Citrix Receiver für Windows 4.4 (LTSR)

Sichere Kommunikation

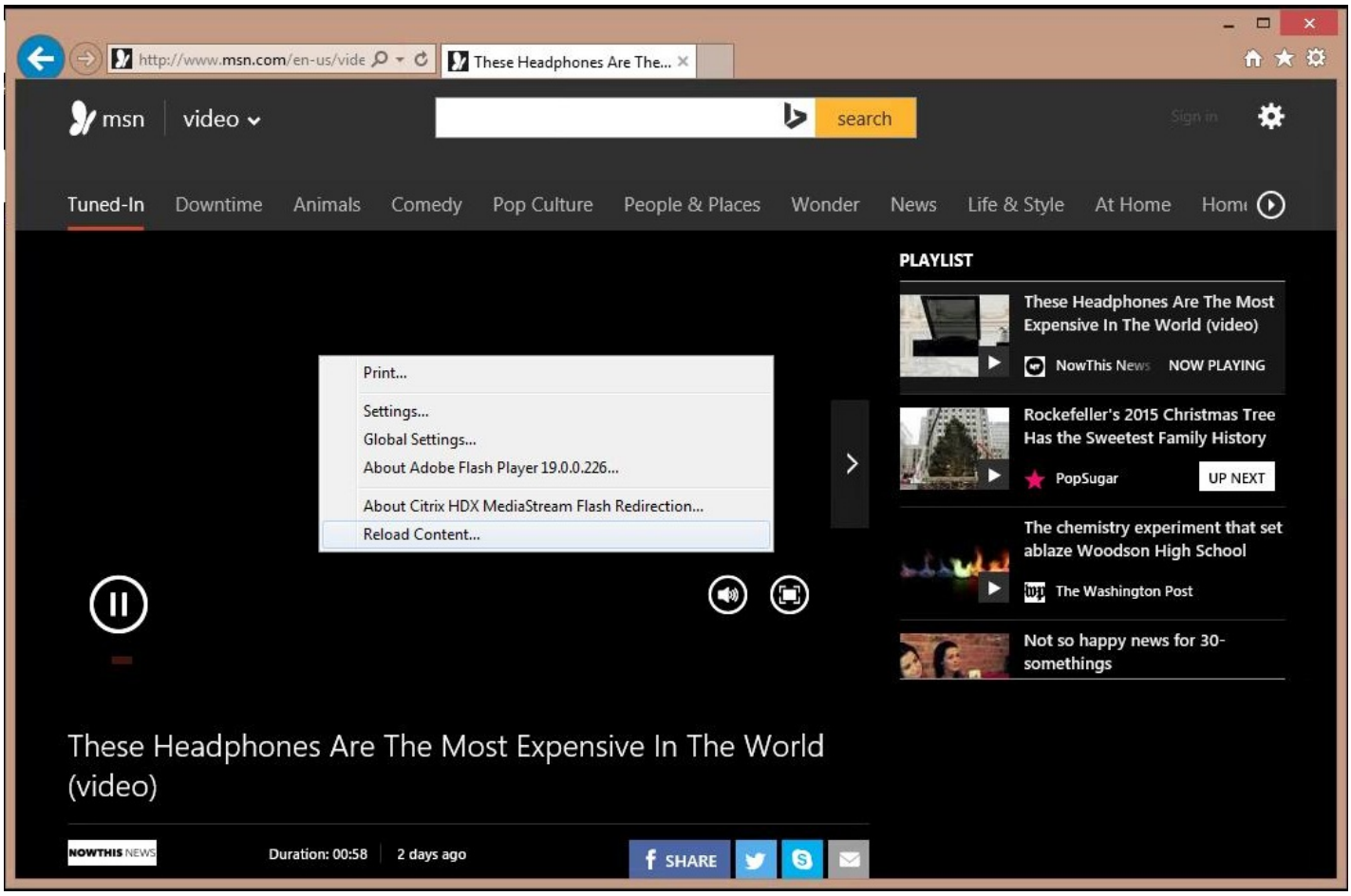
Receiver Desktop Lock

SDK und API für Citrix Receiver für Windows

Info zu diesem Release

Neue Funktionen in diesem Release

Hinweis



-
-

Behobene Probleme in diesem Release

Behobene Probleme

Receiver für Windows 4.4 CU5 (4.4.5000)

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
  -
  -
-

-
-
-
-
-
-
-
-
-
-

-
-

Receiver für Windows 4.4 CU4 (4.4.4000)

-
-
  -
  -

-
  -
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-

Receiver für Windows 4.4 CU3 (4.4.3000)

-
-
-
-

-
-
-

Receiver für Windows 4.4 CU2 (4.4.2000)

-
-

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-
-
-
-

Receiver für Windows 4.4 CU1 (4.4.1000)

-
-

-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-

-

Receiver für Windows 4.4

-
-
-
-
  -

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
  -
  -

-
-
-
-
-
-
-
-
-
  -
  -

-
-
-
-
-
-

-
-
-
-
-

Bekannte Probleme

Bekannte Probleme in Citrix Receiver für Windows 4.4 CU5 (4.4.5000)

Bekannte Probleme in Citrix Receiver für Windows 4.4 CU4 (4.4.4000)

Bekannte Probleme in Citrix Receiver für Windows 4.4 CU3 (4.4.3000)

-

Bekannte Probleme in Citrix Receiver für Windows 4.4 CU2 (4.4.2000)

-

Bekannte Probleme in Citrix Receiver für Windows 4.4 CU1 (4.4.1000)

-

Bekannte Probleme in Citrix Receiver für Windows 4.4

-

> Warnung

-

> Hinweis

-

-

-
-
-
-
-
  -
  -
-
-
-
-

-
-
-
-
-
-
-

Systemanforderungen und Kompatibilität

Gerät

Betriebssystem

Hardware:

-
-
-

-

Touchfähige Geräte

Citrix Server

-
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
-
  -
  -
-
  -
  -
-
  -
  -
-
  -
  -
  -
  -
  -

Browser

-
-
-

> Hinweis

Konnektivität

-
  -
  -
-
  -
  -

> Hinweis

Info zu sicheren Verbindungen und Zertifikaten

> Hinweis

Private (selbstsignierte) Zertifikate

> Hinweis

Installieren von Stammzertifikaten auf Benutzergeräten

Zertifikate mit Platzhalterzeichen

Zwischenzertifikate und NetScaler Gateway

Authentifizierung

Hinweis

Upgrades

Hinweis

Andere Version

-
  -
  -
  -
-
-
  -
  -

Important

Warnung

Installieren

-
  -
  -
  -
-
  -
  -
-
  -

HDX RealTime Media Engine (RTME)

