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 stellt auch Zugriff bei Bedarf auf Windows-, Web- und SaaS-Apps bereit. Benutzer können auf Apps über Stores zugreifen, die von Citrix StoreFront verwalten werden, oder über Legacy-Webseiten, die vom Webinterface verwaltet werden.

Receiver für Windows 4.1.200 enthält Fixes für die Verwendung des Microsoft Lync 2013 VDI Plug-Ins für Windows sowie Fixes für Receiver für Windows 4.0, 4.0.1, 4.1, 4.1.2 und 4.1.100. Receiver für Windows enthält zudem neue Fixes für Probleme in folgenden Bereichen: HDX MediaStream, Drucken, Serverfarmverwaltung, Sitzungsverbindung, Systemausnahmen und Benutzererfahrung. Weitere Informationen zu den behobenen Problemen finden Sie unter CTX138249.

Citrix Receiver für Windows 4.1 unterstützt Windows 8.1 und Windows Server 2012 R2 und umfasst Fehlerbehebungen, die unter Citrix Receiver 4.x - Issues Fixed in This Release erläutert werden.

Citrix Receiver für Windows 3.3 stellt die folgenden neuen Features und Verbesserungen bereit.

- **Unterstützung von XenDesktop 7-Features:** Receiver unterstützt viele Verbesserungen, die von XenDesktop 7 bereitgestellt werden, u. a. clientseitiger Abruf von Windows Media-Inhalten, Multicastunterstützung, Clientordnerumleitung, lokaler App-Zugriff und Unterstützung von IPv6-Verbindungen.
- **Unterstützung von StoreFront 2.0-Features:** Receiver unterstützt viele Verbesserungen, die von StoreFront 2.0 bereitgestellt werden, u. a. Smartcardauthentifizierung und Unterstützung von IPv6-Verbindungen.
- **Integrierte Smartcardauthentifizierung:** Receiver stellt jetzt eine integrierte Smartcardauthentifizierung für StoreFront-Verbindungen bereit, u. a. Unterstützung für Folgendes:
  - Passthrough-Authentifizierung (Single Sign-On): Benutzer von Geräten, die zu einer Domäne gehören, geben die Smartcard-Anmeldeinformationen ein, um sich an Receiver anzumelden. Sie können virtuelle Desktops und Apps ohne erneute Eingabe der Anmeldeinformationen starten.
  - Bimodale Authentifizierung Benutzer können sich mit einer Smartcard anmelden oder den Benutzernamen und das Kennwort eingeben. Dies ermöglicht die Benutzeranmeldung, selbst wenn ein Zertifikat abgelaufen ist oder der Benutzer keine Smartcard hat.
  - Mehrere Zertifikate: Wenn Benutzer eine Smartcard in einen Kartenleser einstecken, wählt Receiver das benötigte Zertifikat aus und kann mehrere Zertifikate von mehreren Karten verwenden.
  - Double-Hop-Sitzungen: Benutzer starten einen virtuellen Desktop und starten dann mit Receiver auf dem virtuellen Desktop eine Anwendung von einer anderen Bereitstellungsgruppe.
  - Smartcard-aktivierte Apps: Benutzer können Dokumente in einem virtuellen Desktop oder in einer App-Sitzung digital signieren oder verschlüsseln.

  Weitere Informationen finden Sie unter Konfigurieren der Smartcardauthentifizierung. Weitere Informationen zu den Systemanforderungen, zur Planung von Smartcardbereitstellungen und zur Konfiguration, die für alle zugehörigen Citrix Komponenten erforderlich ist, finden Sie in der aktuellen XenDesktop- und StoreFront-Dokumentation.
- **Verbesserte Benutzererfahrung:**
  - Receiver zeigt jetzt eine Benachrichtigung an, wenn eine Installation oder ein Update abgeschlossen ist.
  - Wenn die Richtlinie für die Sitzungszuverlässigkeit aktiviert ist, blendet Receiver Apps ab, wenn die Verbindung mit dem

Server unterbrochen ist.

- **H.264-Decodierung:** Wenn Receiver mit XenDesktop 7 verwendet wird, ist die Leistung bei reichhaltigen und professionellen Grafik-Apps in WAN-Netzwerken verbessert.
- **HDX Insight-Unterstützung:** HDX Insight ist die Integration von EdgeSight-Netzwerkanalyse und EdgeSight-Leistungsverwaltung mit Director. Da Receiver dies jetzt unterstützt, können XenDesktop-Administratoren Leistungsmetrik zur Integrität dieser Komponente überprüfen. Dieses Feature muss nicht konfiguriert werden.
- **Geänderte COM-Port- und LPT-Portzuordnung:** In XenDesktop 7-Bereitstellungen ist die COM-Port- und LPT-Portzuordnung standardmäßig deaktiviert. Aktivieren Sie die Zuordnung mit der Richtlinie für die Portumleitung.

Receiver für Windows 4.1 und 4.0 - Behobene Probleme

Oct 21, 2015

Vergleich mit Citrix Receiver für Windows 4.1.100

Receiver für Windows 200 enthält alle Problembehebungen der Versionen Receiver für Windows 4.0, 4.0.1, 4.1 und 4.1.2, 4.1.100 und darüber hinaus folgende neuen Korrekturen:

HDX MediaStream Flash-Umleitung

- Das Durchsuchen bestimmter Websites mit aktivierter HDX MediaStream Flash-Umleitung kann dazu führen, dass Internet Explorer nicht mehr reagiert.

  Für diesen Fix müssen Sie außerdem Fix #LA4151 (VDA/HDX MediaStream für Flash) installieren und auf dem VDA/XenApp-Server folgenden Registrierungsschlüssel festlegen:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: SupportedUrlHeads
  Typ: REG_MULTI_SZ
  Daten: *<jeder Wert auf einer eigenen Zeile, durch Nullen getrennt>*
  http://
  https://
  file://

  [Aus RcvrFürWin4.1_14.1.200][#LA5255]

- Deaktivieren von "Flash - intelligentes Fallback" in einer Sitzung kann dazu führen, dass Internet Explorer nicht mehr reagiert.

  [Von RcvrForWin4.1_14.1.200] [#LA5404]

Drucken

- Mit dem Citrix Druckertreiber (UPD) können keine Barcodes gedruckt werden. Text wird beim Drucken von Dokumenten mit dem Citrix Druckertreiber (cpviewer.exe) oder einem Barcodedrucker in Form von Leerzeichen oder zufälligen Zeichen gedruckt.

  [Von RcvrForWin4.1_14.1.200] [#LC0141]

Server-/Farmverwaltung

- Wenn die Richtlinien "Bandbreitenlimit für Dateiumleitung" und "Bandbreitenlimit für Sitzung insgesamt" festgelegt sind, werden Sitzungen möglicherweise unerwartet beendet.

  Zur Behebung des Problems müssen Sie ein Server- und ein Receiver-Update mit Fix #LA5925 installieren und den folgenden Registrierungsschlüssel auf dem Server festlegen:

  - Erstellen Sie den folgenden Registrierungsschlüssel:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    Name: DisableHighThroughput
    Typ: DWORD
    Wert: 1
  - Ändern Sie den folgenden Registrierungsschlüssel:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    Name: MaxNetCommands
    Typ: DWORD
    Wert: Legen Sie einen kleineren Wert fest.

  [Von RcvrForWin4.1_14.1.200] [#LA5925]

Sitzung/Verbindung

- Wird die Netzwerkverbindung mit einem VDA getrennt und dann wiederhergestellt, kann nicht mehr mit der Maus geklickt werden.

  [Von RcvrForWin4.1_14.1.200] [#LA5743]

- Die COM-Portumleitung kann mit folgender Fehlermeldung fehlschlagen:

  Error in OpenPort: Comport 'COM4'

  [Von RcvrForWin4.1_14.1.200] [#LC0434]

- Bei Reaktivierung eines Endpunkts mit Verbindung mit einem VDA aus dem Standbymodus funktionieren Maus und Tastatur nicht mehr in der VDA-Sitzung.

  [Von RcvrForWin4.1_14.1.200] [#LC0085]

- Ein Sitzungsfenster im Vordergrund kann unerwartet seinen Vordergrundfokus verlieren.

  [Von RcvrForWin4.1_14.1.200] [#LA5489]

Systemausnahmen

- Die Wiedergabe eines Videos in einem Medienplayer in einer Passthrough-Sitzung kann zum unerwarteten Beenden der Sitzung führen.

  [Von RcvrForWin4.1_14.1.200] [#LC0553]

Benutzererfahrung

- Vollbildanwendungen im Seamless-Modus lassen sich nicht glatt verschieben und können flackern, außerdem ist beim Verschieben der Desktophintergrund an den Rändern zu sehen.

[Von RcvrForWin4.1_14.1.200] [#LC0696]

- In Drahtlosnetzwerken kann das Sitzungsfenster vorübergehend als grauer Block angezeigt werden.

  [Von RcvrForWin4.1_14.1.200] [#LC0530]

- In Benutzersitzungen, die durch eine Richtlinie gesteuert werden, die die Tonqualität auf **Hohe Tonqualität; geringste Leistung** festlegt (**Erweiterte Konfiguration** > **Eigenschaften** > **Clientgeräte** > **Resources** > **Audio** > **Tonqualität** > **Hohe Tonqualität; geringste Leistung**) wird kein Ton ausgegeben.

  [Von RcvrForWin4.1_14.1.200] [#LC0329]

- Bei Multimediadateischleifen in RDS-Desktopsitzungen werden Audiodatenströme und Videobilder nach einer Stunde oder mehr beendet.

  [Von RcvrForWin4.1_14.1.200] [#LC0641]

- Der Sitzungsvorabstart funktioniert nur beim ersten Starten von Receiver für Windows, jedoch nicht mehr nach dessen Konfiguration.

  [Von RcvrForWin4.1_14.1.200] [#LC0701]

Vergleich mit Citrix Receiver für Windows 4.1

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

HDX 3D Pro

- Nach ein paar Stunden der Verwendung kann der wfica32.exe-Prozess 100 % der CPU in Anspruch nehmen, wenn HDX 3D Pro mit deaktiviertem H264-Codec und deaktivierter Textprotokollierung verwendet wird.

  [Aus RcvrFürWin4.1_14.1.100][#LA5554]

HDX MediaStream

- Die Wiedergabe von Streamingvideos in einem veröffentlichten Webbrowser (z. B. Internet Explorer) funktioniert möglicherweise nicht wegen eines Fehlers in der HDX MediaStream Flash-Umleitung.

  Zum Implementieren dieses Fixes legen Sie folgende Registrierungsschlüssel fest:

  - *32--Bit-Windows:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Typ: REG_DWORD
    Wert: 0
  - *64-Bit-Windows*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Typ: REG_DWORD
    Daten: 0

  [Von RcvrForWin4.1_14.1.100] [#LA5278]

- Wenn HDX MediaStream für Flash Version 1.0 (erste Generation der Flash-Umleitung) aktiviert ist, wird Microsoft Internet Explorer möglicherweise unerwartet beendet, wenn Adobe Flash Player 11.8 oder höher installiert wird.

  [Von RcvrForWin4.1_14.1.100] [#LA5421]

HDX Plug-n-Play

- Nach Installation von Receiver für Windows 4.0 unter Windows XP SP3, können USB-Ports auf der Dockingstation nicht mehr umgeleitet werden.

  [Von RcvrForWin4.1_14.1.100] [#LA4582]

HDX RealTime

- Die Umleitung für HDX RealTime-Webkameravideokomprimierung unterstützt möglicherweise keine Quarter Video Graphics Array-Auflösung (QVGA, 320 x 240) und kann dazu führen, dass der wfica32.exe-Prozess unerwartet beendet wird.

  [Von RcvrForWin4.1_14.1.100] [#LA5232]

Installieren, Deinstallieren und Aktualisieren

- Beim Upgrade auf eine neuere Version von Receiver für Windows ohne Internet-Verbindung wird die vorherige Version nicht vollständig deinstalliert und die Installation der neueren Version schlägt fehl.

  [Von RcvrForWin4.1_14.1.100] [#LA4896]

Drucken

- Dieser Fix behebt ein Problem im universellen Druckertreiber, durch das Duplexdruck fehlschlägt und manuell ausgeführt werden muss.

