Info zu Citrix Receiver für Android 3.7.x

Oct 02, 2015

Neue Funktionen in Citrix Receiver für Android 3.7.3

Citrix Receiver für Android 3.7.3 ist die aktuelle Version auf Google Play. Benutzer, die Vorversionen ausführen, sollten auf die aktuelle Version aktualisieren.

Citrix Receiver für Android 3.7.3 unterstützt Android M (6.0).

In 3.7.3 behobene Probleme

In Citrix Receiver für Android 3.7.3 wurden sporadische Abstürze bei der Verwendung von Citrix Receiver mit Nexus 9 Bluetooth behoben.

Neue Funktionen in Citrix Receiver für Android 3.7

Dieses Update umfasst Folgendes:

- **Anpassung an Anzeige**: Beim Veröffentlichen einer App mit einer bestimmten Auflösung zeigt Receiver die App nun in einem zentralen Bereich an und skaliert die Anzeige abhängig vom Seitenverhältnis. Die Beziehung zwischen dem Ursprung (App) und dem Ziel (der Anzeige) wird dabei richtig interpretiert.
- **Verbesserte Unterstützung für die Spiegelung der Sitzungsanzeige**: Receiver für Android sorgt durch Anpassen der Anzeigecharakteristiken zwischen der Bildschirmanzeige und dem Android-Gerät für mehr Benutzerfreundlichkeit.
- **Unterstützung für Transport Layer Security (TLS)**: Receiver für Android unterstützt die Protokolle TLS 1.1 und TLS 1.2. Bei Aktivierung gewährleistet TLS die sichere Kommunikation zwischen Server und Client. Diese Funktionalität kann über die Benutzeroberfläche oder mit der Datei **receiverconfig** konfiguriert werden.
- Unterstützung für das Ausblenden der sitzungsinternen Menüleiste für Geräte, auf denen kein Touchscreen unterstützt wird.
- Verbesserte Tastaturhandhabung für das koreanische Hangul-Alphabet.

Bekannte Probleme

Die folgenden Probleme und Einschränkungen sind für dieses Release von Receiver für Android bekannt:

- Im vorherigen Release wurde eingeschränkte Unterstützung für die Spiegelung der Sitzungsanzeige auf einem zweiten Bildschirm geboten. Es wurden nur Geräte unterstützt, deren Auflösung mit der Auflösung des Android-Geräts übereinstimmte. Für dieses Release von Receiver für Android wurde diese Beschränkung aufgehoben. Anzeigegeräte, deren Auflösung von der des Android-Geräts abweicht, werden unterstützt. Es gibt jedoch folgende Einschränkungen: [#549471]
  - Die Sitzungsgröße wird von der natürlichen Auflösung des angeschlossenen Anzeigegeräts bestimmt. Alle anderen Einstellungen werden ignoriert, da die sekundäre Anzeige das Sitzungsbild nicht skalieren kann. Darüber hinaus werden Anfragen zur dynamischen Anpassung der Sitzungsauflösung an die Auflösung einer angeschlossenen Anzeige werden nur teilweise unterstützt. In solchen Umgebungen ermöglicht das Anschließen und Trennen einer sekundären Anzeige nicht das Anfordern einer Größenänderung entsprechend den normalen Benutzereinstellungen.
  - Beim Trennen einer zweiten Anzeige kann es zu Instabilität und zum Absturz von Receiver kommen. Beim Verwenden einer zweiten Anzeige empfiehlt es sich, die Anzeige vor dem Start einer Sitzung an das Android-Gerät anzuschließen.
  - Die Anzeigeleistung der angeschlossenen Anzeige kann beeinträchtigt werden. Auf der angeschlossenen Anzeige können u. U. Anzeigefehler auftreten, wie die fehlerhafte Anzeige des Mauszeigers und Verzögerungen beim

Verschieben von Fenstern.

