Info über Citrix Receiver für iOS 5.9.x

Oct 27, 2015

> **Important**
>
> Citrix Receiver für iOS 5.9.x bietet keine Unterstützung für iOS 9. Wenn Sie Ihr Gerät auf iOS 9 aktualisiert haben, führen Sie ein Upgrade von Citrix Receiver auf die aktuelle Version aus.
>
> Navigieren Sie für ein Upgrade auf die Citrix Downloadseiten: http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

Receiver für iOS 5.9.6

In diesem Release ist ein Problem mit der Interoperabilität einer Bluetooth-Tastatur behoben.

Receiver für iOS 5.9.5

Neue Features

- **X1-Maus**. Sie können die Citrix X1-Maus in Citrix HDX-Sitzungen verbinden und verwenden. Zurzeit unterstützt Receiver nur ein Mausmodell.
  - Sie stellen eine Verbindung mit der Maus her und aktivieren sie, indem Sie in Receiver zu Einstellungen navigieren und **X1-Maus** aktivieren.
  - Die Maustasten können für Linkshänder getauscht werden. Navigieren Sie in Receiver zu Einstellungen und aktivieren Sie **Linkshänder**. Sie können auch in der Windows-Systemsteuerung zu Mauseigenschaften navigieren.

  Weitere Informationen zur Citrix X1-Maus finden Sie unter http://www.citrix.com/products/mouse/overview.html.

- **Verbesserte Unterstützung für externes Display**: Receiver für iOS unterstützt das externe Display auf iPhones und iPads.
  - Zum Aktivieren der externen Anzeige navigieren Sie in Citrix Receiver zu Einstellungen > Darstellung und aktivieren **Externes Display**.
  - Das externe Display ist mit den folgenden Methoden verfügbar:
    - AirPlay
    - Lightning auf VGA-Adapter
    - Lightning Digital AV-Adapter

      Hinweis: Lightning Digital AV-Adapter wurde nicht getestet.
  - Die externe Anzeige wird nicht für ältere iPads (Modelle ohne Air) und iPhones (5c und früher) empfohlen, da hohe Verarbeitungsanforderungen bestehen.
- **Touchpad/Präsentationsmodus - Vorschau**: Sie können bei der Verbindung mit einem externen Display, wie AppleTV oder Lightning auf HDMI-Kabel, einen iPad als Tastatur und Touchpad statt einer Bluetooth-Tastatur verwenden.
  - Zum Aktivieren des Präsentationsmodus navigieren Sie in Citrix Receiver zu Einstellungen > Darstellung und aktivieren **Externes Display** und **Präsentationsmodus**.
  - Touchpad/Präsentationsmodus ist mit der X1-Maus kompatibel.
  - Dies ist eine Vorschau von Touchpad/Präsentationsmodus und ist nicht für eine Verwendung in der Produktion gedacht.

Behobene Probleme

- Tastaturzustandsereignisse werden für das Citrix Mobility Pack falsch zurückgegeben. [#522269]
- Der Sitzungsauflösungsbildschirm hat eine falsche Größe, wenn der AutoAnpassen-Modus in einer Citrix Mobility Pack verbesserten Anwendung verwendet wird. [#545325]
- Der Bildlauf im Sitzungsbildschirm ist nicht einfach. [#545324]

Receiver für iOS 5.9.4

Neue Features

- Unterstützung für TLS 1.0, 1.1 und 1.2. Sie können Ihre Umgebung ändern und alle drei verwenden. Receiver für iOS verwendet 1.2, falls verfügbar, dann 1.1 und greift dann auf TLS 1.0 zurück.
- Verbesserte Grafiken für iPhone 6 Plus und andere Retina-Telefone.
  - Hochauflösungssitzungen können mit der Option Bildschirm autoAnpassen unter Einstellungen > Darstellung gestartet werden.

Behobene Probleme

- Das Mobility SDK gibt jetzt den Wert **5** für Gerät **orientationFaceUp** und den Wert **6** für Gerät **orientationFaceDown** zurück.
- Ein Problem mit beschädigten Farben kann auftreten.
- Ein Verwerfen von 3D Pro-Frames kann auftreten.
- Ein Problem mit einer schwarzen iPad-Bildschirmlupe kann auftreten.

Receiver für iOS 5.9.3

Neue Features

- Verbesserte Benutzererfahrung beim Wiederherstellen einer Verbindung mit einer Sitzung über Worx Home.

Behobene Probleme

- Bei Verwendung einer veröffentlichten Remotedesktopprotokoll (RDP)-Sitzung im Vollbildmodus in einer ICA-Sitzung wurden keine Großbuchstaben gesendet.
- Zeitweiliges Problem mit der Bildschirmtastatur.
- Problem mit der Auflösung bei App Switcher.
- Kleinere Fehler bei der Grafikanzeige beim Drehen des Geräts.
- Gelegentliches Problem beim Start eines Desktops über NetScaler.

Receiver für iOS 5.9.2

Neue Features

- Lösung des Problems, das in vorherigen Releases einen schwarzen Bildschirm verursachte.
- Lösung von Problemen in Verbindung mit dem Mobility SDK.
- Eine Option zum Aktivieren von Tastaturerweiterungen wurde hinzugefügt. Dies ist ein Sicherheitsupdate.
- Um einen erneuten Angriff wie den von "Poodle" gegen das SSLv3-Protokoll zu verhindern, wird die Verwendung des Protokolls von dieser Receiver für iOS-Version deaktiviert. Weitere Informationen finden Sie unter CTX 200238. Hinweis: Sie müssen sicherstellen, dass TLS 1.0 aktiviert ist.

Receiver für iOS 5.9.1

Neue Features

- Support für iOS 8.
- Wiederherstellung der Siri-Diktierfunktion mit Citrix Receiver.
- Benutzer können auf mehrere Anwendungen gleichzeitig zugreifen und zwischen ihnen durch Streichen mit einem Finger wechseln. Der App Switcher wird automatisch beim Öffnen einer zweiten App in derselben Windows-Sitzung gestartet. Streichen Sie vom Bildschirmrand aus, um die nächste ausgeführte App auszuwählen. Für die Verwendung dieses Features müssen die Apps vom IT-Administrator auf dem gleichen Server veröffentlicht sein.
- Das Feature "Workspace Control" ist unter **Einstellungen > Erweitert > Workspace Control** verfügbar.
- Die erweiterte Protokollierung ist aktiviert, um Diagnosedaten für Probleme bei der Authentifizierung, beim Store und bei der Verbindung zu sammeln. Die Protokollierungsoptionen befinden sich unter **Einstellungen > Support > Protokolloptionen**.
- Die Option "ShareFile" unter **Einstellungen > Erweitert** steht nicht mehr zur Verfügung. Laden Sie die Citrix ShareFile-App vom App Store herunter, wenn Sie ShareFile verwenden möchten.

Hinweis: Wenn die Richtlinie für die automatische Anzeige der Tastatur mit der Citrix Richtlinie aktiviert ist, müssen Sie zweimal auf den Texteingabebereich tippen, um die Bildschirmtastatur anzuzeigen.

Receiver für iOS 5.9

Neue Features

- Receiver bietet eine eingeschränkte Unterstützung von Smartcards.
  Hinweis: Kunden mit FIPS NetScaler-Geräten sollten ihre Systeme so konfigurieren, dass SSL-Neuaushandlungen abgelehnt werden. Weitere Informationen finden Sie unter How to configure the -denySSLReneg parameter.
  Die folgenden Produkte und Konfigurationen werden unterstützt.
  - Unterstützte Smartcardleser:
    - Precise Biometrics Tactivo für iPad Mini Firmwareversion 3.8.0
    - Precise Biometrics Tactivo für iPad (4. Generation) und Tactivo für iPad (3. Generation) und iPad 2 Firmwareversion 3.8.0
    - BaiMobile® 301MP und 301MP-L Smartcardleser

    Unterstützte VDA-Smartcard-Middleware
    - ActiveIdentity
  - Unterstützte Smartcards:
    - PIV-Karten
    - Common Access Card (CAC)
  - Unterstützte Konfigurationen:
    - Smartcardauthentifizierung bei NetScaler Gateway mit StoreFront 2.x und XenDesktop ab 5.6 oder ab XenApp 6.5
- Unterstützung für iOS 7.1
- Unterstützung für SHA2-Zertifikate
- Unterstützung für eine Zugriffsimplementierung über einen FQDN

In 5.9 - 5.9.x behobene Probleme

Die folgenden Probleme wurden seit dem letzten Release dieses Produkts behoben:

- Wenn Sie nach dem Öffnen einer App, die editierbare Daten enthält, einen 3-Finger-Tipp durchführen, wird die virtuelle Tastatur ggf. nicht angezeigt.
- Wenn nach dem Starten eines VDA oder beim Verwenden von Control Center oder Notification Center die Anzeige verzerrt ist oder ein schwarzer Bildschirm angezeigt wird, aktualisieren Sie die Sitzung, indem Sie auf den Bildschirm des

Geräts tippen oder das Gerät drehen.

