitere Informationen zu Regeln und deren Syntax finden Sie unter http://support.citrix.com/article/ctx119722/.

Bloomberg-Tastaturen (aber keine anderen USB-Tastaturen) werden in XenDesktop- und XenApp-Sitzungen unterstützt. Die benötigten Komponenten werden automatisch mit dem Plug-in installiert; Sie müssen dieses Feature jedoch entweder während der Installation oder später durch Ändern eines Registrierungsschlüssels aktivieren.

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

Aktivieren bzw. 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 eine Sicherungskopie 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.

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 eine Sicherungskopie 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:

- HKCU\Software\Citrix\XenDesktop\DesktopViewer
- HKLM\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:

- HKCU\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKLM\Software\Policies\Citrix\XenDesktop\DesktopViewer

Die Verwendung der Registrierungsschlüssel ist optional, da XenDesktop-Administratoren und nicht Plug-In-Administratoren oder Benutzer 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:

   1. HKCU\Software\Policies\Citrix\...
   2. HKLM\Software\Policies\Citrix\...
   3. HKCU\Software\Citrix\...
   4. HKLM\Software\Citrix\...

Zusätzlich zu den Konfigurationsoptionen in der Receiver-Benutzeroberfläche können Sie den Gruppenrichtlinienobjekt-Editor und die Vorlagendatei icaclient.adm zum Konfigurieren von Einstellungen verwenden. Mit dem Gruppenrichtlinienobjekt-Editor haben Sie folgende Möglichkeiten:

- Sie können die icaclient-Vorlage erweitern, sodass alle Receiver-Einstellungen abgedeckt werden, indem Sie die Datei icaclient.adm bearbeiten. Weitere Informationen über das Bearbeiten von ADM-Dateien und das Anwenden von Einstellungen auf bestimmte Computer finden Sie in der Microsoft Gruppenrichtliniendokumentation.
- Sie können Änderungen nur für bestimmte oder für alle Benutzer eines Clientgeräts machen.
- Sie können Einstellungen für mehrere Benutzergeräte konfigurieren.

Citrix empfiehlt, Benutzergeräte mit Gruppenrichtlinien remote zu konfigurieren. Sie können aber eine beliebige Methode, einschließlich des Registrierungs-Editors, zum Aktualisieren der relevanten Registrierungseinträge verwenden.

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 icaclient-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 icaclient.adm aus.

5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Bearbeiten Sie die relevanten Einstellungen unter dem Knoten Benutzerkonfiguration oder Computerkonfiguration.

Konfigurieren von StoreFront

Nov 10, 2014

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 Receiver zugreifen. Zusätzlich zu der Konfiguration, die in diesem Abschnitt zusammengefasst ist, müssen Sie außerdem NetScaler Gateway oder Access 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).

1. Installieren und konfigurieren Sie StoreFront, wie in der StoreFront-Dokumentation beschrieben. Receiver für Windows benötigt eine HTTPS-Verbindung. Wenn der StoreFront-Server für HTTP konfiguriert ist, muss ein Registrierungsschlüssel auf dem Benutzergerät eingestellt werden, wie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern unter der Beschreibung der Eigenschaft ALLOWADDSTORE beschrieben.
   Hinweis: Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für Receiver erstellen.

Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage

Feb 05, 2015

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 icaclient.adm zu konfigurieren.

Sie können die Vorlagendatei icaclient.adm für Domänenrichtlinien und lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Dies ist besonders nützlich, wenn Sie Receiver-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 Angeben von Stores mit einem Gruppenrichtlinienobjekt:

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 icaclient-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 icaclient.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 unter dem Knoten Computerkonfiguration zu Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix-Komponenten > Citrix Receiver > StoreFront und wählen Sie StoreFront-Kontenliste.
7. Bearbeiten Sie die Einstellungen. Verwenden Sie die Informationen im nächsten Schritt, um Konten hinzuzufügen oder anzugeben.
8. Geben Sie eine Liste mit StoreFront-Konten ein. Geben Sie für jeden Eintrag die folgenden Informationen durch Semikolons getrennt ein:
   - Storename: Der Name, der dem Benutzer für diesen Store angezeigt wird.
   - Store-URL: Die URL des Stores.
   - Storeaktivierungszustand: Aktiviert (On) oder Deaktiviert (Off).
   - Store-Beschreibung: Die Beschreibung, die dem Benutzer für diesen Store angezeigt wird.

   Beispiel: SalesStore;https://sales.example.com/Citrix/Store/discovery;On;Store für Vertriebsmitarbeiter

Bereitstellen der Kontoinformationen für Benutzer

Oct 08, 2015

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
- Bereitstellen von Kontoinformationen zur benutzerseitigen manuellen Eingabe

Wichtig: Fordern Sie Erstbenutzer von Receiver auf, Receiver nach der Installation neu zu starten. Der Neustart von Receiver stellt sicher, dass Benutzer Konten hinzufügen können, und dass Receiver USB-Geräte erkennen kann, die bei der Installation von Receiver im ausgesetzten Zustand waren.

Wenn Sie Receiver für die Kontodiscovery mit der E-Mail-Adresse konfigurieren, geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration von Receiver ein. Receiver ermittelt den NetScaler Gateway-, Access 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 in Bereitstellungen mit dem Webinterface unterstützt.
Weitere Informationen zur Konfiguration des DNS-Servers für die e-mail-basierte Kontenermittlung finden Sie unter Konfigurieren der e-mail-basierten Kontenermittlung in der StoreFront-Dokumentation.

Weitere Informationen zur Konfiguration von NetScaler Gateway finden Sie unter Connecting to StoreFront by using email-based discovery in der NetScaler Gateway-Dokumentation.

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 Receiver automatisch konfigurieren können. Nach der Receiver-Installation öffnen Benutzer die Datei, um Receiver zu konfigurieren. Wenn Sie Receiver für Web-Sites konfigurieren, können Benutzer Receiver-Provisioningdateien auch von diesen Seiten abrufen.
  Weitere Informationen finden Sie unter Exportieren der Store-Provisioningdateien für Benutzer in der StoreFront-Dokumentation.

