Info über Citrix Receiver für Mac 12

Jun 21, 2016

Citrix Receiver für Mac bietet Benutzern Self-Service-Zugriff auf Ressourcen, die auf XenApp- oder XenDesktop-Servern veröffentlicht sind. Receiver kombiniert einfache Bereitstellung und Verwendung und bietet schnellen, sicheren Zugriff auf gehostete Anwendungen und Desktops.

Sie können das aktuelle Release von der Downloadseite für Citrix Receiver für Mac herunterladen.

Neue Features in 12.1

Smartcardauthentifizierung bei NetScaler Gateway

Dieses Feature ermöglicht Citrix Receiver die Authentifizierung mit Smartcard beim Zugriff auf Apps und Desktops über NetScaler Gateway. Weitere Informationen zu diesem Feature finden Sie unter Anforderungen für die Smartcardauthentifizierung.

Unterstützung für geteilten Bildschirm unter El Capitan

Im vorherigen Release von Citrix Receiver für Mac (12.0) wurde Unterstützung für OS X El Capitan eingeführt. Dieses Release bietet volle Unterstützung für den geteilten Bildschirm in El Capitan.

Automatische Wiederverbindung von Clients und Verbesserungen bei der Sitzungszuverlässigkeit

Die Verbesserungen ermöglichen bessere Interoperabilität mit CloudBridge und NetScaler Gateway. Eine Sitzung kann durch automatische Wiederverbindung von Clients und höhere Sitzungszuverlässigkeit unabhängig vom Verbindungspfad wieder verbunden werden. Die folgenden Verbesserungen wurden in diesem Release umgesetzt:

Verbesserte Verbindungsmeldungen informieren Benutzer über den Verbindungsstatus und ggf. den Verlust der Verbindung und über mögliche Lösungen.

Ein Countdowntimer (in Minuten/Sekunden) zeigt an, wann die Sitzung abläuft. Nach Ablauf des Timers wird die Sitzung beendet. Standardmäßig ist das Sitzungstimeout auf 2 Minuten festgelegt. Sie können den Standardwert in der ICA-Dateieinstellung **TransportReconnectMaxRetrySeconds** ändern.

> ### Hinweis
>
> Dieses Feature bietet Unterstützung für eine zusätzliche Sitzungsverwaltungseinstellung in XenApp und XenDesktop: **TransportReconnectRetryMaxTimeSeconds**.
>
> **TransportReconnectDelay** und **TransportReconnectRetries** werden nicht mehr verwendet. Weitere Informationen finden Sie unter Sitzungsverwaltung.

In 12.0 eingeführte Features

Beim Verwenden von Receiver für Mac zusammen mit den zentralisierten Anpassungs- und Brandingfunktionen von StoreFront 3.0 können Benutzer von Receiver für Chrome Tech Preview von der zentral verwalteten App- und Desktopauswahl in StoreFront profitieren. Dies ist dieselbe konsistente Benutzererfahrung, die Benutzern von Windows Desktop-Receivern sowie HTML5- und Chrome Web-Receivern in Verbindung mit StoreFront 3.0 geboten wird.

Unterstützung für OS X El Capitan (10.11):

Unterstützung von Sitzungscookies: Citrix Receiver für Mac 12.0 unterstützt Websitzungscookies für die neue, für StoreFront 3.0 erforderliche Web-API und für Load Balancing.

Verbesserungen bei Zeitzonen: Citrix Receiver für Mac 12.0 erkennt lokale und Stadtzeitzonen genauer, wenn die XenApp-Zeitzonenumleitung verwendet wird. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Zeitzonensteuerung".

Behobene Probleme in Citrix Receiver für Mac 12

Jun 20, 2016

Behobene Probleme in Citrix Receiver für Mac 12

In diesem Release wurden mehrere mit der Smartcardintegration zusammenhängende Probleme behoben. Einige Probleme konnten noch nicht gelöst werden, aber es wird daran gearbeitet.