  [Aus RcvrFürWin4.1_14.1.100][#261552]

- Der Versuch, ein HTML-Dokument über Internet Explorer 9 auszudrucken, kann bei bestimmten Schriftarten zu einer

fehlerhaften Anzeige im Citrix Print Viewer (cpviewer.exe) und einer fehlerhaften Druckausgabe führen.

[Von RcvrForWin4.1_14.1.100] [#LA3962]

Server-/Farmverwaltung

- Wird StoreFront mit einem Store ohne Authentifizierung konfiguriert, kann die Kontenermittlung bei Verwendung von Receiver für Windows fehlschlagen.

  [Von RcvrForWin4.1_14.1.100] [#LC0004]

- Diese Feature-Erweiterung unterstützt die automatische Erstellung von Verknüpfungen für bevorzugte Anwendungen durch die Verwendung eines Verzeichnisses für bevorzugte Vorlagen. Bei solchen Anwendungen durchsucht das Self-Service Plug-In neben den vorhandenen Bevorzugungsregeln Verknüpfungen im Verzeichnis für bevorzugte Vorlagen. Bei Übereinstimmung mit den Bevorzugungsregeln wird die Verknüpfung in das Startmenü des Benutzers kopiert.

  Standardmäßig ist dies eines der folgenden Verzeichnisse:

  - %systemdrive%:\Programme\Citrix\shortcuts
  - %systemdrive%:\Programme (x86)\Citrix\shortcuts (benutzergerätebasierte Installation)
  - %systemdrive%:\Users\\AppData\Local\Citrix\SelfService\shortcuts (benutzerbasierte Installation)

  Der Standardspeicherort für das Verzeichnis für bevorzugte Vorlagen kann in der Registrierung festgelegt werden.

  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle oder HKEY_CURRENT_USER\Software\Citrix\Dazzle
  Name: PreferTemplateDirectory
  Typ: REG_SZ
  Daten: beliebiger Pfad (z. B. "%systemroot%:\Shortcuts")

  Wenn eine Anwendung anschließend gekündigt oder aus dem Store entfernt wird, wird die aus dem Vorzugsverzeichnis kopierte Verknüpfung gelöscht.

  [Von RcvrForWin4.1_14.1.100] [#LC0005]

Sitzung/Verbindung

- Bei Verwendung von Citrix Receiver in einer virtuellen Desktopsitzung können über XenApp veröffentlichte Anwendungen nicht gestartet werden und folgende Fehlermeldung wird angezeigt:

  This version of Citrix Receiver does not support selected encryption. Wenden Sie sich an den Administrator. [Error 1029: Invalid DLL load].

  [Von RcvrForWin4.1_14.1.100] [#LA4743]

- Liegt bei Receiver für Windows 13.4 mit kumulativem Update 2 der Fokus auf einer Seamlessanwendung, ändert sich die Eingabesprache auf der Sprachenleiste beim Drücken von Alt+Tab zum Wechseln des aktiven Fensters.

  [Von RcvrForWin4.1_14.1.100] [#LA4963]

- Wenn unter Windows XP in den Eigenschaften für Taskleiste und Startmenü die Option "Ähnliche Elemente gruppieren" aktiviert ist, kann das Starten von Anwendungen langsam sein.

  [Von RcvrForWin4.1_14.1.100] [#LA4191]

- Nach einem Upgrade von Version 12.2 des Citrix Online Plug-Ins auf Version 3.x von Citrix Receiver für Windows können Proxyverbindungen mit externen Websites möglicherweise nicht hergestellt werden, wenn die NTLM-Proxyauthentifizierung aktiviert ist.

  [Von RcvrForWin4.1_14.1.100] [#LA3781]

- Wenn ein Benutzergerät keine verbundene Webcam hat und versucht wird, eine veröffentlichte Instanz von Microsoft Lync 2010 zu starten, kann es vorkommen, dass die Verbindung für die Anwendung erst nach mehrfachem Herstellen und Trennen endgültig hergestellt und die Anwendung gestartet wird. Dieses Problem kann auftreten, wenn Sie eine Anwendung installieren, die eine Webcam installiert und es ist keine andere Webcam installiert (z. B. das Motorola Bluetooth-Paket).

  [Von RcvrForWin4.1_14.1.100] [#LA4867]

- Beim Start einer veröffentlichten Anwendung oder eines veröffentlichten Desktops funktioniert die Kerberos-Authentifizierung möglicherweise nicht, wenn die Passthrough-Authentifizierung in einem IPv4- Netzwerk verwendet wird. In diesem Release wurde das Problem nur für IPv4-Netzwerke gelöst.

  [Von RcvrForWin4.1_14.1.100] [#LA5026]

- Dieser Fix behebt Audio-/Videoprobleme beim Microsoft Lync 2013 VDI Plug-In für Windows. Er optimiert die Benutzererfahrung für Lync-Benutzer. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX138408.

  [Von RcvrForWin4.1_14.1.100] [#LA5314]

- Wenn der CANcaseXL-USB-Netzwerkadapter an einen virtuellen Desktop umgeleitet wird, wird er in Windows-Geräte-Manager als nicht funktionierend angezeigt. Dieses USB-Gerät unterstützt den Citrix USB-Umleitungstreiber nicht. Die einwandfreie Funktion des VDA erfordert die Installation von Fix #LA5022.

  [Von RcvrForWin4.1_14.1.100] [#LA5022]

- Dieser Fix ist eine Neuauflage von Fix #LA1257, mit dem die folgenden Probleme nicht vollständig gelöst werden konnten:

  Wenn der Desktop Viewer deaktiviert ist, wird bei Clientsitzungen im Vollbildmodus die Bildschirmauflösung des Virtual Desktop Agent auf Änderung der Bildschirmauflösung auf dem Endpunkt hin nicht angepasst.

  [Von RcvrForWin4.1_14.1.100] [#LA4000]

- Wenn die Verbindung mit einer XenDesktop-Sitzung länger unterbrochen wird, als für das Sitzungszuverlässigkeits-Timeout festgelegt ist, verbleibt der Desktop Viewer auf dem Bildschirm. Die Sitzung selbst wird nach dem Sitzungszuverlässigkeits-Timeout ordnungsgemäß aus dem Connection Center entfernt.

  [Von RcvrForWin4.1_14.1.100] [#LA4856]

Systemausnahmen

- Der wfica32.exe-Prozess kann unerwartet beendet werden und folgende Fehlermeldung wird angezeigt:

  Citrix HDX Engine muss wegen eines Problems beendet werden.

  [Von RcvrForWin4.1_14.1.100] [#LA3964]

- Der wfica32.exe-Prozess kann unerwartet beendet werden und folgende Fehlermeldung wird angezeigt:

  Citrix HDX Engine muss wegen eines Problems beendet werden.

  [Von RcvrForWin4.1_14.1.100] [#LA4695]

- Der wfica32.exe-Prozess wird möglicherweise unerwartet beendet, wenn eine Passthrough-Sitzung auf einem XenApp 6.5-Desktop mit einer über XenApp 4.5 veröffentlichten Anwendung gestartet wird.

  [Von RcvrForWin4.1_14.1.100] [#LA5193]

- Wenn die Multistream-Richtlinie aktiviert ist, reagieren Anwendungen möglicherweise nicht mehr, wenn auf den COM-Port zugegriffen wird.

  [Von RcvrForWin4.1_14.1.100] [#LA5543]

- In Double-Hop-Szenarios kann Starten von Microsoft Outlook oder Communicator dazu führen, dass Receiver für Windows unerwartet beendet wird.

  [Von RcvrForWin4.1_14.1.100] [#LA4813]

Benutzererfahrung

- Beim Herstellen oder Wiederaufnehmen einer Verbindung mit einer unter XenApp für UNIX gehosteten Sitzung erfolgt 90 Sekunden lang keine Bildschirmaktualisierung.

  [Von RcvrForWin4.1_14.1.100] [#LA5244]

Benutzeroberfläche

- Eine mit Version 12.1 des Online-Plug-Ins eingeführte Änderung verursachte eine Verzögerung beim Einblenden der Fortschrittsanzeige für Seamless-Verbindungen. Bei Verbindungen mit langsameren Servern ist dies nicht immer erwünscht. Durch diese Erweiterung wird der folgende Registrierungsschlüssel unterstützt, über den Sie die Dauer der Verzögerung konfigurieren können:

  Unter 32-Bit-Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: NotificationDelay
  Typ: REG_DWORD
  Daten: <*Verzögerung in Millisekunden*>

  Unter 64-Bit-Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Name: NotificationDelay
  Typ: REG_DWORD
  Daten: <*Verzögerung in Millisekunden*>

  [Von RcvrForWin4.1_14.1.100] [#LA0678]

- Nach dem Ändern des Desktop-Farbschemas von der Standardeinstellung Blau in eine andere Farbe wie etwa Olivgrün oder Silber (**Desktop** > **Eigenschaften** > Registerkarte **Darstellung** > **Farbschema**) werden Text und Hintergrund des

Self-Service Plug-Ins in der gleichen Farbe angezeigt, sodass Menüeinträge nicht mehr gelesen werden können.

[Von RcvrForWin4.1_14.1.100] [#LA5121]

Sonstiges

- E-Mail-basierte Kontenermittlung: Wenn der SRV-Eintrag auf der DNS-Seite einen anderen Port als 443 enthält, ignoriert Receiver den Port im SRV-Eintrag und stellt eine Verbindung mit der Zugriffs-/NetScaler Gateway-URL unter Verwendung von Port 443 her.

  [Von RcvrForWin4.1_14.1.100] [#LA4491]

Vergleich mit Citrix Receiver für Windows 4.1

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

Microsoft Lync 2013 VDI Plug-In Installieren, Deinstallieren und Aktualisieren

Microsoft Lync 2013 VDI Plug-In

- Video wird nicht angezeigt, wenn Sie das Lync-Unterhaltungsfenster auf einen zweiten Monitor verschieben.

  [#LA5314, #399447]

- Wenn Sie ein Whiteboard-Präsentationsfenster zu einem anderen Benutzer verschieben, wird das Video des anderen Benutzers nicht in Ihrem Unterhaltungsfenster angezeigt.

  [#LA5314, #399465]

- Receiver kann bei Videoanrufen mit mehreren Teilnehmern unerwartet beendet werden, wenn die Videokonferenz beendet wird.

  [#LA5314, #426035]

- Auf einigen Clientgeräten wird das Video bei Videoanrufen im VDA-Vollbildmodus zeitweilig unterbrochen.

  [#LA5314, #418675]

- Beim Verschieben eines Videokonferenzfensters kann eine Bildverzerrung entstehen.

  [#LA5314, #419898]

Installieren, Deinstallieren und Aktualisieren

- Beim Upgrade auf eine neuere Version von Receiver für Windows ohne Internet-Verbindung wird die vorherige Version nicht vollständig deinstalliert und die Installation der neueren Version schlägt fehl.

  [#LA4896]

Vergleich mit Citrix Receiver für Windows 4.0.1

Receiver für Windows 4.1 enthält alle Problembehebungen der Versionen Receiver für Windows 4.0 und 4.0.1 und darüber hinaus folgende neuen Korrekturen:

HDX MediaStream Flash-Umleitung

- Wenn mehrere Multimediadateien in schneller Abfolge auf http://www.youtube.com/ mit aktivierter HDX MediaStream Flash-Umleitung wiedergegeben werden, kann der PseudoContainer2.exe-Prozess unerwartet beendet werden.

  [#LA3846

HDX MediaStream Windows Media-Umleitung

- In Receiver für Windows Version 3.4 beginnt das Streaming von Multimediadateien mit einer Verzögerung von bis zu zehn Sekunden, wenn die HDX MediaStream-Windows-Medienumleitung aktiviert ist.

  [#LA4141]

HDX Plug-n-Play

- Wird im Desktop Viewer ein USB-Gerät per Mausklick für das Remoting über die HDX Plug-n-Play-USB-Geräteumleitung ausgewählt, kann es vorkommen, dass der Desktop Viewer nicht mehr reagiert.