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:
  NetScalerGatewayFQDNMyStoreName
  Wenn z. B. für Store namens "SalesApps" der Remotezugriff auf server1.com aktiviert ist und für Store namens "HRApps" Remotezugriff auf server2.com aktiviert ist, dann muss ein Benutzer server1.com?SalesApps für den Zugriff auf SalesApps eingeben, oder 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 Angaben für ein neues Konto macht, versucht Receiver, die Verbindung zu überprüfen. Wenn die Verbindung hergestellt werden kann, fordert Receiver den Benutzer auf, sich an dem Konto anzumelden.

Zum Verwalten von Konten öffnet ein Receiver-Benutzer die Receiver-Homepage, klickt auf Symbol "Pfeil-nach-unten" und dann auf Konten.

Optimieren der Receiver-Umgebung

Oct 30, 2014

Sie können die Umgebung optimieren, in der Receiver für die Benutzer ausgeführt wird.

- Verkürzen des Anwendungsstarts
- Vereinfachen der Verbindung von Geräten mit veröffentlichten Ressourcen
- Unterstützen der DNS-Namensauflösung
- Verwenden von Proxyservern für XenDesktop-Verbindungen
- Unterstützen von NDS-Benutzern
- Verwenden von Receiver mit XenApp für UNIX
- Aktivieren des Zugriffs auf anonyme Anwendungen

Weitere Informationen zu anderen Optimierungsoptionen finden Sie den Abschnitten der XenDesktop-Dokumentation, die mit dem Verwalten der Sitzungsaktivität und dem Optimieren der HDX-Benutzererfahrung zusammenhängen.

Verkürzen des Anwendungsstarts

Nov 21, 2014

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 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 Receiver 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 eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.
Die Registrierungsverzeichnisse sind:

HKLM\Software\[Wow6432Node\]Citrix\Dazzle

HKCU\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 Receiver 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 icaclient.adm wird nicht unterstützt. Sie können aber die Vorabstartkonfiguration ändern, indem Sie während oder nach der Receiver-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.

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 Schedule=13:45|1:0:1:0:1:0:0 ein. Tatsächlich wird die Sitzung irgendwann zwischen 13:15 und 13.45 gestartet.

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Die Schlüssel "State" und "Schedule" haben dieselben Werte wie für HKLM.

Zuordnen von Clientgeräten

Sep 29, 2016

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

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

Während der Anmeldung informiert Receiver 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.

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

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.

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 Receiver 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 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 Receiver 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.

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.

1. Aktivieren Sie für XenDesktop 7-Bereitstellungen die Richtlinieneinstellung Client-COM-Portumleitung.
2. Melden Sie sich an Receiver 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.

   Wichtig: Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel. TAPI-Geräte können den COM-Ports der Clients nicht zugeordnet werden.

Unterstützen der DNS-Namensauflösung

Jun 19, 2013

Receiver, die über den Citrix XML-Dienst eine Verbindung zur Serverfarm herstellen, können 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.

Receiver, die über das Webinterface eine Verbindung zu veröffentlichten Anwendungen herstellen, verwenden auch den Citrix XML-Dienst. Für Receiver-Verbindungen über das Webinterface löst der Webserver den DNS-Namen für Receiver auf.

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

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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

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

Verwenden von Proxyservern für XenDesktop-Verbindungen

Apr 13, 2015

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.

Verbessern der Benutzererfahrung

May 19, 2015

Sie können die Benutzererfahrung mit den folgenden Features verbessern.

Receiver 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

Receiver-Benutzer 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.

Sie können maximal acht Monitore mit Receiver verwenden.

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 die Schaltfläche 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 unter CTX115637.

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.

Damit über Windows-Tablets der Touchzugriff auf virtuelle Anwendungen und Desktops möglich ist, zeigt Receiver 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 Receiver den Modus des Geräts nicht genau bestimmen und die Bildschirmtastatur wird u. U. angezeigt, wenn sie nicht benötigt wird.

Bei einem konvertierbaren Gerät (Tablet mit abnehmbarer Tastatur) kann die Anzeige der Bildschirmtastatur unterdrückt werden, indem Sie einen REG_DWORD-Wert unter DisableKeyboardPopup in HKLM\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 HKLM\SOFTWARE\Wow6432Node\ Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver

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 icaclient-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 icaclient.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 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.

Receiver unterstützt jetzt Symbole in 32 Bit High Color und die Farbtiefe wird automatisch für Anwendungen ausgewählt, die im Citrix Connection Center, im Startmenü und in der Taskleiste angezeigt werden, um Anwendungen im Seamless-Modus 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 eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.
Sie können eine bevorzugte Farbtiefe einstellen, indem Sie der Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA 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.

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 hängt davon ab, wie Sie Citrix Receiver für Windows einrichten.

Verwenden Sie Desktop Viewer, wenn Benutzer mit dem lokalen 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 zum Ändern der Bildschirmauflösung auf ihren virtuellen Desktops verwenden. Die Bildschirmauflösung kann nicht in der Windows-Systemsteuerung geändert werden.

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).

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.

Sichern der Verbindungen

May 01, 2013

Zur maximalen Sicherung der Umgebung müssen die Verbindungen zwischen Receiver und den veröffentlichten Ressourcen gesichert sein. Sie können verschiedene Authentifizierungsmethoden für die Receiver-Software konfigurieren, u. a. Smartcard-Authentifizierung, 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

Oct 26, 2015

In diesem Abschnitt wird beschrieben, wie Sie Domänen-Passthrough-Authentifizierung für Citrix Receiver mit XenDesktop oder XenApp aktivieren.

Hinweis: In diesem Beispiel werden die Installation von Receiver, die Anwendung der Computerrichtlinie und die Konfiguration einer vertrauenswürdigen Site auf dem Clientbetriebssystem manuell ausgeführt. Wenn eine Vorlage für ein Gruppenrichtlinienobjekt (GPO) erstellt wurde, können Sie sie auf alle Domänen-Clientcomputer anwenden, auf denen Receiver installiert ist.