- Bei aktivierter Windows-Medienumleitung (auf dem Bildschirm Einstellungen) hat Citrix die folgenden Vorschläge, um die Darstellung zu verbessern. In 5.9.x sind diese Workarounds nicht mehr erforderlich:
  - Wenn Sie ein Video auf dem Windows Media Player auf einem virtuellen Desktop wiedergeben und auf dem iOS-Gerät auf Home tippen, kann der Videobildschirm schwarz sein, wenn Receiver fortgesetzt wird. Tippen Sie auf die Schaltfläche "Anhalten" auf dem Windows Media Player, um die Videowiedergabe beim Fortsetzen von Receiver fortzusetzen. Tippen Sie dann auf Wiedergeben.
  - Wenn Sie an eine neue Stelle in einem Vidoe wechseln möchten, das in Windows Media Player wiedergegeben wird, tippen Sie auf die gewünschte Stelle in der Fortschrittsanzeige statt das Symbol auf die Stelle zu ziehen. Wenn Sie das Symbol auf die neue Stelle ziehen, kann in seltenen Fällen ein schwarzer Bildschirm angezeigt werden. Tippen Sie auf die Fortschrittsanzeige und die Videowiedergabe sollte fortgesetzt werden.
- Wenn Sie die Schaltfläche Anmelden antippen, nachdem Sie ein Kennwort mit einem Zeichen eingegeben haben, können Sie eine veröffentlichte Anwendung erst nach dem Neustart von Receiver starten. [#395745]
- Wenn Receiver auf einem Gerät unter iOS 7 ausgeführt wird, kann das Hinzufügen einer Anwendung zum Store und das Starten der Anwendung zum Absturz von Receiver führen. [#443642]
- Wenn Sie Citrix Receiver auf einem iPad verwenden, kann das Öffnen eines RSA-Tokenlinks von einer E-Mail aus nach dem Start von Receiver zum Absturz führen. [#443365]
- Wenn Sie in Receiver einen neuen Store erstellen und ein neues Clientzertifikat zur Authentifizierung importieren, kann das Eingeben der Zertifikats-URL und das Auswählen des installierten Zertifikats dazu führen, dass das Feld "Benutzername" mit dem Vor- und Nachnamen des Benutzers ausgefüllt wird statt mit benutzername@domäne. [#444021]
- Wenn Sie über Receiver ein Konto hinzufügen, wird möglicherweise nach dem Auswahlbildschirm für das Zertifikat nicht die Authentifizierungsaufforderung für LDAP angezeigt. [#443641]

Bekannte Probleme

- Beim Festlegen eines neuen Kennworts wird der Fehler "Falsche Anmeldeinformationen" angezeigt. Trotz der Fehlermeldung wird das neue Kennwort richtig festgelegt. Die Fehlermeldung kann ignoriert werden. Verwenden Sie bei der nächsten Anmeldung das neue Kennwort. [#70576123]
- Die Leistung kann abfallen, wenn externe Bildschirme mit einer Auflösung mit mehr als 720 Pixeln verwendet werden.
- Die X1-Maus kann nur mit einem anderen Gerät gekoppelt werden, wenn die Option "Dieses Gerät vergessen" in den iOS Bluetooth-Einstellungen verwendet wird.
- Die X1-Maus interagiert u. U. nicht mit Anwendungssymbolen auf dem Bildschirm für den Anwendungsstart. [#560429]
- Audio wird u. U. nicht auf einem AirPlay-Gerät wiedergegeben. [#55671]
- Die X1-Maus interagiert u. U. nicht mit der Sitzungssymbolleiste in einer Sitzung. [#554469]
- Das folgende Problem tritt bei der Verbindung mit einer virtuellen Desktopsitzung von XenDesktop auf: Stellen Sie eine Verbindung mit dem virtuellen Desktop her, öffnen Sie dann Internet Explorer und navigieren Sie zu einer Site mit Texteingabeformularen. Die Bildschirmtastatur wird wie erwartet angezeigt. Wenn Benutzer jedoch die Verbindung zum virtuellen Desktop trennen und dann wieder herstellen, wird die Bildschirmtastatur nicht mehr automatisch angezeigt. Verwenden Sie stattdessen den 3-Fingertipp, um die Bildschirmtastatur zu öffnen. [#461011]
- Nur iPhone: Der horizontale Bildlauf auf dem Home-Bildschirm ist für das Store-Webkonto nicht verfügbar. [#338903]
- Auf der erweiterten Tastatur in Microsoft Excel werden beim Tippen auf die Strg- oder Umschalt-Taste nicht mehrere Zellen in der Kalkulationstabelle ausgewählt. Als Lösungsansatz können Sie auf die aktuelle Zelle tippen und Ihren Finger über angrenzende Zellen ziehen, um sie auszuwählen. [#339030]
- Bei der Konfiguration eines neuen Benutzerkontos kann die Seite für die Zertifikatregistrierung verzögert angezeigt werden. [#339996]
- Das RSA-Softwaretoken fordert falscherweise, dass Benutzer das Kennwort und die PIN (statt nur die PIN) bei jeder

Anmeldung eingeben. [#350169]

- Wenn Sie den Authentifizierungstyp in NetScaler Gateway ändern, nachdem Benutzer ein Konto erstellt haben, wird das neue Authentifizierungsprofil nicht gespeichert und Benutzer können sich ggf. überhaupt nicht anmelden. [#350206]
- Wenn eine gestreamte Audio- oder Videodatei in einer veröffentlichten Anwendung auf dem Desktop ausgeführt wird, und Sie die Einstellung Mobilfunkdaten auf dem Bildschirm Einstellungen von Ein auf Aus und dann wieder auf Ein ändern, reagiert der Desktop nicht mehr. [#387530]
- Wenn Sie sowohl einen Store mit Smartcard als auch einen Store ohne Smartcard verwenden und die Stores nacheinander öffnen, kann der Start des zweiten Stores fehlschlagen. Sie vermeiden das Problem, indem Sie die Receiver-App beenden und neu starten, bevor Sie einen neuen Storetyp starten. [#452347]
- Wenn Sie sich bei einer Sitzung ohne Smartcardauthentifizierung anmelden, können Sie die Smartcard in der Sitzung möglicherweise nicht zum digitalen Signieren verwenden. Sie vermeiden dieses Problem, indem Sie sich bei einer Sitzung mit der Smartcardauthentifizierung anmelden, wenn Sie innerhalb der Sitzung signieren möchten. [#457961]
- Wenn Sie ein Konto hinzufügen und dabei nur den FQDN verwenden, kann der Vorgang fehlschlagen. Sie vermeiden dieses Problem, indem Sie den FQDN im folgenden Format eingeben: https://FQDN, wobei *FQDN* Ihre FQDN-Adresse ist. [#458569]
- Wenn Sie eine App starten, die Sie nicht abonniert haben, bleibt die Sitzung möglicherweise hängen, ohne dass eine Anmeldeaufforderung angezeigt wird. Sie vermeiden dieses Problem, indem Sie sich erst beim Store anmelden oder die App abonnieren, bevor Sie sie starten. [#460159]
- Wenn Sie einen Store hinzufügen und der Smartcardschalter auf "On" festgelegt ist, kann das Löschen und erneute Hinzufügen des Stores innerhalb von 10 Minuten zu einer Fehlermeldung von NetScaler führen.
  Sie vermeiden dieses Problem, indem Sie nach dem Löschen des Stores 10 Minuten mit dem erneuten Hinzufügen warten. [#466490]

- Bei aktivierter Windows-Medienumleitung (auf dem Bildschirm Einstellungen) hat Citrix die folgenden Vorschläge, um die Wiedergabeerfahrung zu verbessern:
  - Wenn Sie auf Geräten, die unter iOS 7 ausgeführt werden, die Tastatur zum Navigieren verwenden, wird "Demo ausprobieren" nicht unterstützt. Tippen Sie im Feld "E-Mail", um fortzufahren und das Konto zu konfigurieren. [#414965]
  - Das iOS-Gerät sollte bei Verwendung der Windows-Medienumleitung freien Speicher haben. Empfohlen werden ca. 1 GB, abhängig von der Größe des Videos.