  [#LA3348]

Installieren, Deinstallieren und Aktualisieren

- Versucht ein Benutzer, der kein Administrator ist, ein Upgrade von Receiver für Windows durchzuführen, wenn Receiver von einem Administrator installiert wurde, kann dies zu einer unvollständigen Installation führen.

  Durch diese Lösung werden Benutzer, die keine Administratoren sind, beim Versuch des Upgrades einer von einem Administrator installierten Receiver-Anwendung durch eine Fehlermeldung informiert und die Installation wird

abgebrochen.

[#LA3425]

Tastatur

- Bei Verwenden von Version 3.3 von Receiver für Windows kann das Drücken der Alt-Taste dazu führen, dass die Taste in der gedrückten Stellung verbleibt. Mit einem anschließenden Drücken der Taste E wird daher Windows Explorer aufgerufen.

  [#LA3288]

- Wenn bei gedrückter Windows-Taste im Vollbildmodus auf die Desktop Viewer-Symbolleiste geklickt wird, kann die Taste in der gedrückten Stellung verbleiben. Mit einem anschließenden Drücken der Taste E wird daher Windows Explorer aufgerufen.

  [#LA3349]

- Dieser Fix behebt Probleme bei der Synchronisierung des Zustands der Feststelltaste, der Num-Taste und der Rollen-Taste in ICA-Sitzungen. Durch diesen Fix wird ein neuer Parameter eingeführt, mit dessen Hilfe Sie die Synchronisierung des Tastatur-LED-Zustands zwischen Client und Server erzwingen können. Um diese Option zu nutzen, fügen Sie den Eintrag "KeyboardForceLEDUpdate=On" dem Abschnitt [WFClient] der Datei appsrv.ini im Pfad des lokalen Benutzerprofils oder der Datei default.ica in der entsprechenden Webinterface-Site hinzu.

  [#LA3682]

- Dieser Fix behebt Probleme bei der LED-Synchronisierung des Zustands der Feststelltaste, der Num-Taste und der Rollen-Taste zwischen Client und Server.

  [#LA4293]

Lokaler App-Zugriff

- Wenn der lokale App-Zugriff aktiviert ist, wird durch Klicken auf den Desktop Viewer die lokale Taskleiste des Clients grundlos ausgeblendet.

  [#LA3049]

Anmeldung und Authentifizierung

- Die Passthrough-Authentifizierung funktioniert nach der Installation von XenDesktop 7 VDA unter Windows Server 2008 R2 möglicherweise nicht mehr. Das Problem tritt auf, weil der ssonsvr.exe-Prozess nicht gestartet wird.

  [#LA4685]

Drucken

- Beim Senden von mehreren Adobe Acrobat-Druckaufträgen an einen Sitzungsdrucker können einzelne Seiten oder ganze Druckaufträge verloren gehen.

  [#LA3643]

- Die Enumeration für Sitzungsdrucker kann übermäßig lange dauern.

[#LA3951]

Sitzung/Verbindung

- Wenn ein Clientgerät mit einer aktiven XenDesktop-Sitzung nach längerer Zeit im Standbymodus oder Ruhezustand reaktiviert wird, wird die Sitzung möglicherweise nicht wie erwartet neu verbunden, sondern bleibt im Verbindungsaufbau hängen und das Sitzungsfenster muss manuell geschlossen werden.

  Dieser Fix behebt das Problem, sodass bei Reaktivieren von Clientgeräten das Sitzungsfenster wie erwartet geschlossen wird, wenn die Wiederverbindung fehlschlägt.

  [#LA2748]

- Beim Starten einer veröffentlichten Anwendung im Seamless-Modus bleibt die Fortschrittsanzeige im Hintergrund.

  Zum Implementieren dieses Fixes legen Sie clientseitig folgende Registrierungsschlüssel fest:

  - *32-Bit-Windows-Systeme:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Name: ForegroundProgressBar
    Typ: DWORD
    Daten: 1
  - *64-Bit-Windows-Systeme:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    Name: ForegroundProgressBar
    Typ: DWORD
    Daten: 1

  [#LA3491]

- Bei Receiver mit Desktop Lock wird ein grauer Bildschirm angezeigt, wenn ein Hardwarefehler auftritt oder die VM zwangsweise über den Hypervisor heruntergefahren wird.

  [#LA3499]

- Wenn auf dem Clientgerät die Taskleistengruppierung aktiviert ist, fragt TaskbarGrpXpVista.dll in wfica32.exe unnötigerweise Informationen zu veröffentlichten Anwendungen, die in der Sitzung ausgeführt werden, auf dem Clientgerät ab. Wird beispielsweise eine veröffentlichte Instanz von cmd.exe ausgeführt, fragt TaskbarGrpXpVista.dll Informationen zu der ausführbaren Datei bei C:\windows\system32\cmd.exe ab. Wird die veröffentlichte Anwendung über die Remotefreigabe ausgeführt, kann dies zu einer unerwünschten Bandbreitennutzung führen.

  [#LA3661]

- Wenn eine GPO-Einstellung die Taskleistengruppierung verhindert, wechselt der Fokus beim Klicken auf Taskleistensymbole unter Windows XP und Vista nicht auf die zugeordneten Fenster.

  [#LA3889]

- Receiver reagiert möglicherweise nicht mehr, wenn auf der Desktop Viewer-Symbolleiste auf das Gerätesymbol geklickt wird, während das Gerätezugriffsdialogfeld für Citrix Receiver geöffnet ist. Dieses Dialogfeld wird angezeigt, wenn für den Gerätezugriff "Jedes Mal fragen" anstelle der Standardeinstellung "Do nothing" eingestellt ist.

  [#LA3899]

- Der Desktop Viewer-Prozess (CDViewer.exe) und der wfica32.exe-Prozess werden möglicherweise unerwartet beendet, wenn die Verbindung mit einer virtuellen Desktopsitzung wiederaufgebaut wird.

  [#LA3944]

- Dieser Fix integriert die IsReconnectInProgress()-API in Citrix Fast Connect 2.0. Durch das Feature wird ermittelt, ob die Wiederverbindung ausgeführt wird, wenn die automatische Wiederverbindung von Clients aktiviert ist.

  [#LA4080]

- Dieser Fix ermöglicht die Wiederverbindung von Passthrough-Anwendungen und aktiviert Workspace Control für Passthrough-Anwendungen.

  Zum Implementieren dieses Fixes legen Sie folgende Registrierungsschlüssel fest:

  Zum Aktivieren von Workspace Control im Passthroughmodus:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
  Name: ForceEnableWSC
  Typ: DWORD
  Daten = 1

  Zum Ermöglichen der Wiederverbindung von Passthrough-Anwendungen:

  HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
  Name: BypassPassThruMode
  Typ: DWORD
  Daten = 1

  Hinweis: Dieser Fix funktioniert nur unter den folgenden Bedingungen:

  - Die beiden (bzw. mehrere) Verbindungs-Hops erfolgen nicht in der gleichen XenApp Services-Site oder -Farm. Das heißt, Receiver auf dem Endpunkt kann eine Verbindung mit einem XenDesktop-VDA in der XenApp Services-Site A herstellen und der Passthrough-Client auf dem VDA kann dann eine Verbindung mit einer veröffentlichten Anwendung oder einem Desktop in einer *anderen* XenApp Services-Site, z. B. Site B, herstellen.
  - Der zweite Verbindungs-Hop muss bei einer XenApp-Terminalsitzung erfolgen, ein Hop bei einem XenDesktop-VDA ist nicht möglich.

  [#LA4206]

- Bei der Verwendung von Remoteunterstützungs-Software für einen Desktop, der als ungerader Prozentsatz (z. B. 95 %) des Clientbildschirms veröffentlicht wurde, wird die Remoteunterstützungs-Sitzung möglicherweise verzerrt angezeigt.

  [#LA4313]

- Durch diese Erweiterung wird die Unterstützung für die HDX Plug-n-Play-USB-Geräteumleitung auf zusätzliche USB-Geräte erweitert.

  [#LA4335]

- Ein Deadlock in wfcrun32.exe kann verhindern, dass neue Sitzungen erfolgreich starten.

  [#LA4344]

- Versuche, eine Verbindung mit XenApp-Servern mit dem Citrix Schnellstarttool herzustellen oder mit statischen ICA-Dateien, in denen "HTTPBrowserAddress=ServerName_Oder_IP:Port" (z. B.: "HTTPBrowserAddress=192.168.1.10:8080") festgelegt ist, können fehlschlagen.

  [#LA4585]

Systemausnahmen

- Der wfica32.exe-Prozess kann unerwartet beendet werden und folgende Fehlermeldung wird angezeigt:

  Citrix HDX Engine muss wegen eines Problems beendet werden.

  [#LA3412]

- In dem wfica32.exe-Prozess kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird.

  [#LA3639]

- Der wfica32.exe-Prozess kann unerwartet beendet werden.

  [#LA4208]

Benutzererfahrung

- Dieser Fix behebt das Problem der unnötigen Anzeige von Anmeldeaufforderungen bei Verwendung von Receiver 4.0 mit StoreFront.

  [#LA4652]

Benutzeroberfläche

- Der Start von Anwendung schlägt fehl, wenn ein Konflikt zwischen dem Anwendungsnamen und dem Anzeigenamen der veröffentlichten Anwendung besteht.

  [#LA3891]

Sonstiges

- Dieses Release enthält die aktuelle Version des SSLSDK Version 12.1.13.

  [#LA3804]

- Dieser Fix verbessert die Funktionsweise der TerminateUser-Funktion von Receiver für Windows in bestimmten Bereitstellungen.

  [#LA3881]

Vergleich mit Citrix Receiver für Windows 4.0

Receiver für Windows 4.0.1 enthält alle Problembehebungen der Versionen Receiver für Windows 4.0 und darüber hinaus folgende neuen Korrekturen:

- Dieser Fix behebt das Problem der unnötigen Anzeige von Anmeldeaufforderungen bei Verwendung von Receiver 4.0 mit

StoreFront.

[#LA4652]

Vergleich mit Citrix Receiver für Windows 3.4

Receiver für Windows 4.0 enthält die folgenden Korrekturen im Vergleich zu Citrix Receiver für Windows 3.4:

HDX MediaStream Flash-Umleitung

- Wenn während der Wiedergabe ein Videofenster teilweise oder vollständig aus dem Bildschirm geschoben wird, kann ein dunkler Bereich auf dem Bildschirm zurückbleiben. Der Bereich bleibt bestehen, selbst wenn das Videofenster wieder zurückgeschoben wird.

  [#LA0599]

- **Wichtig**: Lesen Sie vor dem Installieren dieses Fixes auf einem Clientgerät den Knowledge Center-Artikel CTX126817 mit wichtigen Informationen zu den Auswirkungen des Features für dynamische Sperrlisten auf die clientseitige Flash-Umleitung.

  Wenn die Richtlinie *Serverseitigen Inhaltsabruf aktivieren* auf dem Server aktiviert und auf dem Client die Einstellung *URL-Liste für serverseitigen Flash-Inhaltsabruf* für die Flash-Umleitungsrichtlinie konfiguriert ist, schlägt die Wiedergabe von Flash-Inhalten fehl, wenn die URL des Inhalts Multibyte-/Unicode-Zeichen (wie sie in asiatischen Sprachen üblich sind) enthält.

  Zum vollständigen Implementieren dieses Fixes müssen Sie ein Clienthotfix mit Fix #LA1621 und überdies Folgendes installieren:

  - *XenApp*: HDX Flash-Hotfix mit Fix #LA1621
  - *XenDesktop*: Virtual Desktop Agent-Hotfix mit Fix #LA1621

  Hinweis: Dieser Fix erfordert außerdem die Installation der entsprechenden Sprach-Codepages auf dem Client und dem Server. Die Codepages werden standardmäßig vom Windows-Betriebssystem installiert. Mit der japanischen Version von Windows 7 werden beispielsweise die japanischen Codepages standardmäßig installiert. Wenn Sie jedoch eine URL mit

japanischen Zeichen in einer deutschen Windows 7-Version verwenden, müssen die japanischen Codepages manuell installiert werden. Dies gilt sowohl für den Client als auch für den Server, da URLs vom Client zum Server übertragen werden, wenn der serverseitige Inhaltsabruf aktiviert ist.