1. Installieren Sie Citrix Receiver 4.2 mit dem Schalter "/includeSSON".
    1. 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. Informationen zur Syntax zum Hinzufügen von StoreFront-Stores finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.
    2. Überprüfen Sie, ob die Passthrough-Authentifizierung aktiviert ist, indem Sie Citrix Receiver starten und dann sicherstellen, dass der Prozess **ssonsvr.exe** ausgeführt wird.
2. Fügen Sie die administrative Vorlage "ICA Client GPO" der Lokalen Computerrichtlinie auf der lokalen Maschine des Benutzers und/oder im "Golden Image" des VDA-Desktops hinzu:
    1. Öffnen Sie **gpedit.msc**.
       Hinweis: Das Snap-In für den Gruppenrichtlinien-Editor, gpedit.msc, ist in der Professional, Enterprise und Ultimate Edition von Windows 7 und Windows 8 verfügbar.
    2. Klicken Sie mit der rechten Maustaste auf Computerkonfiguration > Administrative Vorlagen und wählen Sie Vorlagen hinzufügen/entfernen.
    3. Fügen Sie die Vorlage **C:\Programme\Citrix\ICA Client\Configuration\icaclient.adm** hinzu.
3. Aktivieren Sie das Gruppenrichtlinienobjekt des lokalen Computers auf der lokalen Maschine des Benutzers und/oder im "Golden Image" des VDA-Desktops:
    1. Wählen Sie Local user name and password.
    2. Wählen Sie Aktiviert.
    3. Wählen Sie Enable pass-through authentication.
    4. Wählen Sie Allow pass-through authentication for all ICA connections.
    5. Klicken Sie auf OK.
    6. Starten Sie das Golden Image des VDA-Desktops neu.
4. Melden Sie sich bei dem/den Delivery Controller(n) an, öffnen Sie Windows PowerShell und führen Sie die folgenden Befehle aus, damit der Delivery Controller von StoreFront gesendeten XML-Anfragen vertraut.
    1. Laden Sie bei Bedarf die Citrix Cmdlets, indem Sie asnp Citrix*. eingeben. (Der Punkt nach Citrix* ist erforderlich)
    2. Drücken Sie die Eingabetaste.
    3. Geben Sie dann Add-PSSnapin citrix.broker.admin.v2 ein und drücken Sie die Eingabetaste.
    4. Geben Sie anschließend Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True ein und drücken Sie die Eingabetaste.
    5. Schließen Sie PowerShell.
5. Öffnen Sie Internet Explorer auf der lokalen Maschine und/oder im Golden Image des VDA-Desktops.
6. Fügen Sie die vollständig qualifizierten Namen 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.

7. Melden Sie sich von Receiver ab und wieder an.

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

Aktivieren der Passthrough-Authentifizierung, wenn Sites nicht zu den Zonen "Vertrauenswürdige Zonen" oder "Intranet" gehören

Nov 20, 2013

Die Benutzer benötigen ggf. Passthrough-Authentifizierung zum Server mit den Anmeldeinformationen der Benutzer, können jedoch keine Sites den Zonen "Vertrauenswürdige Zonen" oder "Intranet" hinzufügen. Aktivieren Sie diese Einstellung, um die Passthrough-Authentifizierung für alle Sites außer "Eingeschränkte Sites" zuzulassen.

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 icaclient-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 icaclient.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 > User Authentication > Local user name and password .
7. Klicken Sie im Menü Local user name and password Properties auf Enabled und aktivieren Sie dann Enable pass-through authentication und Allow pass-through authentication for all ICA connections .

Konfigurieren von Domänen-Passthrough-Authentifizierung mit Kerberos

Dec 01, 2014

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

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

1. Der Single Sign-On-Dienst von Receiver erfasst die Smartcard-PIN.
2. Receiver verwendet IWA (Kerberos) für die Authentifizierung des Benutzers bei StoreFront. StoreFront stellt Receiver 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 Receiver wird lediglich eine weitere PIN-Eingabe vermieden. Wenn Sie die Kerberos-Authentifizierung nicht verwenden, führt Receiver 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 Receiver sicher, dass für die Kerberos-Konfiguration Folgendes gilt.

- Kerberos funktioniert nur zwischen Receiver 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.

Achtung: 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

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 Receiver 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 Receiver 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 Receiver 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 Smartcard-Authentifizierung und nicht Kerberos verwendet. Verwenden Sie daher nicht die Option ENABLE_KERBEROS=Yes, mit der die HDX Engine zur Verwendung von Kerberos gezwungen wird.

Starten Sie Receiver 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 Clientcomputern 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.

Konfigurieren der Smartcardauthentifizierung

Nov 28, 2014

Receiver für Windows unterstützt die folgenden Features der Smartcard-Authentifizierung. Weitere Informationen zur XenDesktop- und StoreFront-Konfiguration finden Sie in der Dokumentation für diese Komponenten. In diesem Abschnitt wird die Konfiguration von Receiver für Windows für Smartcards beschrieben.

- **Passthrough-Authentifizierung (Single Sign-On):** Die Passthrough-Authentifizierung erfasst Smartcard-Anmeldeinformationen, wenn sich Benutzer an Receiver anmelden. Receiver verwendet die erfassten Anmeldeinformationen wie folgt:
  - Benutzer von in Domänen eingebundenen Geräten, die sich mit Smartcard-Anmeldeinformationen an Receiver anmelden, starten virtuelle Desktops und Anwendungen ohne erneute Authentifizierung.
  - Benutzer von nicht in Domänen eingebundenen Geräten, die sich mit Smartcard-Anmeldeinformationen an Receiver anmelden, müssen zum Starten eines virtuellen Desktops oder einer Anwendung die Anmeldeinformationen erneut eingeben.

  StoreFront und Receiver 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 Receiver. Konfigurieren Sie Receiver, um die Auswahl von Zertifikaten zu ändern.
- **Clientzertifikatauthentifizierung:** NetScaler Gateway bzw. Access Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
  - Für den Zugriff auf StoreFront-Ressourcen über NetScaler Gateway bzw. Access Gateway müssen Benutzer sich ggf. nach dem Entfernen der Smartcard neu authentifizieren.
  - Wenn die SSL-Konfiguration von NetScaler Gateway bzw. Access 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 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.
- Receiver für Windows verbindet keine Sitzungen wieder, wenn eine Smartcard eingesteckt wird.
- Wenn Receiver für Windows für die Smartcard-Authentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung von VPN-Tunneln mit der Smartcard-Authentifizierung 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 Receiver für Windows Updater mit citrix.com u8nd Merchandising Server ist nicht mit der Smartcard-Authentifizierung an NetScaler Gateway kompatibel.