Weitere Probleme, die in diesem Release behoben wurden:

- Eine falsche Meldung wurde im Dialogfeld "Anmeldeinformationen" in japanischen Umgebungen angezeigt ("デモアカウント にログオンしてください", bedeutet "melden Sie sich am Demokonto an"). Diese Meldung sollte lauten "Melden Sie sich am eigenen virtuellen Desktop an." [#LC2682]
- Das gleichzeitige Bereitstellen mehrerer Receiver-Datenträgerimages kann zum Start des falschen Installationsprogramms führen. [#551605]
- OS X-Proxy-Umgehungseinträge in der CIDR-Notation wurden ignoriert. [#564250]
- Nur die ersten 256 Zeichen der OS X-Umgehungsliste werden verwendet. [#567089]
- Eine falsch positive Überprüfung eines internen Beacons kann ggf. für bestimmte ISPs fehlschlagen, die DNS-Fehlerumleitungssoftware von Barefruit installiert haben. [#572456]

Behobene Probleme in Citrix Receiver für Mac 12.1

- Ein Problem wurde behoben, bei dem Citrix Receiver bei aktivem VPN manchmal keine Verbindung mit einem konfigurierten Konto herstellen konnte, wenn die VPN-Unterstützung in OS X integriert war.
- Ein Problem in OS X El Capitan wurde behoben, bei dem Sitzungen nicht richtig in der geteilten Ansicht angezeigt wurden. [582397]
- Ein Problem wurde behoben, bei dem ein Fehler bei der Beaconerkennung auftrat, wenn versucht wurde, über einen F5-Proxy eine externe Verbindung herzustellen. [582885]
- Ein Problem wurde behoben, bei dem in den Systemeinstellungen konfigurierte Tastenkombinationen in der Sitzung nicht angewendet wurden. [583033]
- Ein Problem mit den "+"-Tastatursignalen in Citrix Receiver für Mac 11.9.15 und 12 wurde behoben, das den Absturz des Viewer verursachte. [586179] [577922]
- Ein Problem wurde behoben, bei dem Citrix Receiver nach dem Starten einer App zur Authentifizierung an einer anderen App aufforderte. [592460]
- Ein Problem in Desktopsitzungen wurde behoben, bei dem die Tastenkombination Strg+Q nicht richtig weitergegeben wurde. [600601]

Behobene Probleme in Citrix Receiver für Mac 12.1.100

- Ein Problem wurde behoben, das den Absturz einer Sitzung verursachte, wenn eine App oder ein Desktop gestartet wurde, deren/dessen Name mit einem @ beginnt. [LC4296]
- Ein Problem wurde behoben, das das Fehlschlagen von IPv6-Verbindungen zu NetScaler Gateway verursachte. [LC4512]
- Ein Problem wurde behoben, das das Fehlschlagen einer Receiver für Mac-Sitzung verursachte, wenn die Verbindung über ein Cisco ASA 9.32 SSL VPN hergestellt wurde. [LC3887]
- Ein Problem wurde behoben, das das Trennen von Sitzungen verursachte, sodass folgende Fehlermeldung angezeigt wurde: "Der Remote-SSL-Peer hat eine Warnung über einen MAC-Fehler gesendet." [LC4367]
- Ein Problem wurde behoben, das beim Eingeben eines einzelnen japanischen oder chinesischen Zeichens dazu führte, dass kein Zeichen auf dem Sitzungsdesktop angezeigt wurde. [603635]

Bekannte Probleme in Citrix Receiver für Mac 12

Jun 21, 2016

Bekannte Probleme in Citrix Receiver für Mac 12

In diesem Release bestehen die folgenden bekannten Probleme:

- Unter OS X El Capitan (10.11) werden virtuelle Desktops und Apps in der geteilten Ansicht nicht normal angezeigt. [#582397]
- Bei Verwendung von Smartcardauthentifizierung schlägt der Start von XenDesktop-Sitzungen fehl. [#550781]
- Bei Verwendung einer PIV-Smartcard kann Receiver die Verbindung mit einer XenDesktop 5.6-Sitzung nicht wiederherstellen. [#550986]
- Wenn eine veröffentlichte Eingabeaufforderung beim Trennen einer Sitzung minimiert wird, wird die Eingabeaufforderung ggf. nicht bei einer erneuten Verbindung angezeigt. [#411702]
- Das SSL SDK kennzeichnet eine Zertifikatkette ggf. falsch als "abgelaufen", wenn mehrere Zertifikate installiert werden und einige abgelaufen sind. Mit dem Löschen der abgelaufenen Zertifikate aus der Zertifikatkette wird das Problem behoben. [#511574]
- In Receiver angezeigte Anwendungsnamen reflektieren Updates von Broker und StoreFront möglicherweise nicht, wenn der Benutzer die Anwendungen abonniert hat, bevor die Updates stattfanden. In diesem Fall sollten Benutzer die Anwendungen löschen und erneut abonnieren. [#515097]
- Wenn eine Windows-Anmeldemeldung angezeigt wird und die Größe eines Desktopfensters geändert wird, funktioniert die Sitzung eventuell nicht mehr. [#525833]
- Bei Verwendung von OS X Mountain Lion (10.8) und einem Upgrade von Citrix Receiver 11.9 oder 11.9.15 auf Citrix Receiver 12.0 wird beim Start von Citrix Receiver ggf. eine neue und eine alte Version von Citrix Receiver geöffnet. [#552496]
- Bei Verwendung des Browsers Google Chrome für OS X werden beim Doppelklicken auf die ICA-Datei auf der Downloadleiste ggf. mehrere ICA-Dateien gestartet und es wird eine Fehlermeldung angezeigt. [#564961]
- Benutzer können ggf. das Kennwort nicht ändern, wenn sie sich an einem Webinterface-PNA-Konto anmelden. [#568394]
  Das untere Ende der XenDesktop-Symbolleistenschaltfläche wird u. U. abgeschnitten, wenn Benutzer in einer Videoanrufsitzung in den Vollbildmodus wechseln. [#570480]
- Benutzer von Computern mit OS X Mountain Lion (10.8) sehen u. U. eine Überlappung beim Text "Anmelden" und dem Nach-unten-Symbol auf der Benutzeroberfläche von Citrix Receiver. In diesem Fall können Benutzer auf "Anmelden" oder den Benutzernamen statt des Nach-unten-Symbols klicken. [#504302]
- Wenn für den Viewer der Vollbildmodus eingestellt wird, während DirectX oder OpenGL ausgeführt werden, verschwindet möglicherweise der Cursor. [#510745]
- Wenn die Sprache auf traditionelles Chinesisch festgelegt ist, können Benutzer in einer Sitzung u. U. nicht "[“ oder “]" eingeben. [#511877]
- Beim Bewegen des Cursors wechselt der Lync-Status nicht von "Abwesend" in "Verfügbar", wenn die Statusänderung durch Inaktivität des Benutzers verursacht wurde. In diesem Fall müssen Benutzer den Status manuell in "Verfügbar" ändern. [#512074]
- Bei einer Konfiguration mit mehreren Monitoren werden Seamless-Anwendungen u. U. auf die primäre Anzeige verschoben, wenn eine Anzeige neu konfiguriert wird. [#506532]
- HDX-Apps werden u. U. schwarz. Ziehen Sie die Anwendung in diesem Fall und schließen Sie sie, indem Sie dort klicken, wo die Schaltfläche zum Schließen sein sollte. [#426991]
- In OS X Yosemite (10.10) blockiert u. U. die aktualisierte Version von Safari Citrix Receiver als Popupfenster. Sie lösen dieses Problem, indem Sie das Öffnen von Popupfenstern für Apps/Desktops zulassen.

Bekannte Probleme in Citrix Receiver für Mac 12.1

In diesem Release bestehen die folgenden bekannten Probleme:

- Wenn die Größe eines Desktopfensters geändert wird während eine Windows-Anmeldemeldung angezeigt wird, funktioniert die Sitzung u. U. nicht mehr.

  [525833]
- Nach dem Starten eines virtuellen Desktops in Chrome wird u. U. eine Fehlermeldung angezeigt.

  [564961]
- Der Viewer sendet nicht das richtige Tastaturlayout an den Server, was u. U. zu Problemen bei der Tastaturzuordnung führt.

  [581829]
- Beim SmoothRoaming einer Sitzung auf eine Maschine mit OS X 10.11 (El Capitan) wird die Sitzungsverbindung u. U. nicht wiederhergestellt. Verwenden Sie zum Wiederverbinden den Menü "Apps aktualisieren", um die Verbindung mit der Sitzung wiederherzustellen, wenn es beim ersten Versuch nicht gelingt.
  [601542]

Systemanforderungen für Citrix Receiver für Mac 12

Sep 29, 2016

Unterstützte Betriebssysteme für Citrix Receiver für Mac 12.0.

- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)
- OS X Mountain Lion (10.8)

OS X-Releases vor Mountain Lion werden nicht unterstützt.

Wenn Sie eine Citrix Receiver-Version für Mac OS X Lion (10.7) oder älter benötigen, informieren Sie sich unter Citrix Receiver für Mac 11.9.x.