> Hinweis

-
-
-
-

> Important

Manuelles Upgrade auf Citrix Receiver für Windows

-
-
-
-

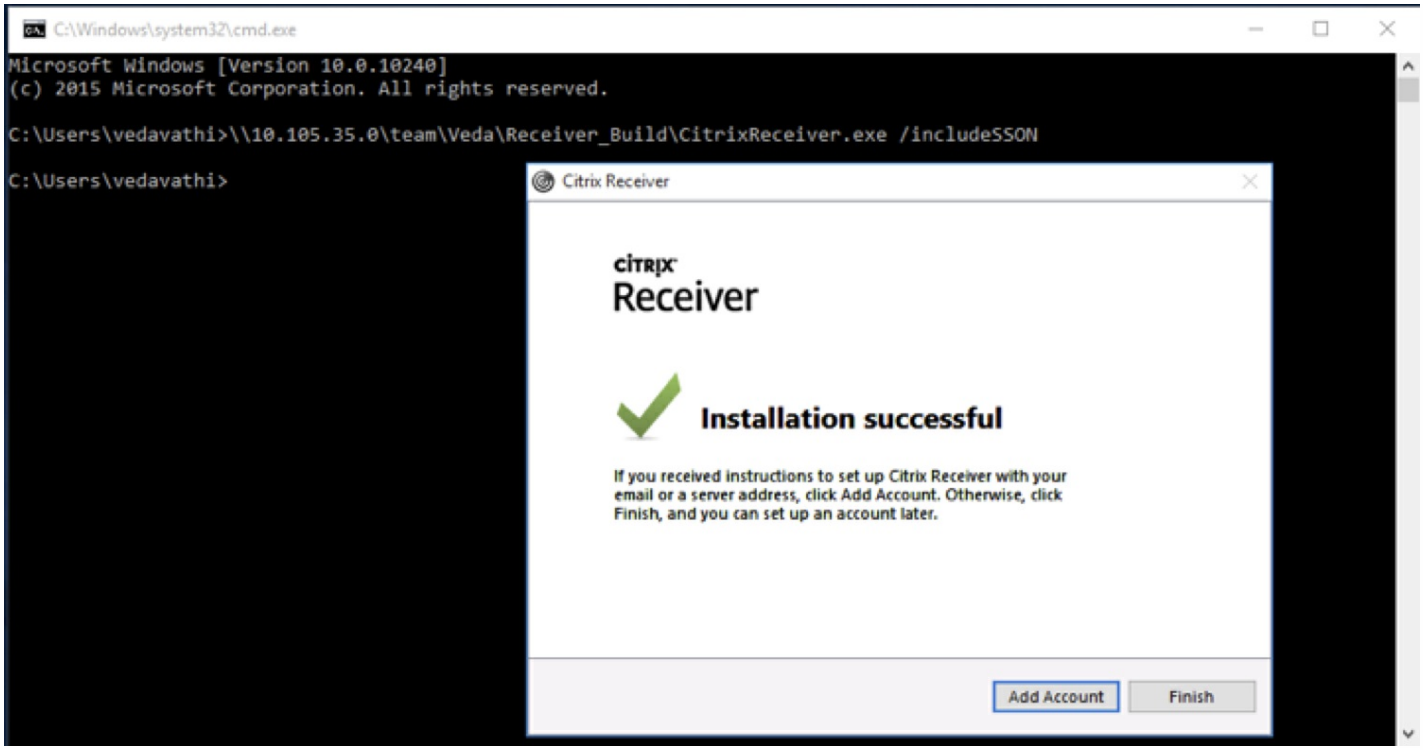
Überlegungen zum Upgrade

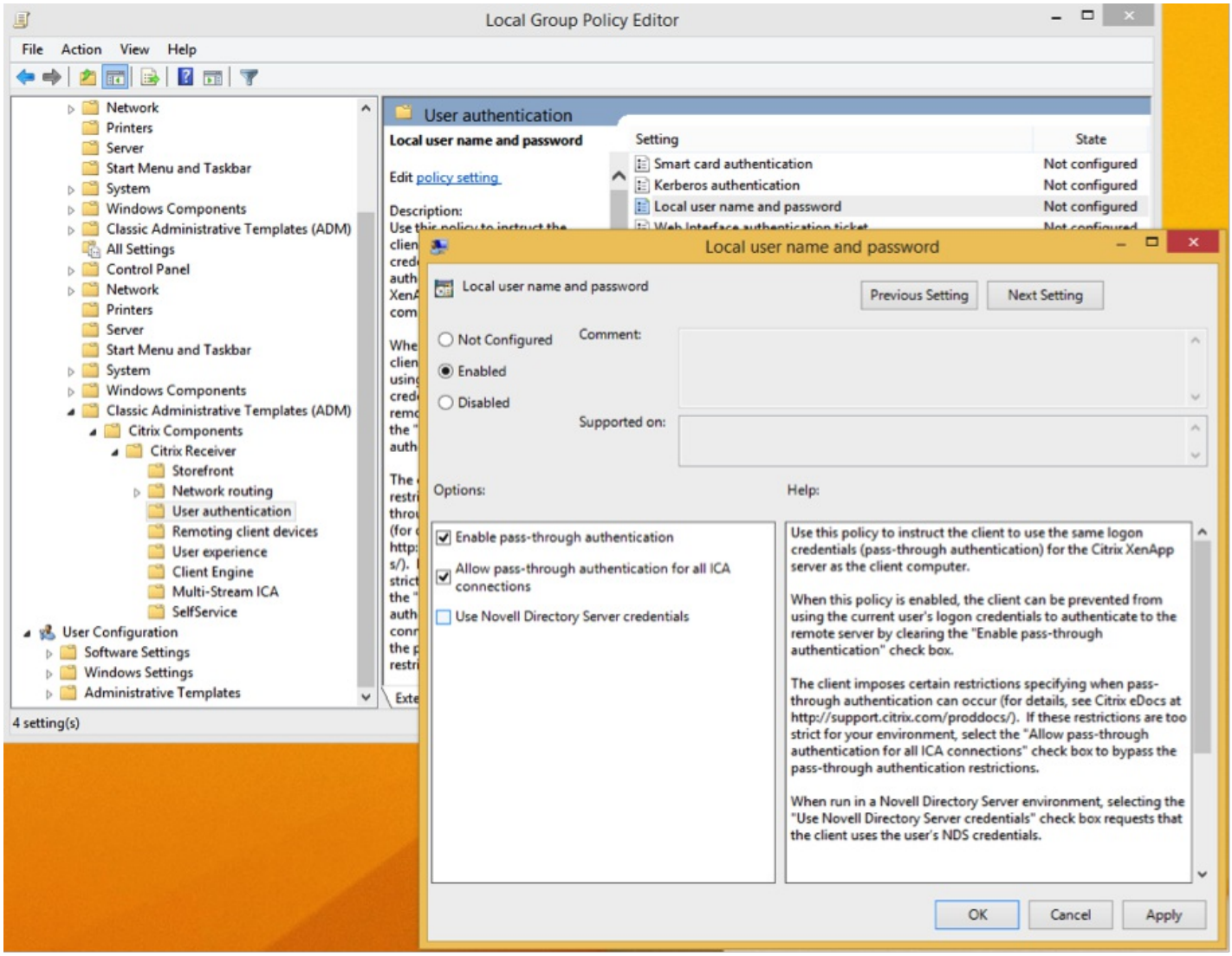
> Tipp

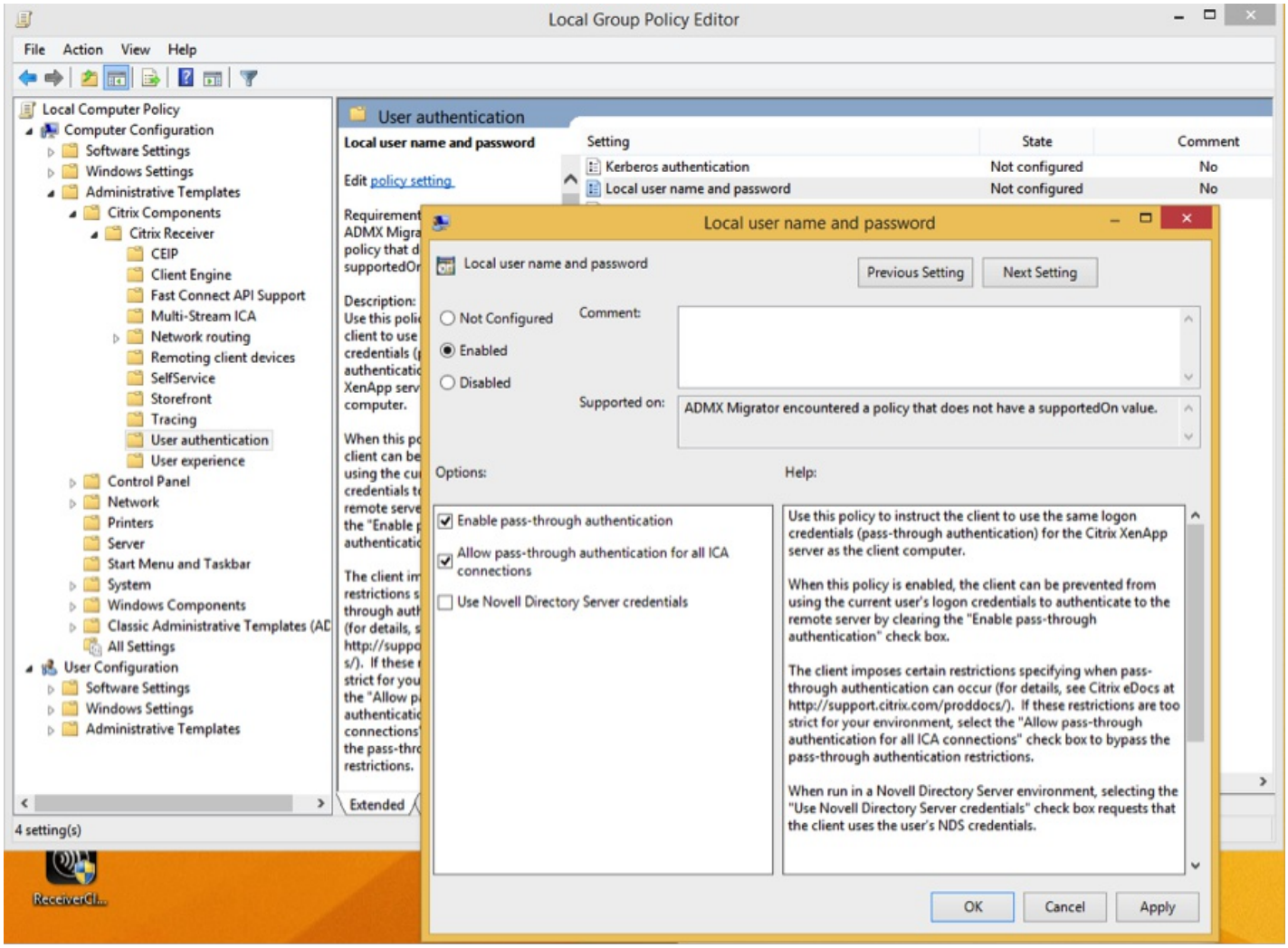
Manuelles Installieren und Deinstallieren von Receiver für Windows

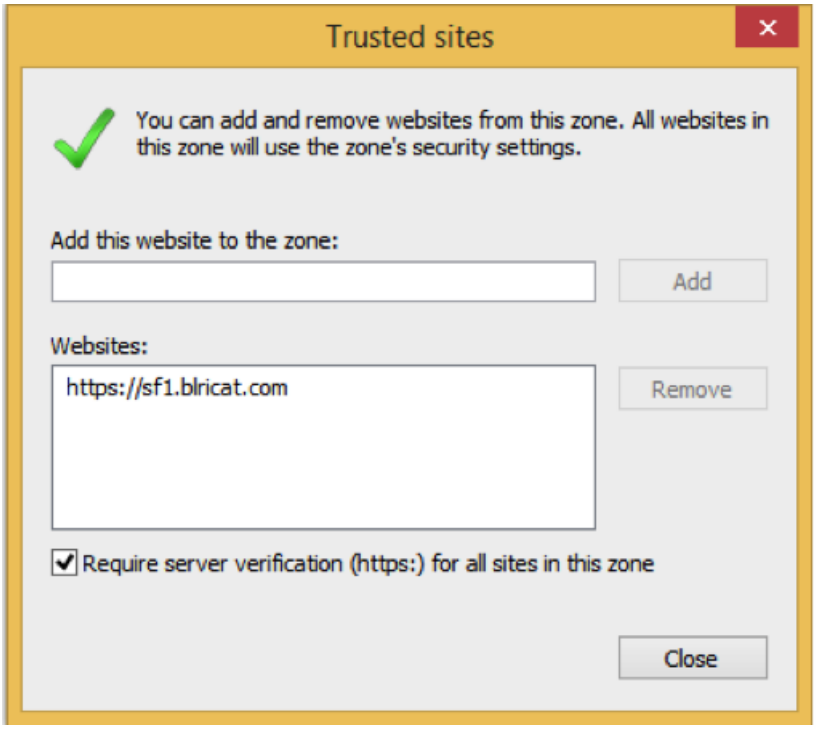
Important

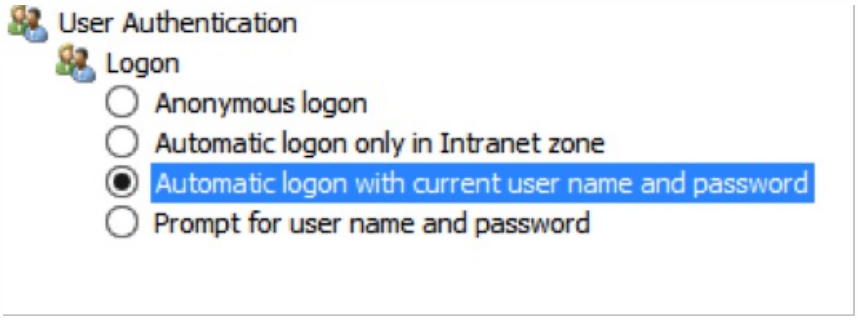
-
-
  -
  -
-











Entfernen von Receiver für Windows

Warnung

Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern

> Warnung

Anzeigen der Verwendungsinformationen

Unterdrücken eines Neustarts bei der Installation der Benutzeroberfläche

Automatische Installation

Aktivieren von Single Sign-On bei der Authentifizierung

Aktiviert Single Sign-On, wenn /includeSSON angegeben ist.

Always-On-Ablaufverfolgung

Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Angeben des Installationsverzeichnisses

Angeben eines Benutzergerätes für eine Serverfarm

Dynamischer Clientname

Installieren bestimmter Komponenten

	• • • • • • • • • • • •

Konfigurieren von Stores, die nicht mit Merchandising Server-Bereitstellungen konfiguriert sind

	• • •

Lokales Speichern von Anmeldeinformationen für Stores mit dem PNAgent-Protokoll

	• • • • • • •

Zertifikat auswählen

Verwalten von Smartcard-PIN-Eingaben mit CSP-Komponenten

Verwenden von Kerberos

Anzeigen von Legacy-FTA-Symbolen

Aktivieren des Vorabstarts

Angeben des Verzeichnisses für Startmenüverknüpfungen

	• •

Angeben des Storenamens

	• • • • • •

Aktivieren der URL-Umleitung auf Benutzergeräten

Aktivieren des Self-Service-Modus

Angeben des Verzeichnisses für Desktopverknüpfungen

Upgrade von einer nicht unterstützten Citrix Receiver-Version

Anzeigen eines Dialogfelds "Installation abgeschlossen" während unbeaufsichtigter Installationen

Hinweis

Problembehebung bei der Installation

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"

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

Starten eines virtuellen Desktops oder einer virtuellen Anwendung über eine Befehlszeile

Bereitstellen von Receiver für Windows mit Active Directory und Beispielstartskripts

-
-

Bearbeiten von Beispielskripts

-

```
set DesiredVersion= 3.3.0.XXXX
```

-
-
-

Hinzufügen von Pro-Computer-Startskripts

Bereitstellen von Receiver auf Pro-Computer-Basis

Entfernen von Receiver auf Pro-Computer-Basis

Verwenden der Beispielsstartskripts auf Benutzerbasis

-
-

Einrichten von Pro-Benutzer-Startskripten

Bereitstellen von Receiver auf Pro-Benutzer-Basis

Entfernen von Receiver auf Pro-Benutzer-Basis

Bereitstellen von Receiver für Windows über Receiver für Web

Bereitstellen von Citrix Receiver für Windows über einen Webinterface-Anmeldebildschirm

Konfigurieren von Citrix Receiver für Windows

-
-
-
  -
  -
  -
-
-

-
-

> **Hinweis**
>
> Beim Starten einer Sitzung im Self-Service-Modus ist das automatische Verbinden standardmäßig aktiviert.