Achtung: 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. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

Fügen Sie zum Konfigurieren von Receiver 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 Receiver 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 Receiver nach der Single Sign-On-Komponente sucht, sodass Receiver 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 Receiver 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:
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  Hierdurch wird verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden, und ermöglicht, dass die PIN durch Receiver bei der Anmeldung bei Receiver 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.

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
2. Installieren Sie die kryptografische Middleware.
3. Installieren und konfigurieren Sie Receiver für Windows.

Wenn mehrere Zertifikate gültig sind, fordert Receiver den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können Receiver auch so konfigurieren, dass das Standardzertifikat (gemäß des Standardanbieters) 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 Receiver-Befehlszeile die Option AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry } an.
  Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Receiver für SmartCardDefault oder LatestExpiry den Benutzer zur Auswahl eines Zertifikats auf.

- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKCU oder HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry } zu. In HKCU definierte Werte haben Priorität über Werte in HKLM, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von 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. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung, können Sie in Receiver 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 Receiver-Befehlszeile die Option AM_SMARTCARDPINENTRY=CSP an.
- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP hinzu.

Aktivieren der Prüfung der Zertifikatssperrliste für erhöhte Sicherheit bei Receiver

Nov 19, 2014

Wenn die Überprüfung von Zertifikatsperrlisten (CRL) aktiviert ist, überprüft Receiver, ob das Zertifikat des Servers widerrufen wurde. Da 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 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 Receiver, wenn er ausgeführt wird. Vergewissern Sie sich, dass alle 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 icaclient-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 icaclient.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 Komponenten > Citrix Receiver > Netzwerkrouting > 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.

Sichern der Receiver-Kommunikation

Mar 03, 2015

Zum Sichern der Kommunikation zwischen XenDesktop-Sites oder XenApp-Serverfarmen und Receiver können Sie Receiver-Verbindungen mit Sicherheitstechnologien integrieren, u. a.:

- Citrix NetScaler Gateway oder Access Gateway. Weitere Informationen finden Sie in den Themen in diesem Abschnitt und in der Dokumentation für NetScaler Gateway, Access 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 Receiver 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. (Informationen zum Konfigurieren von SSL für XenApp 7.6 und XenDesktop 7.6 finden Sie unter SSL.)

Receiver ist kompatibel mit und funktioniert in Umgebungen in denen die Microsoft SSLF-Desktopsicherheitsvorlage (Specialized Security - Limited Functionality) verwendet wird. Diese Vorlagen werden auf den Plattformen Microsoft Windows XP, Windows Vista und Windows 7 unterstützt. Informationen über die Vorlagen und dazugehörige Einstellungen finden Sie in der Sicherheitsdokumentation für Windows XP, Windows Vista und Windows 7 unter http://technet.microsoft.com .

Verbinden mit NetScaler Gateway

Sep 29, 2016

Um Remotebenutzern zu ermöglichen, eine Verbindung über NetScaler Gateway herzustellen, konfigurieren Sie NetScaler Gateway für StoreFront.

- StoreFront-Bereitstellungen: Lassen Sie StoreFront-Verbindungen von internen und Remotebenutzern über NetScaler Gateway zu, indem Sie NetScaler Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf virtuelle Desktops und Anwendungen zu. Benutzer stellen eine Verbindung über Receiver her.

Weitere Informationen zur Konfiguration dieser Verbindungen finden Sie unter Integrating NetScaler Gateway with XenMobile App Edition und anderen Abschnitten unter dem Knoten in der Citrix Produktdokumentation. Weitere Informationen zu den Einstellungen, die für Receiver für Windows benötigt werden, finden Sie in den folgenden Themen:

- Konfigurieren von Sitzungsrichtlinien und -profilen für XenMobile App Edition
- Erstellen des Sitzungsprofils für Receiver für XenMobile App Edition
- Konfigurieren von benutzerdefinierten clientlosen Zugriffsrichtlinien für Receiver

Damit Remotebenutzer über NetScaler Gateway eine Verbindung mit der Webinterface-Bereitstellung herstellen können, konfigurieren Sie NetScaler Gateway für das Webinterface, wie unter Providing Access to Published Applications and Virtual Desktops Through the Web Interface und den Unterabschnitten in der Citrix Produktdokumentation beschrieben.

Verbinden mit Access Gateway Enterprise Edition

Sep 29, 2016

Konfigurieren Sie Access Gateway für StoreFront und App Controller (eine Komponente von CloudGateway), damit Remotebenutzer eine Verbindung über Access Gateway herstellen können.

- StoreFront-Bereitstellungen: Lassen Sie StoreFront-Verbindungen von internen und Remotebenutzern über Access Gateway zu, indem Sie Access Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf virtuelle Desktops und Anwendungen zu. Benutzer stellen eine Verbindung über Receiver her.
- App Controller-Bereitstellungen: Lassen Sie Verbindungen von internen und Remotebenutzern mit App Controller zu, indem Sie Access Gateway und App Controller integrieren. In dieser Bereitstellung verbinden sich Benutzer mit App Controller, um die Web- und SaaS-Anwendungen abzurufen, und ShareFile Enterprise-Dienste werden Receiver-Benutzern bereitgestellt. Benutzer stellen entweder eine Verbindung über Receiver oder das Access Gateway Plug-In her.

Weitere Informationen zur Konfiguration dieser Verbindungen finden Sie unter Integrating Access Gateway with CloudGateway und den anderen Themen unter dem Knoten in der Citrix Produktdokumentation. Weitere Informationen zu den Einstellungen, die für Receiver für Windows benötigt werden, finden Sie in den folgenden Themen:

- Konfigurieren von Sitzungsrichtlinien und -profilen für CloudGateway
- Erstellen des Sitzungsprofils für Receiver für CloudGateway Enterprise
- Erstellen des Sitzungsprofils für Receiver für CloudGateway Express
- Konfigurieren von benutzerdefinierten clientlosen Zugriffsrichtlinien für Receiver

Damit Remotebenutzer sich über Access Gateway mit der Webinterface-Bereitstellung verbinden können, müssen Sie Access Gateway für das Webinterface konfigurieren, wie unter Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface und den Unterabschnitten in der Citrix Produktdokumentation beschrieben.