Systemanforderungen

May 11, 2015

Gerät

> ### Important
>
> Citrix Receiver für iOS 5.9.x bietet keine Unterstützung für iOS 9. Wenn Sie Ihr Gerät auf iOS 9 aktualisiert haben, führen Sie ein Upgrade von Citrix Receiver auf die aktuelle Version aus.
>
> Navigieren Sie für ein Upgrade auf die Citrix Downloadseiten: http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

- Citrix Receiver für iOS 5.9.x unterstützt iOS 6.1.x, 7 und 8.
- Dieses Softwareupdate wird auf den folgenden Geräten unterstützt:
  - iPhone 4, 4S, 5, 5c, 5s, 6 und 6 Plus. Für iPhone 5c und 5s werden nur Receiver für iOS 5.9 und 5.9.x unterstützt.
  - Alle iPad-Modelle.
  - 5. Generation iPod Touch.
- Unterstützung externer Bildschirme
  - iPhone: Keine.
  - iPad: Gemäß Unterstützung von iOS (nicht der ganze Bildschirm wird verwendet).

Wichtig: Weitere Informationen zu sicheren Verbindungen in der Citrix-Umgebung finden Sie unter **Konnektivität** (unten).

Server

Installieren Sie alle aktuellen Hotfixes für die Server.

- Für Verbindungen mit virtuellen Desktops und Apps unterstützt Citrix Receiver Citrix StoreFront und das Webinterface.
  StoreFront:
  - StoreFront 2.6 (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 Safari-Webbrowser. Benutzer müssen die ICA-Datei mit der Browserfunktion zum Öffnen in Receiver manuell öffnen. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

  Webinterface:
  - Webinterface 5.4 mit Webinterface-Sites
  - Webinterface 5.4 mit XenApp Services-Sites
  - Webinterface auf NetScaler (browserbasierter Zugriff nur mit Safari)
    Sie müssen die Rewrite-Richtlinien aktivieren, die von NetScaler bereitgestellt werden.
- **XenDesktop** und **XenApp** (eines der folgenden Produkte):
  - Citrix XenDesktop 4, 5, 5.5, 5.6, 7, 7.x, 7.5 und 7.6
  - Citrix XenApp 7.5 und 7.6.
  - Citrix XenApp 6.5 für Windows Server 2008 R2

- Citrix XenApp 6 für Windows Server 2008 R2
- Citrix XenApp Fundamentals 6.0 für Windows Server 2008 R2
- Citrix XenApp 5 für Windows Server 2008
- Citrix XenApp 5 für Windows Server 2003
- Citrix Presentation Server 4.5

- VDI-in-a-Box 5.2.x und 5.3.x

Konnektivität und Authentifizierung

Für Verbindungen mit StoreFront unterstützt Receiver die folgenden Authentifizierungsmethoden:

	Receiver für Web mit Browsern	**StoreFront Services-Site (nativ)**	**StoreFront XenApp Services-Site (nativ)**	**NetScaler bei Receiver für Web (Browser)**	**NetScaler bei StoreFront Services-Site (nativ)**
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zweistufig (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Nein
Smartcard	Ja	Ja		Ja*	Ja*
Benutzerzertifikat				Ja (NetScaler Gateway-Plug-In)	Ja (NetScaler Gateway-Plug-In)

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

Weitere Informationen zu den NetScaler Gateway- und Access Gateway-Versionen, die von StoreFront unterstützt werden, finden Sie in der NetScaler Gateway-, Access Gateway und StoreFront-Dokumentation in den eDocs.

Für Verbindungen mit dem Webinterface 5.4 unterstützt Receiver die folgenden Authentifizierungsmethoden:
Hinweis: Im Webinterface wird der Begriff Explizit für die Domänen- und Sicherheitstokenauthentifizierung verwendet.

	Webinterface (Browser)	**Webinterface XenApp Services-Site**	**NetScaler bei Web Interface (Browser)**	**NetScaler bei Webinterface XenApp Services-Site**

Anonym Domäne	Ja **Webinterface (Browser)** Ja	**Webinterface XenApp Services-Site** Ja	**NetScaler bei Web Interface (Browser)** Ja*	**NetScaler bei Webinterface XenApp Services-Site**
Domänen-Passthrough	Ja			
Sicherheitstoken			Ja*	
Zweistufig (Domäne mit Sicherheitstoken)			Ja*	
SMS			Ja*	
Smartcard**	Ja			
Benutzerzertifikat			Ja (NetScaler Gateway-Plug-In erforderlich)	

Info zu sicheren Verbindungen und Zertifikaten

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remote-Gateway installiert ist, muss das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Gerät installiert sein, um erfolgreich mit Citrix 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 Anwendungen können jedoch nicht gestartet werden.

Importieren von Stammzertifikaten auf iPad- und iPhone-Geräten

Erwerben Sie das Stammzertifikat des Zertifikatausstellers und senden es per E-Mail an ein E-Mail-Konto, das auf dem Gerät konfiguriert ist. Wenn Sie auf die Anlage klicken, werden Sie zum Importieren des Stammzertifikats aufgefordert.

Zertifikate mit Platzhalterzeichen

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

Zwischenzertifikate und NetScaler Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Zertifikat des NetScaler Gateway- (oder Access Gateway-Servers angehängt werden. Weitere Informationen zur Installation von Zwischenzertifikaten in NetScaler Gateway oder auf Access Gateway finden Sie in der Dokumentation in den eDocs. Weitere Informationen zu Access Gateway-Installationen finden Sie außerdem in dem Knowledge Base-Artikel, der Ihrer Edition entspricht:

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

Siehe auch:

CTX124937: How to Configure Citrix Access Gateway Enterprise Edition for Use with Citrix Receiver for Mobile Devices

RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen (nur über das Webinterface) und alle unterstützten Access Gateway-Konfigurationen unterstützt.

Receiver unterstützt alle Authentifizierungsmethoden, die von Access Gateway unterstützt werden. Weitere Informationen zur Authentifizierung finden Sie in der NetScaler Gateway- oder Access Gateway-Dokumentation und den Abschnitten "Verwalten" in der StoreFront-Dokumentation in den eDocs. Informationen über andere Authentifizierungsmethoden, die das Webinterface unterstützt, finden Sie unter "Konfigurieren der Authentifizierung für das Webinterface" in der Webinterface-Dokumentation.

Smartcards

- Receiver bietet eine eingeschränkte Unterstützung von Smartcards.
  Hinweis: Kunden mit FIPS NetScaler-Geräten sollten ihre Systeme so konfigurieren, dass SSL-Neuaushandlungen abgelehnt werden. Weitere Informationen finden Sie unter How to configure the -denySSLReneg parameter.
  Die folgenden Produkte und Konfigurationen werden unterstützt.
  - Unterstützte Smartcardleser:
    - Precise Biometrics Tactivo für iPad Mini Firmwareversion 3.8.0
    - Precise Biometrics Tactivo für iPad (4. Generation) und Tactivo für iPad (3. Generation) und iPad 2 Firmwareversion 3.8.0
    - BaiMobile® 301MP und 301MP-L Smartcardleser

    Unterstützte VDA-Smartcard-Middleware
    - ActiveIdentity
  - Unterstützte Smartcards:
    - PIV-Karten
    - Common Access Card (CAC)
  - Unterstützte Konfigurationen:
    - Smartcardauthentifizierung bei NetScaler Gateway mit StoreFront 2.x und XenDesktop ab 5.6 oder ab XenApp 6.5

Konfigurieren der Umgebung

Apr 13, 2015

Für Receiver muss das Webinterface für die XenApp-Bereitstellung konfiguriert werden. Es gibt zwei Typen der Webinterface-Sites: XenApp Services-Sites (früher Program Neighborhood Services) und XenApp Web-Sites. Mit Webinterface-Sites können Clientgeräte eine Verbindung mit der Serverfarm herstellen. Die Authentifizierung zwischen Receiver und einer Webinterface-Site kann mit verschiedenen Lösungen gehandhabt werden, u. a. Citrix Access Gateway und Citrix Secure Gateway.