Hardwareanforderungen

- 110 MB freier Datenträgerspeicher
- Eine funktionierende Netzwerk- oder Internetverbindung für die Verbindung mit Servern

Unterstützte Server

- XenApp (eines der folgenden Produkte):
  - Citrix XenApp 7.6 für Windows Server 2012 R2
  - Citrix XenApp 7.5 für Windows Server 2012 R2
  - Citrix XenApp 6.5 für Windows Server 2008 R2
- XenDesktop (eines der folgenden Produkte):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
- Citrix VDI-in-a-Box 5.4 und 5.3
- StoreFront:
  - StoreFront 3.0
  - StoreFront 2.6
  - StoreFront 2.5
  - StoreFront 2.1
- Webinterface:
  - Webinterface 5.4 für Windows mit XenApp Services-Sites (auch PNAgent Services genannt) für den Zugriff auf Anwendungen nativ von Receiver statt über einen Webbrowser.
- Bereitstellen von Receiver
  - Citrix Receiver für Web 2.1, 2.5 und 2.6
  - Citrix Webinterface 5.4

Unterstützte Browser

- Safari 6.0 oder höher
- Mozilla Firefox 22.x oder höher
- Google Chrome 28.x oder höher

Konnektivität

Wenn Ihre Benutzer Citrix Receiver für Mac 12 auf OS X El Capitan ausführen und Probleme beim Herstellen von Verbindungen haben, müssen sie u. U. das NetScaler Gateway-Plug-In aktualisieren. Weitere Informationen finden Sie in dem folgenden Artikel auf der Citrix Downloadseite: NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support).

Citrix Receiver für Mac unterstützt HTTP-, HTTPS- und ICA-über-TLS-Verbindungen mit XenApp oder XenDesktop über eine der folgenden Konfigurationen.

LAN-Verbindungen:

- StoreFront mit StoreFront Services- oder Receiver für Web-Site
- Webinterface 5.4 für Windows mit XenApp Services-Sites

Für sichere Remote- oder lokale Verbindungen:

- Citrix NetScaler Gateway 11.0 einschließlich VPX
- Citrix NetScaler Gateway 10.5 einschließlich VPX
- Citrix NetScaler Gateway 10.1 einschließlich VPX
- Citrix Access Gateway Enterprise Edition 10.x einschließlich VPX
- Citrix Access Gateway Enterprise Edition 9.x einschließlich VPX
- Citrix Access Gateway VPX
- Citrix Secure Gateway 3.x (nur für die Verwendung mit Webinterface)

Weitere Informationen zur Bereitstellung von Access Gateway oder NetScaler Gateway mit StoreFront finden Sie in der Dokumentation für Access Gateway oder NetScaler Gateway und in der StoreFront-Dokumentation.

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*
Domänen-Passthrough					
Sicherheitstoken				Ja*	Ja*
Zweistufig (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Ja*

Smartcard** Benutzerzertifikat	Ja	Ja		Ja*	Ja*
	Receiver für Web mit Browsern	**StoreFront Services-Site (nativ)**	**StoreFront XenApp Services-Site (nativ)**	**NetScaler bei Receiver für Web (Browser)** Ja (NetScaler Gateway-Plug-In)	**NetScaler bei StoreFront Services-Site (nativ)** 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.

**Für die Verwendung von Smartcards auf OS X 10.10 muss mindestens OS X 10.10.2 installiert sein.

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	Ja			
Domäne	Ja	Ja	Ja	Ja
Domänen-Passthrough				
Sicherheitstoken			Ja*	Ja
Zweistufig (Domäne mit Sicherheitstoken)			Ja*	Ja
SMS			Ja*	Ja
Smartcard**	Ja	Ja	Ja	Ja
Benutzerzertifikat			Ja (NetScaler Gateway-Plug-In erforderlich)	Ja (NetScaler Gateway-Plug-In erforderlich)

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

**Smartcard wird nicht von OS X 10.10 unterstützt, da Apple die Smartcard-Unterstützung geändert hat.

Weitere Informationen zur Authentifizierung finden Sie in der NetScaler Gateway- oder Access Gateway-Dokumentation und in der StoreFront-Dokumentation in der Citrix Produktdokumentation. Informationen über andere Authentifizierungsmethoden, die das Webinterface unterstützt, finden Sie unter Konfigurieren der Authentifizierung für das Webinterface in der Webinterface-Dokumentation in der Citrix Produktdokumentation.

Anforderungen für die Smartcardauthentifizierung

Oct 28, 2015

Receiver für Mac unterstützt die Smartcardauthentifizierung für die folgenden Konfigurationen:

- Smartcardauthentifizierung bei Receiver für Web mit StoreFront 2.x und höher und XenDesktop 5.6 und höher oder XenApp 6.5 und höher über browserbasierten Zugriff.
- In smartcard-aktivierten Anwendungen, z. B. Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in virtuellen Desktop- oder Anwendungssitzungen verfügbar sind, digital signieren oder verschlüsseln.
- Mit mehreren Zertifikaten: Receiver für Mac unterstützt die Verwendung von mehreren Zertifikaten mit einer Smartcard oder mit mehreren Smartcards. Wenn ein Benutzer eine Smartcard in einen Kartenleser einsteckt, sind die Zertifikate für alle Anwendungen verfügbar, die auf dem Gerät ausgeführt werden, einschließlich Citrix Receiver.
- In Double-Hop-Sitzungen: Wenn ein Double Hop benötigt wird, wird eine weitere Verbindung zwischen Receiver und dem virtuellen Desktop des Benutzers hergestellt.