- Einige Einschränkungen gelten für die auf der primären Anzeige des Android-Geräts angezeigten Benutzeroberfläche. Beispielsweise funktioniert die Maus entsprechend den Bildschirmabmessungen des Geräts und nicht entsprechend den Abmessungen sekundärer Anzeigen. Darüber hinaus wird auf der Geräteanzeige keine Symbolleiste angezeigt, wenn die Anzeigespiegelung aktiviert ist. [#549471]

- Wenn eine sekundäre Anzeige angeschlossen wird, ist die Bildschirmauflösung der neu angeschlossenen Anzeige dieselbe wie die des Geräts. Dieses Problem tritt auf, wenn das angeschlossene Gerät nach der Initiierung der Sitzung an eine Dockingstation angeschlossen wird und die Maus nicht an die Dockingstation angeschlossen ist. Sie lösen das Problem, indem Sie die Maus für die zweite Sitzung anschließen und so die richtige Auflösung wieder herstellen. Dieses Problem bezieht sich auf die Samsung Galaxy Note II Multimedia-Dockingstation. [#541028]
- Beim Entfernen der Maus aus einer Sitzung, die initiiert wurde, während das Gerät an eine Dockingstation angeschlossen war, wird die Anzeige auf dem Gerät um 90 Grad im Uhrzeigersinn gedreht. Die Ausrichtung der Sitzung normalisiert sich nach kurzer Zeit. Dieses Problem bezieht sich auf die Samsung Galaxy Note II Multimedia-Dockingstation. [#541032]
- Beim Spiegeln der Anzeige auf einen externen Bildschirm mit einem AllCast-Dongle ist bei der Wiedergabe von Mediendateien kein Audio hörbar. Dieses Problem hängt mit der Funktionalität des Anzeigegeräts zusammen. Wenn ein Fernsehgerät mit Lautsprechern verwendet wird, findet die Audioausgabe über das Fernsehgerät statt. Bei einem Bildschirm ohne Lautsprecher sollten die Lautsprecher des Android-Geräts verwendet werden. Dies passiert jedoch nicht. [#544330]
- Wenn die Lupe an den äußersten Rand der Sitzung verschoben wird, zeigt die Lupe u. U. einen Teil des unvergrößerten Hintergrundbilds an. [#542299]
- In einigen Fällen kann das Schließen einer Sitzung zu einer Laufzeitausnahme führen. [#523824]
- Der maximale Vergrößerungsgrad bleibt nach der Drehung des Bildschirms nicht erhalten. Dieses Verhalten kann nach dem Start einer Sitzung auftreten, wenn Sie durch Zusammenführen der Finger die gewünschte Ansicht hergestellt haben und dann das Gerät um 90 Grad drehen. Wenn Sie das Gerät ein zweites Mal drehen, bleibt der zuvor hergestellte Vergrößerungsgrad nicht erhalten. [#538638]
- Die erweiterte Tastatur wird unter bestimmten Bedingungen fälschlicherweise aktiviert. Dies tritt u. U. auf, wenn das Spiegeln der Anzeige gestoppt und das Gerät gedreht wird oder wenn der Gerätebildschirm bei aktivierter Anzeigespiegelung berührt wird. Der Grund hierfür ist möglicherweise, dass das Android-Gerät nicht erkennen kann, ob die Bildschirmtastatur angezeigt wird. Beim Aktivieren des Spiegelungsmodus durch Anschließen eines weiteren Bildschirms wird die Anzeige der erweiterten Tastatur falsch interpretiert. [#545231]
- Die Kontoerstellung schlägt auf ASUS Nexus 7-Geräten mit Android-Version 4.1.1 fehl. Aktualisieren Sie das Gerät auf die aktuelle Android-Software, z. B. 4.2.2, um dieses Problem zu vermeiden.
- Auf einigen Android-Geräten löst das Klicken mit der rechten Maustaste einer Bluetooth-Maus die Aktion "Zurück" aus und das Dialogfeld "Beenden" wird versehentlich angezeigt. Dieses Problem tritt nur auf Geräten mit Firmware auf, die das Klicken mit der rechten Maustaste nicht unterstützen. [#331168]
- In Receiver für Android 3.5 wird das Feature "Full VPN Tunnel" nicht zusammen mit Smartcardauthentifizierung unterstützt. [#456657]
- Wenn Sie eine Verbindung mit einem FIPS NetScaler herstellen, während die Richtlinie "denysslreneg" deaktiviert ist oder Frontend Client und "Clientauthentifizierung" auf "Optional" festgelegt sind, kann beim Anmelden an Receiver der folgende Fehler auftreten.
  - Wenn Sie sich bei Receiver anmelden und "Domäne\Benutzername" im Feld "Benutzername" eingeben, erhalten Sie möglicherweise die Meldung, dass Benutzername oder Kennwort falsch waren. Mit dieser Meldung wird "Domäne\Domäne\Benutzername" im Feld "Benutzername" angezeigt. Sie lösen das Problem, indem Sie einen der Domänennamen entfernen und sich mit dem Format "Domäne|Benutzername" anmelden. [#466022]