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.

Konfigurieren Sie die folgenden Komponenten in der Bereitstellung, wie hier beschrieben, bevor Benutzer auf Anwendungen zugreifen, die in der XenApp- oder XenDesktop-Umgebung ausgeführt werden.

- Ziehen Sie die folgenden Optionen in Betracht, wenn Sie Anwendungen in den Farmen veröffentlichen, um die Erfahrung für die Benutzer zu steigern, die über StoreFront-Stores auf die Anwendungen zugreifen.
  - Verwenden Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen, da diese Beschreibungen Benutzern in Citrix Receiver angezeigt werden.
  - Sie können die Mobilgerätbenutzer auf veröffentlichte Anwendungen aufmerksam machen, wenn Sie die Anwendungen in Citrix Receiver in der Highlightliste einschließen. Wenn Sie dieser Liste Einträge in Citrix Receiver hinzufügen möchten, bearbeiten Sie die Eigenschaften der Anwendungen, die auf den Servern veröffentlicht sind, und hängen Sie die Zeichenfolge KEYWORDS:Featured dem Feld "Anwendungsbeschreibung" an.
  - Zum Aktivieren des AutoAnpassen-Bildschirmmodus, bei dem die Anwendung auf die Bildschirmgröße der Mobilgeräte angepasst wird, müssen Sie die Eigenschaften der Anwendungen bearbeiten, die auf den Servern veröffentlicht sind, und die Zeichenfolge KEYWORDS:mobile dem Wert im Feld "Anwendungsbeschreibung" anhängen. Mit diesem Schlüsselwort wird auch der automatische Bildlauf für die Anwendung aktiviert.
  - Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge KEYWORDS:Auto an die Beschreibung anhängen, die Sie beim Veröffentlichen der Anwendung in XenApp angeben. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.

  Weitere Informationen finden Sie in der Dokumentation für StoreFront.

- Wenn das Webinterface der XenApp- oder XenDesktop-Bereitstellung keine Website oder XenApp Services-Site hat, erstellen Sie eine. Der Name und die Erstellung der Site hängen von der installierten Webinterface-Version ab. Weitere Informationen zur Erstellung dieser Sites finden Sie im Abschnitt "Erstellen von Sites" für die relevante Version des Webinterface.

Konfigurieren von StoreFront

Apr 13, 2015

Konfigurieren von StoreFront

Wichtig:

- Nur Citrix Access Gateway Enterprise Edition 9.3 und 10.0 werden von Receiver für iOS 5.6 und 5.7 mit StoreFront unterstützt.
- Receiver für iOS unterstützt nur XenApp Services-Site auf dem Webinterface.
- Receiver für iOS unterstützt das Starten von Sitzungen über Receiver für Web, wenn der Webbrowser mit Receiver für Web funktioniert. Wenn die Starts nicht erfolgen, konfigurieren Sie Ihr Konto direkt über Receiver für iOS. Benutzer müssen die ICA-Datei mit der Browserfunktion zum Öffnen in Receiver manuell öffnen. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

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

1. Installieren und konfigurieren Sie StoreFront. Weitere Informationen finden Sie unter StoreFront im Abschnitt Technologien > StoreFront in den eDocs. Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für Receiver für iOS erstellen.
2. Stores für StoreFront konfigurieren Sie genauso wie für andere XenApp- und XenDesktop-Anwendungen. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich. Weitere Informationen finden Sie unter *— Benutzerzugriffsoptionen* im StoreFront-Abschnitt in den eDocs. 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 Access Gateway- oder Store-URL, mit der sie auf ihre Desktops und Anwendungen zugreifen können, direkt mitteilen. Für Verbindungen über Access 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 Access Gateway

Wenn Benutzer eine Verbindung von außerhalb des internes Netzwerks herstellen (beispielsweise Benutzer, die eine Verbindung vom Internet oder von Remotestandorten herstellen), konfigurieren Sie die Authentifizierung über Access Gateway.

- Nur Citrix Access Gateway 9.3 und 10.0 Enterprise Edition und Access Gateway 5.0.4 werden von Receiver für iOS 5.6 oder 5.7 mit StoreFront unterstützt.
- Weitere Informationen finden Sie unter den entsprechenden Versionen von Access Gateway in den eDocs.

Konfigurieren von Receiver für den Zugriff auf Anwendungen

1. Geben Sie beim Erstellen eines neuen Kontos im Feld Adresse die entsprechende URL des Stores ein, z. B. storefront.organization.com.
2. Geben Sie die restlichen Felder ein und wählen Sie die Access Gateway-Authentifizierungsmethode, z. B. Aktivieren des Sicherheitstokens, Auswählen des Authentifizierungstyps und Speichern der Einstellungen.

Hinweis: Anmeldungen am Store sind für etwa eine Stunde gültig. Anschließend müssen Benutzer sich neu anmelden, um die Darstellung zu aktualisieren oder andere Anwendungen zu starten.

Konfigurieren der Clientzertifikatauthentifizierung

Apr 13, 2015

Wichtig:

- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für iOS 5.5 und 5.6 mit XenApp Services-Sites unterstützt.
- Die Clientzertifikatauthentifizierung wird von Receiver für iOS 5.5, 5.6, 5.7 und 5.9 unterstützt.
- Nur Access Gateway Enterprise Edition 9.x und 10.x unterstützen die Clientzertifikat-Authentifizierung.
- Die Zweiquellenauthentifizierungstypen müssen CERT und LDAP sein.
- Receiver unterstützt die optionale Clientzertifikatauthentifizierung.
- Nur Zertifikate im P12-Format werden unterstützt.

Benutzer, die sich an einem virtuellen Access Gateway-Server anmelden, können auch anhand der Attribute des Clientzertifikats authentifiziert werden, das dem virtuellen Server präsentiert wird. Die Clientzertifikatauthentifizierung kann zusammen mit einem anderen Authentifizierungstyp, LDAP, verwendet werden, um eine Zweiquellenauthentifizierung bereitzustellen.

Um Benutzer basierend auf Clientzertifikatattributen zu authentifizieren, sollte die Clientauthentifizierung auf dem virtuellen Server aktiviert sein und das Clientzertifikat angefordert werden. Sie müssen ein Stammzertifikat an den virtuellen Server von Access Gateway binden.

Wenn sich Benutzer an dem virtuellen Access Gateway-Server anmelden, werden nach der Authentifizierung die Benutzernamensinformationen aus dem angegebenen Feld des Zertifikats extrahiert. Üblicherweise ist es das Feld Subject:CN. Wurde der Benutzername erfolgreich extrahiert, wird der Benutzer authentifiziert. Wenn der Benutzer kein gültiges Zertifikat während des TLS-Handshakes bereitstellt oder wenn der Benutzername nicht extrahiert werden kann, schlägt die Authentifizierung fehl.

Sie können Benutzer anhand des Clientzertifikats authentifizieren, indem Sie für den Standardauthentifizierungstyp die Verwendung des Clientzertifikats angeben. Sie können auch eine Zertifikataktion erstellen, mit der Sie definieren, was während der Authentifizierung basierend auf einem Client-SSL-Zertifikat geschehen soll.

Konfigurieren der XenApp Services-Site

Wenn keine XenApp Services-Site vorhanden ist, erstellen Sie eine XenApp Services-Site für Mobilgeräte in der XenApp-Konsole oder der Webinterface-Konsole (abhängig von der installierten XenApp-Version).

Receiver für Mobilgeräte ruft über eine XenApp Services-Site (früher Program Neighborhood Agent-Site) Informationen über die Anwendungen ab, für die ein Benutzer berechtigt ist und bietet sie Receiver an, der auf dem Gerät ausgeführt wird. Dies gleicht der Weise, wie das Webinterface für traditionelle SSL-basierte XenApp-Verbindungen, für die ein Access Gateway konfiguriert werden kann, verwendet wird.

