Citrix Receiver für Android 3.13

Contents

Neue Features

January 11, 2019

Neue Features in 3.13.9

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

Neue Features in 3.13.8

Unterstützung für Dateitypzuordnung in StoreFront

Wenn Sie Anwendungen veröffentlichen, ordnen Sie diese bestimmten Dateitypen zu, die auf dem Server vorhanden sind. Auf diese Weise leiten Sie den Inhalt vom Benutzergerät zum Server um. Geräte, auf denen Receiver für Android ausgeführt wird, öffnen Dateien eines zugeordneten Typs mit einer bestimmten veröffentlichten Anwendung. Wenn Benutzer beispielsweise auf eine E-Mail-Anlage doppelklicken, wird die Anlage in der zugeordneten Anwendung geöffnet.

Weitere Informationen finden Sie unter Zugreifen auf Dateien mit Dateitypzuordnung.

Unterstützung für das Anheften auf Chromebook

Verknüpfungen zu Ihren bevorzugten Apps und Desktops sind automatisch im Chrome App Launcher verfügbar, nachdem Sie Ihr Konto zu Citrix Receiver für Android auf einem Chromebook hinzugefügt haben. Dies gilt nicht nur für die Verbindung mit StoreFront, sondern auch für XenApp Services-Sites (früher als PNA-Konten bezeichnet).

> **Hinweis:**
>
> Dieses Feature wird im Webinterface nicht unterstützt.

Neue Features in 3.13.7

NetScaler-Kompatibilitätsmodus

Die Option **NetScaler-Kompatibilitätsmodus** ist verfügbar, um den TLS-Handshakefehler oder Fehler mit dem Code 41E bei Verbindungen über frühere Versionen von NetScaler zu beheben. Weitere Informationen zum TLS-Handshakefehler finden Sie im Knowledge Center-Artikel CTX221453. Standardmäßig ist die Option “TLS-Versionen” auf TLS 1.0, 1.1, 1.2 festgelegt.

Neue Features in 3.13.6

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

Neue Features in 3.13.5

Hinzufügen von Favoriten-Apps und -Desktops zum Chrome Launcher

Nachdem Sie Ihr Konto zu Citrix Receiver für Android auf einem Chromebook hinzugefügt haben, werden Ihre Favoriten-Apps und -Desktops automatisch dem Chrome Launcher für schnellen Zugriff hinzugefügt.

Unterstützung von HTTPS für Citrix Ready Workspace Hub

HTTPS-Verbindungen werden jetzt zwischen Citrix Receiver für Android und dem Citrix Ready Workspace Hub unterstützt.

Neue Features in 3.13.4

Unterstützung für Citrix Ready Workspace Hub

Citrix Ready Workplace Hub basiert auf der Raspberry Pi 3-Plattform und bietet eine sichere Verbindung zu autorisierten Apps und Daten. Citrix Receiver für Android unterstützt die Benutzerauthentifizierung bei Citrix Ready Workspace Hubs als experimentelles Feature.

Ab diesem Release unterstützt Citrix Receiver für Android Citrix Casting. Citrix Casting ermöglicht Benutzern das sichere und nahtlose Verschieben virtueller App- und Desktopsitzungen von einem mobilen Gerät auf einen Citrix Ready Workspace Hub mithilfe von Sitzungsroaming und drahtlosem Docking. Durch Sitzungsroaming kann sich Ihr Telefon bei einem Citrix Ready Workspace Hub authentifizieren und die Benutzersitzung sicher zum Workspace Hub verschieben. Durch das drahtlose Docking können Benutzer mit ihrem Telefon interagieren und jede App oder Desktopsitzung auf einen beliebigen Workspace Hub um sie herum übertragen.

Dynamische Berechtigungen

In früheren Releases hat Citrix Receiver für Android während der Installation nach allen Berechtigungen gefragt. Ab diesem Release, das auf Geräten mit Android 6.x und höher ausgeführt wird, fordert Citrix Receiver dynamisch Berechtigungen an, wenn sie für den Zugriff auf SD-Karten, den Standort und den Telefonzugriff benötigt werden.

Bearbeiten von Gateways und Authentifizierungstypen

Benutzer können nun das bevorzugte Gateway und den Authentifizierungstyp nach dem Hinzufügen eines Kontos bearbeiten.

> **Hinweis:**
>
> Citrix Receiver füllt automatisch alle von StoreFront veröffentlichten Authentifizierungstypen aus. Benutzer müssen sich an ihren Administrator wenden, um die unterstützten Authentifizierungstypen für das ausgewählte Gateway zu erhalten.

Neue Features in 3.13.3

Sitzungsstart mit nicht vertrauenswürdigem Zertifikat

Auf vielfachen Wunsch können Benutzer jetzt Sitzungen mit einem nicht vertrauenswürdigen Zertifikat starten.

> **Hinweis:**
>
> Die Annahme eines nicht vertrauenswürdigen Zertifikats ist ein Risiko. Administratoren sollten vertrauenswürdige Zertifikate möglichst auf andere Weise (E-Mail, Downloadlinks, vorhandenes MDM usw.) bereitstellen.

Vereinfachte Anmeldung

Nach der ersten Anmeldung werden die Felder “Benutzername” und “Domäne” auf dem Anmeldebildschirm automatisch von Citrix Receiver für Android ausgefüllt, um die Anmeldung zu erleichtern.

QR-Codes für Workspace Hub

Citrix Receiver für Android erkennt Workspace Hub jetzt anhand QR-Codes.

Neue Features in 3.13.2

Tastaturlayoutsynchronisierung

Ab diesem Release bietet Citrix Receiver für Android die dynamische Synchronisierung des Tastaturlayouts vom Client zum VDA in einer Sitzung. Damit können Benutzer zwischen bevorzugten Tastaturlayouts auf dem Clientgerät wechseln und auf diese Weise eine konsistente Benutzererfahrung genießen, wenn sie beispielsweise von der englischen Tastatur zur spanischen wechseln. Wenn

Benutzer das Layout wechseln, wird kurz eine Meldung angezeigt, während die Synchronisierung erfolgt. Anschließend können die Benutzer das neue Tastaturlayout verwenden.

> **Hinweis:**
>
> Dieses Feature funktioniert nur auf den Bildschirmtastaturen von Geräten, nicht auf externen Tastaturen. Das Kontrollkästchen "Client-IME" unter "Einstellungen" in Citrix Receiver für Android muss aktiviert sein, um diese Funktion zu aktivieren.

Anmelden über das Webinterface

Mit Citrix Receiver für Android 3.13.2 können Benutzer sich in einem Webbrowser anmelden statt über die native Benutzeroberfläche von früheren Versionen.