Verbinden mit Secure Gateway

Oct 12, 2012

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Secure Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen Receiver und dem Server bereitzustellen. Eine Receiver-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 Receiver Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Weitere Informationen zur Konfiguration der Einstellungen für den Proxyserver für Receiver finden Sie in den Abschnitten über das Webinterface.

Wenn Secure Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Secure Gateway Proxy im Relaymodus verwenden. Weitere Informationen zum Relaymodus finden Sie in den Abschnitten über Secure Gateway.

Wenn Sie den Relaymodus verwenden, fungiert der Secure Gateway-Server als Proxy und Sie müssen Receiver 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 nacheinander 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

Oct 12, 2012

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss Receiver über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können. Die Firewall muss HTTP-Datenübertragungen für die Kommunikation zwischen Benutzergerät und Webserver zulassen (meist über den HTTP-Standardport 80 oder 443, wenn ein sicherer Webserver verwendet wird). Für die Kommunikation zwischen Receiver und dem Citrix Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

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. Receiver stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her. Weitere Informationen finden Sie in der Dokumentation zum Webinterface.

Durchsetzen von Vertrauensbeziehungen

Nov 20, 2014

Die Konfiguration mit vertrauenswürdigen Servern dient dazu, Vertrauensbeziehungen bei Receiver-Verbindungen zu identifizieren und durchzusetzen. Diese Vertrauensbeziehung erhöht die Zuversicht von Receiver-Administratoren und Benutzern in die Integrität der Daten auf den Benutzergeräten und verhindert die böswillige Verwendung von Receiver-Verbindungen.

Wenn diese Funktion aktiviert ist, können Receiver Anforderungen für die Vertrauensstellung angeben und ermitteln, ob sie der Verbindung zu dem Server vertrauen wollen. Beispiel: Ein Receiver, 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 die Konfiguration vertrauenswürdiger Server aktiviert ist, müssen verbundene Server der Zone vertrauenswürdiger Sites von Windows hinzugefügt werden. (Eine detaillierte Anleitung, wie Sie Server der Zone vertrauenswürdiger Sites von Windows hinzufügen, finden Sie in der Onlinehilfe von Internet Explorer.)

Aktivieren der Konfiguration mit vertrauenswürdigen Servern

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.

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 icaclient-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 icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Erweitern Sie unter dem Knoten Benutzerkonfiguration den Eintrag Administrative Vorlagen.
7. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
8. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert.

Erhöhte Rechte und wfcrun32.exe

May 01, 2013

Wenn die Benutzerkontensteuerung auf Geräten unter Windows 8, Windows 7 oder Windows Vista 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 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.

Receiver-Verbindungen über einen Proxyserver

Jan 02, 2013

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Proxyserver werden zum Beschränken des Netzwerkzugriffs sowie beim Herstellen von Verbindungen zwischen Receiver und Servern verwendet. Receiver 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.

Verbinden mit dem SSL-Relay (Secure Sockets Layer)

May 19, 2015

Diese Informationen gelten nicht für XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 und XenApp 7.5.

Sie können Receiver in eine Umgebung mit dem SSL (Secure Sockets Layer)-Relay integrieren. Receiver unterstützt das TLS-Protokoll. Receiver für Windows 4.2 unterstützt nur TLS 1.0.

- TLS (Transport Layer Security) ist die neueste normierte Version des SSL-Protokolls. Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von SSL als offenem Standard übernahm. TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie FIPS 140 (Federal Information Processing Standard). FIPS 140 ist ein Standard für die Kryptografie.

Das Citrix SSL-Relay verwendet standardmäßig den TCP-Port 443 auf dem XenApp-Server für TLS-gesicherte Kommunikation. Wenn das SSL-Relay eine TLS-Verbindung empfängt, werden die Daten entschlüsselt und dann an den Server übergeben. Wenn der Benutzer TLS+HTTPS-Browsing gewählt hat, werden die Daten an den Citrix XML-Dienst übergeben.

Wenn Sie SSL-Relay so konfigurieren, dass ein anderer Port (d. h. nicht Port 443) abgehört wird, müssen Sie das Plug-in für diese geänderte Portnummer konfigurieren.

Mit dem Citrix SSL-Relay kann folgende Kommunikation gesichert werden:

- Verbindung zwischen einem TLS-fähigen Client und einem Server. Verbindungen, bei denen TLS-Verschlüsselung verwendet wird, werden im Connection Center mit einem Vorhängeschloss gekennzeichnet.
- Bei einem Webinterface-Server die Kommunikation zwischen dem XenApp-Server und dem Webserver.

Weitere Informationen zum Konfigurieren und Sichern der Installation mit SSL-Relay finden Sie in der XenApp-Dokumentation.

Zusätzlich zu den Systemanforderungen müssen Sie Folgendes sicherstellen:

- Das Benutzergerät unterstützt die 128-Bit-Verschlüsselung.
- Auf dem Benutzergerät ist ein Stammzertifikat installiert, mit dem die Signatur der Zertifizierungsstelle für das Serverzertifikat verifiziert werden kann.
- Receiver ist die Nummer des TCP-Abhörports bekannt, der vom SSL-Relaydienst in der Serverfarm verwendet wird.
- Alle von Microsoft empfohlenen Service Packs oder Upgrades sind installiert.

Wenn Sie Internet Explorer verwenden und den Verschlüsselungsgrad nicht kennen, gehen Sie auf die Website von Microsoft unter http://www.microsoft.com und installieren Sie ein Service Pack, das 128-Bit-Verschlüsselung bietet.

Wichtig: Receiver unterstützt Zertifikatschlüssellängen von bis zu 4096 Bits. Stellen Sie sicher, dass die Bitlänge der Stamm- und Zwischenzertifikate von der Zertifizierungsstelle sowie die Bitlänge der Serverzertifikate nicht die Bitlänge überschreitet, die Receiver unterstützt wird, andernfalls könnten Verbindungen fehlschlagen.

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.