  Bereitstellungen, die Double Hop unterstützen, werden in der Dokumentation für XenApp und XenDesktop beschrieben. Weitere Informationen finden Sie unter Smartcardbereitstellungen.

Info über Smartcardauthentifizierung bei NetScaler

Wenn Sie eine Smartcard zur Authentifizierung einer Verbindung verwenden und auf der Smartcard mehrere verwendbare Zertifikate sind, fordert Citrix Receiver Sie auf, ein Zertifikat auszuwählen. Nach der Auswahl des Zertifikats werden Sie von Citrix Receiver aufgefordert, das Smartcard-Kennwort einzugeben. Nach erfolgter Authentifizierung wird die Sitzung gestartet.

Wenn auf der Smartcard nur ein passendes Zertifikat ist, verwendet Citrix Receiver das Zertifikat und Sie müssen keine Auswahl treffen. Sie müssen allerdings das Kennwort für die Smartcard eingeben, um die Verbindung zu authentifizieren und die Sitzung zu starten.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung

Mit den erweiterten Konfigurationsoptionen in den Einstellungen von Citrix Receiver können Sie das PKCS#11-Modul für Authentifizierungszwecke angeben:

1. Wählen Sie in Citrix Receiver **Einstellungen**.
2. Wählen Sie im Fenster "Einstellungen" die Option **Erweitert**.
3. Wählen Sie in dem Feld für PKCS#11 das entsprechende Modul aus. Klicken Sie auf **Weitere** und navigieren Sie zum Speicherort des PKCS#11-Moduls, wenn das gewünschte Modul nicht aufgeführt wird.
4. Wählen Sie das entsprechende Modul aus und klicken Sie auf **Hinzufügen**.

Unterstützte Leser, Middleware und Smartcardprofile

Receiver für Mac unterstützt die meisten, mit Mac OS X kompatiblen Smartcardleser und kryptografische Middleware. Die Funktion der folgenden Smartcardleser wurde von Citrix überprüft.

Unterstützte Smartcardleser:

- Gängige Smartcardleser mit USB-Anschluss

Unterstützte Middleware:

- Clariify
- Activeidentity (Clientversion)
- Charismathics (Clientversion)

Unterstützte Smartcards:

- PIV-Karten
- Common Access Card (CAC)

Folgen Sie zum Konfigurieren von Benutzergeräten den Anweisungen des Mac OS X-kompatiblen Smartcardlesers und der kryptografischen Middleware.

Einschränkungen

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Receiver für Mac speichert nicht die Zertifikatauswahl des Benutzers.
- Receiver für Mac speichert nicht die Smartcard-PIN des Benutzers. PIN-Abfragen werden vom Betriebssystem gehandhabt, das möglicherweise seinen eigenen Zwischenspeicherungsmechanismus hat.
- Receiver für Mac verbindet keine Sitzungen wieder, wenn eine Smartcard eingesteckt wird.
- Für die Verwendung von VPN-Tunneln mit der Smartcard-Authentifizierung müssen Benutzer das NetScaler Gateway Plug-In installieren und sich über eine Webseite anmelden und sich mit den Smartcards und PINs an jedem Schritt authentifizieren. Die Passthrough-Authentifizierung bei StoreFront mit dem NetScaler Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.

Weitere Informationen

Weitere Informationen finden Sie unter:

- Configuring Citrix XenDesktop 7.6 andNetScaler Gateway 10.5 with PIV SmartCard Authentication (PDF)
- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2

Installieren, Einrichten, Aktualisieren, Bereitstellen und Entfernen von Citrix Receiver für Mac

Sep 22, 2016

Dieses Release von Citrix Receiver für Mac enthält ein Installationspaket, CitrixReceiver.dmg, und unterstützt Remotezugriff über NetScaler Gateway, Access Gateway und Secure Gateway.