Konfigurieren der Anwendungsbereitstellung

-
-
-

Konfigurieren des Self-Service-Modus

-
-

-

Konfigurieren von Speicherorten für App-Verknüpfungen

SelfServiceMode true
SelfServiceMode false

- SelfServiceMode false
-
-
-
- UseCategoryAsStartMenuPath
- [/DESKTOPDIR="Dir_name"]
CategoryPath
- AutoReInstallModifiedApps

Konfigurieren von Speicherorten für App-Verknüpfungen mit Gruppenrichtlinienobjektvorlagen

-
-
-
-
-
-
-

Konfigurieren von Speicherorten für App-Verknüpfungen mit Registrierungsschlüsseln

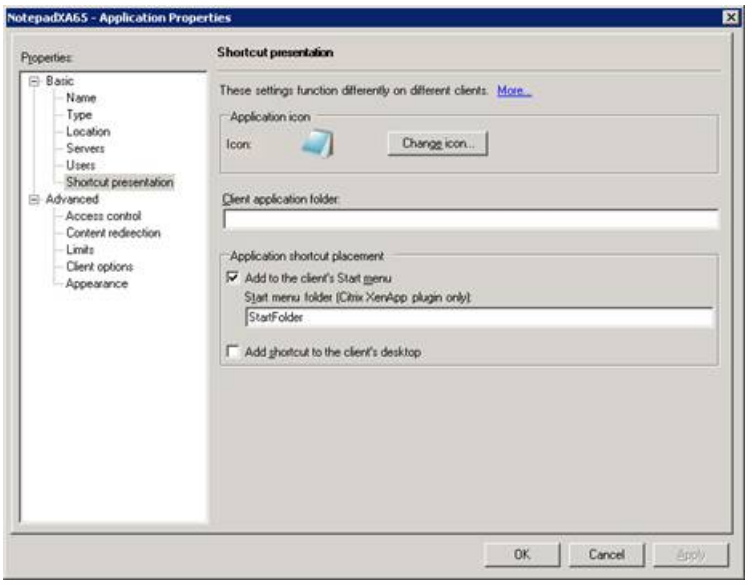
> Hinweis

Konfigurieren von Speicherorten für App-Verknüpfungen mit StoreFront-Kontoeinstellungen

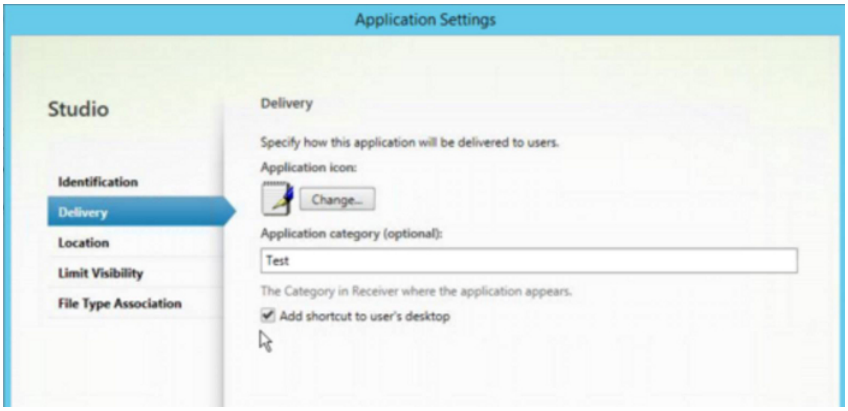
-
-
-

-
-
-
-
-

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



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



Reduzieren von Enumerationsverzögerungen oder digitales Signieren von Anwendungsstubs

Anwendungsfälle

-

- - -

-

-

Konfigurieren der XenDesktop-Umgebung

Konfigurieren der USB-Unterstützung für XenDesktop- und XenApp-Verbindungen

Funktionsweise der USB-Unterstützung

Massenspeichergeräte

In der Standardeinstellung zulässige USB-Geräteklassen

-
-
-
-
    -
    -
    -
    -
    -
    -
-
-

-
-

In der Standardeinstellung nicht zugelassene USB-Geräteklassen

-
-

-
-
-

Aktualisieren der für Remoting verfügbaren USB-Geräteliste

Konfigurieren von Bloomberg-Tastaturen

-
-

Verhindern des Abblendens des Desktop Viewer-Fensters

-
-

-
-

Konfigurieren von Einstellungen für mehrere Benutzer und Geräte

-

-
-

Konfigurieren von StoreFront

Hinweis

Konfigurieren von StoreFront

Wiederverbindung über Workspace Control verwalten

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

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

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

WSCReconnectMode-Schlüsseleinstellungen für Windows Receiver:

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

Deaktivieren von Workspace Control für Windows Receiver

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

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

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectModeUser**

Typ: REG_SZ

Wert: 0

Ändern Sie den folgenden Schlüssel vom Standardwert 3 auf 0

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

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectMode**

Typ: REG_SZ

Wert: 0

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

Ändern des Timeouts der Statusanzeige

Warnung

Konfigurieren von Receiver mit der Gruppenrichtlinienobjektvorlage

Hinweis

Hinweis

Hinweis

> Hinweis

Info zu TLS und Gruppenrichtlinien

-
-
-
-

> Tipp

-
-
-
-

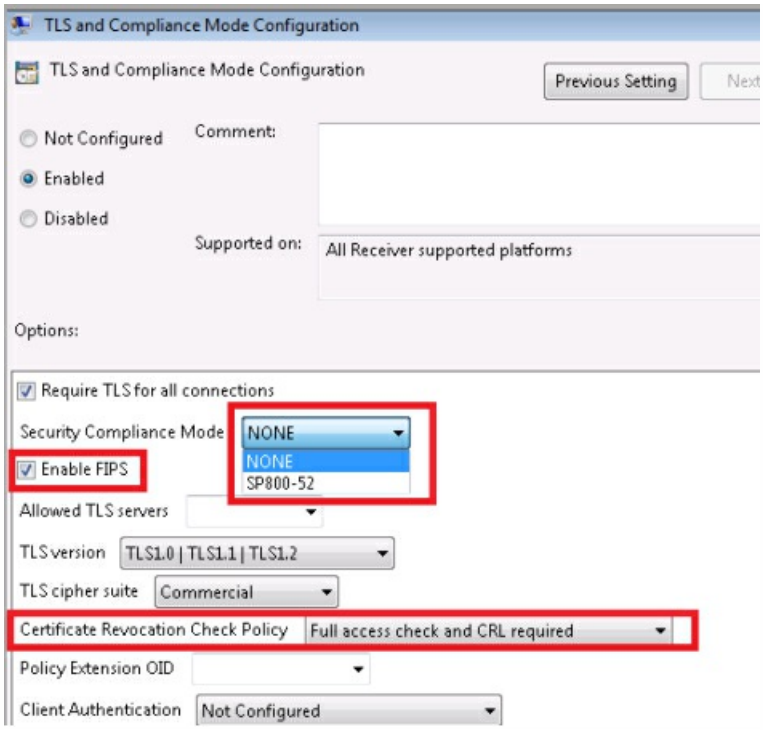
-
-
-

-
-
-
-

Einhaltung der FIPS-Sicherheitsstandards

> Hinweis

-
-
-



Hinweis

Konfigurieren von FIPS

-
-

-
-
-

Info zur ADMX-Vorlage

Hinweis

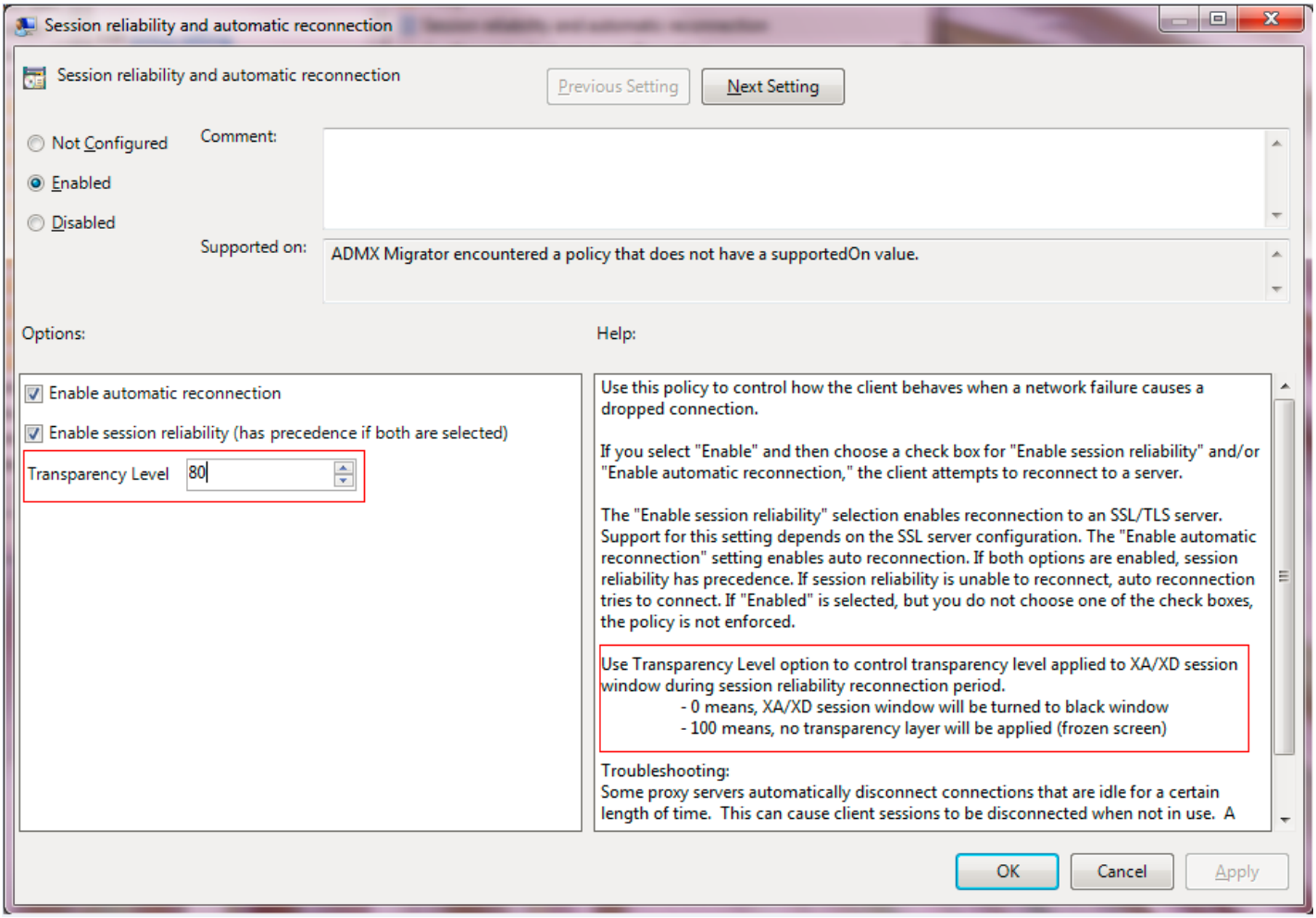
ADMX- und ADML-Dateinamen und Speicherorte

Hinweis

Hinweis

Gruppenrichtlinie für Sitzungszuverlässigkeit

Hinweis



Bereitstellen der Kontoinformationen für Benutzer

-
-
-

> Important

Konfigurieren der e-mail-basierten Kontenermittlung

> Hinweis

Bereitstellen von Provisioningdateien für Benutzer

-

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

-
-
  -
  -

Automatisches Freigeben von mehreren Store-Konten

> Warnung

Optimieren der Citrix Receiver-Umgebung

Verkürzen des Anwendungsstarts

-
-

-
-

HKLM-Registrierungswerte

HKCU-Registrierungswerte

Zuweisen von Clientgeräten

-
-
-

Deaktivieren von Benutzergerätzuordnungen

Umleiten von Clientordnern

Zuordnen von Clientlaufwerken zu serverseitigen Laufwerksbuchstaben

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

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

Jan 06, 2016

Sie können die Benutzererfahrung mit den folgenden Features verbessern.