Neue Features in 3.13.1

Neue Benutzeroberfläche für Citrix Receiver für Android

Die Benutzeroberfläche von Citrix Receiver für Android wurde basierend auf dem umfassenden Feedback der Benutzer und gemäß den neuen Material Design-Richtlinien von Google für Android-Anwendungen neu gestaltet.

Die neue Benutzeroberfläche bietet u. a. folgende Vorteile:

- Ein optimierter Workflow für alle Aufgaben. Es ist jetzt einfacher, die Anforderungen der Benutzer umzusetzen.
- Navigationsrichtlinien, um sich mit der neuen Benutzeroberfläche vertraut zu machen.
- Unterstützung für Feedback in der App, damit Citrix durch die automatische Protokollerfassung schnell helfen kann.
- Android Toasts und Snackbars an verschiedenen Stellen, um den Betriebsstatus anzuzeigen und Vorgänge rückgängig zu machen.

Unterstützung für Citrix Ready Workspace Hub

Citrix Ready Workplace Hub basiert auf der Raspberry Pi 3-Plattform und bietet eine sichere Verbindung zu autorisierten Apps und Daten. Mit diesem Release unterstützt Citrix Receiver für Android die Benutzerauthentifizierung bei Citrix Ready Workspace Hubs als experimentelles Feature. Dadurch können authentifizierte Benutzer ihre Sitzungen an Workspace Hub übertragen. Dieses Feature ist standardmäßig deaktiviert.

> **Hinweis:**
>
> Für das experimentelle Feature “Citrix Ready Workspace Hub” ist eine Standortberechtigung erforderlich. Sie können diese Berechtigung verweigern, wenn keine Workspace Hubs vorhanden sind.

DTLS-Unterstützung durch adaptiven Transport

Die DTLS-Unterstützung wurde mit NetScaler Gateway für den adaptiven Transport aktiviert. Um DTLS zu verwenden, muss EDT im Menü “Einstellungen” von Citrix Receiver für Android aktiviert sein.

Empfohlene Überprüfungsszenarien für die DTLS-Unterstützung:

- Verwenden Sie die Store-URL, um den Store hinzuzufügen und Sitzungen zu starten.
- Konfigurieren Sie die Richtlinie für den adaptiven Transport und erleben Sie XenApp- und XenDesktop-Sitzungen über EDT statt TCP.

Weitere Informationen zum Konfigurieren von adaptivem Transport finden Sie unter Adaptiver Transport.

Automatische Konfiguration

Citrix Receiver für Android 3.13.1 konfiguriert und erkennt Stores für Benutzer automatisch.

> **Hinweis:**
>
> Die manuelle Konfiguration von Stores wurde entfernt.

Behobene Probleme

August 31, 2018

Behobene Probleme in 3.13.9

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

Behobene Probleme in 3.13.8

- Nach dem Hinzufügen eines Kontos werden die Einstellungen von “Kennwort speichern” des Webinterface-Kontos möglicherweise nicht in einer Sitzung wirksam. [RFANDROID-570]

- Auf einem VDA, der mit dem kumulativen Update 5 der Version 7.5 ausgeführt wird, können Sie möglicherweise keine Textbearbeitungsanwendungen wie Editor in einer Sitzung starten. [RFANDROID-2164]

Behobene Probleme in 3.13.7

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

Behobene Probleme in 3.13.6

- Citrix Receiver für Android startet möglicherweise keine Sitzung, wenn eine heruntergeladene ICA-Datei über den Browser geöffnet wird. [#RFANDROID-2098]

Behobene Probleme in 3.13.5

- Citrix Receiver für Android startet SaaS-Anwendungen (Software-as-a-Service) möglicherweise nicht ordnungsgemäß. [#RFANDROID-1963]

Behobene Probleme in 3.13.4

- Mit diesem Fix können Sie Citrix Receiver bei Verwendung eines Chromebooks dynamisch anpassen. [#RFANDROID-1991]

Behobene Probleme in 3.13.3

- Grafiken werden auf veröffentlichten Desktops möglicherweise verzerrt angezeigt, wenn Sie ein Demo-Konto unter Android Nougat 7.1.1 verwenden. [#RFANDROID-1990]
- Wenn Stores mit internen Beacons konfiguriert sind, die auf einen umgeleiteten Speicherort verweisen, stellen die Stores in einem internen Netzwerk möglicherweise keine Verbindung her. [#RFANDROID-1992]

Behobene Probleme in 3.13.2

- Getrennte Sitzungen werden nicht gestartet, wenn Sie das Konto hinzufügen oder im Menü auf “Aktualisieren” tippen. [#RFANDROID-1456]

- Bei der Verwendung von XenApp 6.5 enumeriert Citrix Receiver für Android keine Anwendungen.[#RFANDROID-1887]
- Citrix Receiver für Android wird beim Rendern von Legacy-Symbolen möglicherweise unerwartet beendet. [#RFANDROID-1958]
- Citrix Receiver für Android wird möglicherweise unerwartet beendet, wenn ein Demokonto registriert wird und der Vor- oder Nachname des Benutzers Leerzeichen enthält. [#RFANDROID-1960]
- Citrix Receiver für Android wird möglicherweise nicht auf Chromebooks installiert, die Android-Anwendungen unterstützen. [#RFANDROID-1968]

Behobene Probleme in 3.13.1

- Citrix Receiver erkennt den Clientnamen in der Datei default.ica nicht, wenn er unter einem anwendungsspezifischen Eintrag aufgeführt ist. [#LC7539]
- Der VDI-Bildschirm flackert bei der Verwendung von Citrix Receiver für Android 3.11.1. [#RFANDROID-1642, #LC7800]
- Wenn nur Zertifikate zum Authentifizieren einer Sitzung verwendet werden, erkennt Citrix Receiver für Android das Gateway möglicherweise nicht. [#RFANDROID-1882]
- Kennwörter mit einem Leerzeichen am Anfang oder am Ende werden nicht berücksichtigt. [#RFANDROID-1890]
- Citrix Receiver für Android wird möglicherweise unerwartet beendet, wenn eine Verbindung zu Stores hergestellt wird, die ohne Authentifizierung konfiguriert wurden. [#RFANDROID-1929]
- StoreFront-Stores, die ohne Authentifizierung auf NetScaler Gateway eingerichtet wurden, werden möglicherweise nicht erkannt. [#RFANDROID-1936]
- Benutzer können möglicherweise keine Verbindung zu Webinterface-Sites herstellen, die hinter NetScaler Gateway konfiguriert sind. [#RFANDROID-1937]
- 16-Bit-Anwendungen können auf Geräten mit Android Oreo grafisch verzerrt erscheinen. [#RFANDROID-1938]
- PNA- und XenApp-Store-Verbindungsprobleme wurden behoben. Wenn der Fehlercode 547 angezeigt wird, aktivieren Sie die Option “Legacy-Storezugriff zulassen” und versuchen Sie erneut, eine Verbindung herzustellen.