Dieser Abschnitt enthält folgende Themen:

- Manuelle Installation von Receiver für Mac
- Upgrade auf Receiver für Mac 12.0
- Info zum Bereitstellen und Konfigurieren von Receiver für Mac
- Bereitstellen von Receiver über Receiver für Web
- Bereitstellen von Receiver von einem Webinterface-Anmeldebildschirm
- Entfernen von Receiver für Mac

Installation

Receiver kann auf folgende Art installiert werden:

- Von einem Benutzer von Citrix.com
  - Ein Erstbenutzer von Receiver, der Receiver von Citrix.com oder Ihrer eigenen Downloadsite herunterlädt, kann ein Konto durch Eingabe einer E-Mail-Adresse statt einer Server-URL einrichten. Receiver ermittelt den der E-Mail-Adresse zugeordneten NetScaler Gateway oder StoreFront-Server und fordert anschließend den Benutzer zur Anmeldung und Fortsetzung der Installation auf. Dieses Feature wird als e-mail-basierte Kontenermittlung bezeichnet.
    Hinweis: Ein Erstbenutzer ist ein Benutzer, auf dessen Gerät Receiver nicht installiert ist.
  - Die e-mail-basierte Kontenermittlung für einen Erstbenutzer gilt nicht, wenn Receiver von einem anderen Speicherort (d. h. nicht Citrix.com) heruntergeladen wird (z. B. einer Receiver für Web-Site).
  - Wenn Receiver für Ihre Site konfiguriert werden muss, verwenden Sie eine andere Bereitstellungsmethode.
- Automatisch von Receiver für Web oder vom Webinterface
  - Ein Erstbenutzer von Receiver kann ein Konto durch Eingabe einer Server-URL oder durch Download einer Provisioningdatei einrichten.
- Mit einem ESD-Tool (Electronic Software Distribution)
  - Ein Erstbenutzer von Receiver muss eine Server-URL für das Einrichten des Kontos eingeben.

Manuelle Installation von Receiver für Mac

Benutzer können Receiver vom Webinterface, von einer Netzwerkfreigabe oder direkt auf dem Benutzergerät installieren, wenn sie die DMG-Datei für Citrix Receiver von der Citrix Website unter http://www.citrix.com herunterladen.

Installieren von Receiver für Mac

1. Laden Sie die DMG-Datei für die gewünschte Version von Receiver von der Citrix Website herunter und öffnen sie.
2. Klicken Sie auf der Eröffnungsseite auf Weiter.
3. Klicken Sie auf der Seite Lizenzierung auf Weiter.
4. Klicken Sie auf Akzeptieren, um die Bedingungen der Lizenzvereinbarung zu akzeptieren.
5. Klicken Sie auf der Seite Installationstyp auf Installieren.
6. Geben Sie den Benutzernamen und das Kennwort eines Administrators für das lokale Gerät ein.

Upgrade auf Receiver für Mac 12.0

Upgrades werden von den Versionen 10.x und 11.x des Online Plug-Ins für Mac unterstützt. Sie können auch ein Upgrade von den Versionen 11.3, 11.4, 11.5, 11.6, 11.7.x, 11.8.x und 11.9.x von Receiver für Mac durchführen.

Die ShareFile-Integration wurde von Version 11.8 entfernt. Wenn Receiver für Mac mit ShareFile integriert ist, werden Sie beim Upgrade aufgefordert, die ShareFile-Anwendung herunterzuladen, damit Sie weiterhin auf die Remotedaten zugreifen können.

Info zum Bereitstellen und Konfigurieren von Receiver für Mac

Bereitstellungen mit StoreFront:

- Sie sollten NetScaler Gateway und StoreFront 2.x so konfigurieren, wie es in der Citrix Dokumentation für diese Produkte beschrieben wird. Senden Sie die von StoreFront erstellte Provisioningdatei als Anlage in einer E-Mail und teilen Sie den Benutzern mit, wie die Aktualisierung und das Öffnen der Provisioningdatei nach der Installation von Receiver ausgeführt werden.
- Als Alternative zum Verwenden einer Provisioningdatei können Benutzer auch die URL eines NetScaler Gateways eingeben. Wenn Sie die e-mail-basierte Kontenermittlung konfiguriert haben, wie in der StoreFront-Dokumentation beschrieben, fordern Sie die Benutzer zur Eingabe ihrer E-Mail-Adresse auf.
- Eine andere Methode ist die Konfiguration einer Receiver für Web-Site, wie in der StoreFront-Dokumentation beschrieben. Geben Sie den Benutzern die Informationen zum Upgrade von Receiver, zum Zugriff auf die Receiver für Web-Site und zum Download der Provisioningdatei von der Receiver für Web-Oberfläche (klicken Sie auf den Benutzernamen und dann auf Aktivieren).