[#LA1621]

- Einige Benutzerinteraktionen mit Flash-Inhalten, z. B. Klicken auf Schaltflächen, kann dazu führen, dass Pseudocontainer2.exe unerwartet beendet wird.

  [#LA1948]

- Die clientseitige Inhaltsumleitung kann in folgenden Situationen bei bestimmten Arten von Flash-Inhalten fehlschlagen und auf serverseitige Wiedergabe wechseln:

  1. Vom Flash-Inhalt wird versucht, eine weitere Flash-Datei herunterzuladen, die nicht vorhanden ist oder nicht gefunden wird.
  2. Von Adobe Captive erstellter Flash-Inhalt besteht einige Logikprüfungen des Features für clientseitige Inhaltsumleitung nicht.
  3. Durch Flash-Inhalt wird bewirkt, dass die clientseitige Inhaltsumleitung ein Remoting nicht unterstützter Schnittstellen an den Server durchführt.
  4. Der Client versucht, Flash-Inhalt abzurufen, obwohl dessen URL in der ServerContentFetching-Sperrliste konfiguriert ist.

  Zum Implementieren dieses Fixes müssen Sie ein HDX Flash- und ein Receiver für Windows-Hotfix installieren, das Fix #LA2198 enthält. Zum Lösen des o. g. Problems 1 müssen Sie außerdem den folgenden Registrierungsschlüssel auf dem Client festlegen:

  - *32--Bit-Windows:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Typ: REG_DWORD
    Daten: 0
  - *64-Bit-Windows:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Typ: REG_DWORD
    Daten: 0

  [#LA2198]

- Wird der Fokus vom Flash-Fenster (untergeordnetes Seamlessfenster eines Webbrowsers) auf ein lokales Fenster verschoben und dann wieder zurück auf die Adressleiste des Browser-Seamlessfensters, kann möglicherweise keine Eingabe in der Adressleiste des gemacht werden.

  [#LA2685]

- Wichtig: Lesen Sie vor dem Installieren dieses Fixes auf einem Clientgerät den Knowledge Center-Artikel CTX126817 mit wichtigen Informationen zu den Auswirkungen des Features für dynamische Sperrlisten auf die clientseitige Flash-Umleitung.

  Die HDX MediaStream Flash-Umleitung funktioniert möglicherweise nicht bei Dailymotion-Videos (http://www.dailymotion.com) und ein Fehler wird angezeigt. Das Problem tritt auf, wenn Client und Server sich an

verschiedenen geografischen Standorten befinden.

Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
Name: DisableRegionFiltering
Typ: REG_DWORD
Daten: 1

[#LA3134]

HDX Plug-n-Play

- Durch diese Feature-Erweiterung wird die standardmäßige Funktionsweise der USB-Umleitung wie folgt modifiziert:
  - Wenn der Desktop Viewer aktiviert ist, können Benutzer USB-Geräte manuell umleiten.
  - Wenn der Desktop Viewer nicht aktiviert ist, werden USB-Geräte automatisch umgeleitet.

  [#LA0108]
- Nach fehlgeschlagenen Versuchen, bestimmte USB-Geräte einer virtuellen Desktopsitzung zuzuordnen, verschwinden die Geräte aus Device Manager, bis der Endpunkt neu gestartet wird.

  [#LA0954]
- Wird im Desktop Viewer ein USB-Gerät per Mausklick für das Remoting über die HDX Plug-n-Play-USB-Geräteumleitung ausgewählt, kann es vorkommen, dass der Desktop Viewer nicht mehr reagiert.

  [#LA3348]

Installieren, Deinstallieren und Aktualisieren

- Nach dem Upgrade auf Receiver 3.xkönnen Benutzer keine veröffentlichten Anwendungen starten und die folgende Fehlermeldung wird angezeigt:

  This version of Citrix Receiver does not support selected encryption. Wenden Sie sich an den Administrator. Error 1046: The Virtual Driver is not loaded.

  [#LA3120]

Tastatur

- Bei Minimieren einer virtuellen Desktopsitzung durch Klicken auf "Home" im Desktop Viewer funktioniert die TAB-Taste auf dem Endpunkt möglicherweise zeitweilig nicht, bis die Sitzung getrennt wird.

  [#LA2925]
- Ab Version 3.0 von Receiver für Windows funktioniert die KeyboardTimer-Einstellung von HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard nicht mehr. Durch diesen Fix wird diese Funktion wiederhergestellt.

  [#LA2949]
- Dieser Fix behebt Probleme bei der Synchronisierung des Zustands der Feststelltaste, der Num-Taste und der Rollen-Taste zwischen Client und Server bei Passthrough-Sitzungen, die im Vordergrund ausgeführt werden.

[#LA3288]

- Dieser Fix behebt Probleme bei der Synchronisierung des Zustands der Feststelltaste, der Num-Taste und der Rollen-Taste zwischen Client und Server bei Passthrough-Sitzungen, die im Hintergrund ausgeführt werden.

  [#LA3310]

Drucken

- Wenn auf **Einstellungen des lokalen Druckers** auf der Registerkarte **Clienteinstellungen** des Dialogfelds **Eigenschaften** eines UDP-Druckers geklickt und das Einstellungsdialogfeld dann geschlossen wird, reagiert das Dialogfeld **Eigenschaften** möglicherweise nicht mehr.

  [#259485]

Seamlessfenster

- Beim Abmelden von einer Seamlesssitzung mit nicht gespeicherten Daten mit dem Connection Center oder dem Webinterface wird ein schwarzes Fenster angezeigt.

  Die darin enthaltene Meldung weist darauf hin, dass Programme noch geschlossen werden müssen, und es werden die Optionen "Abmelden erzwingen" und "Abbrechen" angeboten. Die Option "Abbrechen" funktioniert nicht.

  Nach der Installation dieses Fixes funktioniert die Option "Abbrechen" einwandfrei. Citrix empfiehlt, dass Sie nach Verwendung der Schaltfläche "Abbrechen" die Daten speichern und sich dann von der Sitzung abmelden, um weitere Leistungsminderungen zu verhindern.

  [#LA0318]

Sitzung/Verbindung

- Nach dem Trennen der Verbindung mit einer virtuellen Desktopsitzung und anschließendem Wiederverbinden kann die Audioaufzeichnung aus der Sitzung heraus fehlschlagen. Zum vollständigen Implementieren dieses Fixes müssen Sie ein Server- und ein Clienthotfix mit Fix #LA0821 installieren.

  [#LA0821]

- Die Dateiübertragung in einer Clientsitzung kann langsamer sein als in einer RDP-Sitzung.

  Zum vollständigen Implementieren dieses Fixes müssen Sie ein Server- und ein Clienthotfix mit Fix #LA0821 installieren.

  [#LA1263]

- Wenn die Auflösung einer virtuellen Desktopsitzung geändert wird und die Sitzung dann unerwartet getrennt wird (z. B. aufgrund eines Netzwerkausfalls), ist die Auflösung nach Wiederherstellen der Verbindung möglicherweise anders.

  [#LA1377]

- Serielle Barcodescanner können keine Etiketten verarbeiten, deren Datengröße 512 Byte überschreitet. Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: CommBufferSize

Typ: REG_DWORD
Daten: Bereich zwischen 512 und 2048

[#LA1695]

- Deaktivieren des Netzwerklistendiensts und/oder des Diensts für Netzwerkadressinformationen gemäß Knowledge Center-Artikel CTX131577 führt dazu, dass Version 12.3 des Online Plug-Ins die Verbindung verliert.

  [#LA2024]

- Der Start einer Seamlessanwendung, die für einen UNC-Pfad über eine Verbindung mit geringer Bandbreite veröffentlicht wurde, kann länger als zwei Minuten dauern.

  [#LA2170]

- Das Aufrufen der Eingabemethode einer Seamlesssitzung über Strg+Umschalt kann auch die clientseitige lokale Eingabemethode ändern. Zur Vermeidung dieses Problems legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: Showlocallanguagebar
  Typ: REG_DWORD
  Daten: 1 *< zum Anzeigen der lokalen Sprachleiste>*; 0

  [#LA2180]

- Wenn die automatische Clientumleitung aktiviert ist, schlagen Wiederverbindungsversuche nach Auswahl des Ruhezustands und automatischem Beenden des Clients möglicherweise fehl.

  Mit diesem Fix kann ein System mit Client-USB-Geräteumleitung, das angehalten oder in den Ruhezustand versetzt wurde, bei Reaktivierung automatisch wieder verbunden werden.

  [#LA3061]

- Veröffentlichte Anwendungen können möglicherweise nicht gestartet werden, wenn die ICA-Komprimierung für Citrix Receiver für Windows 3.x über HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off deaktiviert wurde.

  [#LA3072]

- In einer Umgebung mit mehreren Monitoren wird die Desktop Viewer-Symbolleiste möglicherweise nicht mehr angezeigt, wenn auf einen zweiten Monitor im Vollbildmodus umgeschaltet wird.

  [#LA3083]

- In Konfigurationen mit zwei Monitoren, von denen einer ein Laptopmonitor ist, und Verbindung mit einem Virtual Desktop Agent werden Sitzungen nur noch auf dem primären Monitor angezeigt, wenn der Laptopmonitor aus- und wieder eingeschaltet wird.

  [#LA3202]

- Bei Verwendung von Version 3.3 des kumulativen Updates 1 oder von Version 3.4 von Receiver für Windows auf einem Computer mit Windows XP, auf dem Internet Explorer 8 ausgeführt wird, kann die Originalanwendung möglicherweise nicht über das Webinterface gestartet werden.

[#LA3234]

- Konsolen- und XenDesktop-Sitzungen reagieren möglicherweise nicht mehr (bleiben beim Willkommen-Bildschirm hängen), wenn versucht wird, die Verbindung mit einer getrennten virtuellen Desktopsitzung über Receiver für Linux wiederherzustellen. Das Problem tritt auf, wenn der WDDM-Treiber auf dem Virtual Desktop Agent aktiviert ist und eine weitere virtuelle Desktopsitzung in der Sitzung ausgeführt wird.

  [#LA3241]

- Version 3.4 von Receiver für Windows kann möglicherweise nicht gestartet werden, wenn für "Regions- und Sprachoptionen" unter Windows 7 "Kasachisch (Kasachstan)" eingestellt ist.

  [#LA3517]

Systemausnahmen

- Der wfica32.exe-Prozess kann in Umgebungen, in denen EdgeSight for Load Testing bereitgestellt ist, unerwartet beendet werden.

  [#LA0289]

- Der wfcrun.exe-Prozess kann in Umgebungen, in denen HP LoadRunner bereitgestellt ist, unerwartet beendet werden.

  [#LA0859]

- Wenn die Audiorichtlinie auf High Definition festgelegt ist, kann der wfica32.exe-Prozess unerwartet beendet werden, wenn beliebige Beispielaudiodateien über das Audiosteuerungsfeld auf einem veröffentlichten Desktop wiedergegeben werden.

  [#LA1000]

- Version 12.3 des Online Plug-Ins kann unerwartet beendet werden, wenn eine Sitzung von einer Webinterface-Site getrennt wird und eine Microsoft Excel 2007-Tabelle geöffnet ist.

  [#LA2274]

- Wenn der lokale App-Zugriff aktiviert ist, kann der Versuch des Aufbaus einer Verbindung mit einem Virtual Desktop Agent fehlschlagen, wenn für diesen rechtliche Hinweise konfiguriert sind.

  [#LA2351]

- Der Pnamain.exe-Prozess kann beim Wiederherstellen der Verbindung mit einer Sitzung unerwartet beendet werden.

  [#LA2704]

- Die Verbindung von Sitzungen Aero-aktivierter Windows-Client mit Einzelmonitor kann unerwartet abbrechen. Das Problem kann auftreten, wenn eine Vorschau im Rahmen der dynamischen Fenstervorschau an den Client gesendet wird; zum gleichen Zeitpunkt kann ein twi3.dll-Thread den Winlogon.exe-Prozess beenden, was wiederum zum Trennen der Sitzungsverbindung führt.

  Zur Problemlösung müssen Sie ein XenApp- und ein Receiver-Hotfix mit Fix #LA2858 installieren.

  [#LA2858]

- Der wfica32.exe-Prozess kann unerwartet beendet werden. Das Problem tritt aufgrund einer ungültigen Speicherdereferenzierung auf.