Bekannte Probleme

August 31, 2018

Bekannte Probleme in 3.13.9

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in 3.13.8

Wenn Sie das per Dateitypzuordnung konfigurierte Store-Konto zu Receiver für Android Version 3.13.7 oder niedriger hinzufügen und Receiver auf die neueste Version aktualisieren, wird Citrix Receiver nicht als Option im Dialogfeld “Öffnen mit” angezeigt, wenn Sie eine Datei zum Starten auswählen.

Um das Problem zu umgehen, navigieren Sie zu **Einstellungen** und wählen Sie **Aktualisieren**.[RFANDROID-2241]

Bekannte Probleme in 3.13.7

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in 3.13.6

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in 3.13.5

Citrix Receiver für Android startet möglicherweise keine Sitzung, wenn eine heruntergeladene ICA-Datei über den Browser geöffnet wird. Als Workaround laden Sie eine Datei-Explorer-App aus dem Google Play Store herunter, suchen Sie die Datei auf Ihrem Gerät und öffnen Sie sie dann direkt. [#RFANDROID-2098]

Bekannte Probleme in 3.13.4

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in 3.13.3

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in 3.13.2

- Die Option “An Telefon anheften” zum Hinzufügen von Anwendungen und Desktops zum Telefonbildschirm funktioniert nicht. [#RFANDROID-1896]
- Diese Version von Citrix Receiver für Android funktioniert möglicherweise nicht ordnungsgemäß, wenn NetScaler Gateway mit XenApp Services und der Website integriert ist.

  Führen Sie als Workaround folgende Schritte aus:

  1. Tippen Sie unter “Einstellungen” auf “Abmelden (alle)”.
  2. Tippen Sie auf “Konten wechseln”, um zur Seite “Konten” zu wechseln.
  3. Löschen Sie den Store auf der Seite “Konten”.
  4. Fügen Sie das Konto erneut hinzu. [#RFANDROID-1900]

Bekannte Probleme in 3.13.1

- Getrennte Sitzungen werden nicht gestartet, wenn Sie das Konto hinzufügen oder im Menü auf “Aktualisieren” tippen. [#RFANDROID-1456]
- Auf XenApp 6.5 veröffentlichte Anwendungen werden nicht gestartet. [#RFANDROID-1887]
- Die Option “An Telefon anheften” zum Hinzufügen von Anwendungen und Desktops zum Telefonbildschirm funktioniert nicht. [#RFANDROID-1896]
- Diese Version von Citrix Receiver für Android funktioniert möglicherweise nicht ordnungsgemäß, wenn NetScaler Gateway mit XenApp Services und der Website integriert ist.

  Führen Sie als Workaround folgende Schritte aus:

  1. Tippen Sie unter “Einstellungen” auf “Abmelden (alle)”.
  2. Tippen Sie auf “Konten wechseln”, um zur Seite “Konten” zu wechseln.
  3. Löschen Sie den Store auf der Seite “Konten”.
  4. Fügen Sie das Konto erneut hinzu. [#RFANDROID-1900]

Hinweise zu Drittanbietern

August 31, 2018

Citrix Produkte enthalten häufig Code von Drittanbietern, der von Citrix für die Verwendung und Umverteilung unter einer Open-Source-Lizenz lizenziert ist. Um Kunden besser zu informieren, veröffentlicht Citrix den in Citrix-Produkten enthaltenen Open-Source-Code in einer Liste mit lizenziertem Open-Source-Code.

Sie können die Open-Source-Liste hier einsehen: https://www.citrix.com/buy/licensing/open-source.html

Weitere Informationen zur Quelle finden Sie hier: https://www.citrix.com/downloads/citrix-receiver/receiver-for-android-source/htmlparser.html

Systemanforderungen

October 5, 2018

Geräteanforderungen

Dieses Release von Citrix Receiver für Android und höhere Releases unterstützen Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat) und 8.x (Oreo).

Aktualisieren Sie die Android-Geräte auf die aktuelle Android-Software, um die besten Ergebnisse zu erhalten.

Citrix Receiver für Android unterstützt das Starten von Sitzungen über Receiver für Web, sofern der verwendete Browser mit Receiver für Web funktioniert. Erfolgen keine Sitzungsstarts, konfigurieren Sie Ihr Konto direkt über Citrix Receiver für Android.

Weitere Informationen zum Sichern der Verbindungen mit Ihrer Citrix Umgebung finden Sie im Abschnitt “Verbindungen”.

> **Wichtig**
>
> Wenn eine Tech Preview-Version von Citrix Receiver für Android installiert ist, deinstallieren Sie sie, bevor Sie die neue Version installieren.

Serveranforderungen

StoreFront:

- StoreFront 2.6 oder höher

  Bietet direkten Zugriff auf StoreFront-Stores. Receiver unterstützt auch vorherige Versionen von StoreFront.

- StoreFront konfiguriert mit einer Receiver für Web-Site

  Bietet Zugriff auf StoreFront-Stores über einen Webbrowser. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

Webinterface (wird nicht für XenDesktop 7-Bereitstellungen und höhere Versionen unterstützt):

- Webinterface 5.4 mit Webinterface-Sites
- Webinterface 5.4 mit XenApp Services-Sites

Webinterface auf NetScaler:

Sie müssen die Rewrite-Richtlinien aktivieren, die von NetScaler bereitgestellt werden.

XenApp und XenDesktop (eines der folgenden Produkte):

- XenApp 7.5 oder höher
- XenApp 6.5 für Windows Server 2008 R2
- XenDesktop 7.x oder höher

Konnektivität

Citrix Receiver für Android unterstützt HTTP-, HTTPS- und ICA-über-TLS-Verbindungen mit einer XenApp-Serverfarm über eine der folgenden Konfigurationen.

LAN-Verbindungen:

- StoreFront 2.6 oder höher
- Webinterface 5.4
- XenApp Services-Site (früher Program Neighborhood Agent)

Sichere Remoteverbindungen (eines der folgenden Produkte):

- Citrix NetScaler Gateway 10 und 11 (einschließlich Versionen von VPX, MPX und SDX)
- XenMobile wird nur für die Versionen 9 und 10 unterstützt.

Sichere Verbindungen und TLS-Zertifikate

Beim Sichern von Remoteverbindungen mit TLS überprüft das Mobilgerät die Echtheit des TLS-Zertifikats des Remote-Gateways unter Verwendung eines lokalen Speichers mit vertrauenswürdigen Stammzertifizierungsstellen. Das Gerät erkennt automatisch kommerziell ausgestellte Zertifikate (z. B. VeriSign und Thawte), wenn das Stammzertifikat für die Zertifizierungsstelle im lokalen Schlüsselspeicher vorhanden ist.