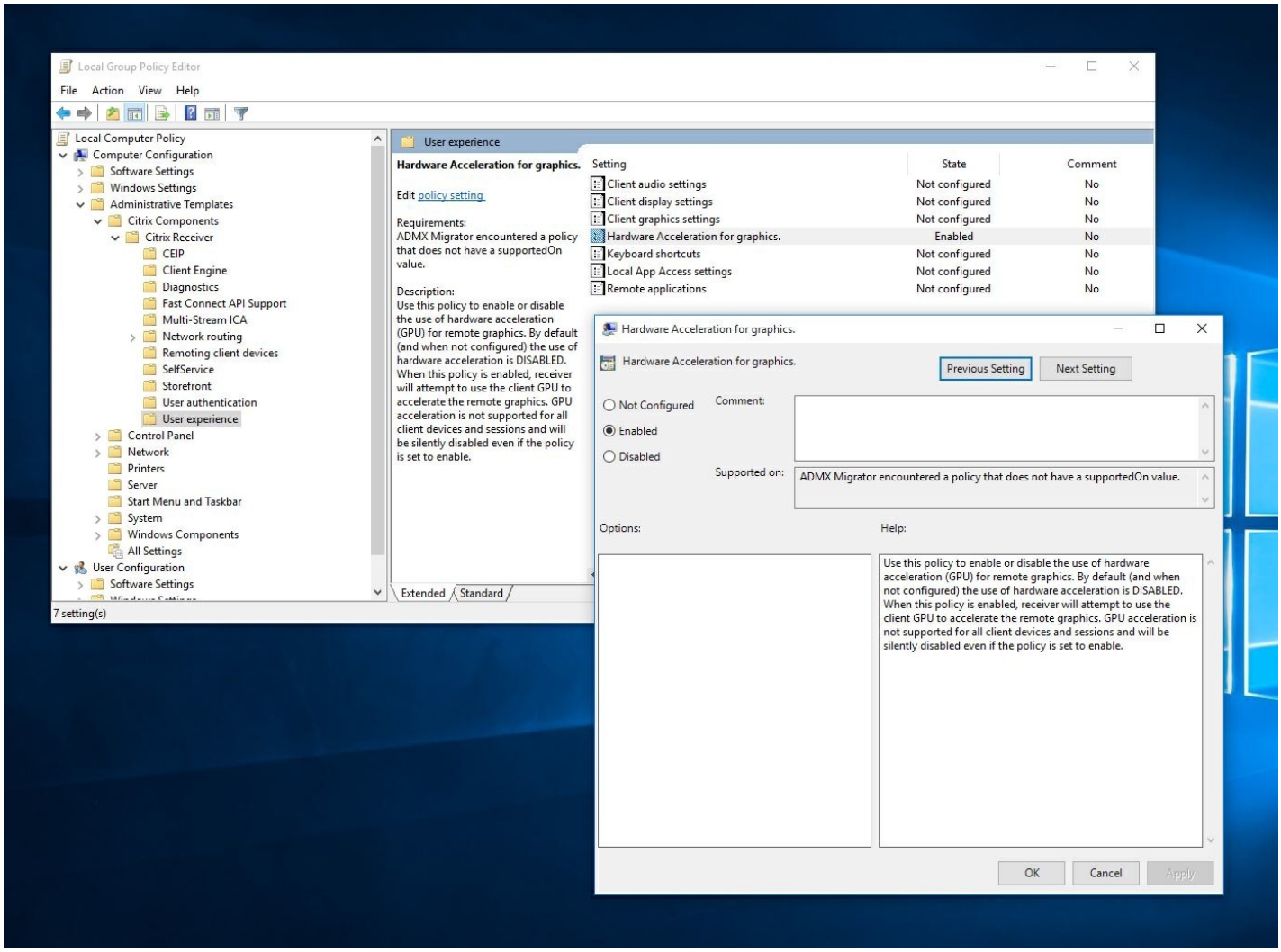
Wenn Sie Citrix Receiver für Windows Version 4.4 (mit HDX Engine 14.4) verwenden, kann die GPU für H.264-Decodierung verwendet werden, wenn sie auf dem Client verfügbar ist. Die für GPU-Decodierung verwendete API-Ebene ist DXVA (DirectX Video Acceleration).

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

> ## Hinweis
>
> Standardmäßig ist das Feature für die Hardwaredecodierung deaktiviert. Es kann über clientseitige Richtlinien aktiviert werden.

Aktivieren der Hardwaredecodierung:

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



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

Registrierungspfad: HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\

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

Wenn Sie das Hardwaredecodierungsfeature verwenden, berücksichtigen Sie folgende Einschränkungen:

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

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.

Aktualisiert: 28.11.2014

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.

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

Überschreiben der Druckereinstellungen auf dem Benutzergerät

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

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

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

Bei einem konvertierbaren Gerät (Tablet mit abnehmbarer Tastatur) kann die Anzeige der Bildschirmtastatur unterdrückt werden, indem Sie einen REG_DWORD-Wert unter DisableKeyboardPopup in HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver erstellen und den Wert auf 1 festlegen.
Hinweis: Erstellen Sie den Wert auf einer 64-Bit-Maschine in HKLM\SOFTWARE\Wow6432Node\ Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver

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

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

   Hinweis: Wenn Sie die icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.

6. Navigieren Sie im Gruppenrichtlinien-Editor zu Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzererfahrung > Tastenkombinationen.
7. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert und die gewünschten Optionen.

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

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.
Sie können eine bevorzugte Farbtiefe einstellen, indem Sie der Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences einen neuen Zeichenfolgenschlüssel "TWIDesiredIconColor" hinzufügen und den gewünschten Wert angeben. Die möglichen Werte für die Farbtiefe von Symbolen sind 4, 8, 16, 24 und 32 Bits pro Pixel. Benutzer können eine geringere Farbtiefe für die Symbole wählen, wenn die Netzwerkverbindung langsam ist.

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

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

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

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

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

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

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

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

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

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

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

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

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

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

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.

Sichern der Verbindungen

May 01, 2013

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

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

Konfigurieren von Domänen-Passthrough-Authentifizierung

Nov 03, 2015

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

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

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

- Aktivieren über die Befehlszeile
- Aktivieren über die grafische Benutzeroberfläche

Aktivieren von Domänen-Passthrough über die Befehlszeilenschnittstelle

Aktivieren von Domänen-Passthrough (SSON) über die Befehlszeilenschnittstelle

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

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

Aktivieren von Domänen-Passthrough über die grafische Benutzeroberfläche

Aktivieren von Domänen-Passthrough über die grafische Benutzeroberfläche

1. Navigieren Sie zur Installationsdatei von Citrix Receiver (CitrixReceiver.exe).
2. Doppelklicken Sie auf **CitrixReceiver.exe**, um das Installationsprogramm zu starten.
3. Aktivieren Sie im Installationsassistenten zum Aktivieren von Single Sign-On das Kontrollkästchen "Single Sign-On

aktivieren", sodass Citrix Receiver mit aktiviertem SSON-Feature installiert wird. Diese Methode entspricht der Installation von Citrix Receiver mit der Befehlszeilenoption **/includeSSON**.

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

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

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

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

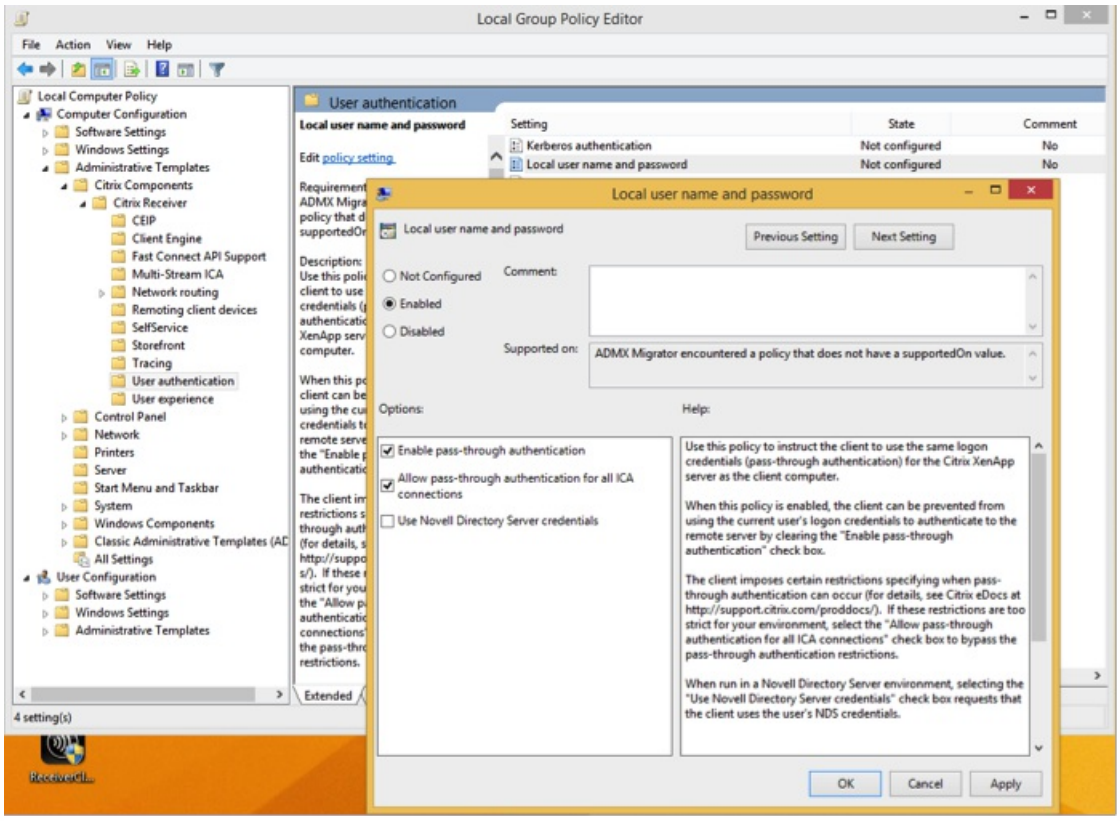
> ## Hinweis
>
> Der Standardwert der GPO-Richtlinieneinstellung für SSON ist **Passthrough-Authentifizierung aktivieren** und mit dieser Einstellung funktioniert SSON. Folgen Sie zum Ändern der Einstellung den Anleitungen unten.

Verwenden einer ADMX-Datei für die SSON-Gruppenrichtlinie

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

1. Laden Sie die entsprechenden Gruppenrichtliniendateien. Bei Installationen mit Citrix Receiver 4.3 und höher verwenden Sie **Receiver.ADMX** oder **Receiver.ADML** im Ordner %SystemDrive%\Programme (x86)\Citrix\ICA Client\Configuration.