  [#LA2860]

- Beim Drucken in bestimmten Double Hop-Szenarios wird gemeldet, dass Citrix HDX Engine nicht mehr funktioniert, und der Wfica32.exe-Prozess wird unerwartet beendet. Das Problem tritt auf, wenn Portnamen über 260 Zeichen enthalten.

  Zur Problemlösung müssen Sie ein Server- und ein Receiver-Hotfix mit Fix #LA3009 (XA650R01W2K8R2X64056; RcvrForWin3.3_13.3.104 oder die ersetzenden Hotfixes) installieren.

  [#LA3009]

- Citrix Receiver kann mehrere Instanzen des selfserviceplugin.exe-Prozesses erzeugen, was zu Speichermangel im System führt.

  [#LA3460]

- Der Desktop Viewer kann während der Abmeldung unerwartet beendet werden.

  [#LA3567]

- PNMain.exe kann unerwartet beendet werden, wenn das Online Plug-In als Passthrough-Client verwendet wird.

  [#LA0785]

Benutzererfahrung

- Bei Verwendung der USB-Umleitung können SpaceMouse-USB-Geräte nach ein paar Stunden des Gebrauchs aus einer virtuellen Desktopsitzung verschwinden.

  [#LA2256]

- Diese Feature-Erweiterung für Version 3.4 von Receiver für Windows ermöglicht die Unterdrückung der Authentifizierungsmeldung für VPN-Anmeldungen, die angezeigt wird, wenn ein Benutzer zwischen Netzwerkverbindungen wechselt.

  Zum Unterdrücken der Meldung erstellen Sie folgenden Registrierungsschlüssel:

  - *32--Bit-Windows*:
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    Name: AutoSecureConnection
    Typ: REG_DWORD
    Wert: 0 (deaktiviert die VPN-Aufforderung)
  - *64--Bit-Windows*:
    HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
    Name: AutoSecureConnection
    Typ: REG_DWORD
    Wert: 0 (deaktiviert die VPN-Aufforderung)

  [#LA3772]

Benutzeroberfläche

- Durch diesen Fix wird die koreanische Übersetzung der Symbolbezeichnung für den Home-Desktop auf der Desktop Viewer-Symbolleiste präziser.

  [#232198]

- Bei Klicken auf **Abbrechen** in dem Authentifizierungs-Dialogfeld, das angezeigt wird, wenn eine Desktopgruppen-Verknüpfung auf einem Endpunkt ausgeführt wird, wird die folgende irreführende Meldung angezeigt:

  The application or desktop could not be launched. Überprüfen Sie die Netzwerkverbindung.

  [#259081]

- In maximierten Sitzungsfenstern wird die Desktop Viewer-Symbolleiste möglicherweise nicht richtig dargestellt, wenn im USBMultiInsertDialogue-Dialogfeld **nach** Ausblenden des Sitzungsverbindungsbildschirms auf *Verbinden* geklickt wird.

  [#260390]

- Im Hilfethema zur Clientlaufwerkzuordnung von icaclient.adm wird fälschlicherweise angegeben, dass Richtlinien keinen Vorrang vor der Auswahl von Benutzern haben. Richtlinien setzen eine Benutzerauswahl außer Kraft.

  [#LA0398]

- Bei einigen benutzerdefinierten Anwendungen wird in Bearbeitungsfenstern der SpeedScreen-Latenzreduktion mit lokalem Textecho während der Eingabe ein schwarzer Balken angezeigt.

  [#LA0544]

- Die Begrüßungs- und/oder Abschlussmeldung nach der ersten erfolgreichen Bereitstellung von Merchandising Server wird nicht angezeigt.

  [#LA2277]

- Das Symbol für Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO) kann aus dem Infobereich der Windows-Taskleiste unerwartet verschwinden, wenn eine veröffentlichte Anwendung gestartet wird.

  [#LA3190]

- Auf die lokale Taskleiste kann nicht mehr zugegriffen werden, wenn sie auf "Automatisch im Hintergrund" festgelegt ist und von ihrer Standardposition nach oben links oder rechts verschoben wird.

  [#LA3400]

Sonstiges

- Bei der Wiedergabe von UDP-Audiodatenströmen kann die Handleanzahl des wfica32.exe-Prozesses deutlich ansteigen.

  [#LA3094]

- Durch diesen Fix wird die Beschränkung auf nur eine Program Neighborhood Webinterface 5.4-Site in Receiver für Web 3.3 aufgehoben.

  [#LA3142]

Receiver für Windows 4 - Bekannte Probleme

Oct 21, 2015

Dieser Abschnitt enthält:

- Installations- und Upgradeprobleme
- Allgemeine Probleme
- Bekannte Probleme - Desktopverbindungen
- Probleme mit dem Microsoft Lync 2013 VDI Plug-In

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.

Installations- und Upgradeprobleme

- Bei Upgrades von Receiver für Windows 3.4 von citrix.com werden ausstehende Updates, z. B. für Plug-Ins, nicht abgeschlossen. Führen Sie ein manuelles Upgrade von Receiver durch, um das Problem zu beheben.
- Upgrades auf Receiver für Windows 3.3 von citrix.com funktionieren nicht. Führen Sie die Upgrades manuell durch, um dieses Problem zu beheben.
- Receiver für Windows kann nur richtig auf Computern unter Windows 8 installiert werden, wenn .NET 3.5 installiert ist. Wenn Sie Receiver auf solchen Computern installieren, werden Sie vom Receiver-Installationsprogramm zum Download und zur Installation von .NET 3.5 aufgefordert. Nach dem Abschluss der .NET-Installation wird die Receiver-Installation gestartet, aber nicht abgeschlossen. Deinstallieren Sie Receiver mit "Programme und Funktionen" und installieren Sie das Programm dann neu.
- Wenn Sie während der Receiver-Installation auf einem Windows 8-Computer, auf dem .NET 3.5 nicht installiert oder aktiviert ist, die Aufforderung zur Installation von .NET 3.5 abbrechen und dann versuchen, Receiver zu deinstallieren, schlägt die Deinstallation fehl. Installieren oder aktivieren Sie .NET 3.5 auf dem Computer und deinstallieren Sie dann Receiver. Navigieren Sie zum Aktivieren von .NET 3.5 auf einem Computer unter Windows 8 zu Systemsteuerung > Programme und Funktionen > Windows-Funktionen ein- oder ausschalten und wählen Sie .Net Framework 3.5. [#354996]
- Bei der Installation des Receiver-Pakets auf einem Windows 8-Client mit Merchandising Server wird das Receiver-Symbol nicht in der Taskleiste angezeigt. Starten Sie die Maschine des Benutzers neu, um das Problem zu beheben. Sie können Receiver auch vom Ordner starten, in dem Receiver.exe gespeichert ist.
- Eine Installation ohne Benutzereingriffe auf einem Windows 8-Computer wartet unbegrenzt (obwohl Receiver erfolgreich installiert wird). Als Lösungsansatz sollten Sie nicht den Parameter -wait an der PowerShell-Befehlszeile verwenden.
- Wenn Receiver mit Merchandising Server auf einem Windows 8-Gerät installiert wird, wird das Receiver-Symbol ggf. nicht in der Taskleiste angezeigt. Starten Sie Receiver vom Installationsordner, um dieses Problem zu beheben.
- In einer Umgebung mit App Controller 2.0 gibt Receiver nicht an, dass ein Benutzer angemeldet ist: Das Receiver-Menü enthält den Befehl "Anmelden" und der Benutzername wird nicht im Receiver-Fenster angezeigt. Alle anderen Features des Receiver-Fensters funktionieren wie erwartet. Aktualisieren Sie auf App Controller 2.5, bevor Benutzer Receiver aktualisieren, um dieses Problem zu vermeiden.
- Für Bereitstellungen mit Merchandising Server müssen Sie auf Receiver Updater für Windows 3.4 aktualisieren, damit Receiver deinstalliert werden kann. Teilen Sie den Benutzern auch mit, wie sie auf die Aufforderung nach dem Neustart

von Receiver reagieren sollen. Das heißt, ein Benutzer muss auf Später klicken. Receiver wird nicht deinstalliert, wenn ein Benutzer auf Neu starten klickt. [#346341]

- Wenn ein Benutzer ein älteres Online Plug-In installiert hat und eine Verbindung mit einer Receiver für Web-Site von Internet Explorer 10 herstellt, wird das Plug-In nicht auf die aktuelle Version von Receiver für Windows aktualisiert. Verwenden Sie einen anderen unterstützten Browser oder deinstallieren Sie das Online Plug-In, um das Problem zu beheben. [#393929]
- Wenn ein Benutzer ein Plug-In über die Systemsteuerung deinstalliert und den Computer neu startet, ist das Plug-In weiterhin in der Liste enthalten, die angezeigt wird, wenn Sie mit der rechten Maustaste auf das Receiver-Symbol klicken, dann auf Info klicken und Erweitert anzeigen. Dies tritt nur auf, wenn Receiver von Citrix.com oder Ihrer eigenen Downloadsite installiert wird.
- Plug-In-Updates unter Windows XP, 64-Bit-Edition, schlagen fehl. Installieren Sie als Lösungsansatz den Hotfix, der unter http://support.microsoft.com/kb/968730/en-us verfügbar ist. [#328081]
- Bevor Sie Receiver für Windows auf einem Thin Client-Gerät mit Windows XP Embedded installieren, sollten Sie die Arbeitsspeicherbeschränkung des Geräts auf 100 MB erhöhen.

Allgemeine Probleme

- Informationen zu nicht unterstützten Features finden Sie in der Citrix Receiver feature matrix.
- Das Dialogfeld "Smartcard-Authentifizierung" verliert ggf. den Fokus und verhindert die Authentifizierung des Benutzers, wenn er versucht, eine Anwendung über Receiver zu starten. Dies tritt auf, wenn Single Sign-On nicht aktiviert ist. Der Benutzer sollte in dieser Situation die Sitzung neu starten. Stellen Sie als Lösungsansatz TWISeamlessFlag auf 1 im folgenden Registrierungsschlüssel ein: [#379878]
  32-Bit-Maschinen: HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

  64-Bit-Maschinen: HKEY_LOCAL_MACHINE\Software\ Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

- Eine SaaS-Anwendung mit einem Symbol, das größer als 48x48 ist, kann in Receiver nicht abonniert werden. [#353794]
- Wenn ein Benutzer im Info-Dialogfeld auf Update und dann auf Erweitert klickt, wird der Link Receiver zurücksetzen nicht mehr angezeigt. Schließen und öffnen Sie das Info-Dialogfeld erneut, um dieses Problem zu beheben.[#383110]
- Nach der Verwendung des Befehls zum Zurücksetzen von Receiver auf einer Windows 2008 R2-Maschine kann Receiver nicht vom Startmenü aus gestartet werden und der Befehl "Öffnen" wird nicht mehr im Receiver-Menü angezeigt. Starten Sie als Lösungsansatz Receiver nach dem Zurücksetzen neu. (Klicken Sie zum Zurücksetzen von Receiver mit der rechten Maustaste auf das Receiver-Symbol und wählen Sie Info aus; erweitern Sie Erweitert und klicken Sie auf Receiver zurücksetzen.)
- Wenn Receiver mit mehreren Stores konfiguriert ist, kann Receiver die Gateways verwechseln, die für die Verbindung mit einem Store benötigt werden. Den Benutzern stehen dann falsche Apps zur Verfügung. Lösungsansatz: Konfigurieren Sie nur einen Store.
- Bei Receiver können in den folgenden Situationen Probleme beim automatischen Wiederherstellen der Verbindung auftreten: Receiver ist mit einer Webinterface-Site verbunden und die Datei default.ica enthält den Eintrag SessionReliabilityTTL=60. Bearbeiten Sie für das Beheben des Problems die Datei default.ica file und entfernen Sie entweder den Eintrag SessionReliabilityTTL (damit der Standardwert von 180 verwendet wird) oder ändern Sie den Eintrag in SessionReliabilityTTL=180.
- Wenn ein Benutzer Apps startet, die über eine Webinterface-Verbindung bereitgestellt werden, listet das Connection Center die Sitzungen nicht auf.
- Wenn ein Benutzer eine virtuelle App startet, die für Access Gateway gefiltert ist, können andere virtuelle Apps nicht

gestartet werden.