Konfigurieren Sie die XenApp Services-Site für den Receiver für Mobilgeräte, um Verbindungen von einer Access Gateway-Verbindung zu ermöglichen.

1. Wählen Sie in der XenApp Services-Site Sicheren Clientzugriff verwalten > Einstellungen für sicheren Clientzugriff verwalten.
2. Ändern Sie die Zugriffsmethode zu Gateway: direkt.
3. Geben Sie den FQDN des Access Gateway-Geräts ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.

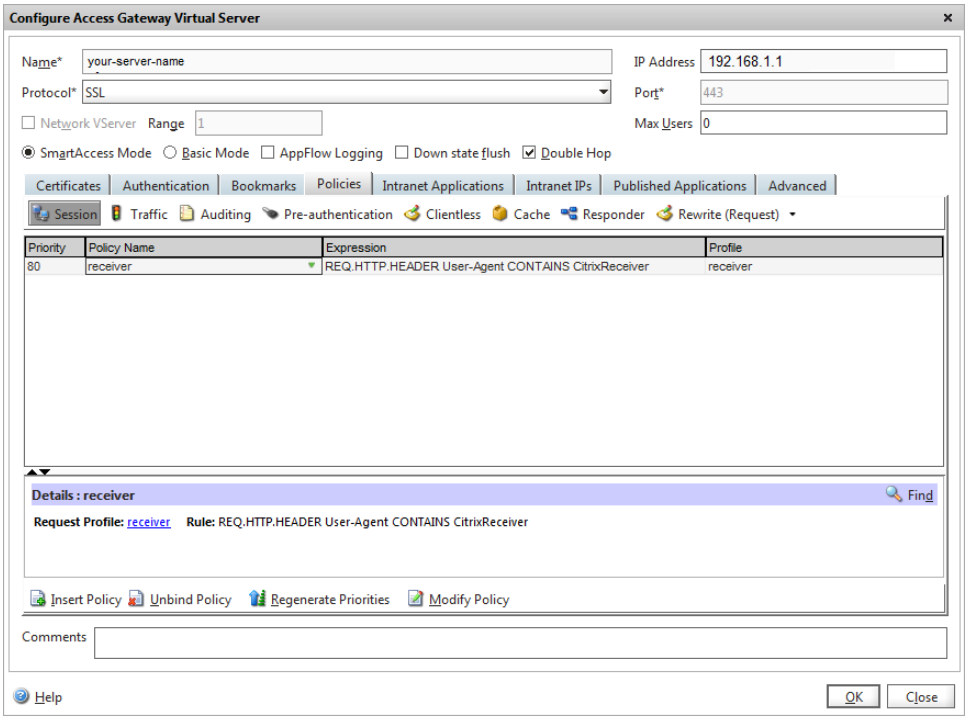
Konfigurieren des Access Gateway-Geräts

Konfigurieren Sie das Access Gateway für die Clientzertifikatauthentifizierung mit der Zweifaktorauthentifizierung und den zwei Authentifizierungsrichtlinien: Cert und LDAP. Weitere Informationen finden Sie in Ihrer Version von Access Gateway Enterprise Edition (nur 9.x) oder unter Access Gateway 10 in den eDocs und suchen Sie nach
— Configuring Client Certificate Authentication

.

1. Erstellen Sie eine Sitzungsrichtlinie auf dem Access Gateway, um eingehende XenApp-Verbindungen von Receiver zuzulassen, und geben Sie den Speicherort der neu erstellten XenApp Services-Site an.
   - Erstellen Sie eine neue Sitzungsrichtlinie, mit der Sie angeben, dass die Verbindung von Receiver für Mobilgeräte ist. Konfigurieren Sie bei der Erstellung der Sitzungsrichtlinie den folgenden Ausdruck und wählen Sie Match All Expressions als Operator aus:

     REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



   - Stellen Sie in der zugeordneten Profilkonfiguration für die Sitzungsrichtlinie auf der Registerkarte Security den Eintrag Default Authorization auf Allow.
     Wenn dies auf der Registerkarte Published Applications keine globale Einstellung ist (das Kontrollkästchen Override Global ist aktiviert), stellen Sie sicher, dass das Feld ICA-Proxy auf OFF eingestellt ist.

     Geben Sie im Feld für die Webinterface-Adresse die URL mit der Datei config.xml für die XenApp Services-Site ein, die Gerätebenutzer verwenden, beispielsweise http://XenAppServerName/Citrix/PNAgent/config.xml oder http://XenAppServerName/BenutzerdefinierterPfad/config.xml.

   - Binden Sie die Sitzungsrichtlinie an den virtuellen Server.
   - Erstellen Sie Authentifizierungsrichtlinien für Cert und LDAP.
   - Binden Sie die Authentifizierungsrichtlinien an den virtuellen Server.
   - Konfigurieren Sie den virtuellen Server so, dass Clientzertifikate im SSL-Handshake angefordert werden. Öffnen Sie

dafür auf der Registerkarte Certificate die Option SSL-Parameters und stellen Sie für die Clientauthentifizierung Client Certificate auf Mandatory.
Wichtig: Wenn das auf dem Access Gateway verwendete Serverzertifikat Teil einer Zertifikatskette ist (mit einem Zwischenzertifikat), müssen Sie sicherstellen, dass die Zwischenzertifikate auch richtig auf dem Access Gateway installiert werden. Weitere Informationen zur Installation von Zertifikaten finden Sie in der Access Gateway-Dokumentation.

Konfigurieren des mobilen Geräts für die Receiver-Anwendung

Wenn die Clientzertifikatauthentifizierung in Access Gateway aktiviert ist, werden Benutzer basierend auf bestimmten Attributen des Clientzertifikats authentifiziert. Nachdem die Authentifizierung erfolgreich abgeschlossen ist, werden der Benutzername oder der Benutzer- und Gruppenname des Benutzers aus dem Zertifikat extrahiert und alle für den Benutzer angegebenen Richtlinien angewendet.

1. Öffnen Sie in Receiver das Konto und geben Sie im Feld Server den entsprechenden FQDN des Access Gateway-Servers ein, z. B. GatewayClientCertificateServer.organization.com. Receiver erkennt automatisch, dass das Clientzertifikat benötigt wird.
2. Benutzer können entweder ein neues Zertifikat installieren oder eines aus der Liste der bereits installierten Zertifikate auswählen. Für die iOS-Clientzertifikatauthentifizierung muss das Zertifikat heruntergeladen und nur von der Receiver-Anwendung installiert werden.
3. Nach der Auswahl eines gültigen Zertifikats wird im Feld für den Benutzernamen auf dem Anmeldebildschirm der Benutzername vom Zertifikat angezeigt; Benutzer geben die restlichen Angaben ein, u. a. Kennwort und Domäne für die Domänenauthentifizierung.
4. Wenn die Clientzertifikatauthentifizierung optional ist, können Benutzer die Zertifikatauswahl überspringen, wenn sie auf der Zertifikatseite auf Back klicken. In diesem Fall stellt Receiver die Verbindung her und zeigt dem Benutzer einen Anmeldebildschirm.
5. Nachdem Benutzer die Erstanmeldung abgeschlossen haben, können Sie Anwendungen ohne erneute Angabe des Zertifikats starten. Receiver speichert das Zertifikat für das Konto und verwendet es automatisch für weitere Anmeldungen.

Konfigurieren von Secure Gateway

Apr 13, 2015

Konfigurieren der XenApp Services-Site

Wichtig:

- Secure Gateway 3.x wird von Receiver für iOS mit XenApp Services-Sites unterstützt.
- Secure Gateway 3.x wird von Receiver für iOS mit XenApp Web-Sites unterstützt.
- Nur einstufige Authentifizierung wird für XenApp Services-Sites unterstützt; einstufige und zweistufige Authentifizierung werden für XenApp Web-Sites unterstützt.
- Sie müssen Webinterface 5.4 verwenden, das von allen integrierten Browsern unterstützt wird.

Installieren und konfigurieren Sie Secure Gateway für die Verwendung mit dem Webinterface, bevor Sie mit dieser Konfiguration beginnen. Sie können diese Anweisungen an ihre spezifische Umgebung anpassen.

Wenn Sie eine Secure Gateway-Verbindung verwenden, konfigurieren Sie keine Citrix Access Gateway-Einstellungen auf dem Receiver.