Systemanforderungen für Receiver für Android 3.7.x

Oct 02, 2015

Gerät

- Citrix Receiver für Android 3.7.3 unterstützt die Android-Versionen 4, 5 und 6 (Android M).
- Citrix Receiver für Android 3.7, 3.7.1 und 3.7.2 unterstützt die Android-Versionen 4 und 5.
- Aktualisieren Sie die Android-Geräte auf die aktuelle Android-Software, um die besten Ergebnisse zu erhalten.
- 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 Receiver für Android.
- Wenn eine Technology Preview-Version von Citrix Receiver installiert ist, deinstallieren Sie sie, bevor Sie die neue Version installieren.

Wichtig: Weitere Informationen zum Sichern der Verbindungen mit Ihrer Citrix Umgebung finden Sie im Abschnitt **Verbindungen** (unten).

Server

Für Verbindungen mit virtuellen Desktops und Apps unterstützt Citrix Receiver Citrix StoreFront und das Webinterface.
StoreFront:

- StoreFront 3.0 (empfohlen)
  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 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.x
  - XenApp 6.5 für Windows Server 2008 R2
  - XenApp 6 für Windows Server 2008 R2
  - XenApp Fundamentals 6.0 für Windows Server 2008 R2
  - XenApp 5 für Windows Server 2008
  - XenApp 5 für Windows Server 2003
  - Citrix Presentation Server 4.5
  - XenDesktop 7.x
  - XenDesktop 7
  - XenDesktop 5, 5.5 und 5.6

Konnektivität

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

LAN-Verbindungen:

- StoreFront 2.x oder 2.6 (empfohlen), Webinterface 5.4 oder eine XenApp Services-Site (früher Program Neighborhood Agent).

Sichere Remoteverbindungen (eines der folgenden Produkte):

- Citrix NetScaler Gateway 10 (einschließlich Versionen von VPX, MPX und SDX)
- Citrix Access Gateway Enterprise Edition 9.x und 10.x (einschließlich Versionen von VPX, MPX und SDX)
  - CloudGateway wird nur ab Version 9.3 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; die Anwendung kann jedoch nicht gestartet werden.

Importieren von Stammzertifikaten auf Android-Geräten

Geräte mit Android 4.x unterstützen den Import von Stammzertifikaten ohne Rootzugriff auf dem Gerät. Android-Geräte vor 4.0 unterstützen nicht den automatischen Import von Stammzertifikaten.

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 das Access Gateway

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

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition

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

CTX124937: How to Configure Citrix Access Gateway Enterprise Edition 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 das Access Gateway.