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 icaclient-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 die Plug-ins (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.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 Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften, wählen Sie Aktiviert und geben Sie die neue Portnummer in das Feld Allowed SSL servers in folgendem Format ein:

server:SSL relay port number

wobei SSL relay port number die Nummer des Abhörports ist. Um mehrere Server anzugeben, können Sie einen Platzhalter verwenden. Beispiel: *.Test.com:SSL relay port number umfasst alle Verbindungen zu Test.com über einen angegebenen Port.

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.

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 icaclient-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 (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.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 Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften, wählen Sie Aktiviert und geben Sie eine durch Kommas getrennte Liste vertrauenswürdiger Server sowie die neue Portnummer in folgendem Format in das Feld Allowed SSL servers ein:
   servername:SSL relay port number;servername:SSL relay port number

   wobei SSL relay port number die Nummer des Abhörports ist. Sie können eine durch Kommas getrennte Liste bestimmter vertrauenswürdiger SSL-Server ähnlich wie in folgendem Beispiel angeben:
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444

Dies führt zu folgendem Ergebnis in dieser Musterdatei von appsrv.ini: [Word]

```
[Word]

SSLProxyHost=csghq.Test.com:443

[Excel]

SSLProxyHost=csghq.Test.com:444

[Editor]

SSLProxyHost=fred.Test.com:443
```

Konfigurieren und Aktivieren von Receiver für TLS

May 19, 2015

Diese Informationen gelten nicht für XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 und XenApp 7.5.

Wenn Sie für Receiver eine Verbindung mit TLS erzwingen möchten, müssen Sie TLS auf dem Secure Gateway-Server oder im SSL-Relaydienst angeben. Weitere Informationen finden Sie in den Abschnitten über Secure Gateway oder in der Dokumentation für den SSL-Relaydienst.

Sie müssen außerdem sicherstellen, dass das Benutzergerät alle Systemanforderungen erfüllt.

Wenn Sie ausschließlich TLS-Verschlüsselung für die Receiver-Kommunikation verwenden möchten, konfigurieren Sie das Benutzergerät, Receiver und, wenn Sie das Webinterface verwenden, den Webinterface-Server. Informationen zum Sichern der StoreFront-Kommunikation finden Sie in den Abschnitten unter "Sicherung" in der StoreFront-Dokumentation.

Für das Sichern der Kommunikation mit TLS zwischen TLS-aktiviertem Receiver und der Serverfarm muss auf dem Clientgerät ein Stammzertifikat vorhanden sein, mit dem die Signatur der Zertifizierungsstelle für das Serverzertifikat bestätigt wird.

Receiver unterstützt die Zertifizierungsstellen, die vom Windows-Betriebssystem unterstützt werden. Die Stammzertifikate für diese Zertifizierungsstellen werden mit Windows installiert und mit Windows-Dienstprogrammen verwaltet. Microsoft Internet Explorer verwendet dieselben Stammzertifikate.

Wenn Sie eine andere Zertifizierungsstelle verwenden, müssen Sie ein Stammzertifikat von der zuständigen Stelle erwerben und es auf jedem Benutzergerät installieren. Microsoft Internet Explorer und Receiver verwenden dann dieses Stammzertifikat und sehen es als vertrauenswürdig an.

Sie können das Stammzertifikat mit anderen Administrations- oder Bereitstellungsverfahren installieren, u. a.

- Verwenden des Konfigurationsassistenten und des Profilmanagers im Microsoft Internet Explorer Administration Kit (IEAK)
- Bereitstellungstools von Drittherstellern

Stellen Sie sicher, dass die vom Windows-Betriebssystem installierten Zertifikate die Sicherheitsanforderungen des Unternehmens erfüllen, oder verwenden Sie Zertifikate, die von der Zertifizierungsstelle Ihres Unternehmens ausgestellt sind.

1. Wenn Sie die Anwendungsauflistung und die Startdaten, die zwischen Receiver und dem Webinterface-Server übergeben werden, mit TLS verschlüsseln möchten, konfigurieren Sie die entsprechenden Einstellungen im Webinterface. Sie müssen den Computernamen des XenApp-Servers einschließen, der das SSL-Zertifikat hostet.
2. Wenn Sie die zwischen Receiver und dem Webinterface-Server übergebenen Konfigurationsdaten mit HTTP (HTTPS) sichern möchten, geben Sie die Server-URL im Format https://servername ein. Klicken Sie im Windows-Infobereich mit der rechten Maustaste auf das Receiver-Symbol und wählen Sie Einstellungen.
3. Klicken Sie mit der rechten Maustaste auf den Eintrag Online Plug-In unter Plug-In-Status und wählen Sie Server ändern .

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.

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 mit Active Directory arbeiten.
   Hinweis: Wenn Sie die icaclient-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 icaclient.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 Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften, wählen Sie Aktiviert und wählen Sie in den Listenfeldern die TLS-Einstellungen aus.
   - Setzen Sie TLS Version auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, stellt Receiver eine Verbindung mit TLS-Verschlüsselung her.
   - Setzen Sie "SSL cipher suite" auf Detect version, damit Receiver eine geeignete Verschlüsselungssammlung aus kommerziellen (Commercial) und Regierungs (Government)-Verschlüsselungssammlungen aushandeln kann. Sie können die Verschlüsselungssammlungen auf "Behörden" oder "Kommerziell" beschränken.
   - Setzen Sie "CRL verification" auf Require CRLs for connection. Bei dieser Einstellung versucht Receiver Zertifikatsperrlisten von den jeweiligen Zertifikatausgabestellen abzurufen.

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.

Verwenden Sie zum Erfüllen der FIPS 140-Sicherheitsanforderungen die Gruppenrichtlinienvorlage, um die Parameter zu konfigurieren oder fügen Sie die Parameter in der Datei Default.ica auf dem Webinterface-Server ein. Weitere Informationen zur Datei Default.ica finden Sie in der Webinterface-Dokumentation.

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 icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 3 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 icaclient.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 Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.

7. Klicken Sie im Menü Aktion auf Eigenschaften , wählen Sie Aktiviert und wählen Sie in den Dropdownlisten die richtigen TLS-Einstellungen aus.
   - Setzen Sie TLS Version auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, versucht Receiver eine Verbindung mit TLS-Verschlüsselung herzustellen.
   - Setzen Sie SSLciphersuite auf Government.
   - Setzen Sie CRL verification auf Require CRLs for connection.