Receiver für Mobilgeräte ruft über eine XenApp Services-Site (früher Program Neighborhood Agent-Site) Informationen über die Anwendungen ab, für die ein Benutzer berechtigt ist und bietet sie Receiver an, der auf dem Gerät ausgeführt wird. Dies gleicht der Weise, wie das Webinterface für traditionelle SSL-basierte XenApp-Verbindungen, für die ein Access Gateway konfiguriert werden kann, verwendet wird. Diese Konfiguration ist in XenApp Services-Sites integriert, die auf einem Server mit dem Webinterface 5.x ausgeführt werden.

Konfigurieren Sie die XenApp Services-Site, um Verbindungen von einer Secure Gateway-Verbindung zu unterstützen.

1. Wählen Sie in der XenApp Services-Site Sicheren Clientzugriff verwalten > Einstellungen für sicheren Clientzugriff verwalten.
2. Ändern Sie die Zugriffsmethode zu Gateway: direkt.
3. Geben Sie den FQDN von Secure Gateway ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.
   Hinweis: Citrix empfiehlt, für Secure Gateway den Citrix Standardpfad für diese Site zu verwenden (http://XenAppServername/Citrix/PNAgent). Mit dem Standardpfad können Benutzer den FQDN von Secure Gateway angeben, zu dem Sie eine Verbindung herstellen, anstatt des vollständigen Pfads zu der Datei config.xml, die sich auf der XenApp Services-Site befindet (z. B. http://XenAppServername/BenutzerdefinierterPfad/config.xml).

Konfigurieren von Secure Gateway

1. Verwenden Sie den Secure Gateway-Konfigurationsassistenten, um Secure Gateway für die Verwendung mit dem Server im sicheren Netzwerk, der die XenApp Services-Site hostet, zu konfigurieren. Nachdem Sie die Option Indirect ausgewählt haben, geben Sie den FQDN-Pfad Ihres Secure Gateway-Servers ein und setzen Sie den Assistenten fort.
2. Testen Sie eine Verbindung von einem Benutzergerät aus, um sicherzustellen, dass Netzwerk und Zertifikatzuteilung für Secure Gateway richtig konfiguriert sind.

Konfigurieren des mobilen Geräts für die Receiver-Anwendung

1. Öffnen Sie die Kontoeinstellungen und geben Sie im Adressfeld denselben FQDN Ihres Secure Gateway-Servers ein:
   - Wenn Sie die XenApp Services-Site mit dem Standardpfad (/Citrix/PNAgent) erstellt haben, geben Sie den Secure Gateway-FQDN ein: SecureGatewayFQDN.Unternehmen.com .

- Wenn Sie den Pfad der XenApp Services-Site angepasst haben, geben Sie den vollständigen Pfad zur Datei config.xml an, z. B.: SecureGatewayFQDN.Unternehmen.com/BenutzerdefinierterPfad/config.xml .

2. Deaktivieren Sie in den Citrix Access Gateway-Einstellungen Access Gateway.

Konfigurieren von Access Gateway Enterprise Edition

Apr 13, 2015

Wichtig:

- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für iOS mit XenApp Services-Sites oder im Legacymodus auf StoreFront-Servern unterstützt.
- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für iOS mit XenApp Web-Sites unterstützt.
- Receiver für Web wird von Receiver für iOS nicht unterstützt.
- Access Gateway Enterprise Edition 9.x und 10.x werden von Receiver für iOS 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, können Sie Access Gateway für StoreFront konfigurieren. Die Methode für das Aktivieren des Zugriffs hängt von der in der Bereitstellung verwendeten CloudGateway-Edition ab:

- 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 unter dem Knoten in den eDocs.

Weitere Informationen zu den Einstellungen, die für Receiver für Mobilgeräte benötigt werden, finden Sie in den folgenden Themen:

- Erstellen des Sitzungsprofils für Receiver für CloudGateway Enterprise
- Erstellen des Sitzungsprofils für Receiver für CloudGateway Express
- Konfigurieren von benutzerdefinierten clientlosen Zugriffsrichtlinien für Receiver
- Configuring Secure Browse in Access Gateway (nur iOS-Geräte, wird nicht für Android-Geräte benötigt)
- Zugriff von Mobilgeräten
- MDX Toolkit für mobile Apps

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.

Konfigurieren des Webinterface

Apr 13, 2015

Konfigurieren der Webinterface-Site

Benutzer mit iPhone- und iPad-Geräten können Anwendungen über Ihre Webinterface-Site und den integrierten Safari-Browser auf dem Mobilgerät starten. Konfigurieren Sie die Webinterface-Site genauso wie für andere XenApp-Anwendungen. Wenn keine XenApp Services-Site für das Mobilgerät konfiguriert ist, verwendet Receiver automatisch die Webinterface-Site. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich.

Das Webinterface 5.x wird vom integrierten Safari-Browser unterstützt.

Starten von Anwendungen auf dem iOS-Gerät

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

Manuelles Konfigurieren von Konten

Apr 13, 2015

Wenn Receiver eine Verbindung mit einem Access Gateway herstellt, sucht Receiver im Allgemeinen nach der Authentifizierung eine XenApp Services-Site oder XenApp Web-Site. Wenn keine Site erkannt wird, zeigt Receiver einen Fehler an. Konfigurieren Sie ein Konto manuell, um diese Situation zu vermeiden, damit Receiver eine Verbindung mit Access Gateway herstellen kann.

Manuelles Konfigurieren von Konten

1. Tippen Sie oben rechts auf das Symbol Konten und tippen Sie dann auf dem Bildschirm Konten auf das Pluszeichen (+). Der Bildschirm Neues Konto wird angezeigt.
2. Tippen Sie unten links auf dem Bildschirm auf das Symbol links neben Optionen und tippen Sie dann auf Manuelles Setup. Zusätzliche Felder werden auf dem Bildschirm angezeigt.
3. Geben Sie im Feld Adresse die sichere URL der Site oder des Access Gateways an, zu der bzw. dem Sie eine Verbindung herstellen möchten (z. B. agee.mycompany.com).
4. Wählen Sie eine der folgenden Verbindungsoptionen. Die restlichen Felder auf dem Bildschirm werden abhängig der Auswahl geändert.
   - Webinterface: Bei Auswahl zeigt Receiver eine XenApp-Website an, die einem Webbrowser ähnelt. Dies wird auch Webansicht genannt.
   - XenApp Services: Bei Auswahl sucht Receiver eine bestimmte XenApp Services-Site, für die eine Authentifizierung über Access Gateway nicht konfiguriert ist. Geben Sie für die zusätzlichen Optionen, die auf diesem Bildschirm angezeigt werden, die Anmeldeinformationen für die Site an.
     - http://: Bei mehreren Stores wird eine Liste angezeigt und der Benutzer kann den Store auswählen, der hinzugefügt wird.
     - http:///citrix/: Der StoreFront-Store wird hinzugefügt.
     - http:///citrix/PnAgent/config.xml: Der Standard-PNAgent-Legacystore wird hinzugefügt.
     - http:///citrix//PnAgent/config.xml: Der PNAgent-Legacystore, der zugeordnet ist, wird hinzugefügt.
   - Access Gateway: Bei Auswahl stellt Receiver eine Verbindung mit einer XenApp Services-Site über einen bestimmten Access Gateway her. Wählen Sie in den zusätzlichen Optionen auf diesem Bildschirm die Serveredition und die Anmeldeinformationen aus, einschließlich des ggf. erforderlichen Sicherheitstokens für die Authentifizierung.
5. Verwenden Sie für die Zertifikatssicherheit die Einstellung im Feld Zertifikatwarnungen ignorieren und legen Sie fest, ob eine Verbindung mit dem Server hergestellt wird, selbst wenn das Zertifikat ungültig, selbstsigniert oder abgelaufen ist. Die Standardeinstellung ist Aus.
   Wichtig: Wenn Sie diese Option nicht aktivieren, stellen Sie sicher, dass Sie eine Verbindung mit dem richtigen Server herstellen. Citrix empfiehlt dringend, dass alle Server ein gültiges Zertifikat haben, um Benutzergeräte vor Onlinesicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt, dass die Zertifikatsicherheit nicht ausgelassen wird.
6. Tippen Sie auf Speichern.
7. Geben Sie den Benutzernamen und das Kennwort (oder das Token, wenn Sie die zweistufige Authentifizierung ausgewählt haben) ein und tippen Sie dann auf Anmelden. Der Citrix Receiver-Bildschirm wird angezeigt, von dem Sie auf die Desktops zugreifen und die Anwendungen hinzufügen und öffnen können.