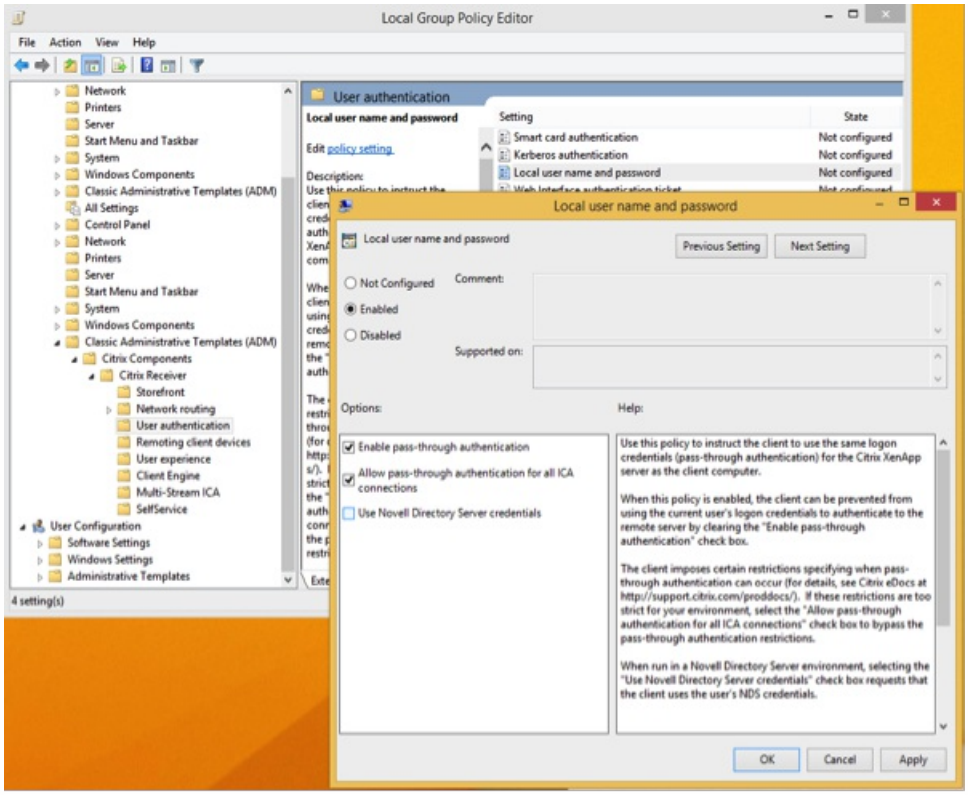
2. Öffnen Sie **gpedit.msc** und klicken Sie mit der rechten Maustaste auf **Computerkonfiguration > Administrative Vorlagen > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung**.
3. Aktivieren Sie die GPO-Einstellungen des lokalen Computers (auf der lokalen Maschine des Benutzers und/oder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



Verwenden einer ADM-Datei für die SSON-Gruppenrichtlinie

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

1. Öffnen Sie den Editor für lokale Gruppenrichtlinien, indem Sie Folgendes auswählen: **Computerkonfiguration > Rechtsklick auf Administrative Vorlagen > Vorlagen hinzufügen/entfernen**.
2. Klicken Sie auf **Hinzufügen**, um eine ADM-Vorlage hinzuzufügen.
3. Wenn Sie die Vorlage **receiver.adm** hinzugefügt haben, erweitern Sie **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Components > Citrix Receiver > User Authentication**.



4. Öffnen Sie Internet Explorer auf der lokalen Maschine und/oder im Golden Image des VDA-Desktops.

5. Fügen Sie die vollqualifizierten Domänennamen der StoreFront-Server (ohne den Storepfad) unter **Internetoptionen > Sicherheit > Vertrauenswürdige Sites** der Liste hinzu. Beispiel: https://storefront.example.com.

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

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

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

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

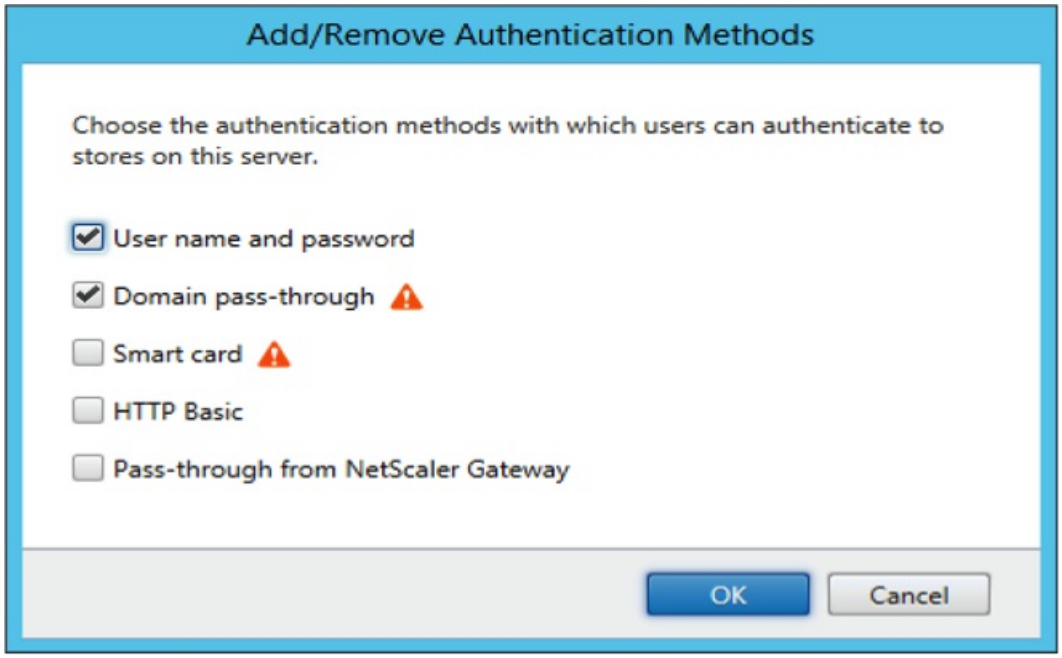
1. Melden Sie sich am Delivery Controller als Administrator an.
2. Öffnen Sie Windows PowerShell (mit Administratorrechten). In PowerShell geben Sie Befehle, damit der Delivery

Controller den von StoreFront gesendeten XML-Anfragen vertraut.

3. Laden Sie ggf. die Citrix Cmdlets, indem Sie **Add-PSSapin Citrix*** eingeben und die Eingabetaste drücken.
4. Drücken Sie die Eingabetaste.
5. Geben Sie dann **Add-PSSnapin citrix.broker.admin.v2** ein und drücken Sie die Eingabetaste.
6. Geben Sie**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True** ein und drücken Sie dieEingabetaste.
7. Schließen Sie PowerShell.

Konfigurieren von StoreFront

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



Konfiguration des Webinterface

Sie konfigurieren SSON auf dem Webinterface, indem Sie **Citrix Web Interface Management -> XenApp Services Sites -> Authentication Methods** auswählen und die Option **Pass-through** aktivieren.

Die FastConnect-API verwendet die HTTP Basic-Authentifizierungsmethode, die oft mit den für Domänenpassthrough verwendeten Authentifizierungsmethoden Kerberos und IWA verwechselt wird. Citrix empfiehlt, dass Sie IWA auf StoreFront und in der ICA-Gruppenrichtlinie deaktivieren.

Konfigurieren von Domänen-Passthrough-Authentifizierung mit Kerberos

Dec 01, 2014

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

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

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

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

1. Der Single Sign-On-Dienst von Citrix Receiver erfasst die Smartcard-PIN.
2. Citrix 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 Citrix 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.

> ## Warnung
>
> Für einige der in diesem Abschnitt beschriebenen Konfigurationen muss die Registrierung bearbeitet werden. Die unsachgemäße

> Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. 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 Citrix Receiver installieren, fügen Sie die folgende Befehlszeilenoption hinzu:

- /includeSSON
  Mit dieser Option wird die Single Sign-On-Komponente auf dem in die Domäne eingebundenen Computer installiert, sodass Receiver mit IWA (Kerberos) die Authentifizierung bei StoreFront durchführen kann. Die Single Sign-On-Komponente speichert die Smartcard-PIN, die dann von der HDX Engine verwendet wird, wenn sie eine Remoteverbindung zwischen Smartcard-Hardware und -Anmeldeinformationen und XenDesktop herstellt. XenDesktop wählt automatisch ein Zertifikat von der Smartcard aus und ruft die PIN von der HDX Engine ab.

  Eine verwandte Option, ENABLE_SSON, ist standardmäßig aktiviert und sollte unverändert bleiben.

  Wenn eine Sicherheitsrichtlinie die Aktivierung von Single Sign-On auf einem Gerät verhindert, konfigurieren Sie Receiver mit der folgenden Richtlinie:

  Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort

  Hinweis: In diesem Szenario lassen Sie zu, dass die HDX Engine Smartcard-Authentifizierung und nicht Kerberos verwendet. Verwenden Sie daher nicht die Option ENABLE_KERBEROS=Yes, mit der die HDX Engine zur Verwendung von Kerberos gezwungen wird.

Starten Sie Receiver auf dem Benutzergerät neu, um die Einstellungen zu übernehmen.

Konfigurieren von StoreFront

- Legen Sie in der Datei default.ica auf dem StoreFront-Server DisableCtrlAltDel auf false fest.
  Hinweis: Dieser Schritt ist nicht erforderlich, wenn auf allen Clientcomputern Receiver für Windows 4.2 oder höher ausgeführt wird.
- Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie das Kontrollkästchen Domänen-Passthrough. Mit dieser Einstellung wird die integrierte Windows-Authentifizierung aktiviert. Das Kontrollkästchen Smartcard muss nur aktiviert werden, wenn Sie auch Clients haben, die nicht in Domänen eingebunden sind und mit Smartcards eine Verbindung zu StoreFront herstellen.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

Die FastConnect-API verwendet die HTTP Basic-Authentifizierungsmethode, die oft mit den für Domänenpassthrough verwendeten Authentifizierungsmethoden Kerberos und IWA verwechselt wird. Citrix empfiehlt, dass Sie IWA auf StoreFront

und in der ICA-Gruppenrichtlinie deaktivieren.

Konfigurieren der Smartcardauthentifizierung

Nov 28, 2014

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

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

  StoreFront und Receiver müssen für die Passthrough-Authentifizierung konfiguriert werden.

- **Bimodale Authentifizierung:** Bei der bimodalen Authentifizierung können Benutzer zwischen einer Smartcard und der Eingabe des Benutzernamens und des Kennworts wählen. Dieses Feature ist nützlich, wenn die Smartcard nicht verwendet werden kann (z. B. wenn sie vom Benutzer zu Hause vergessen wurde oder das Zertifikat abgelaufen ist). Hierfür müssen dedizierte Stores pro Site eingerichtet werden, damit die Methode DisableCtrlAltDel zur Smartcardverwendung auf False festgelegt werden kann. Die bimodale Authentifizierung erfordert eine StoreFront-Konfiguration. Umfasst die Lösung NetScaler Gateway, muss auch dies konfiguriert werden.
  Die bimodale Authentifizierung ermöglicht dem StoreFront-Administrator nun außerdem das Anbieten der Authentifizierung über Benutzernamen/Kennwort und per Smartcard bei dem gleichen Store, indem er diese in der StoreFront Management Console auswählt. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

- **Mehrere Zertifikate:** Mehrere Zertifikate können für eine Smartcard verfügbar sein, wenn mehrere Smartcards verwendet werden. Wenn ein Benutzer eine Smartcard in einen Kartenleser einsteckt, stehen die Zertifikate für alle Anwendungen zur Verfügung, die auf dem Benutzergerät ausgeführt werden, einschließlich Receiver. Konfigurieren Sie Receiver, um die Auswahl von Zertifikaten zu ändern.
- **Clientzertifikatauthentifizierung:** NetScaler Gateway bzw. Access Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
  - Für den Zugriff auf StoreFront-Ressourcen über NetScaler Gateway bzw. Access Gateway müssen Benutzer sich ggf. nach dem Entfernen der Smartcard neu authentifizieren.
  - Wenn die SSL-Konfiguration von NetScaler Gateway bzw. Access Gateway auf die verbindliche Clientzertifikatauthentifizierung eingestellt ist, ist der Betrieb sicherer. Die verbindliche Clientzertifikatauthentifizierung ist jedoch nicht mit der bimodalen Authentifizierung kompatibel.
- **Double-Hop-Sitzungen:** Wenn ein Double Hop benötigt wird, wird eine weitere Verbindung zwischen Receiver und dem virtuellen Desktop des Benutzers hergestellt. Bereitstellungen, die Double Hop unterstützen, werden in der XenDesktop-Dokumentation beschrieben.
- **Smartcard-aktivierte Anwendungen:** In smartcard-aktivierten Anwendungen, wie Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in virtuellen Desktop- oder Anwendungssitzungen verfügbar sind, digital signieren oder verschlüsseln.