Bereitstellungen mit dem Webinterface:

- Aktualisieren Sie die Webinterface-Site mit Receiver für Mac 11.9 und teilen Sie den Benutzern mit, wie Receiver aktualisiert wird. Sie können beispielsweise Benutzern Installationsmeldungen auf dem Bildschirm Meldungen bereitstellen, damit Benutzer wissen, dass sie auf die aktuelle Receiver-Version aktualisieren müssen.

Bereitstellen von Receiver über Receiver für Web

Sie können Receiver über Receiver für Web bereitstellen, um sicherzustellen, dass Receiver auf dem Benutzergerät installiert ist, bevor der Benutzer versucht, über einen Browser eine Verbindung zu einer Anwendung herzustellen. Mit Receiver für Web-Sites können Benutzer über eine Webseite auf StoreFront-Stores zugreifen. Wenn die Receiver für Web-Site erkennt, dass ein Benutzer keine kompatible Receiver-Version hat, wird der Benutzer zum Download und zur Installation von Receiver aufgefordert. Weitere Informationen finden Sie in der Dokumentation für StoreFront .

Bereitstellen von Receiver von einem Webinterface-Anmeldebildschirm

Sie können Receiver auf einer Webseite bereitstellen, um sicherzustellen, dass Receiver auf dem Benutzergerät installiert ist, bevor sie das Webinterface verwenden. Das Webinterface enthält einen Clienterkennungs- und -bereitstellungsprozess, der erkennt, welche Citrix Clients in der Umgebung des Benutzers bereitgestellt werden können, und der die Benutzer bei der Bereitstellung unterstützt.

Die Clienterkennung und -bereitstellung kann automatisch ausgeführt werden, wenn Benutzer auf eine XenApp-Website zugreifen. Wenn das Webinterface erkennt, dass ein Benutzer keine kompatible Receiver-Version hat, wird der Benutzer zum Download und zur Installation von Receiver aufgefordert.

Sie können Benutzern auch Installationsmeldungen bereitstellen, die Benutzern als Links auf der Seite Meldungen angezeigt werden. Durch Klicken auf solch einen Link können sie den Clienterkennungs- und -bereitstellungsprozess starten. Mit Installationsmeldungen können Sie Benutzern auch ermöglichen, auf den Clienterkennungs- und -bereitstellungsprozess

zuzugreifen, um die Citrix Clients auf eine neuere Version zu aktualisieren.

Für den Clienterkennungs- und -bereitstellungsprozess müssen die Receiver-Installationsdateien auf dem Webinterface-Server vorhanden sein. Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Receiver-Installationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Receiver von der Citrix Website herunterladen oder ältere Versionen von Receiver bereitstellen möchten, prüfen Sie, ob die richtigen Namen der Receiver-Installationsdatei für den Parameter ClientIcaMac in den Konfigurationsdateien Ihrer XenApp Web-Sites angegeben sind.

Weitere Informationen finden Sie in der Dokumentation zum Webinterface .

Entfernen von Receiver für Mac

Sie können Receiver manuell deinstallieren. Öffnen Sie die Datei CitrixReceiver.dmg und wählen Sie Citrix Receiver deinstallieren aus. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen.

Konfigurieren von Citrix Receiver für Mac

Oct 28, 2015

Nach der Installation der Receiver-Software können die Benutzer mit den folgenden Konfigurationsschritten auf ihre gehosteten Anwendungen und Desktops zugreifen:

- Konfigurieren der Anwendungsbereitstellung: Stellen Sie sicher, dass die XenApp-Umgebung richtig konfiguriert ist. Machen Sie sich mit den Optionen vertraut und geben Sie aussagekräftige Anwendungsbeschreibungen für Benutzer an.
- Konfigurieren des Self-Service-Modus: Konfigurieren Sie den Self-Service-Modus, der Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Receiver ermöglicht.
- Konfigurieren von StoreFront: Erstellen Sie Stores, die Desktops und Anwendungen von XenDesktop-Sites und XenApp-Farmen auflisten und aggregieren und diese Ressourcen Benutzern zur Verfügung stellen.
- Bereitstellen der Kontoinformationen für Benutzer: Teilen Sie den Benutzern die Informationen mit, die sie zum Zugriff auf die Konten benötigen, unter denen die Anwendungen und Desktops ausgeführt werden. In einigen Umgebungen müssen Benutzer den Zugriff auf Konten manuell einrichten.
- Wenn Benutzer eine Verbindung von außerhalb des internen Netzwerks herstellen (beispielsweise Benutzer, die eine Verbindung vom Internet oder von Remotestandorten herstellen), konfigurieren Sie die Authentifizierung über NetScaler Gateway. Weitere Informationen finden Sie unter NetScaler Gateway .