- Für Windows 8-Geräte, die Touchtastaturen unterstützen, müssen Sie den lokalen Eingabemethoden-Editor (IME) für asiatische Sprachen aktivieren, damit Benutzer Zeichen in virtuelle Anwendungen eingeben können. Führen Sie hierfür den folgenden Befehl an einer Eingabeaufforderung aus: [#350071]
  32-Bit-Computer: %PROGRAMFILES%/Citrix/ICA client/wfica32 /localime:on

  64-Bit-Computer: %PROGRAMFILES(X86)%/Citrix/ICA client/wfica32 /localime:on

- Wenn Versionen von Receiver in traditionelles Chinesisch, Koreanisch oder Russisch übersetzt und mit Access Gateway Standard Edition integriert sind, wird der Receiver-Anmeldebildschirm auf Englisch angezeigt, da Access Gateway Standard Edition Sprachen nur eingeschränkt unterstützt.
- Wenn die Überprüfung von Zertifikatsperrlisten (CRL) in den Internetoptionen auf dem Benutzergerät deaktiviert ist, wird die Registrierungseinstellung CertificateRevocationCheck für Receiver überschrieben. Damit können Benutzer u. U. auf Websites zugreifen, die keine gültigen Zertifikate haben. Um dies zu umgehen, stellen Sie sicher, dass die Option für Zertifikatsperrüberprüfung unter Einstellungen > Systemsteuerung > Internetoptionen > Erweitert aktiviert ist.
- Receiver unterstützt nicht das VPN-Schlüsselwort im Access Gateway-Modus ClientChoices.
- Wenn die VPN-Verbindung Schlüsselwort von einer app entfernt wird, wenn ein Benutzer es Receiver abonniert weiterhin, versuchen Sie eine Access Gateway-Verbindung für die App. Workaround: haben der Benutzer haben und dann die app neu abonnieren. Aktion gelöscht das VPN-Schlüsselwort von Receiver. [#298387]
- Das Receiver-Symbol wird statt des App-Symbols in der Taskleiste angezeigt, wenn ein Benutzer eine App startet, die in XenApp 5.0 oder früheren Versionen veröffentlicht wurde.
- Wenn Sie mit Internet Explorer in SharePoint ein Microsoft Office-Dokument im Bearbeitungsmodus verwenden, zeigt Microsoft Office möglicherweise eine Zugriff-Verweigert-Meldung an. Lösungsansatz: Gehen Sie zu der SharePoint-Site und checken Sie das Dokument aus. Bearbeiten Sie das Dokument und checken Sie die Datei wieder in SharePoint ein. Workaround: Gehen Sie zu der SharePoint-Site und Auschecken das Dokument, bearbeiten sie Sie und die Datei wieder in SharePoint Kontrollkästchen. [#258725]

Desktopverbindungen

- Ein Verlust von Video tritt auf, wenn Dateien mit einer veröffentlichten Version von Windows Media Player über eine virtuelle Desktopsitzung wiedergegeben werden und die Anzeige des XenDesktop Viewer-Fensters von Vollbild zu Fenster gewechselt wird. Als Lösungsansatz können Sie das Media Player-Fenster minimieren und wiederherstellen und dann die App anhalten und fortsetzen (oder stoppen und neu starten).
- Sie können sich nicht ohne Fehler von virtuellen Desktops unter Windows XP 32 Bit abmelden, wenn Sie Receiver in der Desktopsitzung starten (sich jedoch nicht anmelden). Wenn das Receiver-Anmeldedialogfeld nicht ausgefüllt ist, können Sie sich nicht vom Desktop abmelden. Lösungsansatz: Füllen Sie das Anmeldedialogfeld aus oder schließen Sie es. Das Problem tritt nicht auf anderen Betriebssystemen virtueller Desktops auf.
- Beim Klicken auf das Gerätesymbol wird das Desktop Viewer-Gerätemenü nicht geschlossen. Es bleibt geöffnet, nachdem das dazugehörige Dialogfeld geschlossen wurde. Klicken Sie in diesem Fall erneut auf das Gerätesymbol.
- Windows Media Player arbeitet nicht wie erwartet, wenn er auf dem nicht primären Monitor eines Windows-Benutzergerätes mit zwei Monitoren angezeigt wird. Aufgrund eines Problems mit dem DirectX-Videowiedergabefilter VMR-9 ist der Bildschirm schwarz und es gibt keinen Ton, obwohl die Statusanzeige des Players weiter rückt. Sie beheben dieses Problem, indem Sie die Registrierung auf dem Benutzergerät bearbeiten, über das die XenDesktop-Verbindung gestartet wird. Erstellen Sie im Unterschlüssel "HKEY_CURRENT_USER\Software\Citrix" den Schlüssel "HdxMediaStream". Nennen Sie den Schlüssel "DisableVMRSupport". Legen Sie den Typ als "REG_DWORD" fest. Geben Sie dem Schlüssel den Wert "3".

Probleme mit dem Microsoft Lync 2013 VDI Plug-In

- Nach dem Wiederverbinden einer virtuellen Desktopsitzung wird das VDI-Anmeldedialogfeld nicht angezeigt und Lync in der virtuellen Umgebung ist nicht mehr mit dem Lync VDI Plug-In gepaart. Melden Sie sich von Lync ab und dann erneut an, um das Problem zu beheben.
- Wenn die virtuelle Desktopsitzung während eines Lync-Videoanrufs getrennt wird, wird der Anruf nicht von der Sitzung getrennt und das Lync-Unterhaltungsfenster reagiert nicht mehr, wenn Sie es schließen.
- Die Bewegung des Mauszeigers ist nicht im Lync-Unterhaltungsfenster eines Benutzers sichtbar, der den virtuellen Desktop freigegeben hat.
- Video wird nicht angezeigt, wenn Sie das Lync-Unterhaltungsfenster auf einen zweiten Monitor verschieben.
- Wenn Sie ein Whiteboard-Präsentationsfenster zu einem anderen Benutzer verschieben, wird das Video von dem anderen Benutzer nicht in Ihrem Unterhaltungsfenster angezeigt.
- Wenn ein Lync-Anruf gestartet wird, verringert Receiver die Lautstärke auf dem Gerät. Erhöhen Sie die Lautstärke mit den Audiosteuerelementen des Geräts.

Weitere Informationen finden Sie unter XenDesktop 7, XenApp 6.x and Citrix Receiver 4.0 Support for Microsoft Lync 2013 VDI Plug-in.

Systemanforderungen

Oct 19, 2016

Betriebssystem

In der folgenden Liste der Anforderungen werden nur Editionen oder Service Packs aufgeführt, die begrenzt unterstützt werden.

- Nur Receiver für Windows 4.1: 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 XP Professional SP3, 32-Bit-Edition und Windows XP Professional SP2, 64-Bit-Edition (einschließlich Embedded Edition)
  Der Support für Windows XP endet am 8. April 2014, wenn Microsoft den erweiterten Support für Windows XP beendet. Der Support für Windows XP Embedded wird fortgesetzt.

- Windows Vista, 32-Bit- und 64-Bit-Editionen
- Windows Thin PC
  Keine Unterstützung für das Self-Service Plug-In. Weitere Informationen finden Sie unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.

- Nur Receiver für Windows 4.1: Windows Server 2012 R2, 64-Bit-Edition
- Windows Server 2003, 64-Bit-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

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.

- XenApp (eines der folgenden Produkte):
  - 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 1 oder 2, für UNIX-Betriebssysteme
- XenDesktop (eines der folgenden Produkte):
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0

    - XenDesktop 5.6 Feature Pack 1
    - XenDesktop 5.6
    - XenDesktop 5.5
    - XenDesktop 5
    - XenDesktop 4
- Citrix VDI-in-a-Box
    - VDI-in-a-Box 5.3
    - VDI-in-a-Box 5.2
    - VDI-in-a-Box 5.1
- Citrix Receiver kann auf virtuelle Desktops und Apps mit StoreFront, App Controller und dem Webinterface zugreifen.
  StoreFront:
    - StoreFront 2.6 (empfohlen), 2.5 oder 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.

  App Controller 9.0 und 2.10:

  Bietet Zugriff auf Web- und SaaS-Apps. Bietet auch ShareFile-Kontoprovisioning und Single Sign-On. App Controller ist eine Komponente der XenMobile App Edition.

  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 Legacy-XenApp Services- oder XenDesktop Services-Sites.
- Bereitstellen von Receiver
    - Citrix Receiver für Web-Site (mit StoreFront konfiguriert)
    - Citrix Merchandising Server 2.x
    - Citrix Webinterface 5.4
    - 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)

Citrix Receiver für Windows unterstützt HTTPS- und ICA-über-SSL-Verbindungen über eine der folgenden Konfigurationen:

- LAN-Verbindungen:
    - StoreFront mit StoreFront Services- oder Receiver für Web-Sites.

Für Single Sign-On an Web- und SaaS-Apps, die über App Controller veröffentlicht werden, ist StoreFront erforderlich.

- Webinterface 5.4 für Windows mit Webinterface-Sites oder Legacy-XenApp Services- oder XenDesktop 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 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX
  - Citrix Access Gateway 5.0 (nur für die Verwendung mit Webinterface)
  - Citrix Secure Gateway 3.x (nur für die Verwendung mit Webinterface)

  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 SSL-Zertifikaten

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

Beim Sichern von Remoteverbindungen mit SSL verifiziert Receiver die Authentizität des SSL-Zertifikats des Remotegateways mit einem lokalen Speicher vertrauenswürdiger Stammzertifizierungsstellen. Receiver erkennt automatisch kommerziell ausgestellte Zertifikate (z. B. VeriSign und Thawte), wenn das Stammzertifikat für die Zertifizierungsstelle im lokalen Schlüsselspeicher vorhanden ist.

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.

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:

- Domäne (nicht für Verbindungen von NetScaler Gateway verfügbar)
- Domänen-Passthrough
  (Receiver für Web-Sites unterstützen keine Domänen-Passthrough-Authentifizierung.) Nicht für Verbindungen von NetScaler Gateway verfügbar.
- Sicherheitstoken*
- Zweifaktor (Domäne plus Sicherheitstoken)*
- SMS*
- Smartcard (erfordert StoreFront 2.1 oder 2.0)
- Benutzerzertifikat* (kann allein oder zusammen mit anderen Authentifizierungsmethoden verwendet werden)

* Nur für Receiver für Web-Sites verfügbar und für Bereitstellungen, die NetScaler Gateway mit oder ohne installiertem zugeordneten Plug-In auf dem Gerät enthalten.

Für Verbindungen mit App Controller unterstützt Receiver die folgenden Authentifizierungsmethoden:

- Domäne
- Sicherheitstoken*
- Zweifaktor (Domäne plus Sicherheitstoken)*
- SMS*

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

Für Verbindungen mit dem Webinterface 5.4 unterstützt Receiver die folgenden Authentifizierungsmethoden: (Im Webinterface wird der Begriff "explizit" für die Domänen- und Sicherheitstokenauthentifizierung verwendet.)

- Domäne
- Domänen-Passthrough (nur für Verbindungen über einen Webbrowser verfügbar)
- Sicherheitstoken*
- Zweifaktor (Domäne plus Sicherheitstoken)*
- SMS*
- Smartcard
- Benutzerzertifikat* (kann allein oder zusammen mit anderen Authentifizierungsmethoden verwendet werden)

* 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.

Upgrades werden nur für das Citrix Online Plug-in 12.x und Receiver für Windows 3.x unterstützt.

Einige Features und Funktionen von Receiver stehen nur in Verbindungen mit neueren XenDesktop- und XenApp-Versionen zur Verfügung und erfordern ggf. die aktuellen Hotfixes.

- **Kompatible Plug-Ins**
  Eine Liste der kompatiblen Plug-Ins finden Sie unter Verwalten von Citrix Receiver-Updates.

- **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 7, XenApp 6.x and Citrix Receiver 4.0 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.
    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.
  - SSL/TLS+HTTPS

- Vorherige Versionen von Presentation Server Client/Online Plug-In und die aktuelle Datei icaclient.adm: Vorherige Versionen des Presentation Server Clients und des Online Plug-ins sind nicht mit der Datei icaclient.adm für Receiver für Windows 3.4 kompatibel.