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remote-Gateway installiert ist, muss das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Mobilgerät installiert sein, um erfolgreich mit Receiver auf Citrix Ressourcen zuzugreifen.

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

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Citrix Receiver für Android unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate und NetScaler Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Access Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie im Knowledge Center-Artikel, der für Ihre Edition von Access Gateway relevant ist:

CTX114146: How to Install an Intermediate Certificate on NetScaler Gateway

Zusätzlich zu den Konfigurationsabschnitten in diesem Abschnitt der Produktdokumentation finden Sie weitere Informationen auch an folgender Stelle:

CTX124937: How to Configure NetScaler Gateway for Use with Citrix Receiver for Mobile Devices

Authentifizierung

> **Hinweis:**
>
> RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen nicht unterstützt. Wenn Sie RSA SecurID verwenden möchten, verwenden Sie NetScaler Gateway.

Citrix Receiver für Android unterstützt die Authentifizierung über NetScaler Gateway mit den folgenden Methoden (abhängig von Ihrer Edition):

- Keine Authentifizierung (nur Standard- und Enterprise-Versionen)
- Domänenauthentifizierung

- RSA SecurID, einschließlich Softwaretokens für WiFi-Geräte und Geräte ohne WiFi
- Domänenauthentifizierung zusammen mit RSA SecurID
- SMS-Passcode-Authentifizierung (Einmal-PIN)
- Smartcardauthentifizierung

> **Hinweis:**
>
> Die Smartcardauthentifizierung an Webinterface-Sites wird nicht unterstützt.

Citrix Receiver für Android unterstützt jetzt die folgenden Produkte und Konfigurationen.

Unterstützte Smartcardleser:

- BaiMobile 3000MP Bluetooth-Smartcardleser

Unterstützte Smartcards:

- PIV-Karten
- Common Access Cards

Unterstützte Konfigurationen:

- Smartcardauthentifizierung bei NetScaler Gateway mit StoreFront 2 oder 3 und XenDesktop 7.x und höher oder XenApp 6.5 und höher
- Smartcardauthentifizierung bei NetScaler Gateway ab Webinterface 5.4.2 und XenDesktop 7.x und höher oder XenApp 6.5 und höher

> **Hinweis:**
>
> Andere tokenbasierte Authentifizierungslösungen können mit RADIUS konfiguriert werden. Informationen zur SafeWord-Tokenauthentifizierung finden Sie unter Configuring SafeWord Authentication.

Bereitstellen

January 11, 2019

Bereitstellen von Zugriffsinformationen für Endbenutzer von Android-Geräten

Sie müssen den Benutzern die Citrix Receiver-Kontoinformationen bereitstellen, die für den Zugriff auf die gehosteten Anwendungen, Desktops und Daten benötigt werden. Sie können diese Informationen folgendermaßen bereitstellen:

- Konfigurieren der Kontenermittlung mit der E-Mail-Adresse
- Bereitstellen einer Provisioningdatei für Benutzer

- Bereitstellen von Kontoinformationen zur benutzerseitigen manuellen Eingabe

Konfigurieren der e-mail-basierten Kontenermittlung

Sie können Citrix Receiver für die e-mail-basierte Kontenermittlung konfigurieren. Nach der Konfiguration geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration von Citrix Receiver ein. Citrix Receiver ermittelt den Access Gateway- oder StoreFront-Server, der der E-Mail-Adresse zugeordnet ist, auf der Basis von DNS-Dienstdatensätzen und fordert die Benutzer zur Anmeldung auf, sodass sie auf ihre gehosteten Anwendungen, Desktops und Daten zugreifen können.

> **Hinweis:**
>
> Die e-mail-basierte Kontenermittlung wird nicht unterstützt, wenn Citrix Receiver eine Verbindung zu einer Webinterface-Bereitstellung herstellt.

Bereitstellen einer Provisioningdatei für Benutzer

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

Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

Wenn Sie den Benutzern Kontoangaben für die manuelle Eingabe bereitstellen, stellen Sie sicher, dass die folgenden Informationen bereitgestellt werden, damit die Benutzer erfolgreich eine Verbindung zu den gehosteten Anwendungen und Desktops herstellen können:

- Die StoreFront-URL oder die XenApp Services-Site, z. B.: servername.company.com.
- Geben Sie für den Zugriff mit NetScaler Gateway die NetScaler Gateway-Adresse und die erforderliche Authentifizierungsmethode an.

  Weitere Informationen zur Konfiguration von NetScaler Gateway finden Sie in der NetScaler Gateway-Dokumentation.

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

Bereitstellen von RSA SecurID-Authentifizierung für iOS-Geräte

Wenn Sie NetScaler Gateway für die RSA SecurID-Authentifizierung konfigurieren, unterstützt Citrix Receiver den Modus “Nächster Token”. Wenn dieses Feature aktiviert ist und ein Benutzer drei (Standardwert) falsche Kennwörter eingibt, fordert das NetScaler Gateway Plug-In den Benutzer auf, so lange mit der Anmeldung zu warten, bis das nächste Token aktiv ist. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers, der sich zu oft mit einem falschen Kennwort anmeldet, deaktiviert wird.

Anweisungen zum Konfigurieren der Authentifizierung finden Sie unter Authentication and Authorization.

> **Tipp**
>
> RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen nicht unterstützt. Wenn Sie RSA SecurID verwenden möchten, verwenden Sie das NetScaler Gateway.

Installieren von RSA SecurID-Softwaretoken

Eine RSA SecurID-Softwareauthentifikatordatei hat eine SDTID-Dateierweiterung. Konvertieren Sie die SDTID-Datei mit dem RSA SecurID-Softwaretoken-Konvertierungsprogramm in eine numerische Zeichenfolge mit 81 Stellen im XML-Format. Die aktuelle Software und weitere Informationen finden Sie auf der RSA-Website.

Führen Sie diese allgemeinen Schritte aus:

1. Laden Sie das Konvertierungstool von diesem Link auf einen Computer (nicht ein Mobilgerät) herunter. Folgen Sie den Anweisungen auf der Website und in der Readmedatei, die Teil des Konvertierungstools ist.
2. Fügen Sie die konvertierte numerische Zeichenfolge in eine E-Mail ein und senden Sie sie an die Benutzergeräte.
3. Stellen Sie auf dem Mobilgerät sicher, dass das Datum und die Uhrzeit richtig sind, da sie für die Authentifizierung benötigt werden.
4. Öffnen Sie die E-Mail auf dem Mobilgerät und klicken Sie auf die Zeichenfolge, um das Softwaretoken zu importieren.

Nach der Installation des Softwaretokens auf dem Gerät wird eine neue Option auf der Registerkarte “Einstellungen” angezeigt, mit der Sie das Token verwalten können.