Voraussetzungen

In diesem Abschnitt wird davon ausgegangen, dass Sie mit den Smartcardabschnitten in der XenDesktop- und StoreFront-Dokumentation vertraut sind.

Einschränkungen

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Zertifikatauswahl wird in Receiver für Windows nicht speichert, es kann jedoch die PIN gespeichert werden, wenn sie konfiguriert ist. Die PIN wird nur im nicht ausgelagerten Speicher für die Dauer der Benutzersitzung zwischengespeichert. Sie wird zu keinem Zeitpunkt auf der Festplatte gespeichert.
- Receiver für Windows verbindet keine Sitzungen wieder, wenn eine Smartcard eingesteckt wird.
- Wenn Receiver für Windows für die Smartcard-Authentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung von VPN-Tunneln mit der Smartcard-Authentifizierung müssen Benutzer das NetScaler Gateway Plug-In installieren und sich über eine Webseite anmelden und sich mit den Smartcards und PINs an jedem Schritt authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem NetScaler Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Die Kommunikation von Receiver für Windows Updater mit citrix.com u8nd Merchandising Server ist nicht mit der Smartcard-Authentifizierung an NetScaler Gateway kompatibel.

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

Fügen Sie zum Konfigurieren von Receiver bei der Installation die folgende Befehlszeilenoption hinzu:

- ENABLE_SSON=Yes
  Single Sign-On ist ein anderer Begriff für Passthrough-Authentifizierung. Wenn diese Einstellung aktiviert ist, zeigt Receiver keine zweite PIN-Eingabeaufforderung an.

Alternativ können Sie die Konfiguration über die folgenden Richtlinien- und Registrierungsänderungen ausführen:

- Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort
- Wenn die Single Sign-On-Komponente nicht installiert ist, legen Sie in einem der folgenden Registrierungsschlüssel die Option SSONCheckEnabled auf false fest. Der Schlüssel verhindert, dass der Authentifizierungsmanager von Receiver nach der Single Sign-On-Komponente sucht, sodass Receiver die Authentifizierung bei StoreFront durchführen kann.
  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

Alternativ können Sie die Smartcardauthentifizierung bei StoreFront anstelle von Kerberos aktivieren. Zum Aktivieren der Smartcardauthentifizierung bei StoreFront anstelle von Kerberos installieren Sie Receiver mit den unten aufgeführten Befehlszeilenoptionen. Hierfür sind Administratorprivilegien erforderlich. Der Computer muss nicht in eine Domäne

eingebunden sein.

- /includeSSON installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Aktiviert das Zwischenspeichern der Anmeldeinformationen und die Verwendung der domänenbasierten Passthrough-Authentifizierung.
- Meldet sich der Benutzer beim Endpunkt mit einer anderen Authentifizierungsmethode an (z. B. über den Benutzernamen und das Kennwort), verwenden Sie folgende Befehlszeile:
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  Hierdurch wird verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden, und ermöglicht, dass die PIN durch Receiver bei der Anmeldung bei Receiver gespeichert wird.

- Wechseln Sie zu Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort.
  Passthrough-Authentifizierung aktivieren: Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise die Option Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen aktivieren, damit die Passthrough-Authentifizierung funktioniert.

Konfigurieren von StoreFront

- Wenn Sie den Authentifizierungsdienst konfigurieren, aktivieren Sie das Kontrollkästchen Smartcard.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter Konfigurieren des Authentifizierungsdiensts in der StoreFront-Dokumentation.

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

Wenn mehrere Zertifikate gültig sind, fordert Receiver den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können Receiver auch so konfigurieren, dass das Standardzertifikat (gemäß des Standardanbieters) oder das Zertifikat mit dem spätesten Ablaufdatum verwendet wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden.

Ein gültiges Zertifikat muss die drei folgenden Merkmale haben:

- Die aktuelle Uhrzeit auf dem lokalen Computer liegt im Gültigkeitszeitraum des Zertifikats.
- Der öffentliche Schlüssel des Subjekts muss den RSA-Algorithmus verwenden und eine Schlüssellänge von 1024, 2048 oder 4096 Bits haben.
- Die Schlüsselverwendung muss digitale Signatur enthalten.
- Der alternative Name des Subjekts muss den UPN enthalten.
- Die erweiterte Schlüsselverwendung muss Smartcard-Anmeldung und Clientauthentifizierung oder alle Schlüsselverwendungen enthalten.
- Eine der Zertifizierungsstellen in der Ausstellerkette des Zertifikats muss mit einem der Distinguished Names übereinstimmen, den der Server im TLS-Handshake sendet.

Ändern Sie mit einer der folgenden Methoden, wie Zertifikate ausgewählt werden:

- Geben Sie an der Receiver-Befehlszeile die Option AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry } an.
  Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Receiver für SmartCardDefault oder LatestExpiry den Benutzer zur Auswahl eines Zertifikats auf.
- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKCU oder HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry } zu.
  In HKCU definierte Werte haben Priorität über Werte in HKLM, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von Receiver und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Receiver fordert Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN den Smartcard-Kryptografiedienstanbieter. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung, können Sie in Receiver konfigurieren, dass die PIN-Eingabe, einschließlich der Aufforderung für eine PIN von den CSP-Komponenten verwaltet wird.

Ändern Sie mit einer der folgenden Methoden, wie die PIN-Eingabe gehandhabt wird:

- Geben Sie an der Receiver-Befehlszeile die Option AM_SMARTCARDPINENTRY=CSP an.
- Fügen Sie den folgenden Schlüsselwert dem Registrierungsschlüssel HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP hinzu.

Aktivieren der Überprüfung von Zertifikatsperrlisten

Nov 19, 2014

Wenn die Überprüfung von Zertifikatsperrlisten (CRL) aktiviert ist, überprüft Receiver, ob das Zertifikat des Servers widerrufen wurde. Da Citrix Receiver zu einer Überprüfung gezwungen wird, wird die kryptografische Authentifizierung für den Server sowie die allgemeine Sicherheit der TLS-Verbindung zwischen einem Benutzergerät und einem Server verbessert.

Sie können für die Überprüfung der Zertifikatsperrlisten mehrere Stufen einstellen. Sie können beispielsweise Citrix Receiver so konfigurieren, dass nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft werden. Außerdem können Sie die Überprüfung der Zertifikate so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Wenn Sie diese Änderung auf einem lokalen Computer durchführen, beenden Sie Receiver, wenn er ausgeführt wird. Vergewissern Sie sich, dass alle Citrix Receiver-Komponenten, einschließlich Connection Center, geschlossen sind.

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
   Hinweis: Wenn Sie die icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert.
8. Wählen Sie im Dropdownmenü CRL verification eine der Optionen aus.
   - Deaktiviert: Es wird keine Überprüfung von Zertifikatsperrlisten durchgeführt.
   - Nur lokal gespeicherte CRLs prüfen Es werden vorher heruntergeladene oder installierte Zertifikatsperrlisten für die Zertifikatüberprüfung verwendet. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen wurde.
   - CRLs für Verbindung erforderlich: Es werden lokale Zertifikatsperrlisten von relevanten Zertifikatausgabestellen im Netzwerk überprüft. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen oder nicht gefunden wurde.
   - CRLs vom Netzwerk abrufen: Zertifikatsperrlisten von relevanten Zertifikatausgabestellen werden überprüft. Die Verbindung schlägt fehl, wenn das Zertifikat zurückgerufen wurde.

   Wenn Sie CRL verification nicht einstellen, ist die Standardeinstellung Nur lokal gespeicherte CRLs prüfen.

Sichern der Receiver-Kommunikation

Mar 03, 2015

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

- Citrix NetScaler Gateway (Access Gateway). Weitere Informationen finden Sie in den Themen in diesem Abschnitt und in der Dokumentation zu NetScaler Gateway und StoreFront.
  Hinweis: Citrix empfiehlt, die Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit NetScaler Gateway zu sichern.
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie Receiver mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.
- Konfiguration vertrauenswürdiger Server.
- Nur für XenApp- oder Webinterface-Bereitstellungen, gilt nicht für XenDesktop 7: Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, bzw. HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das und vom Netzwerk ein und verarbeiten Verbindungen zwischen Receiver und Servern. Receiver unterstützt die Protokolle SOCKS und Secure Proxy.
- Nur für XenApp- oder Webinterface-Bereitstellungen, gilt nicht für XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 und XenApp 7.5: SSL-Relay-Lösungen mit TLS-Protokollen (Transport Layer Security).
- Für XenApp 7.6 und XenDesktop 7.6 können Sie eine SSL-Verbindung direkt zwischen Benutzern und VDAs aktivieren. (Informationen zum Konfigurieren von SSL für XenApp 7.6 und XenDesktop 7.6 finden Sie unter SSL.)

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

Verbinden mit NetScaler Gateway

Nov 10, 2014

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

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

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

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 NetScaler Gateway Enterprise Edition

Aug 01, 2016

Konfigurieren Sie NetScaler Gateway für StoreFront und App Controller (eine Komponente von CloudGateway), damit Remotebenutzer eine Verbindung über NetScaler 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 NetScaler Gateway Plug-In her.

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

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

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

Nov 20, 2014

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

Wenn diese Funktion aktiviert ist, können Receiver Anforderungen für die Vertrauensstellung angeben und ermitteln, ob sie der Verbindung zu dem Server vertrauen wollen. Beispiel: Ein Receiver, der eine Verbindung zu einer bestimmten Adresse herstellt (wie https://*.citrix.com) und dabei einen bestimmten Verbindungstyp verwendet (wie TLS), wird an eine vertrauenswürdige Zone auf dem Server weitergeleitet.

Wenn die Konfiguration vertrauenswürdiger Server aktiviert ist, müssen verbundene Server der Zone vertrauenswürdiger Sites von Windows hinzugefügt werden. (Eine detaillierte Anleitung, wie Sie Server der Zone vertrauenswürdiger Sites von Windows hinzufügen, finden Sie in der Onlinehilfe von Internet Explorer.)

Aktivieren der Konfiguration mit vertrauenswürdigen Servern

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

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
   Hinweis: Wenn Sie die icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Erweitern Sie unter dem Knoten Benutzerkonfiguration den Eintrag Administrative Vorlagen.
7. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
8. Klicken Sie im Menü Aktion auf Eigenschaften und wählen Sie Aktiviert.