Sie müssen im Webinterface den Computernamen des Servers angeben, der das SSL-Zertifikat hostet. Weitere Informationen zum Sichern der Kommunikation zwischen Receiver und dem Webserver mit TLS finden Sie in der Webinterface-Dokumentation.

1. Wählen Sie im Menü Konfigurationseinstellungen die Option Servereinstellungen.
2. Wählen Sie SSL/TLS für Kommunikation zwischen Clients und Webserver verwenden.
3. Speichern Sie die Änderungen.

Durch Wählen von SSL/TLS werden alle URLs geändert, sodass sie das HTTPS-Protokoll verwenden.

Sie können den XenApp-Server so konfigurieren, dass TLS zum Sichern der Kommunikation zwischen Receiver und dem Server verwendet wird.

1. Öffnen Sie in der Citrix Verwaltungskonsole für den XenApp-Server das Dialogfeld Eigenschaften der Anwendung, die Sie sichern möchten.
2. Wählen Sie Erweitert > Clientoptionen und stellen Sie sicher, dass SSL- und TLS-Protokoll aktivieren ausgewählt ist.
3. Wiederholen Sie diese Schritte für jede Anwendung, die Sie sichern möchten.

Sie müssen im Webinterface den Computernamen des Servers angeben, der das SSL-Zertifikat hostet. Weitere Informationen zum Sichern der Kommunikation zwischen Receiver und dem Webserver mit TLS finden Sie in der Webinterface-Dokumentation.

Sie können Receiver konfigurieren, sodass TLS zum Sichern der Kommunikation zwischen Receiver und dem Webinterface-Server verwendet wird.

Stellen Sie sicher, dass ein gültiges Stammzertifikat auf dem Benutzergerät installiert ist. Weitere Informationen finden Sie unter Installieren von Stammzertifikaten auf den Benutzergeräten.

1. Klicken Sie im Windows-Infobereich mit der rechten Maustaste auf das Receiver-Symbol und wählen Sie Einstellungen.
2. Klicken Sie mit der rechten Maustaste auf den Eintrag Online Plug-In unter Plug-In-Status und wählen Sie Server ändern.
3. Im Dialogfeld Server ändern wird die aktuell konfigurierte URL angezeigt. Geben Sie die Server-URL im Textfeld im Format https://servername ein, um die Konfigurationsdaten mit TLS zu verschlüsseln.
4. Klicken Sie auf Aktualisieren, um die Änderung zu übernehmen.
5. Aktivieren Sie TLS im Browser des Benutzergeräts. Weitere Informationen finden Sie in der Onlinehilfe des Browsers.

ICA-Dateisignierung: Schutz vor dem Starten von Anwendungen oder Desktops von nicht vertrauenswürdigen Servern

May 19, 2015

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 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 Receiver-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 Receiver 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 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 ica-file-signing.adm.
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 Komponenten > Citrix Receiver und dann auf ICA-Dateisignierung aktivieren.
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	Nur richtig signierte Anwendungs- oder Desktopstarts von einem vertrauenswürdigen Server sind zulässig. Dem Benutzer wird eine Sicherheitswarnung im Receiver angezeigt, wenn eine

Option	Beschreibung
(sicherer)	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).

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.

Konfigurieren eines Webbrowsers und einer ICA-Datei zum Aktivieren von Single Sign-On und zum Verwalten sicherer Verbindungen mit vertrauenswürdigen Servern

Dec 02, 2012

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Wenn Sie Single Sign-On verwenden und sichere Verbindungen mit vertrauenswürdigen Servern verwalten möchten, müssen Sie die Site des Citrix Servers den Zonen Lokales Intranet oder Vertrauenswürdige Sites in Internet Explorer unter Extras > Internetoptionen > Sicherheit auf dem Benutzergerät hinzufügen. Die Adresse kann die Platzhalterzeichen-Formate (*) enthalten, die vom ISM-Dienst unterstützt werden, oder so genau wie protocoll ://URL[:port] sein.

Dasselbe Format muss in der ICA-Datei und in den Einträgen der Sites verwendet werden. Beispiel: Bei Verwendung des vollqualifizierten Domänennamens (FQDN) in der ICA-Datei müssen Sie den FQDN im Eintrag für die Sitezone verwenden. XenDesktop-Verbindungen verwenden nur ein Desktopgruppennamenformat.

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://Hostname

http[s]://fqdn.beispiel.com

http[s]://*.beispiel.com

http[s]://cname.*.beispiel.com

http[s]://*.beispiel.co.uk

desktop://gruppe-20name

ica[s]://xaserver1

ica[s]://xaserver1.beispiel.com

Fügen Sie die genaue Adresse der Webinterface-Site der Zone "Sites" hinzu.

Muster-Websiteadressen

https://mein.unternehmen.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

Fügen Sie die Adresse im Format desktop://Desktop Group Name hinzu. Wenn der Name der Desktopgruppe Leerstellen enthält, ersetzen Sie jede Leerstelle durch -20.

Verwenden Sie eines der folgenden Formate in der ICA-Datei für die Adresse der Citrix-Serversite. Verwenden Sie dasselbe Format, um sie der Zone Lokales Intranet oder Vertrauenswürdige Sites in Internet Explorer unter Extras > Internetoptionen > Sicherheit auf dem Benutzergerät hinzuzufügen:

Beispiel eines HttpBrowserAddress-Eintrags in der ICA-Datei

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

Beispiele eines XenApp Server Address-Eintrags in der ICA-Datei

Wenn die ICA-Datei nur das Feld **Adresse** des XenApp-Servers enthält, verwenden Sie eines der folgenden Eingabeformate:

icas://10.20.30.40:1494

icas://mein.xenapp-server.unternehmen.com

ica://10.20.30.40

Festlegen der Clientressourcenberechtigungen

Oct 30, 2014

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Clientressourcenberechtigungen mit vertrauenswürdigen und eingeschränkten Siteregionen wie folgt einstellen:

- Hinzufügen der Webinterface-Site zur Liste der vertrauenswürdigen Sites
- Ändern der neuen Registrierungseinstellungen