> **Hinweis:**
>
> Für Mobilgeräte, die die SDTID-Datei nicht mit Receiver assoziieren, ändern Sie die Dateinamenerweiterung zu .xml und importieren Sie sie dann.

Speichern von Kennwörtern

In der Citrix Webinterface-Verwaltungskonsole konfigurieren Sie die Authentifizierungsmethode, damit Benutzer ihre Kennwörter speichern können. Wenn Sie das Benutzerkonto konfigurieren, wird das verschlüsselte Kennwort gespeichert, bis der Benutzer das erste Mal eine Verbindung herstellt.

- Wenn Sie das Speichern des Kennworts aktivieren, speichert Citrix Receiver das Kennwort für zukünftige Anmeldungen auf dem Gerät und fordert nicht zur Kennworteingabe auf, wenn Benutzer eine Verbindung zu Anwendungen herstellen.

> **Hinweis:**
>
> Das Kennwort wird nur gespeichert, wenn Benutzer beim Erstellen eines Kontos ein Kennwort eingeben. Wenn kein Kennwort für das Konto eingegeben wird, wird kein Kennwort gespeichert, unabhängig von der Servereinstellung.

- Wenn Sie das Speichern des Kennworts deaktivieren (Standardeinstellung), fordert Citrix Receiver Benutzer jedes Mal zur Kennworteingabe auf, wenn sie eine Verbindung herstellen.

> **Hinweis:**
>
> Für direkte StoreFront-Verbindungen können Kennwörter nicht gespeichert werden.

Überschreiben der Kennwortspeicherung

Wenn der Server Kennwörter speichert, können Benutzer, die eine Kennworteingabe bei der Anmeldung bevorzugen, das Speichern des Kennworts überschreiben:

- Machen Sie beim Erstellen des Kontos keine Eingabe in das Feld “Kennwort”.
- Löschen Sie beim Bearbeiten eines Kontos das Kennwort und speichern Sie das Konto.

Konfiguration

October 5, 2018

Bereitstellen von Zugriff auf virtuelle Apps und Desktops

Citrix Receiver erfordert die Konfiguration von Webinterface oder StoreFront zum Bereitstellen von Apps und Desktops mit der XenApp- oder XenDesktop-Bereitstellung.

Webinterface

Es gibt zwei Typen der Webinterface-Sites: XenApp Services-Sites (früher Program Neighborhood Services) und XenApp Websites. Mit Webinterface-Sites können Benutzergeräte eine Verbindung mit der Serverfarm herstellen.

StoreFront

Sie können StoreFront für die Authentifizierungs- und Ressourcenbereitstellungsdienste für Citrix Receiver konfigurieren. Dann können Sie zentralisierte Unternehmensstores erstellen, die das Bereitstellen von Desktops, Anwendungen und anderen Ressourcen über XenApp und XenDesktop sowie das Bereitstellen mobiler Worx-Apps und mit XenMobile für Ihr Unternehmen vorbereiteter mobiler Apps für Benutzer ermöglichen.

Die Authentifizierung zwischen Citrix Receiver und einer Webinterface-Site oder einem StoreFront-Store kann auf verschiedene Weise erfolgen:

- Benutzer innerhalb der Firewall können eine direkte Verbindung mit dem Webinterface oder StoreFront herstellen.
- Benutzer außerhalb der Firewall können eine Verbindung mit StoreFront oder mit dem Webinterface über NetScaler Gateway herstellen.
- Benutzer außerhalb der Firewall können eine Verbindung mit StoreFront über NetScaler Gateway herstellen.

Verbindung über NetScaler Gateway

NetScaler Gateway 10 und 11 werden von Citrix Receiver für Android für den Zugriff auf Folgendes unterstützt:

- Webinterface 5.4, XenApp Services-Sites und XenApp Web-Sites
- StoreFront-Stores Versionen 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 und 3.11

Sowohl Einquellen- als auch Zweiquellenauthentifizierung wird für Webinterface-Sites und StoreFront unterstützt.

Sie können mehrere Sitzungsrichtlinien auf demselben virtuellen Server erstellen, abhängig vom Typ der Verbindung (z. B. ICA, CVPN oder VPN) und vom Typ von Receiver (Web Receiver oder lokal installierte Citrix Receiver-Instanzen). Alle Richtlinien können auf einem virtuellen Server erstellt werden.

Wenn Benutzer Konten in Citrix Receiver erstellen, sollten sie die Kontoanmeldeinformationen, z. B. die E-Mail-Adresse oder den entsprechenden FQDN des NetScaler Gateway-Servers eingeben. Wenn die Verbindung beispielsweise bei der Verwendung des Standardpfads fehlschlägt, sollten Benutzer den vollständigen Pfad zum NetScaler Gateway-Server eingeben.

Verbinden mit XenMobile

Damit Remotebenutzer sich über NetScaler Gateway mit der XenMobile-Bereitstellung verbinden können, können Sie NetScaler Gateway für App Controller oder StoreFront (Komponenten von XenMobile) konfigurieren. Die Methode für das Aktivieren des Zugriffs hängt von der in der Bereitstellung verwendeten XenMobile-Edition ab:

Aktivieren von Zugriff auf XenMobile 9:

Clientzertifikatauthentifizierung

Aktivieren von Zugriff auf XenMobile 10:

NetScaler Gateway und XenMobile

Wenn Sie XenMobile im Netzwerk bereitstellen, lassen Sie Verbindungen von Remotebenutzern mit App Controller zu, indem Sie XenMobile und App Controller integrieren. In dieser Bereitstellung verbinden sich Benutzer mit App Controller, um die Web-, SaaS- und Mobilanwendungen zu erhalten und von ShareFile aus auf Dokumente zuzugreifen. Benutzer stellen eine Verbindung entweder über Citrix Receiver oder das NetScaler Gateway Plug-In her.

Wenn Sie XenMobile im Netzwerk bereitstellen, lassen Sie Verbindungen von internen oder Remotebenutzern mit StoreFront über NetScaler Gateway zu, indem Sie NetScaler Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf von XenApp veröffentlichte Anwendungen und auf von XenDesktop virtualisierte Desktops zu. Benutzer stellen eine Verbindung über Citrix Receiver her.

Sie müssen Windows-Apps und benutzerdefinierte Apps, die Sie Ihren Benutzern bereitstellen, mit dem MDX Toolkit umschließen. Weitere Informationen finden Sie hier:

MDX Toolkit

Verbinden mit StoreFront

Citrix Receiver für Android unterstützt das Starten von Sitzungen über Receiver für Web, sofern der verwendete Browser mit Receiver für Web funktioniert. Erfolgen keine Sitzungsstarts, konfigurieren Sie Ihr Konto direkt über Citrix Receiver für Android.