Erhöhte Rechte und wfcrun32.exe

May 01, 2013

Wenn die Benutzerkontensteuerung auf Geräten unter Windows 8, Windows 7 oder Windows Vista aktiviert ist, können nur Prozesse, die dieselben erhöhten Rechte bzw. Integritätsebene wie wfcrun32.exe haben, virtuelle Anwendungen starten.

Beispiel 1:

Wenn wfcrun32.exe als Standardbenutzer (keine Rechteanhebung) ausgeführt wird, müssen andere Prozesse, u. a. Receiver, als Standardbenutzer ausgeführt werden, um Anwendungen über wfcrun32 zu starten.

Beispiel 2:

Wenn wfcrun32.exe mit erhöhten Rechten ausgeführt wird, können andere Prozesse, u. a. Receiver, Connection Center und Anwendungen von Drittherstellern, die das ICA-Clientobjekt verwenden, die ohne erhöhte Rechte ausgeführt werden, nicht mit wfcrun32.exe kommunizieren.

Receiver-Verbindungen über einen Proxyserver

Jan 02, 2013

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Proxyserver werden zum Beschränken des Netzwerkzugriffs sowie beim Herstellen von Verbindungen zwischen Receiver und Servern verwendet. Receiver unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit der Serverfarm verwendet Receiver die Einstellungen für den Proxyserver, die remote auf dem Receiver für Web- oder Webinterface-Server konfiguriert wurden. Informationen zur Proxyserverkonfiguration finden Sie in der StoreFront- oder Webinterface-Dokumentation.

Für die Kommunikation mit dem Webserver verwendet Receiver die Einstellungen für den Proxyserver, die über die Internetoptionen des Standardwebbrowsers auf dem Benutzergerät konfiguriert wurden. Sie müssen die Internetoptionen des Standardwebbrowsers auf dem Benutzergerät entsprechend konfigurieren.

Verbinden mit dem SSL-Relay (Secure Sockets Layer)

Oct 05, 2016

Dieses Thema gilt für XenDesktop 7.6 und höher oder XenApp 7.5.

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

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

Dieses Thema gilt für XenDesktop 7.6 und höher oder XenApp 7.5.

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

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

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

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

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

Anforderungen für Benutzergeräte

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.

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 in das Textfeld Allowed SSL servers die neue Portnummer im folgenden 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 serversein:: 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]