Citrix Receiver unterstützt die Authentifizierung über das Access 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 (OTP)
- Smartcardauthentifizierung*

* Receiver für Android unterstützt jetzt die folgenden Produkte und Konfigurationen.
Hinweis: Die Smartcard-Authentifizierung an Webinterface-Sites wird nicht unterstützt.
Unterstützte Smartcardleser:

- BaiMobile 3000MP Bluetooth-Smartcardleser

Unterstützte Smartcards:

- PIV-Karten
- Common Access Cards

Unterstützte Konfigurationen:

- Smartcardauthentifizierung bei NetScaler Gateway ab StoreFront 2.x und XenDesktop 5.6 sowie ab XenApp 6.5
- Smartcardauthentifizierung bei NetScaler Gateway ab Webinterface 5.4.2 und XenDesktop 5.6 oder ab XenApp 6.5

Hinweis: Andere token-basierte Authentifizierungslösungen können mit RADIUS konfiguriert werden. Wenn Sie weitere Informationen zur SafeWord-Token-Authentifizierung benötigen, suchen Sie in eDocs nach "SafeWord-Authentifizierung konfigurieren" und lesen Sie die für Ihre Edition von Access Gateway relevanten Abschnitte.

Verwalten

Jun 20, 2013

Für Receiver muss das Webinterface für die Bereitstellung konfiguriert werden. 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. Die Authentifizierung zwischen Receiver und einer Webinterface-Site kann mit mehreren Lösungen erfolgen, die in diesem Abschnitt beschrieben sind.

Außerdem können Sie StoreFront für die Authentifizierungs- und Ressourcenbereitstellungsdienste für Receiver konfigurieren; Sie können dann zentralisierte Unternehmensstores erstellen, die Desktops, Anwendungen und anderen Ressourcen den Benutzern bereitstellen.

Weitere Informationen über das Konfigurieren von Verbindungen, einschließlich von Videos, Blogs und einem Supportforum finden Sie unter http://community.citrix.com.

Installieren von Receiver auf einer SD-Karte

Mar 23, 2015

Receiver für Mobilgeräte 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 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.

Konfigurieren von Access Gateway Enterprise Edition für Citrix Receiver für Android

Jan 30, 2015

Wichtig:

- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für Android mit XenApp Services-Sites unterstützt.
- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für Android mit XenApp Web-Sites unterstützt.
- Receiver für Web wird von Receiver für Android nicht unterstützt.
- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für Android für den Zugriff auf StoreFront-Stores unterstützt.
- Sowohl Einquellen- als auch Zweiquellenauthentifizierung wird für Webinterface-Sites und StoreFront unterstützt.
- Sie müssen Webinterface 5.4 verwenden, das von allen integrierten Browsern unterstützt wird.
- 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 Receiver-Instanzen). Alle Richtlinien können auf einem virtuellen Server erstellt werden.
- Wenn Benutzer Konten in Receiver erstellen, sollten Sie die Kontoanmeldeinformationen, z. b. die E-Mail-Adresse oder den entsprechenden FQDN des Access Gateway-Servers eingeben. Wenn die Verbindung beispielsweise bei der Verwendung des Standardpfads fehlschlägt, sollten Benutzer den vollständigen Pfad zum Access Gateway-Server eingeben.

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

- Wenn Sie CloudGateway Enterprise im Netzwerk bereitstellen, lassen Sie Verbindungen von 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-, SaaS- und Mobilanwendungen zu erhalten und von ShareFile aus auf Dokumente zuzugreifen. Benutzer stellen eine Verbindung entweder über Citrix Receiver oder das Access Gateway Plug-In her.
- Wenn Sie CloudGateway Express im Netzwerk bereitstellen, lassen Sie Verbindungen von internen oder Remotebenutzern mit StoreFront über Access Gateway zu, indem Sie Access Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf von XenApp veröffentliche Anwendungen und auf von XenDesktop virtualisierte Desktops zu. Benutzer stellen eine Verbindung über Citrix Receiver her.

Weitere Informationen zur Konfiguration dieser Verbindungen finden Sie unter "Integrating Access Gateway with CloudGateway" und den anderen Themen in der Dokumentation zu Access Gateway 10.

Informationen über die erforderlichen Einstellungen für Receiver für Mobilgeräte finden Sie in den folgenden Abschnitten in der Dokumentation zu Access Gateway 10:

- Erstellen des Sitzungsprofils für Receiver für CloudGateway Enterprise
- Erstellen des Sitzungsprofils für Receiver für CloudGateway Express
- Konfigurieren von benutzerdefinierten clientlosen Zugriffsrichtlinien für Receiver
- Zugriff von Mobilgeräten

Weitere Informationen finden Sie zudem im folgenden Abschnitt in der XenMobile-Dokumentation:

- App Preparation Tool für Mobilanwendungen

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 in der Dokumentation zu Access Gateway 10 beschrieben.