> **Tipp**
>
> Wenn Citrix Receiver für Web über einen Browser verwendet wird, werden Sitzungen nicht automatisch gestartet, wenn Sie eine ICA-Datei herunterladen. Die ICA-Datei muss nach dem Herunterladen manuell geöffnet werden, damit die Sitzung gestartet wird.

Mit Receiver StoreFront bestehen die erstellten Stores aus Diensten, die eine Authentifizierungs- und Ressourcenbereitstellungsinfrastruktur für Citrix Receiver bereitstellen. Erstellen Sie Stores, die Desk-

tops und Anwendungen von XenDesktop-Sites und XenApp-Farmen auflisten und aggregieren und diese Ressourcen Benutzern zur Verfügung stellen.

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

Stores für StoreFront konfigurieren Sie genauso wie für andere XenApp- und XenDesktop-Anwendungen. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich. Verwenden Sie für Mobilgeräte eine dieser Methoden:

Provisioningdateien:Sie können Benutzern Provisioningdateien (.cr) bereitstellen, die Verbindungsdetails für die Stores enthalten. Nach der Installation öffnen Benutzer die Datei auf dem Gerät, um Citrix Receiver automatisch zu konfigurieren. Receiver für Web-Sites bieten Benutzern standardmäßig eine Provisioningdatei für den einen Store, für den die Site konfiguriert ist. Alternativ können Sie mit der Citrix StoreFront-Verwaltungskonsole Provisioningdateien für einen oder mehrere Stores generieren und manuell an die Benutzer verteilen.

Manuelle Konfiguration:Sie können Benutzern die Informationen zur erforderlichen NetScaler Gateway- oder Store-URL, mit der sie auf ihre Desktops und Anwendungen zugreifen können, direkt mitteilen. Für Verbindungen über NetScaler Gateway benötigen Benutzer außerdem die Produktedition und erforderliche Authentifizierungsmethode. Nach der Installation geben Benutzer diese Informationen in Citrix Receiver ein. Citrix Receiver fordert die Benutzer auf, sich anzumelden, falls die Verbindung erfolgreich überprüft werden konnte.

Konfigurieren von Citrix Receiver für den Zugriff auf Anwendungen:

Geben Sie beim Erstellen eines neuen Kontos im Feld Adresse die entsprechende URL des Stores ein, z. B. storefront.organization.com.

Geben Sie die restlichen Felder ein und wählen Sie die NetScaler Gateway-Authentifizierungsmethode, z. B. Aktivieren des Sicherheitstokens, Auswählen des Authentifizierungstyps und Speichern der Einstellungen.

Beim Hinzufügen eines Kontos mit einer automatischen Konfiguration können Sie den FQDN eines StoreFront-Servers oder von NetScaler eingeben oder Sie verwenden alternativ eine E-Mail-Adresse zum Erstellen eines neuen Kontos. Sie werden dann aufgefordert, zur Anmeldung Ihre Anmeldeinformationen einzugeben.

Weitere Informationen:

Weitere Informationen zum Konfigurieren von Zugriff auf StoreFront über NetScaler Gateway finden Sie unter folgenden Links:

Verwalten des Zugriffs auf StoreFront über NetScaler Gateway

Integrieren von StoreFront mit NetScaler Gateway

Verbinden mit dem Webinterface

Citrix Receiver kann Anwendungen über die Webinterface-Site starten. Konfigurieren Sie die Webinterface-Site genau so, wie Sie sie für andere XenApp- und XenDesktop-Apps und Desktops konfigurieren würden. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich.

Citrix Receiver unterstützt nur die Webinterface-Version 5.4. Benutzer können Anwendungen auch vom Webinterface 5.4 mit dem Firefox-Mobilbrowser starten.

Starten von Anwendungen auf dem Android-Gerät

Benutzer melden sich vom Mobilgerät mit Ihren normalen Anmeldeinformationen und dem Kennwort an der Webinterface-Site an.

Weitere Informationen zum Konfigurieren von Webinterface-Sites finden Sie unter folgenden Links:

Konfigurieren des Webinterface

Tastaturlayoutsynchronisierung

Um die Tastaturlayoutsynchronisierung zu aktivieren, gehen Sie in Citrix Receiver für Android zu “Einstellungen” und aktivieren Sie **Client-IME**.

Hinweise:

- Der VDA muss Version 7.16 oder höher sein.
- Administratoren müssen die erweiterte Unterstützung für asiatische Sprachen im VDA aktivieren. Standardmäßig ist das Feature aktiviert. Auf einem Windows Server 2016 VDA müssen Sie jedoch einen neuen Schlüssel mit der Bezeichnung DisableKeyboardSync hinzufügen und in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme den Wert auf 0 setzen, um das Feature zu aktivieren.
- Administratoren müssen die Unicode-Tastaturlayoutzuordnung auf dem VDA aktivieren. Standardmäßig ist das Feature deaktiviert. Um es zu aktivieren, erstellen Sie unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme den Schlüssel CtxKlMap und legen Sie unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap den DWORD-Wert EnableKlMap auf 1 fest.

Einschränkungen:

- Dieses Feature funktioniert nur auf den Bildschirmtastaturen von Geräten, nicht auf externen Tastaturen.
- Bestimmte mobile Geräte, z. B. das Nexus 5x, unterstützen möglicherweise die Tastaturlayoutsynchronisierung nicht vollständig.
- Das Tastaturlayout kann nur vom Client zum Server synchronisiert werden. Wenn Sie das serverseitige Tastaturlayout ändern, kann das Tastaturlayout des Clients nicht geändert werden.

- Wenn Sie für das Clienttastaturlayout ein nicht kompatibles Layout wählen, wird das Layout möglicherweise auf dem VDA synchronisiert, die Funktionalität kann jedoch nicht bestätigt werden.
- Bei Remoteanwendungen, die mit erhöhten Rechten ausgeführt werden (z. B. wenn Sie Anwendungen als Administrator ausführen), kann keine Synchronisierung mit dem Clienttastaturlayout erfolgen. Um dieses Problem zu umgehen, ändern Sie das Tastaturlayout manuell auf dem VDA oder deaktivieren Sie die Benutzerkontensteuerung (UAC).

Aktivieren der Smartcardunterstützung

Receiver für Android für Mobilgeräte unterstützt Bluetooth-Smartcardleser mit StoreFront, einer Webinterface-Site und einer PNA-Site. Wenn die Smartcardunterstützung aktiviert ist, können Sie Smartcards zu folgenden Zwecken einsetzen:

- Smartcard-Anmeldeauthentifizierung: Verwendung von Smartcards zur Authentifizierung von Benutzern an Receiver.
- Smartcard-Anwendungsunterstützung: Zugriff auf lokale Smartcardgeräte über smartcardfähige veröffentlichte Anwendungen.
- Signieren von Dokumenten und E-Mails. Anwendungen, wie Microsoft Word und Outlook, die in ICA-Sitzungen gestartet werden, können auf Smartcards auf dem Mobilgerät für die Signatur von Dokumenten und E-Mail zugreifen.