Bereitstellen von RSA SecurID-Authentifizierung für iOS-Geräte

Aug 12, 2015

RSA SecurID-Authentifizierung für Citrix Receiver wird für Secure Gateway-Konfigurationen (nur über das Webinterface) und alle NetScaler Gateway-Konfigurationen unterstützt.

Weitere Informationen zur Konfiguration der RSA SecurID-Authentifizierung bei NetScaler Gateway finden Sie unter:

- Konfigurieren von RSA SecurID-Authentifizierung auf NetScaler Gateway 11.0
- Konfigurieren von RSA SecurID-Authentifizierung auf NetScaler Gateway 10.5
- Konfigurieren von RSA SecurID-Authentifizierung auf NetScaler Gateway 10.1

Für den Softwaretoken auf Receiver benötigtes URL-Schema: Der RSA SecurID-Softwaretoken, der von Receiver verwendet wird, registriert nur das URL-Schema com.citrix.securid.

Wenn Benutzer die Citrix Receiver-Anwendung und die RSA SecurID-Anwendung auf dem iOS-Gerät installiert haben, müssen Benutzer das URL-Schema "com.citrix.securid" auswählen, um den RSA SecurID-Softwareauthentifikator (Softwaretoken) in Receiver auf den Geräten zu installieren.

Importieren eines RSA SecurID-Softwaretokens in Citrix Receiver

Für die Verwendung eines RSA-Softwaretokens mit Citrix Receiver müssen Benutzer folgende Schritte ausführen.

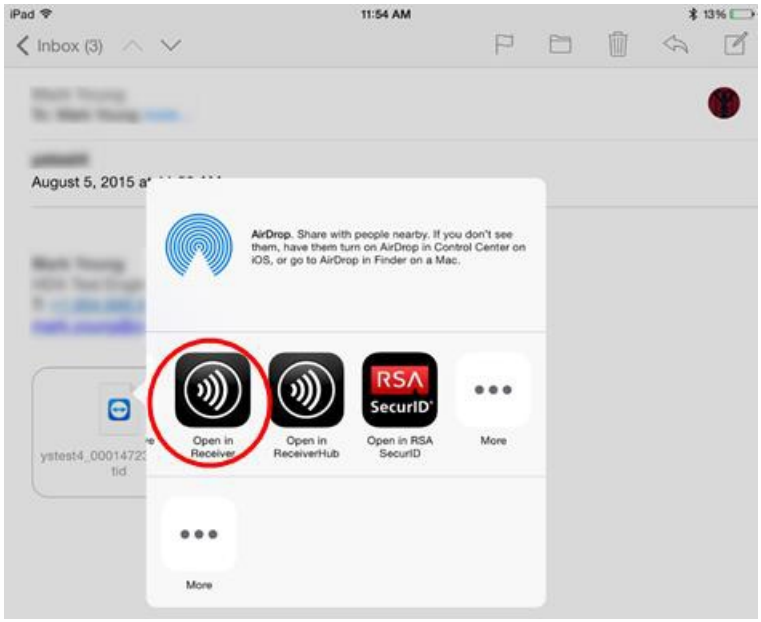
Die Richtlinie für die PIN-Länge, den Typ der PIN (nur nummerisch, alphanumerisch) und die Einschränkungen für die PIN-Wiederverwendung werden auf dem RSA-Verwaltungsserver festgelegt.

Die Benutzer müssen dies nur einmal ausführen. Nach der Authentifizierung am RSA-Server. Nach der Überprüfung der PINs werden sie auch am StoreFront-Server authentifiziert, und er zeigt verfügbare veröffentlichte Anwendungen und Desktops an.

Verwenden eines RSA-Softwaretokens mit Citrix Receiver

1. Importieren Sie den RSA-Softwaretoken, den Ihre Organisation bereitgestellt hat.

Wählen Sie in der E-Mail mit der angehängten SecurID-Datei **In Receiver öffnen** als Importzielort aus.



Nach dem Import des Softwaretokens wird Citrix Receiver automatisch geöffnet.

2. Falls Ihre Organisation ein Kennwort für den Abschluss des Imports bereitgestellt hat, geben Sie das bereitgestellte Kennwort ein und klicken Sie auf **OK**.

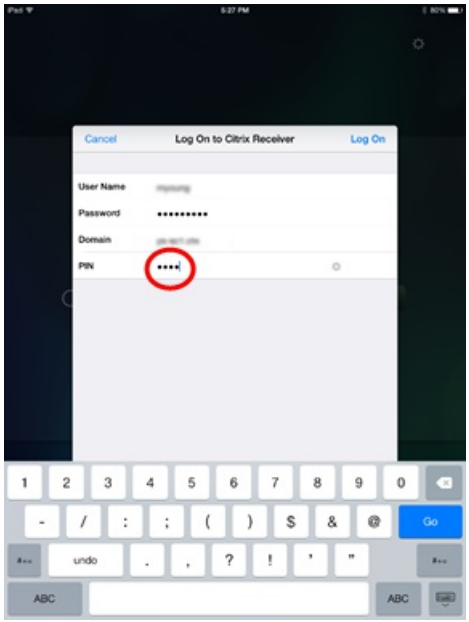
Nach dem Klicken auf **OK** gibt eine Meldung den erfolgreichen Import des Tokens an.

3. Schließen Sie die Importmeldung und klicken Sie in Citrix Receiver auf **Konto hinzufügen**.

- Geben Sie die URL des von der Organisation bereitgestellten Stores ein.
- Klicken Sie auf **Weiter.**

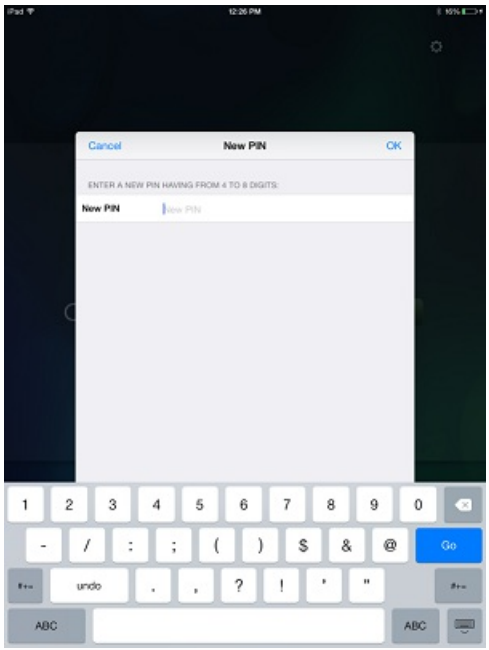
4. Auf dem Anmeldebildschirm:

- Geben Sie Ihre Anmeldeinformationen ein: Benutzername, Kennwort und Domäne (z. B. Beispiel.com).
- Geben Sie im Feld "PIN" **0000** ein, wenn Ihnen keine andere Standard-PIN bereitgestellt wurde. (Die PIN 0000 ist ein RSA-Standard; Ihre Organisation hat sie ggf. geändert, um eigene Sicherheitsrichtlinien einzuhalten.)
- Klicken Sie oben links auf **Anmelden**.



5. Nach dem Klicken auf die Schaltfläche "Anmelden" werden Sie zum Erstellen einer neuen PIN aufgefordert.

Geben Sie eine PIN mit 4 bis 8 Stellen ein und klicken Sie auf **OK**.



6. Sie müssen die neue PIN dann bestätigen. Geben Sie Ihre PIN erneut ein und klicken Sie auf **OK**.

Nach dem Klicken Auf "OK" können Sie auf die Apps und Desktops zugreifen.

Unterstützung für den Modus "Nächstes Token"

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.