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

[Excel]
SSLProxyHost=csghq.Test.com:444

[Editor]
SSLProxyHost=fred.Test.com:443
```

Konfigurieren und Aktivieren von Receiver für TLS

Oct 05, 2016

Dieses Thema gilt für XenDesktop 7.6 und höher oder XenApp 7.5.

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

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

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

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

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

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

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

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

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

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

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

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie mit Active Directory arbeiten.
   Hinweis: Wenn Sie die icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften, wählen Sie Aktiviert und wählen Sie in den Listenfeldern die TLS-Einstellungen aus.
   - Setzen Sie "TLS Version" auf TLS oder Detect all , um TLS zu aktivieren. Wenn Detect all ausgewählt ist, stellt Receiver eine Verbindung mit TLS-Verschlüsselung her.
   - Setzen Sie "SSL cipher suite" auf Detect version, damit Receiver eine geeignete Verschlüsselungssammlung aus kommerziellen (Commercial) und Regierungs (Government)-Verschlüsselungssammlungen aushandeln kann. Sie können die Verschlüsselungssammlungen auf "Behörden" oder "Kommerziell" beschränken.
   - Setzen Sie "CRL verification" auf Require CRLs for connection. Bei dieser Einstellung versucht Receiver Zertifikatsperrlisten von den jeweiligen Zertifikatausgabestellen abzurufen.

Wenn Sie dies auf einem lokalen Computer ändern, müssen Sie alle Receiver-Komponenten, einschließlich Connection Center, schließen.
Verwenden Sie zum Erfüllen der FIPS 140-Sicherheitsanforderungen die Gruppenrichtlinienvorlage, um die Parameter zu konfigurieren oder fügen Sie die Parameter in der Datei Default.ica auf dem Webinterface-Server ein. Weitere Informationen zur Datei Default.ica finden Sie in der Webinterface-Dokumentation.

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
   Hinweis: Wenn Sie die icaclient-Vorlage bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 3 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Konfigurationsordner für Receiver (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie icaclient.adm aus.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und klicken Sie dann auf Schließen, um zum Gruppenrichtlinien-Editor zurückzukehren.
6. Navigieren Sie im Gruppenrichtlinien-Editor auf Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Receiver > Netzwerkrouting > TLS/SSL data encryption and server identification.
7. Klicken Sie im Menü Aktion auf Eigenschaften, wählen Sie Aktiviert und wählen Sie in den Dropdownlisten die richtigen TLS-Einstellungen aus.

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

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

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

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

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

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

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

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

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

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

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

Nov 19, 2014

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface und Verwendung von administrativen Vorlagen.

Die ICA-Dateisignierung hilft, Benutzer vor unautorisierten Anwendungs- oder Desktopstarts zu schützen. Citrix Receiver prüft, ob eine vertrauenswürdige Quelle die Anwendung oder den Desktop gestartet hat und verhindert basierend auf administrativen Richtlinien das Starten von Ressourcen auf nicht vertrauenswürdigen Servern. Sie können die Receiver-Sicherheitsrichtlinie für die Prüfung der Signatur beim Anwendungs- oder Desktopstart mit Gruppenrichtlinienobjekten, StoreFront oder Citrix Merchandising Server konfigurieren. Die ICA-Dateisignierung ist in der Standardeinstellung nicht aktiviert. Informationen zum Aktivieren der ICA-Dateisignierung für StoreFront finden Sie in der StoreFront-Dokumentation.

In Webinterface-Bereitstellungen ermöglicht und konfiguriert das Webinterface mit dem Citrix ICA-Dateisignierungsdienst, dass beim Start von Anwendungen und Desktops eine Signatur eingeschlossen wird. Der Dienst kann ICA-Dateien mit einem Zertifikat des lokalen Zertifikatspeichers des Computers signieren.

Citrix Merchandising Server mit Receiver aktiviert und konfiguriert das Prüfen der Signatur beim Start mit dem Assistenten Citrix Merchandising Server Administrator Console > Deliveries und fügt vertrauenswürdige Zertifikatfingerabdrücke hinzu.

Aktivieren und Konfigurieren der Prüfung der Signatur beim Anwendungs- oder Desktopstart mit Gruppenrichtlinienobjekten:

1. Öffnen Sie als Administrator den Gruppenrichtlinien-Editor, indem Sie gpedit.msc lokal vom Menü Start ausführen, wenn Sie einen einzelnen Computer ändern, oder indem Sie die Gruppenrichtlinien-Verwaltungskonsole verwenden, wenn Sie Domänenrichtlinien anwenden.
   Hinweis: Wenn Sie die Vorlage ica-file-signing-adm bereits in den Gruppenrichtlinien-Editor importiert haben, können Sie die Schritte 2 bis 5 überspringen.
2. Wählen Sie im linken Bereich des Gruppenrichtlinien-Editors den Ordner "Administrative Vorlagen" aus.
3. Klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen, navigieren Sie zum Receiver-Konfigurationsordner (üblicherweise C:\Programme\Citrix\ICA Client\Configuration) und wählen Sie ica-file-signing.adm 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 und dann auf ICA-Dateisignierung aktivieren.
7. Wenn Sie Enabled wählen, können Sie Fingerabdrücke von Signaturzertifikaten der Positivliste der vertrauenswürdigen Zertifikatfingerabdrücke hinzufügen, oder Sie können auf Show klicken und auf dem Bildschirm Show Contents Fingerabdrücke von Signaturzertifikaten aus der Positivliste entfernen. Sie können die Fingerabdrücke von Signaturzertifikaten von den Eigenschaften des Signaturzertifikats kopieren und einfügen. Klicken Sie in der Dropdownliste Policy auf Only allow signed launches (more secure) oder Prompt user on unsigned launches (less secure).

Option	Beschreibung
Nur signierte Starts zulassen	Nur richtig signierte Anwendungs- oder Desktopstarts von einem vertrauenswürdigen Server sind zulässig. Dem Benutzer wird eine Sicherheitswarnung im Receiver angezeigt, wenn eine

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

Bei der Auswahl eines digitalen Signaturzertifikats empfiehlt Citrix eine Auswahl aus dieser Prioritätsliste:

1. Erwerben Sie ein codesigniertes Zertifikat oder ein SSL-Signaturzertifikat einer öffentlichen Zertifizierungsstelle.
2. Wenn Ihr Unternehmen eine private Zertifizierungsstelle hat, erstellen Sie ein codesigniertes oder SSL-Signaturzertifikat mit der privaten Zertifizierungsstelle.
3. Verwenden Sie ein vorhandenes SSL-Zertifikat, z. B. das Webinterface-Serverzertifikat.
4. Erstellen Sie ein neues Stammzertifikat der Zertifizierungsstelle und verteilen es mit einem Gruppenrichtlinienobjekt oder einer manuellen Installation auf die Benutzergeräte.

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

Dec 02, 2012

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

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

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

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://Hostname

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

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

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

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

desktop://gruppe-20name

ica[s]://xaserver1

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

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

Muster-Websiteadressen

https://mein.unternehmen.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

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

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

Beispiel eines HttpBrowserAddress-Eintrags in der ICA-Datei

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

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

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

icas://10.20.30.40:1494

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

ica://10.20.30.40

Festlegen der Clientressourcenberechtigungen

Oct 30, 2014

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

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

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

> ## Hinweis
>
> Aufgrund von aktuellen Verbesserungen an Citrix Receiver wurde die INI-Prozedur, die in früheren Versionen des Plug-Ins/Receivers verfügbar war, durch diese Prozeduren ersetzt.

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

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

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

Wenn Citrix Receiver Anwendungen enumeriert und mit StoreFront kommuniziert, wird die Kryptografie der Windows-Plattform verwendet.

Für TCP-Verbindungen zwischen Citrix Receiver und XenApp/XenDesktop unterstützt Citrix Receiver TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

Für auf UDP basierende Verbindungen unterstützt Citrix Receiver DTLS 1.0 mit den folgenden Verschlüsselungssammlungen:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Aktivieren des Konformitätsmodus SP 800-52

Unter "Computerkonfiguration" > "Administrative Vorlagen" > "Citrix Komponenten" > "Netzwerkrouting" > "Konfiguration von TLS und Konformitätsmodus" gibt es ein neues Kontrollkästchen: **FIPS aktivieren**.Hiermit wird gewährleistet, dass nur für FIPS genehmigte Kryptografie für alle ICA-Verbindungen verwendet wird. Standardmäßig ist diese Option deaktiviert.

Ein neuer Sicherheitskonformitätsmodus wird eingeführt: SP 800-52. Standardmäßig ist diese Option auf NONE festgelegt und deaktiviert. Unter folgendem Link finden Sie eine Beschreibung der für NIST SP 800-52 erforderlichen Konformität: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295.

> **Hinweis**
>
> Der Konformitätsmodus SP800-52 erfordert FIPS-Konformität. Wenn SP800-52 aktiviert ist, ist der FIPS-Modus unabhängig von der FIPS-Einstellung ebenfalls aktiviert. Die zulässigen Werte für die Richtlinie "Zertifikatsperrüberprüfung" sind "Volle Zugriffsprüfung und CRL erforderlich" oder "Volle Zugriffsprüfung und alle CRL erforderlich".

Einschränken von TLS-Versionen und Verschlüsselungssammlungen

Sie können durch die Konfiguration von Citrix Receiver TLS-Versionen und Verschlüsselungssammlungen einschränken. Mit einer Option können die zulässigen TLS-Protokollversionen ausgewählt werden, wodurch das TLS-Protokoll für ICA-Verbindungen bestimmt wird. Die höchste TLS-Version, die auf Client und Server verfügbar ist, wird ausgewählt. Die folgenden Optionen sind verfügbar:

- TLS 1.0 | TLS 1.1 | TLS 1.2 (Standard)
- TLS 1.1 | TLS 1.2
- TLS 1.2

Für die Auswahl der TLS-Verschlüsselungssammlung ist auch eine Option verfügbar. Citrix Receiver hat folgende Wahl:

- Beliebig
- Kommerziell
- Behörden

Kommerzielle Verschlüsselungssammlungen

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Verschlüsselungssammlungen für Behörden

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Hinweis**
>
> Wenn **TLS für alle Verbindungen verwenden** aktiviert ist, müssen Verbindungsanfragen an StoreFront über HTTPS gesendet werden. Das Hinzufügen eines Stores als HTTP schlägt fehl und ein VDA ohne SSL (XenDesktop und XenApp) kann nicht gestartet werden.

Receiver Desktop Lock

Aug 09, 2016

Sie können Receiver Desktop Lock verwenden, wenn Benutzer nicht mit dem lokalen Desktop arbeiten müssen. Benutzer können weiterhin den Desktop Viewer (falls aktiviert) verwenden, es sind jedoch nur die erforderlichen Optionen auf der Symbolleiste: Strg+Alt+Entf, Einstellungen, Geräte und Trennen.

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

Sie müssen Citrix Receiver für Windows mit dem Flag /includeSSON installieren. Konfigurieren Sie den Store und Single Sign-On mit der ADM/ADMX-Datei oder über die Befehlszeilenoption. Weitere Informationen finden Sie unter Installieren und Konfigurieren von Citrix Receiver an der Befehlszeile.

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

Systemanforderungen für Citrix Receiver Desktop Lock

- Unterstützung für Windows 7 (einschließlich Embedded Edition), Windows 7 Thin PC, Windows 8 und Windows 8.1.
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

Lokaler App-Zugriff

> **Important**
>
> Aktivieren des lokalen App-Zugriffs kann den lokalen Desktopzugriff ermöglichen, es sei denn, es wurde eine vollständige Sperrung über die Gruppenrichtlinienobjektvorlage oder eine ähnliche Richtlinie angewendet. Weitere Informationen finden Sie unter Konfigurieren von lokalem App-Zugriff und URL-Umleitung in XenApp und XenDesktop.

Arbeiten mit Receiver Desktop Lock

- Receiver Desktop Lock kann mit den folgenden Features von Receiver für Windows verwendet werden:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013-Plug-In und lokaler App-Zugriff.
  - Nur Domänen-, Smartcard- oder zweistufige Authentifizierung.
- Trennen der Receiver Desktop Lock-Sitzung führt zu Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Receiver Desktop Lock ohne die Eigenschaften Home, Restore, Maximize und Display optimiert.
- Strg+Alt+Entf steht über die Viewer-Symbolleiste zur Verfügung.
- Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben, Ausnahme bildet Windows+L. Weitere Informationen finden Sie unter Weitergeben von Windows-Tastenkombinationen an die Remotesitzung.
- Strg+F1 löst Strg+Alt+Entf aus, wenn Sie die Verbindung oder Desktop Viewer für Desktopverbindungen deaktivieren.

Mit diesen Schritten installieren Sie Receiver für Windows, sodass virtuelle Desktops mit Receiver Desktop Lock angezeigt werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter So konfigurieren Sie Smartcards für die Verwendung mit Geräten mit Receiver Desktop Lock.

1. Melden Sie sich mit einem lokalen Administratorkonto an.
2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus (befindet sich im Ordner "Citrix Receiver and Plug-ins > Windows > Receiver" auf dem Installationsmedium).
   Beispiel:
   CitrixReceiver.exe
   /includeSSON
   STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   Informationen zu den Befehlen finden Sie in der Installationsdokumentation zu Receiver für Windows unter Konfigurieren und Installieren von Receiver für Windows mit Befehlszeilenparametern.
3. Doppelklicken Sie im selben Ordner auf dem Installationsmedium auf CitrixReceiverDesktopLock.msi. Der Assistent "Citrix Desktop Lock" wird geöffnet. Folgen Sie den Anweisungen.
4. Wenn die Installation abgeschlossen ist, starten Sie das Benutzergerät neu. Wenn Sie Zugriffsrechte für einen Desktop haben und sich als Domänenbenutzer anmelden, zeigt das neu gestartete Gerät Receiver Desktop Lock an.

Um die Verwaltung des Benutzergeräts nach der Installation zu ermöglichen, wird das Konto, das für die Installation von CitrixReceiverDesktopLock.msi verwendet wurde, bei der Ersatz-Shell ausgeschlossen. Wenn das Konto später gelöscht wird, können Sie sich nicht bei dem Gerät anmelden und es verwalten.

Verwenden Sie zum Installieren von Receiver Desktop Lock **ohne Benutzereingriff** die folgende Befehlszeile: msiexec /i CitrixReceiverDesktopLock.msi /qn

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

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

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

- Stellen Sie sicher, dass die Dateien Receiver.admx (oder Receiver.adml) und Receiver_usb.admx (.adml) in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter "Computerkonfiguration" bzw. "Benutzerkonfiguration" > "Administrative Vorlagen" > "Klassische administrative Vorlagen (ADMX)" > "Citrix Components" angezeigt werden). Die ADMX-Dateien sind in %Programme%\Citrix\ICA Client\Configuration\.
- USB-Einstellungen: Wenn ein Benutzer ein USB-Gerät anschließt, erfolgt ein automatisches Remoting des Geräts zum virtuellen Desktop. Es ist kein Benutzereingriff erforderlich. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.
  - Aktivieren Sie die USB-Richtlinienregel.
  - Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" > "Generisches USB-Remoting" die Richtlinien Vorhandene USB-Geräte und Neue USB-Geräte.
- Laufwerkszuordnung: Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" die Richtlinie "Clientlaufwerkzuordnung".
- Mikrofon: Aktivieren und konfigurieren Sie unter "Citrix Receiver" > "Remoting von Clientgeräten" die Richtlinie "Clientmikrofon".

1. Konfigurieren von StoreFront
    1. Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
    2. Konfigurieren Sie StoreFront-Sites für HTTPS-Zugriff, erstellen Sie ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde und fügen Sie HTTPS-Bindung zur Standardwebsite hinzu.
    3. Stellen Sie sicher, dass Passthrough mit Smartcard aktiviert ist (standardmäßig aktiviert).
    4. Aktivieren Sie Kerberos.
    5. Aktivieren Sie Kerberos und Passthrough mit Smartcard.
    6. Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
    7. Stellen Sie sicher, dass für die IIS-Standardwebsite kein SSL erforderlich ist, und dass Clientzertifikate ignoriert werden.
2. Verwenden Sie die Gruppenrichtlinien-Verwaltungskonsole zum Konfigurieren lokaler Computerrichtlinien auf dem Benutzergerät.
    1. Importieren Sie die Vorlage Receiver.admx aus %Programme%\Citrix\ICA Client\Configuration\.
    2. Erweitern Sie "Administrative Vorlagen" > "Klassische administrative Vorlagen (ADMX)" > "Citrix Komponenten" > "Citrix Receiver" > "Benutzerauthentifizierung".
    3. Aktivieren Sie "Smartcardauthentifizierung".
    4. Aktivieren Sie "Lokaler Benutzername und Kennwort".
3. Konfigurieren Sie das Benutzergerät vor der Installation von Receiver Desktop Lock.
    1. Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu.
    2. Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" im Format: //delivery-group-name hinzu.
    3. Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Receiver Desktop Lock auf dem Benutzergerät installiert ist, wird eine konsistente Richtlinie für das Entfernen der Smartcard zwingend angewendet. Wird die Richtlinie für das Entfernen der Smartcard beispielsweise für den Desktop auf Abmelden erzwingen festgelegt, muss der Benutzer sich auch vom Benutzergerät abmelden, unabhängig davon, wie die Richtlinie dort eingestellt ist. Dadurch wird sichergestellt, dass das Benutzergerät sich nicht in einem inkonsistenten Zustand befindet. Dies gilt nur für Benutzergeräte mit Receiver Desktop Lock.

Stellen Sie sicher, dass beide der unten aufgeführten Komponenten entfernt werden.

1. Melden Sie sich mit demselben lokalen Administratorkonto an, das bei der Installation und Konfiguration von Receiver Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:
    - Entfernen Sie Citrix Receiver Desktop Lock.
    - Entfernen Sie Citrix Receiver.

Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. In diesem Abschnitt finden Sie einige der gebräuchlichsten Tastenkombinationen.

Windows

- Win+D - Minimieren aller Fenster auf dem Desktop.
- Alt+Tab - Wechseln des aktiven Fensters.
- Strg+Alt+Entf - über Strg+F1 und die Desktop Viewer-Symbolleiste.
- Alt+Umschalt+Tab
- Windows+Tab

- Windows+Umschalt+Tab
- Windows+Alle Zeichentasten

Windows 8

- Win+C - Charms öffnen.
- Win+Q - Charm "Suche".
- Win+H - Charm "Teilen".
- Win+K - Charm "Geräte".
- Win+I - Charm "Einstellungen".
- Win+Q - Apps durchsuchen.
- Win+W - Einstellungen durchsuchen.
- Win+F - Dateien durchsuchen.

Windows 8 Apps

- Win+Z - App-Optionen anzeigen.
- Win+. - App links andocken.
- Win+Umschalt+. - App rechts andocken.
- Strg+Tab - Zum App-Verlauf wechseln.
- Alt+F4 - App schließen.

Desktop

- Win+D - Desktop öffnen.
- Win+, - Desktop kurz anzeigen.
- Win+B - Zurück zum Desktop.

Andere Version

- Win+U - Center für erleichterte Bedienung öffnen.
- Strg+Esc - Startbildschirm.
- Win+Eingabetaste - Windows Sprachausgabe öffnen.
- Win+X - Menü für Systemprogrammeinstellungen öffnen.
- Win+Druck - Bildschirmfoto erstellen und unter "Bilder" speichern.
- Win+Tab - Liste zum Wechseln öffnen.
- Win+T - Vorschau offener Fenster in Taskleiste anzeigen.

SDK und API für Citrix Receiver für Windows

Apr 05, 2017

Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für zusätzliche virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanalanwendungen sind auf XenApp- oder XenDesktop-Servern. Diese Version des SDK bietet Unterstützung zum Schreiben neuer virtueller Kanäle für Receiver für Windows. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an den technischen Support von Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VDAPI) wird mit dem virtuellen Kanal im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VDAPI bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Die Windows Monitoring API, die die visuelle Darstellung verbessert und Unterstützung für Anwendungen von Drittanbietern bietet, die in ICA integriert sind.
- Funktionierender Quellcode für Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WFAPI SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Weitere Informationen zum SDK finden Sie unter Citrix Virtual Channel SDK for Citrix Receiver for Windows.

Fast Connect 3 Credential Insertion API

Die Fast Connect 3 Credential Insertion API bietet eine Schnittstelle zum Bereitstellen von Benutzeranmeldeinformationen für Single Sign-On (SSON). Dieses Feature ist für Citrix Receiver für Windows 4.2 und höher verfügbar. Mit dieser API können Citrix Partner Authentifizierungs- und SSO-Produkte bereitstellen, die StoreFront oder das Webinterface verwenden, um Benutzer an virtuellen Anwendungen oder Desktops anzumelden und die Verbindungen zu diesen Sitzungen auch wieder zu trennen.

Weitere Informationen zur Fast Connect API finden Sie unter Fast Connect 3 Credential Insertion API for Citrix Receiver for Windows.