Installieren von Receiver für Windows

Dec 24, 2014

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 den StoreFront-Server oder das virtuelle App Controller-Gerät, der bzw. das 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), oder wenn Receiver Updater für Windows installiert ist.
  - Benutzer von Receiver können über die Receiver-Benutzeroberfläche automatisch nach Updates suchen.
  - 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 einrichten.
  - XenDesktop 7 (unterstützt nicht das Webinterface)
- 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.
  - Sie können Updates mit Merchandising Server oder anderen Methoden bereitstellen.
    Wenn Sie die Kontodiscovery mit der E-Mail-Adresse oder URL für das Einrichten des Kontos verwenden, können Sie Stores mit Merchandising Server Receiver hinzufügen. Stellen Sie mit Merchandising Server jedoch nicht die gleichen Stores bereit, die mit der e-mail- oder URL-basierten Kontenermittlung bereitgestellt werden.

Weitere Informationen finden Sie auch unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern, Manuelles Installieren von Deinstallieren von Receiver für Windows und Bereitstellen von Receiver mit Active Directory und Beispielstartupskripts.

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.

Hinweis: Sites, die Legacy-VDAs verwenden, müssen nicht aktualisiert werden und sollten Receiver Enterprise weiter verwenden.
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 die aktuellen Versionen von NetScaler Gateway und StoreFront konfigurieren, wie in der Dokumentation für

diese Produkte in den eDocs beschrieben. 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.
Wenn Sie auch App Controller (2.5 oder höher) verwenden, können Sie mit App Controller eine E-Mail an Receiver-Benutzer senden und die Provisioningdatei als Anlage schicken. Die Provisioningdatei enthält die Einstellungen, die Receiver für eine Verbindung mit App Controller benötigt.

- 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 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).

Für Bereitstellungen mit dem Webinterface (wird nicht für XenDesktop 7 unterstützt)

- Wenn Sie App Controller verwenden, konfigurieren Sie die Konnektoren wie unter Configuring Additional Parameters in Application Connectors in der App Controller-Dokumentation beschrieben.
- Aktualisieren Sie Ihre Webinterface-Site mit Receiver für Windows 4.0 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.

Dieser Abschnitt gilt für Updates, die von Merchandising Server erhalten wurden.

Deaktivieren Sie automatische Updates von Receiver für Desktops, die von gepoolten Maschinen bereitgestellt werden, sodass Receiver-Updates vom Masterimage gesteuert werden, mit dem die Desktops erstellt wurden.

Wenn Sie das Masterimage vorbereiten, deaktivieren Sie die automatischen Updates wie folgt:

1. Folgen Sie den Anweisungen unter To use Merchandising Server to install and set up Citrix Receiver for Windows on a shared XenDesktop image in der Merchandising Server-Dokumentation.
2. Stellen Sie den folgenden Registrierungsschlüssel auf dem Masterimage ein:
   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.
   Auf 32-Bit-Computern:

   DWORD:00000001 HKLM\SOFTWARE\Citrix\Receiver\Inventory\NoPluginUpdates

   Verwenden Sie 64-Bit-Maschinen.

   DWORD:00000001 HKLM\Software\Wow6432Node\Citrix\Receiver\Inventory\NoPluginUpdates

Manuelles Installieren und Deinstallieren von Receiver für Windows

Aug 17, 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.

Wenn Receiver mit Citrix Receiver Updater installiert wurde, können Sie Receiver mit Updater deinstallieren. Wenn Receiver nicht mit Citrix Receiver Updater installiert wurde, können Sie Receiver mit dem Windows-Hilfsprogramm "Programme und Funktionen" (Programme hinzufügen/entfernen) deinstallieren.

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

Dec 09, 2014

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.

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.

- PROPERTY=Value

Wobei PROPERTY eine der folgenden in Großbuchstaben geschriebenen Variablen (Schlüssel) ist, die mit einem Value angegeben 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 directory angeben, 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, um die Unterstützung dynamischer Clientnamen zu deaktivieren.
- ADDLOCAL=feature[,...] 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.

  Eine Liste mit Befehlszeilenparametern für das Self-Service Plug-In finden Sie unter http://support.citrix.com/article/CTX138514.

  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. Wenn das Self-Service Plug-In nicht installiert ist, müssen Benutzer auf virtuelle Desktops und Anwendungen von einer Webseite aus zugreifen.

  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.

- 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 string: 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.

  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.

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 hinzufügen: EnableFTU=0.