Hinweis: Aufgrund von Erweiterungen zu Receiver, wurde die INI-Prozedur, die in früheren Versionen des Plug-Ins/Receivers verfügbar war, durch diese Schritte ersetzt.
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

Hinzufügen der Webinterface-Site zur Liste der vertrauenswürdigen Sites

1. Klicken Sie in Internet Explorer im Menü Extras auf Internetoptionen > Sicherheit.
2. Wählen Sie das Symbol Vertrauenswürdige Sites und klicken Sie auf die Schaltfläche Sites.
3. Geben Sie im Textfeld Diese Website zur Zone hinzufügen die URL der Webinterface-Site ein und klicken Sie auf Hinzufügen.
4. Laden Sie die Registrierungseinstellungen von http://support.citrix.com/article/CTX133565 herunter und ändern Sie die Registrierung. Verwenden Sie SsonRegUpx86.reg für Win32-Benutzergeräte und SsonRegUpx64.reg für Win64-Benutzergeräte.
5. Melden Sie sich vom Benutzergerät ab und dann erneut an.

Ändern der Clientressourcenberechtigungen in der Registrierung

1. Laden Sie die Registrierungseinstellungen von http://support.citrix.com/article/CTX133565 herunter und importieren Sie die Einstellungen auf jedem Benutzergerät. Verwenden Sie SsonRegUpx86.reg für Win32-Benutzergeräte und SsonRegUpx64.reg für Win64-Benutzergeräte.
2. Navigieren Sie im Registrierungs-Editor auf HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust und ändern Sie im relevanten Bereich den Standardwert für die folgenden Ressourcen auf die benötigten Zugriffswerte:

Ressourcenschlüssel	Ressourcenbeschreibung
FileSecurityPermission	Clientlaufwerke
MicrophoneAndWebcamSecurityPermission	Mikrofone und Webcams
ScannerAndDigitalCameraSecurityPermission	USB- und andere Geräte

Wert	Beschreibung
0	Kein Zugriff

Wert	Beschreibung
1	Lesezugriff
2	Vollzugriff
3	Benutzer bei Zugriff fragen

Receiver Desktop Lock

Apr 21, 2015

Sie können Receiver Desktop Lock verwenden, wenn Benutzer nicht mit dem lokalen Desktop arbeiten müssen. Benutzer 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.

Receiver Desktop Lock funktioniert auf in Domänen eingebundenen Computern, die für SSON (Single Sign-On) und mit einem Store konfiguriert sind. PNA-Sites werden nicht unterstützt. Vorherige Versionen von Desktop Lock werden beim Upgrade auf Receiver für Windows 4.2.x nicht unterstützt.

Sie müssen Citrix Receiver für Windows mit dem Flag /includeSSON installieren. Konfigurieren Sie den Store und Single Sign-On mit der ADM-Datei oder über die Befehlszeilenoption.

Installieren Sie dann Receiver Desktop Lock als Administrator mit dem Installationspaket CitrixReceiverDesktopLock.MSI, das unter citrix.com/downloads verfügbar ist.

Systemanforderungen für Citrix Receiver Desktop Lock

- Unterstützung für Windows XP (Embedded Edition), Windows 7 (einschließlich Embedded Edition), Windows 7 Thin PC, Windows 8 und Windows 8.1.
- Verbindung mit StoreFront nur über native Protokolle.
- In Domänen eingebundene Endpunkte:
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

Hinweis: Support für Windows XP endete zusammen mit dem erweiterten Support für Windows XP durch Microsoft am 8. April 2014.

Lokaler App-Zugriff

Achtung: 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 unter Konfigurieren von lokalem App-Zugriff und URL-Umleitung in XenApp und XenDesktop.

Arbeiten mit Receiver Desktop Lock

- Receiver Desktop Lock kann mit den folgenden Features von 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 Receiver Desktop Lock-Sitzung führt zu Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Receiver 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. Weitere Informationen 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 Receiver Desktop Lock

Mit diesen Schritten installieren Sie Receiver für Windows, sodass virtuelle Desktops mit Receiver Desktop Lock angezeigt

werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter So konfigurieren Sie 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 > Receiver" auf dem Installationsmedium).
   Für Receiver für Windows 4.2:
   CitrixReceiver.exe
   /includeSSON
   STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   Informationen zu den Befehlen finden Sie in der Installationsdokumentation zu 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 Receiver Desktop Lock

Gewähren Sie pro Benutzer nur Zugriff auf einen virtuellen Desktop mit Receiver Desktop Lock.

Verhindern Sie mit Active Directory-Richtlinien, dass Benutzer virtuelle Desktops in den Ruhezustand versetzen.

Verwenden Sie das Administratorkonto zum Konfigurieren von Receiver Desktop Lock, das Sie für die Installation verwendet haben.

- Stellen Sie sicher, dass die Dateien icaclient.adm und icaclient_usb.adm in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter "Computerkonfiguration" bzw. "Benutzerkonfiguration" > "Administrative Vorlagen" > "Klassische administrative Vorlage (ADM)" > "Citrix Components" angezeigt werden). Die ADM-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 Receiver Desktop Lock

1. Konfigurieren von StoreFront

1. Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
2. 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.
3. Stellen Sie sicher, dass Passthrough mit Smartcard aktiviert ist (standardmäßig aktiviert).
4. Aktivieren Sie Kerberos.
5. Aktivieren Sie Kerberos und Passthrough mit Smartcard.
6. Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
7. 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.
   1. Importieren Sie die Vorlage icaclient.adm aus %Programme%\Citrix\ICA Client\Configuration\.
   2. Erweitern Sie Administrative Vorlagen> Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung .
   3. Aktivieren Sie "Smartcardauthentifizierung".
   4. Aktivieren Sie "Lokaler Benutzername und Kennwort".
3. Konfigurieren Sie das Benutzergerät vor der Installation von Receiver Desktop Lock.
   1. Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu.
   2. Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" im Format: desktop:// delivery-group-namehinzu.
   3. Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Receiver 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 Receiver Desktop Lock.

Entfernen von Receiver 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 Receiver Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:
   - Entfernen Sie Citrix Receiver Desktop Lock.
   - Entfernen Sie Citrix Receiver.

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.

Andere Version

- 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.