Konfigurieren des Webinterface für Citrix Receiver für Android

Jun 14, 2013

Konfigurieren der Webinterface-Site

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

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.

Um Anwendungen von der Webinterface-Site zu starten, wenn Sie Receiver für Android verwenden, muss die SD-Karte auf dem Gerät verfügbar sein, um die Sitzung zu starten. Wenn die SD-Karte nicht verfügbar ist (z. B. weil sie verwendet wird oder nicht eingelegt ist), schlägt der Sitzungsstart fehl.

Aktivieren der Smartcard-Unterstützung

Apr 07, 2015

Receiver für Android für Mobilgeräte unterstützt Bluetooth-Smartcardleser mit einer PNA-Site. Wenn die Smartcard-Unterstützung 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 Smartcard-Unterstützung 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. Beispiel: Weitere Informationen zum Koppeln des baiMobile Bluetooth-Smartcardlesers mit dem Android-Gerät finden Sie unter http://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v2.0.pdf.
   Für die Smartcard-Unterstützung 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. Weitere Informationen finden Sie unter http://www.biometricassociates.com/products/smart-card-readers/android-supported-devices/.
   - 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 eine Einschränkung von Drittparteien.
   - Die Smartcard-Authentifizierung 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 Smartcard-Authentifizierung 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 PNAgent-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, wählen Sie Konten und dann Konto hinzufügen oder bearbeiten Sie ein vorhandenes Konto.
4. Konfigurieren Sie die Verbindung und aktivieren Sie die Option "Smartcard".

Bereitstellen von RSA SecurID-Authentifizierung für Android-Geräte

Jun 19, 2013

Wenn Sie Access Gateway für die RSA SecurID-Authentifizierung konfigurieren, unterstützt Receiver den Modus "Nächster Token". Wenn dieses Feature aktiviert ist und ein Benutzer drei (Standardwert) falsche Kennwörter eingibt, fordert das Access 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.

Informationen über das Konfigurieren der RSA SecurID-Authentifizierung finden Sie in eDocs. Erweitern Sie den Knoten für Ihre Access Gateway-Version und gehen Sie zu
— Konfigurieren der RSA SecurID-Authentifizierung
.

RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen nicht unterstützt. Wenn Sie RSA SecurID verwenden möchten, verwenden Sie das Access 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 http://www.rsa.com/node.aspx?id=2521 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 dann.

Bereitstellen von Zugriffsinformationen für Android für Endbenutzer

Mar 23, 2015

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

- Konfigurieren der Kontenermittlung mit der E-Mail-Adresse
- Bereitstellen einer Provisioningdatei für Benutzer
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

Konfigurieren der e-mail-basierten Kontenermittlung

Sie können 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 Receiver ein. 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 Receiver eine Verbindung zu einer Webinterface-Bereitstellung herstellt.
Weitere Informationen zur Konfiguration des DNS-Servers für die e-mail-basierte Kontenermittlung finden Sie unter Konfigurieren der e-mail-basierten Kontenermittlung in der StoreFront-Dokumentation.

Weitere Informationen zur Konfiguration von Access Gateway, sodass Benutzerverbindungen angenommen werden und die e-mail-basierte Ermittlung der StoreFront- oder Access Gateway-URL durchgeführt wird, finden Sie unter Connecting to StoreFront by Using Email-Based Discovery in der Access Gateway-Dokumentation.

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 Receiver automatisch konfigurieren können. Nach der Receiver-Installation öffnen Benutzer die CR-Datei auf dem Gerät, um Receiver zu konfigurieren. Wenn Sie Receiver für Web-Sites konfigurieren, können Benutzer Receiver-Provisioningdateien auch von diesen Seiten abrufen.