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

Behandlung von Installationsproblemen

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

CtxInstall-ICAWebWrapper.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"
```

Das Self-Service Plug-In erstellt eine Stubanwendung für jeden abonnierten Desktop und 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 mit Active Directory und Beispielstartskripts

May 08, 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.

Verwenden der Beispielsstartskripts auf Benutzerbasis

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 Anmeldeeigenschaften auf Dateien anzeigen, kopieren Sie das entsprechende Skript in den angezeigten Ordner und schließen Sie dann das Fenster.
5. Klicken Sie in den Anmeldeeigenschaften auf Hinzufügen und verwenden Sie Durchsuchen, um das soeben erstellte Skript zu finden.

Bereitstellen von Receiver auf Pro-Benutzer-Basis

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

Entfernen von Receiver auf Pro-Benutzer-Basis

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

Bereitstellen von Receiver über Receiver für Web

Aug 12, 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.

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 08, 2015

Mit den folgenden Konfigurationsschritten greifen Benutzer auf ihre virtuellen Desktops und Anwendungen zu:

- Konfigurieren der Anwendungsbereitstellung und der XenDesktop-Umgebung: Konfigurieren Sie NetScaler Gateway oder Access Gateway, um Remotebenutzern sicheren Zugriff auf die virtuellen Desktops und Anwendungen bereitzustellen.
- Konfigurieren von StoreFront und App Controller Erstellen Sie Stores, die Ressourcen von XenDesktop-Sites, XenApp-Farmen und App Controller auflisten und zusammenstellen, um Ressourcen den Benutzern zur Verfügung zu stellen.
- Anpassen von Receiver mit einer Gruppenrichtlinienobjektvorlage: Konfigurieren Sie Regeln für das Routing, die Proxyserver, die Remoteclientgeräte usw.
- 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.

Konfigurieren der Anwendungsbereitstellung

Nov 04, 2013

Berücksichtigen Sie die folgenden Optionen, wenn Sie Anwendungen mit XenDesktop oder XenApp bereitstellen, um die Benutzerfreundlichkeit für die Benutzer zu erhöhen, die über StoreFront-Stores auf die Anwendungen zugreifen. Weitere Informationen zur Bereitstellung von Anwendungen mit XenDesktop 7 finden Sie unter Erstellen einer Bereitstellungsgruppenanwendung in der XenDesktop 7-Dokumentation.

- Fügen Sie aussagekräftige Beschreibungen für Anwendungen in einer Bereitstellungsgruppe hinzu. Beschreibungen werden Receiver-Benutzern angezeigt.
- Fügen Sie den Beschreibungen, die Sie für Bereitstellungsgruppenanwendungen eingeben, Schlüsselwörter hinzu:
  - Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, wenn Sie die Zeichenfolge KEYWORDS:Auto der Beschreibung anhängen. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
  - Hängen Sie die Zeichenfolge KEYWORDS:Featured der Anwendungsbeschreibung an, um den Benutzern Anwendungen anzukündigen oder häufig verwendete Anwendungen in der Liste Highlights anzuzeigen.
  - 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

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

Informationen zu anderen Schlüsselwörtern finden Sie im Abschnitt "Zusätzliche Empfehlungen" unter Optimieren der Benutzererfahrung in der StoreFront-Dokumentation.

Konfigurieren der USB-Unterstützung für XenDesktop-Verbindungen

May 08, 2015

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-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

Hinweis: USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unter Konfigurieren von Bloomberg-Tastaturen. Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie unter CTX119722.
In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über XenDesktop unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre in diesem Fall nicht angebracht. Die folgenden Typen von USB-Geräten können standardmäßig nicht in einer 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.

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.

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.

Die Benutzererfahrung hängt vom Typ des Desktops ab, zu dem eine Verbindung hergestellt wird.

Über Desktop Viewer angezeigte Desktops: Wenn ein Benutzer ein USB-Gerät anschließt, wird der Benutzer in einem Dialogfeld gefragt, ob er ein Remoting des Geräts zum virtuellen Desktop wünscht. 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	Plug & Play-USB-Geräte
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Ja
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 USB-Plug & Play 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-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. Hinweis: Für manche Spezialgeräte (z. B. VOIP-Telefone) ist eine zusätzliche Konfiguration erforderlich. Weitere 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. Weitere 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. 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. Weitere 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.

Verschiedene Klassen der USB-Geräte werden von den USB-Standardrichtlinienregeln in der Grundeinstellung nicht

zugelassen.

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a): Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein Gerät möglicherweise die Verbindung zum virtuellen Desktop bereitstellt.
- HID (Human Interface Devices) (Geräteklasse 03): Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktabletts, Sensoren, Game Controller, Tasten und Steuerfunktionen.
  Die Unterklasse 01 wird "Boot Interface"-Klasse genannt und für Tastaturen und Maus verwendet.

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

- USB-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 stellen u. U. wichtigen Netzwerkzugang bereit oder schließen wichtige Peripheriegeräte an, z. B. Bluetooth-Tastaturen oder -Mäuse.
  Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

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-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.

Verhindern des Abblendens des Desktop Viewer-Fensters

Mar 30, 2011

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 Benutzern normalerweise die Richtlinieneinstellungen mit der Gruppenrichtlinie steuern. Vor der Verwendung dieser Registrierungsschlüssel sollten Sie beim XenDesktop-Administrator nachfragen, ob eine Richtlinie für dieses Feature festgelegt wurde.
2. Stellen Sie den Eintrag auf einen Wert ungleich Null ein, z. B. 1 oder true.

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

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

Konfigurieren von Einstellungen für mehrere Benutzer und Geräte

Jan 23, 2012

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 und App Controller

Nov 04, 2013

Citrix StoreFront authentifiziert Benutzer an XenDesktop, XenApp, App Controller 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.
2. Konfigurieren Sie Stores für App Controller genauso wie für Anwendungen, die von XenDesktop oder XenApp bereitgestellt werden. Für Receiver ist keine spezielle Konfiguration erforderlich. Weitere Informationen finden Sie unter Konfigurieren von Stores in der StoreFront-Dokumentation.

App Controller, eine Komponente der XenMobile App Edition, stellt Enterprise-Web- und -SaaS-Anwendungen, native iOS-Anwendungen und integrierte ShareFile-basierte Daten den Receiver-Benutzern sicher bereit.

Wenn Sie die e-mail-basierte Kontenermittlung verwenden, ermittelt Receiver den App Controller, der einer E-Mail-Adresse des Benutzers zugeordnet ist.

Wenn Sie die e-mail-basierte Kontenermittlung nicht verwenden, stellen Sie Benutzern eine Provisioningdatei bereit, die Receiver mit den Verbindungseinstellungen für App Controller konfiguriert. Von der App Controller-Konsole können Sie eine Provisioningdatei (.cr) per E-Mail an Benutzer senden. Weitere Informationen finden Sie unter Connection Users to Citrix Receiver in der App Controller-Dokumentation.

Sie können auch eine Receiver für Web-Site konfigurieren. Benutzer erhalten dann eine Receiver-Provisioningdatei von dieser Site, wenn sie in Receiver auf Aktivieren klicken.

Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage

Jun 19, 2013

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.

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.

Bereitstellen der Kontoinformationen für Benutzer

Dec 03, 2013

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 oder das virtuelle App Controller-Gerät, der bzw. das 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 und App Controller stellen Provisioningdateien bereit, die Benutzer für eine Verbindung mit Stores und App Controller 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.

- App Controller kann Receiver-Benutzern eine E-Mail senden, der die Provisioningdatei angehängt ist. Die Provisioningdatei enthält die Einstellungen, die Receiver für eine Verbindung mit App Controller benötigt. Weitere Informationen finden Sie unter Downloading the Receiver Configuration File in der App Controller-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 oder App Controller teilen Sie den Benutzern die URL für den Server mit. Beispiel: https://servername.company.com

Für Legacybereitstellungen 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

Apr 30, 2013

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

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

May 17, 2013

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.

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

May 08, 2015

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:
Bei einer	Bei einer
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:
Bei einer	Bei einer
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 aufeinanderfolgende 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 den eDocs.

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 in der XenDesktop- oder XenApp-Dokumentation in den eDocs.

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 einer Eingabeaufforderung net use comx: \\client\com: ein
   Wobei x der Name des Client-COM-Ports ist, 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 01, 2013

Sie können die Benutzererfahrung mit den folgenden Features verbessern.

- Clientseitige Mikrofoneingabe
- Multimonitorunterstützung
- Überschreibung von Druckereinstellungen auf Geräten
- Tastenkombinationen
- Receiver-Unterstützung für Symbole in 32-Bit-Farben
- Bereitstellen von virtuellen Desktops für Receiver-Benutzer
- Tastatureingabe in Desktop Viewer-Sitzungen
- Verbinden mit virtuellen Desktops

Clientseitige Mikrofoneingabe

May 01, 2013

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.

Multimonitorunterstützung

Jun 19, 2013

Sie können maximal acht Monitore mit Receiver verwenden.

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

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

- Vollbildmodus: Mehrere Monitore werden in der Sitzung angezeigt; Anwendungen werden genauso wie beim lokalen Desktop an Monitore angedockt.
  XenDesktop: Sie können das Desktop Viewer-Fenster über jede rechteckige Untergruppe von Monitoren anzeigen, wenn Sie die Größe des Fensters über einen Monitorbereich ändern und auf 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.

Überschreibung von Druckereinstellungen auf Geräten

May 01, 2013

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.

Tastenkombinationen

Dec 03, 2012

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-Unterstützung für Symbole in 32-Bit-Farben

May 08, 2013

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.

Bereitstellen von virtuellen Desktops für Receiver-Benutzer

Oct 18, 2013

Jedes Unternehmen hat andere Ausgangsanforderungen und außerdem können sich die Unternehmenswünsche und -anforderungen an den Benutzerzugriff auf virtuelle Desktops 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. Für den benutzerseitigen Zugriff auf virtuelle Desktops stehen zwei Optionen zu Verfügung: Desktop Viewer oder Citrix Desktop Lock.

Verwenden Sie Desktop Viewer, wenn die Benutzer mit dem lokalen und dem virtuellen Desktop arbeiten. 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.
Weitere Informationen zu Desktop Lock, das nur für CitrixReceiverEnterprise.exe unterstützt wird, finden Sie in der XenDesktop 7-Dokumentation in den eDocs.

Tastatureingabe in Desktop Viewer-Sitzungen

Jul 25, 2013

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

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

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

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

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

Hinweis: Wenn Desktop Viewer maximiert ist, können Sie mit Alt+Tab standardmäßig zwischen Fenstern in der Sitzung wechseln. Wenn Desktop Viewer in einem Fenster angezeigt wird, wechseln Sie mit Alt+Tab zwischen Fenstern außerhalb der Sitzung.
Citrix hat bestimmte Tastenkombinationen entwickelt. Beispiel: Mit Strg+F1 reproduzieren Sie Strg+Alt+Entf und mit Umschalt+F2 wechseln Sie Anwendungen vom Vollbild- in den Fenstermodus und umgekehrt. Sie können Tastenkombinationen nicht mit virtuellen Desktops verwenden, die in Desktop Viewer angezeigt werden (d. h. mit XenDesktop-Sitzungen). Sie können sie aber mit veröffentlichten Anwendungen verwenden (d. h. mit XenApp-Sitzungen).

Verbinden mit virtuellen Desktops

Oct 12, 2012

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 der Smartcardauthentifizierung

Oct 30, 2013

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). StoreFront und NetScaler Gateway müssen für die bimodale Authentifizierung konfiguriert werden.
- **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 Awendungen 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.

- Receiver für Windows speichert nicht die PIN des Benutzers oder die Zertifikatauswahl.
- 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 direkte Smartcard-Authentifizierung an App Controller wird nicht unterstützt. Sie können App Controller jedoch hinter StoreFront bereitstellen und den Zertifikatauthentifizierungsdienst von StoreFront verwenden. Web-Apps, die eine Clientzertifikatauthentifizierung verwenden, benötigen getrennte Smartcardaufforderungen, damit der Browser eine eigene SSL-Verbindung herstellt.
- 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\

Konfigurieren von StoreFront

- In der Datei default.ica, die sich auf dem StoreFront-Server befindet, legen Sie Set DisableCtrlAltDel auf false fest.
- Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie das Kontrollkästchen Domänen-Passthrough und lassen Sie das Kontrollkästchen Smartcard deaktiviert.
  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 SSL-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

May 08, 2015

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 SSL/TLS-Verbindungen 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.

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

May 08, 2015

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

Nov 20, 2013

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

- In der Datei default.ica, die sich auf dem StoreFront-Server befindet, legen Sie Set DisableCtrlAltDel auf false fest.
- 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.

Sichern der Receiver-Kommunikation

May 01, 2013

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, HTTPS-Proxyserver oder SSL-Tunneling-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: SSL-Relay-Lösungen mit SSL- (Secure Sockets Layer) und TLS-Protokollen (Transport Layer Security).

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

Jun 01, 2013

Konfigurieren Sie NetScaler Gateway für StoreFront und App Controller (eine Komponente der XenMobile App Edition), damit Remotebenutzer eine Verbindung über NetScaler Gateway herstellen können.

- 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.
- App Controller-Bereitstellungen: Lassen Sie Verbindungen von Remotebenutzern mit AppController zu, indem Sie NetScaler 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 NetScaler Gateway Plug-In her.

Weitere Informationen zur Konfiguration dieser Verbindungen finden Sie unter Integrating NetScaler Gateway with XenMobile App Edition und anderen Abschnitten unter dem Knoten in den Citrix eDocs. 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 den eDocs beschrieben.

Verbinden mit Access Gateway Enterprise Edition

May 01, 2013

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 den Citrix eDocs. 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 den Citrix eDocs 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

May 03, 2013

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 SSL), 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.)

Wenn Sie die Verbindung über SSL herstellen, müssen Sie den Servernamen im Format https://CN hinzufügen, wobei CN der allgemeine Name (Common Name) ist, der im SSL-Zertifikat angegeben wird. Wählen Sie sonst das Format, das Receiver für die Verbindung verwendet. Wenn Receiver eine Verbindung über eine IP-Adresse herstellt, geben Sie also beispielsweise die IP-Adresse des Servers an.

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

May 08, 2015

Dieser Abschnitt gilt nicht für XenDesktop 7.

Sie können Receiver in eine Umgebung mit dem SSL (Secure Sockets Layer)-Relay integrieren. Receiver unterstützt sowohl das SSL- als auch das TLS-Protokoll.

- SSL bietet starke Verschlüsselung, um die Sicherheit der ICA-Verbindungen zu erhöhen, und zertifikatbasierte Serverauthentifizierung, um die Identität des Servers zu gewährleisten, zu dem Sie eine Verbindung herstellen.
- 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. Da nur geringe technische Unterschiede zwischen SSL Version 3.0 und TLS Version 1.0 bestehen, können die für SSL in der Softwareinstallation verwendeten Zertifikate auch für TLS verwendet werden. 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 SSL/TLS-gesicherte Kommunikation. Wenn das SSL-Relay eine SSL-Verbindung empfängt, werden die Daten entschlüsselt und dann an den Server übergeben. Wenn der Benutzer SSL+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 SSL/TLS-fähigen Client und einem Server. Verbindungen, bei denen SSL/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 zur Konfiguration von SSL-Relay, um die Installation zu sichern, finden Sie unter Konfigurieren von SSL/TLS zwischen Servern und Clients 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 SSL und TLS

May 08, 2015

Dieser Abschnitt gilt nicht für XenDesktop 7.

SSL und TLS werden auf gleiche Art und Weise konfiguriert, verwenden dieselben Zertifikate und sind gleichzeitig aktiviert.

Wenn Sie SSL und TLS aktivieren, versucht Receiver beim Herstellen einer Verbindung zuerst TLS und dann SSL zu verwenden. Wenn die Verbindung mit SSL fehlschlägt, wird eine Fehlermeldung angezeigt.

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 SSL/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 SSL/TLS zwischen SSL/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 SSL/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.
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 "SSL/TLS Version" auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, stellt Receiver eine Verbindung mit TLS-Verschlüsselung her. Wenn eine Verbindung mit TLS fehlschlägt, stellt Receiver eine Verbindung mit SSL 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 SSL/TLS Version auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, versucht Receiver eine Verbindung mit TLS-Verschlüsselung herzustellen. Wenn eine Verbindung mit TLS fehlschlägt, versucht Receiver eine Verbindung mit SSL 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 SSL/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 SSL/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 SSL/TLS finden Sie in der Webinterface-Dokumentation.

Sie können Receiver konfigurieren, sodass SSL/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.

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 SSL/TLS im Browser des Benutzergeräts. Weitere Informationen finden Sie in der Onlinehilfe des Browsers.

Installieren von Stammzertifikaten auf Benutzergeräten

Oct 12, 2012

Für das Sichern der Kommunikation mit SSL/TLS zwischen SSL/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.

Konfigurieren des Webinterface für die Verwendung von SSL/TLS für Receiver

Feb 22, 2012

1. Wenn Sie die Anwendungsauflistung und die Startdaten, die zwischen Receiver und dem Webinterface-Server übergeben werden, mit SSL/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.

Konfigurieren der TLS-Unterstützung

Dec 03, 2012

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 "SSL/TLS Version" auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, stellt Receiver eine Verbindung mit TLS-Verschlüsselung her. Wenn eine Verbindung mit TLS fehlschlägt, stellt Receiver eine Verbindung mit SSL 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.

Erfüllen der FIPS 140-Sicherheitsanforderungen beim Webinterface mit der Gruppenrichtlinienvorlage

Dec 03, 2012

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 SSL/TLS Version auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, versucht Receiver eine Verbindung mit TLS-Verschlüsselung herzustellen. Wenn eine Verbindung mit TLS fehlschlägt, versucht Receiver eine Verbindung mit SSL herzustellen.
   - Setzen Sie SSLciphersuite auf Government.
   - Setzen Sie CRL verification auf Require CRLs for connection.

Konfigurieren des Webinterface zum Verwenden von SSL/TLS für die Kommunikation mit Citrix Receiver

Mar 18, 2011

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 SSL/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.

Konfigurieren von Citrix XenApp für die Verwendung von SSL/TLS für die Kommunikation mit Citrix Receiver

Mar 18, 2011

Sie können den XenApp-Server so konfigurieren, dass SSL/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 SSL/TLS finden Sie in der Webinterface-Dokumentation.

Konfigurieren von Citrix Receiver für die Verwendung von SSL/TLS für die Kommunikation mit dem Webinterface-Server

May 02, 2013

Sie können Receiver konfigurieren, sodass SSL/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 SSL/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 08, 2015

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface und Verwendung von veralteten 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	Nur richtig signierte Anwendungs- oder Desktopstarts von einem vertrauenswürdigen Server sind

Option	Beschreibung
Starts zulassen (sicherer)	zulässig. Dem Benutzer wird eine Sicherheitswarnung im Receiver angezeigt, wenn eine gestartete Anwendung oder ein Desktop eine ungültige Signatur haben. Der Benutzer kann nicht weiterarbeiten, und der nicht autorisierte Start wird blockiert.
Benutzer bei nicht signierten Starts auffordern (weniger sicher)	Bei jedem versuchten Start einer nicht signierten oder falsch signierten Anwendung oder eines Desktops wird dem Benutzer eine Aufforderung angezeigt. Der Benutzer kann den Anwendungsstart fortsetzen oder ihn abbrechen (Standardeinstellung).

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

Sep 16, 2013

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.

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.

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
PdaSecurityPermission	PDA-Geräte
ScannerAndDigitalCameraSecurityPermission	USB- und andere Geräte

Wert	Beschreibung
0	Kein Zugriff
1	Lesezugriff
2	Vollzugriff
3	Benutzer bei Zugriff fragen