Unterstützte Smartcards:

- PIV-Karten
- Common Access Cards

Konfigurieren der Smartcardunterstützung auf dem Gerät

1. Sie müssen die Smartcard mit dem Mobilgerät koppeln. Weitere Informationen zum Koppeln von Smartcardlesern mit dem Gerät finden Sie in den technischen Daten des Smartcardlesers.

   Für die Smartcardunterstützung für Android-Geräte bestehen die folgenden Voraussetzungen und Einschränkungen:

   - Receiver unterstützt dieses Feature auf allen Android-Geräten, die von der Biometric Associates Middleware aufgeführt sind.
   - Einige Benutzer haben ggf. eine globale PIN für Smartcards. Wenn sich Benutzer jedoch an einem Smartcardkonto anmelden, sollten sie die PIV-PIN und nicht die globale Smartcard-PIN eingeben. Dies ist ein Drittanbieterproblem.
   - Die Smartcardauthentifizierung kann langsamer als die Kennwortauthentifizierung sein. Beispiel: Warten Sie nach dem Trennen einer Sitzung ca. 30 Sekunden, bevor Sie eine

Wiederverbindung versuchen. Bei einer zu schnellen Wiederverbindung mit einer getrennten Sitzung kann Receiver fehlschlagen.

- Die Smartcardauthentifizierung wird nicht für den browserbasierten Zugriff oder von einer XenApp-Site unterstützt.

2. Installieren Sie den Android PC/SC-Lite-Dienst auf dem Android-Gerät, bevor Sie ein smartcardfähiges Konto hinzufügen. Dieser Dienst ist als APK-Datei im baiMobile SDK verfügbar.

   Für Android kann die Datei PC/SC-Lite.apk aus dem Google Play Store heruntergeladen werden.

3. Wählen Sie in Receiver das Symbol “Einstellungen” aus und tippen Sie dann auf **Konten** und dann auf **Konto hinzufügen** oder bearbeiten Sie ein vorhandenes Konto.
4. Konfigurieren Sie die Verbindung und aktivieren Sie die Option “Smartcard”.

Installieren von Citrix Receiver auf einer SD-Karte

Citrix Receiver für Android wurde für die lokale Installation auf Benutzergeräten optimiert. Wenn die Geräte jedoch nicht ausreichend freien Speicherplatz haben, können Sie Receiver auf einer externen SD-Karte installieren und auf dem Gerät bereitstellen, um veröffentlichte Anwendungen auf den Mobilgeräten zu starten. Dies wird standardmäßig unterstützt und eine zusätzliche Konfiguration ist nicht erforderlich.

Zum Starten einer Anwendung mit der SD-Karte wählen Benutzer die App aus der Liste der Receiver-Apps auf dem Benutzergerät aus und wählen dann Zu SD-Karte verschieben.

Wenn Benutzer Receiver auf einer externen SD-Karte installieren, um Anwendungen zu starten, bestehen die folgenden Probleme:

- Wenn eine SD-Karte zusätzlich zu einem USB-Speichergerät auf dem Mobilgerät bereitgestellt wird, ist die SD-Karte nicht mehr verfügbar; ausgeführte Apps werden angehalten, wenn das USB-Gerät bereitgestellt wird.
- Einige AppWidgets (z. B. die Homebildschirm-Widgets) sind nicht verfügbar, wenn eine App von der SD-Karte ausgeführt wird. Wenn die Bereitstellung der SD-Karte aufgehoben wird, müssen die Benutzer die AppWidgets neu starten.

Wenn Benutzer Receiver lokal auf dem Benutzergerät installieren, können sie Receiver bei Bedarf auf die SD-Karte verschieben.

Zugreifen auf Dateien mit Dateitypzuordnung

Als Voraussetzung für dieses Feature müssen Sie in den Einstellungen von Receiver für Android die Option **Gerätespeicher verwenden** auf **Vollzugriff** festlegen.

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

Wählen Sie auf dem Benutzergerät die Datei, die Sie starten möchten, im Datei-Explorer aus und klicken Sie auf “Öffnen”. Das Android-Betriebssystem bietet eine Option zum Starten der Datei mit Receiver für Android (wobei die vom Administrator konfigurierte Dateitypzuordnung angewendet wird) oder mit einer anderen Anwendung. Abhängig von Ihrer zuvor getroffenen Auswahl ist u. U. eine Standardanwendung festgelegt. Sie können die Standardanwendung mit der Option “Standard ändern” ändern.

> **Hinweis:**
>
> Dieses Feature ist nur für StoreFront verfügbar und erfordert XenApp und XenDesktop Version 7 oder höher.

Einschränkung

- Mit dem Dateitypzuordnungsfeature können Sie nur auf MIME-Dateiformate zugreifen, die von Microsoft Office-, Adobe Acrobat Reader- und Editor-Anwendungen unterstützt werden.

Aktivieren des Citrix Ready Workspace Hubs

October 4, 2018

Der Citrix Ready Workspace Hub ist in Citrix Receiver für Android standardmäßig deaktiviert. Führen Sie folgende Schritte aus, um den Hub mit einem Android-Gerät zu verwenden.

Gerätevoraussetzungen:

- Citrix Receiver für Android 3.13.5 oder höher installiert
- Bluetooth aktiviert (für Proximityauthentifizierung)
- Mobilgerät und Workspace Hub verwenden dasselbe WLAN-Netzwerk

Proximityauthentifizierung ermöglicht die automatische Authentifizierung von Benutzern und den Start einer Sitzung.

1. Für die Proximityauthentifizierung aktivieren Sie Bluetooth auf dem mobilen Gerät, um sicherzustellen, dass das Kontrollkästchen “Kontotyp als Webinterface hinzufügen” beim Einrichten des Citrix Receiver-Kontos nicht aktiviert ist.
2. Wechseln Sie in Citrix Receiver zu **Einstellungen** und wählen Sie **Workspace Hub verwenden**.

3. Klicken Sie auf **Konfiguration**, um die Seite für die Konfiguration aufzurufen.

Berührungsloser Modus ist ein Schalter, mit dem Sie die Proximityauthentifizierung aktivieren oder deaktivieren. Wenn der berührungslose Modus deaktiviert ist, ist Proximityauthentifizierung nicht verfügbar. Die anderen Funktionen des Citrix Ready Workspace Hubs stehen jedoch zur Verfügung. Für den berührungslosen Modus sollte Bluetooth auf dem Gerät aktiviert sein.