Weitere Informationen finden Sie in der Dokumentation für StoreFront .

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.
- Stellen Sie für den Zugriff mit Access Gateway die Access Gateway-Adresse und die erforderliche Authentifizierungsmethode bereit.
  Weitere Informationen zur Konfiguration von Access Gateway oder Secure Gateway finden Sie in der Dokumentation für Access Gateway oder XenApp (für Secure Gateway).

Wenn ein Benutzer Angaben für ein neues Konto macht, versucht Receiver, die Verbindung zu überprüfen. Wenn die

Verbindung hergestellt werden kann, fordert Receiver den Benutzer auf, sich an dem Konto anzumelden.

Speichern von Kennwörtern

Jun 19, 2013

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 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 Konto 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 Receiver Benutzer jedes Mal zur Kennworteingabe auf, wenn sie eine Verbindung herstellen.

Hinweis: Für 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.

Ändern von Citrix Receiver-Einstellungen auf Geräten

Mar 23, 2015

Folgende Einstellungen können über die Registerkarte "Einstellungen" in Citrix Receiver für Android angepasst werden:

- **Anzeige**
  - Sitzungsauflösung: Wählen Sie die Auflösung für Sitzungen aus. Die Standardeinstellung ist **Wie Bildschirm**.
- **Tastatur**
  - Textvorhersage: Hiermit können Sie die Textvorhersage aktivieren bzw. deaktivieren. Der Standardwert ist **Aus**.
  - Erweiterte Tastatur: Hiermit können Sie die erweiterte Tastatur aktivieren bzw. deaktivieren. Der Standardwert ist **Aus**.
  - Erweiterte Tasten: Hiermit können Sie Sondertasten, z. B. Alt und Strg, zur Anzeige auf der erweiterten Tastatur konfigurieren.
  - Client-IME: Wenn der clientseitige Eingabemethoden-Editor (IME) aktiviert ist, können Benutzer an der Einfügemarke statt in einem separaten Fenster Text eingeben. Der Standardwert ist **Aus**.
- **Audio**
  - Audiostreaming: Hier können Sie Sitzungsaudioeinstellungen auf "Audio aus", "Wiedergeben" oder "Wiedergeben und Aufzeichnen" festlegen. Die Standardeinstellung ist **Wiedergeben**.
- **Erweitert**
  - Gerätespeicher verwenden: Berechtigung zum Verwenden des Gerätespeichers. Die Standardeinstellung ist **Kein Zugriff**.
  - Vor Beenden fragen: Hier können Sie die Bestätigung vor dem Beenden festlegen. Der Standardwert ist **Ein**.
  - Zwischenablage: Hier können Sie die Verwendung der Zwischenablage aktivieren bzw. deaktivieren. Der Standardwert ist **Aus**.
  - Anzeigeausrichtung: Hier können Sie für die Anzeigeausrichtung "Querformat", "Hochformat" oder "Automatisch" (dynamisch) festlegen. Die Standardeinstellung ist **Automatisch**.
  - Anzeige nicht abschalten: Hier können Sie festlegen, dass die Anzeige nicht abgeschaltet werden soll. Der Standardwert ist **Aus**.
- **ShareFile**: Dieses Feature wird nicht mehr unterstützt und wird bei einem künftigen Update entfernt. Verwenden Sie die ShareFile-App.
- **Info**: Informationen zur Version von Citrix Receiver und Copyright-Angaben.

Ausprobieren der Demo-Site

Jun 19, 2013

Wenn Benutzer Citrix Receiver zum ersten Mal starten, können sie auf der Willkommenseite ein Demokonto in der Citrix Cloud starten.

Benutzer schließen die Kontoregistrierung durch Eingabe der Namen und E-Mail-Adressen ab (die E-Mail-Adressen werden auf einigen Geräten automatisch ausgefüllt). Die Demo-Site ist bereits mit veröffentlichten Anwendungen konfiguriert und Benutzer können Citrix Receiver sofort ausprobieren.

Benutzer können ihre Konten in Receiver hinzufügen, ändern und entfernen.