Bereitstellen von Zugriffsinformationen für Endbenutzer von iOS-Geräten

Jun 26, 2013

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

- Konfigurieren der e-mail-basierten Kontenermittlung
- Bereitstellen einer Provisioningdatei für Benutzer
- Bereitstellen einer automatisch erstellten Setup-URL 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 oder das virtuelle AppController-Gerät, der bzw. das 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 einer automatisch erstellten Setup-URL für Benutzer

Sie können Receiver für Mobilgeräte mit Generierungsprogramm für die Setup-URL konfigurieren. Nach der Installation von Receiver klicken Benutzer auf die URL, um ihr Konto zu konfigurieren und auf die Ressourcen zuzugreifen. Konfigurieren Sie mit diesem Hilfsprogramm Einstellungen für Konten und E-Mail oder stellen Sie diese Informationen allen Benutzern gleichzeitig zur Verfügung.

Weitere Informationen finden Sie unter Automatisches Konfigurieren von Mobilgeräten.

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.

Sitzungsfreigabe

Wenn sich Benutzer auf dem iPad von einem Receiver-Konto abmelden und noch Verbindungen mit Anwendungen oder Desktops bestehen, können sie die Verbindung trennen oder sich abmelden:

- **Trennen**: Abmelden vom Konto; die auf dem Server ausgeführten Windows-Anwendungen oder Desktops werden nicht heruntergefahren. Der Benutzer kann dann ein anderes Gerät starten, Receiver öffnen und sich mit dem letzten Zustand wiederverbinden, bevor er die Verbindung mit dem iPad trennt. Mit dieser Option können sich Benutzer von einem Gerät mit einem anderen Gerät wiederverbinden und in den ausgeführten Anwendungen weiterarbeiten.
- **Abmelden**: Abmelden vom Konto, die Windows-Anwendung wird geschlossen das Konto wird vom XenApp- oder XenDesktop-Server abgemeldet. Mit dieser Option können Benutzer die Verbindung mit dem Server trennen und das Konto abmelden. Wenn sie Receiver erneut starten, wird er im Standardzustand geöffnet.

Automatisches Konfigurieren von Mobilgeräten

Apr 13, 2015

Administratoren oder Benutzer können mit dem Citrix Mobile Receiver Setup URL Generator auf einem PC oder Mac die Konfiguration von Citrix Receiver für Mobilgeräte vereinfachen. Konfigurieren Sie mit diesem Dienstprogramm die Einstellungen für XenApp-Konten und senden Sie die Konfigurationen per E-Mail gleichzeitig an viele Geräte.

Da der Benutzer den Benutzernamen und das Kennwort eingibt, werden nur der Servername, die Serveradresse, der Domänenname und die Access Gateway-Informationen für die Konfiguration benötigt.

1. Öffnen Sie den URL-Generator von Mobile Receiver Setup auf einem PC oder MAC über http://community.citrix.com/MobileReceiverSetupUrlGenerator/.
2. Geben Sie im Feld Account Description den Namen des Kontos ein, z. B. die Gruppe oder Abteilung (Produktion oder Vertrieb).
3. Geben Sie im Feld Server Address die Adresse der XenApp-Serverfarm ein, z. B. gateway.meineServerfarm.net.
4. Geben Sie für Domain den Domänennamen der Serverfarm ein, mit der sich die Benutzer verbinden.
5. Aktivieren Sie das Kontrollkästchen Use Gateway, um eine Access Gateway-Konfiguration zu ermöglichen.
    1. Wählen Sie unter Gateway type die Access Gateway-Edition, die in der Serverfarm bereitgestellt ist, mit der sich die Benutzer verbinden. (Wenden Sie sich an Ihren Administrator, wenn Sie die richtige Edition nicht kennen.)
    2. Wählen Sie unter Gateway Authentication Type die Authentifizierungsmethode aus, die in der Infrastruktur verwendet wird.
6. Klicken Sie auf Generate URL.
7. Klicken Sie in Your Result auf configuration link und kopieren Sie den erstellten Link.

Senden Sie den Link direkt per E-Mail an Mobilgeräte, damit Benutzer die Konfiguration des Kontos für Receiver auf dem Gerät abschließen können.
Wichtig: Bei einigen BlackBerry-Geräten muss eine Nur-Text-E-Mail verwendet werden, um die vorkonfigurierte URL richtig Receiver zuzuordnen. Die URL sollte aus diesem Grund immer in einer Nur-Text-E-Mail an BlackBerry-Benutzer gesendet werden.

Speichern von Kennwörtern

Mar 22, 2013

In der Webinterface Management Console können Sie die XenApp-Authentifizierungsmethode konfigurieren, 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.

Ausprobieren der Demo-Site

Oct 30, 2012

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.

Problembehandlung

Dec 08, 2014

Getrennte Sitzungen

Benutzer können eine Receiver-Sitzung wie folgt trennen (kein Abmelden):

- Drücken der Home-Taste auf dem Mobilgerät.
- Tippen auf Home oder Wechseln im Dropdownmenü der App.

Die Sitzung bleibt im getrennten Zustand. Benutzer können sich mit dieser Sitzung später wieder verbinden. Administratoren können aber auch sicherstellen, dass getrennte Sitzungen nach einem bestimmten Zeitraum deaktiviert werden. Hierfür konfigurieren Sie ein Sitzungstimeout für die ICA-tcp-Verbindung in der Konfiguration des Remotedesktop-Sitzungsserverhosts (früher "Terminaldienstekonfiguration" genannt). Weitere Informationen zur Konfiguration von Remotedesktopdiensten (früher "Terminaldienste" genannt) finden Sie in der Produktdokumentation für Microsoft Windows Server.

Probleme mit numerischen Tasten in Anwendungen

Wenn Benutzer feststellen, dass numerische Tasten in veröffentlichten Anwendungen nicht richtig funktionieren, können Sie die Unicode-Tastatur in Receiver deaktivieren. Tippen Sie hierfür auf der Registerkarte Einstellungen auf Tastaturoptionen und stellen Sie den Schalter für Unicode-Tastatur verwenden auf Aus.

Verlust der HDX-Audioqualität von XenDesktop

Von XenDesktop kann die Qualität von HDX-Audio zu Receiver für iOS verringert sein, wenn Audio und Video verwendet wird. Das Problem tritt auf, wenn die XenDesktop-HDX-Richtlinien die Audiodatenmenge mit den Videodaten nicht handhaben können. Empfehlungen zum Erstellen von Richtlinien für eine verbesserte Audioqualität finden Sie unter http://support.citrix.com/article/ctx123543.

Demo-Konten sind in der Citrix Cloud verfügbar

Benutzer, die kein Konto haben, können zu Demonstrationszwecken auf der Citrix Cloud-Demosite unter http://citrixcloud.net/ ein Benutzerkonto erstellen.

Citrix Cloud gibt Benutzern die Möglichkeit, die Leistung von Citrix Lösungen zu sehen, ohne dass eine eigene Umgebung eingerichtet und konfiguriert werden muss. In der Citrix Cloud-Demoumgebung werden zahlreiche wichtige Citrix Lösungen, unter anderem XenServer, XenApp, NetScaler und Access Gateway, verwendet.

In dieser Demoumgebung werden jedoch keine Daten gespeichert und wenn Sie die Verbindung trennen, können Sie sich u. U. nicht wieder an der Sitzung anmelden.

Abgelaufene Kennwörter

Receiver unterstützt das benutzerseitige Ändern abgelaufener Kennwörter. Benutzer werden zur Eingabe der benötigten Informationen aufgefordert.

Langsame Verbindungen

Wenn die Verbindung mit der XenApp Services-Site langsam ist oder Probleme wie fehlende Programmsymbole oder Meldungen zu "Protokolltreiberfehler" auftreten, können Sie als Workaround auf dem XenApp-Server und Citrix Secure Gateway oder dem Webinterface-Server die folgenden Citrix PV-Ethernetadapter-Eigenschaften für die Netzwerkkarte

deaktivieren (alle Eigenschaften sind standardmäßig aktiviert):

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

Ein Serverneustart ist nicht erforderlich. Dieser Workaround gilt für Windows Server 2003 und 2008 (32 Bit). Bei Windows Server 2008 R2 tritt das Problem nicht auf.

Eine Verbindung mit einem Proxy wird nicht unterstützt

Receiver kann keine Verbindung mit Netzwerken mit WiFi oder LAN-Proxies herstellen.

Anwendungen werden ggf. in verschiedenen Sitzungen geöffnet

Dieses serverseitige Problem kann auftreten, wenn die Anwendungsfreigabe aktiviert ist. Dies ist ein zeitweiliges Problem und es gibt keinen Workaround.