RSSI repräsentiert die Bluetooth-Signalstärke relativ zum Abstand zwischen dem mobilen Gerät und dem Hub. Eingangs-RSSI ist die Reichweite, innerhalb der Workspace Hub-Beacons erkannt werden. Ausgangs-RSSI ist der Anfang der Reichweite, außerhalb der das mobile Gerät nicht mehr mit dem Workspace Hub kommuniziert. Ausgangs-RSSI muss gleich oder kleiner als Eingangs-RSSI sein und die Werte müssen negativ sein. Die Standardwerte sind -40 (Eingangs-RSSI) bzw. -70 (Ausgangs-RSSI). Sie können diese Werte abhängig von Ihrer Umgebung und Ihrer Entfernung zum Workspace Hub anpassen.

Wenn Ihr Mobilgerät in Reichweite 1 ist, wird die Proximityauthentifizierung ausgelöst und Ihr Standarddesktop bzw. Ihre Standard-App wird automatisch auf dem Workspace Hub gestartet (siehe unten). Solange das Mobilgerät sich in Reichweite 1 oder 2 befindet, wird der Standarddesktop bzw. die Standard-App weiter auf dem Workspace Hub ausgeführt. Wenn das Gerät nicht mehr in Reichweite 1 und 2 ist, wird der Desktop bzw. die App automatisch geschlossen.

Bevorzugte Ressource ist der Standarddesktop bzw. die Standard-App, der/die gestartet wird, wenn das Mobilgerät in Reichweite für die Proximityauthentifizierung ist. Diese Einstellung ist spezifisch für das Konto, das für die Anmeldung an Citrix Receiver verwendet wird. Wenn Sie mehrere Konten haben, müssen Sie für jedes Konto eine bevorzugte Ressource festlegen. Diese Einstellung ist persistent, d. h. Sie müssen Ihre bevorzugte Ressource nur einmal pro Konto festlegen. Nachdem Sie die Einstellung vorgenommen haben, wird Ihre bevorzugte Ressource jedes Mal gestartet, wenn Sie in Reichweite für Proximityauthentifizierung sind, bis Sie die Einstellung ändern.

Problembehandlung

August 31, 2018

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

Citrix Receiver für Android hat eine strenge Validierungsrichtlinie für Serverzertifikate.

> **Wichtig**
>
> Bestätigen Sie vor der Installation dieser Version von Citrix Receiver für Android, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender

> Ursachen können Verbindungen fehlschlagen:
>
> - Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
> - Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
> - Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
> - Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet Citrix Receiver für Android jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases von Citrix Receiver für Android wird dann auch überprüft, ob die Zertifikate vertrauenswürdig sind.Wenn nicht alle Zertifikate vertrauenswürdig sind, schlägt die Verbindung fehl.

Diese Richtlinie ist strenger als die Zertifikatrichtlinie in Webbrowsern.Viele Webbrowser enthalten eine große Anzahl Stammzertifikate, denen sie vertrauen.

Der Server bzw. das Gateway muss mit den richtigen Zertifikaten konfiguriert sein.Sind nicht die richtigen Zertifikate vorhanden, schlägt die Verbindung von Citrix Receiver für Android u. U. fehl.

Angenommen, ein Gateway ist mit gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen. Dabei wird genau ermittelt, welches Stammzertifikat Citrix Receiver für Android verwendet:

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

Citrix Receiver für Android überprüft, ob alle Zertifikate gültig sind.Citrix Receiver für Android überprüft ebenfalls, ob dem “Beispielstammzertifikat” bereits vertraut wird. Wenn Citrix Receiver für Android dem “Beispielstammzertifikat” nicht vertraut, schlägt die Verbindung fehl.

> **Wichtig**
>
> Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet. Beispielsweise gibt es derzeit zwei Zertifikate (“DigiCert”/”GTE CyberTrust Global Root” und “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”), mit denen die gleichen Serverzertifikate validiert werden können. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar (“DigiCert Baltimore Root”/”Baltimore CyberTrust Root”). Wenn Sie “GTE CyberTrust Global Root” auf dem Gateway konfigurieren, schlagen Citrix Receiver für Android-Verbindungen auf diesen Benutzergeräten fehl.Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist.Beachten Sie außerdem, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.

> **Hinweis**
>
> Einige Server und Gateways senden nie das Stammzertifikat, selbst wenn es konfiguriert ist. Ein strengere Validierung ist dann nicht möglich.

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

Citrix Receiver für Android verwendet dann die beiden Zertifikate. Dann sucht Receiver nach einem Stammzertifikat auf dem Benutzergerät.Wenn er ein gültiges findet, das auch vertrauenswürdig ist (z. B. "Beispielstammzertifikat"), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt das von Citrix Receiver für Android benötigte Zwischenzertifikat zur Verfügung und ermöglicht Citrix Receiver für Android die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"
- "Falsches Stammzertifikat"

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Citrix Receiver für Android ignoriert das falsche Stammzertifikat jedoch nicht und die Verbindung schlägt fehl.

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat 1"
- "Beispielzwischenzertifikat 2"

> **Wichtig**
>
> Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat.Dies ist für Situationen vorgesehen, wenn mehr als ein Stammzertifikat vorhanden ist und ein früher ausgestelltes Stammzertifikat zur gleichen Zeit wie ein später ausgestelltes Stammzertifikat verwendet wird.In diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden.Beispielsweise hat das früher ausgestellte Stammzertifikat "Class 3 Public Primary Certification Authority" das entsprechende übergreifende Zwischenzertifikat "VeriSign Class 3 Public Primary Certification Authority - G5".Ein entsprechendes später ausgestelltes Stammzertifikat "VeriSign Class 3 Public Primary Certification Authority - G5" ist ebenfalls verfügbar und es ersetzt "Class 3 Public Primary Certification Authority". Das später ausgestellte Stammzertifikat verwendet kein

> übergreifendes Zwischenzertifikat.
>
> **Hinweis**
>
> Das übergreifende Zwischenzertifikat und das Stammzertifikat haben den gleichen Antragstellernamen (Ausgestellt an), aber das übergreifende Zwischenzertifikat hat einen anderen Ausstellernamen (Ausgestellt durch). Dadurch unterscheidet sich das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat wie “Beispielzwischenzertifikat 2”.

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

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”

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

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

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

- “Beispielserverzertifikat”

In diesem Fall schlägt die Verbindung fehl, wenn Citrix Receiver für Android nicht alle Zwischenzertifikate finden kann.

SDK und API

August 31, 2018

Citrix Virtual Channel SDK

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

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver AIDL-Schnittstellen **IVCService.aidl** und **IVCCallback.aidl** werden mit den Funktionen des virtuellen Kanals im Citrix Server API SDK (WFAPI-SDKS) verwendet, um neue virtuelle Kanäle zu erstellen.
- Eine Hilfsklasse **Marshall.java** wurde entwickelt, um Ihnen das Schreiben Ihrer eigenen virtuellen Kanäle zu erleichtern.
- Funktionierender Quellcode für drei 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 Android.

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