Konfigurieren der Anwendungsbereitstellung

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit XenDesktop oder XenApp, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen zu erhöhen:

Webzugriffsmodus

Ohne jegliche Konfiguration bietet Receiver für Mac im Webzugriffsmodus browserbasierten Zugriff auf Anwendungen und Desktops. Benutzer greifen einfach über einen Browser auf eine Receiver für Web- oder Webinterface-Site zu und wählen die gewünschten Anwendungen zur Verwendung aus. Im Webzugriffsmodus werden keine Appverknüpfungen im App-Ordner auf den Benutzergeräten platziert.

Self-Service-Modus

Sie konfigurieren den Self-Service-Modus durch Hinzufügen eines StoreFront-Kontos zu Receiver oder durch Verweisen von Receiver auf eine StoreFront-Site. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über Receiver. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores. Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren. Wenn ein Benutzer eine Anwendung auswählt, wird eine Verknüpfung für die Anwendung im App-Ordner auf dem Benutzergerät platziert.

Beim Zugreifen auf eine StoreFront 3.0-Site erleben Benutzer die Receiver Tech Preview Benutzererfahrung. Weitere Informationen zur Benutzererfahrung mit Receiver Tech Preview finden Sie unter Receiver und StoreFront 3.0 Technology Preview.

Wenn Sie Anwendungen auf einer XenApp-Farm veröffentlichen, können Sie die Erfahrung für Benutzer verbessern, die auf diese Anwendungen über StoreFront-Stores zugreifen, indem Sie aussagekräftige Beschreibungen für die veröffentlichten Anwendungen hinzufügen. In Citrix Receiver sind diese Beschreibungen für Benutzer sichtbar.

Konfigurieren des Self-Service-Modus

Wie schon erläutert konfigurieren Sie den Self-Service-Modus durch Hinzufügen eines StoreFront-Kontos zu Receiver oder durch Verweisen von Receiver auf eine StoreFront-Site. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Receiver. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

- 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.
- Hängen Sie die Zeichenfolge KEYWORDS:Featured der Anwendungsbeschreibung an, um den Benutzern Anwendungen anzukündigen oder häufig verwendete Anwendungen in der Liste Highlights anzuzeigen.

Weitere Informationen finden Sie in der Dokumentation für StoreFront.

Wenn das Webinterface in der XenApp-Bereitstellung keine XenApp Services-Site hat, erstellen Sie eine Site. Der Name und die Erstellung der Site hängen von der installierten Webinterface-Version ab. Weitere Informationen finden Sie in der Dokumentation zum Webinterface.

Konfigurieren von StoreFront

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 in der StoreFront-Dokumentation .

   Hinweis: Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für Receiver erstellen.
2. Stores für CloudGateway konfigurieren Sie genauso wie für andere XenApp- und XenDesktop-Anwendungen. Für Receiver ist keine spezielle Konfiguration erforderlich. Weitere Informationen finden Sie unter *— Konfigurieren von Stores* in der StoreFront -Dokumentation.

Bereitstellen der Kontoinformationen für Benutzer

Nach der Installation müssen Sie den Benutzern die Kontoinformationen bereitstellen, die für den Zugriff auf die gehosteten Anwendungen und Desktops benötigt werden. Sie können diese Informationen folgendermaßen bereitstellen:

- Konfigurieren der Kontenermittlung mit der E-Mail-Adresse
- 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 NetScaler Gateway-, Access Gateway- oder StoreFront-Server, der der E-Mail-Adresse auf der Basis von DNS-

Dienstdatensätzen zugeordnet ist, und fordert den Benutzer dann zur Anmeldung auf, um auf gehostete Anwendungen und Desktops zuzugreifen.

Weitere Informationen zur Konfiguration des DNS-Servers für die e-mail-basierte Discovery finden Sie im Abschnitt *— Konfigurieren der e-mail-basierten Kontenermittlung* in der StoreFront-Dokumentation.

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

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 Datei, um Receiver zu konfigurieren. Wenn Sie Receiver für Web-Sites konfigurieren, können Benutzer Receiver-Provisioningdateien auch von diesen Seiten abrufen.

Weitere Informationen finden Sie in der Dokumentation für StoreFront.

Bereitstellen einer automatisch erstellten Setup-URL für Benutzer

Mit dem Citrix Receiver für Mac Setup URL Generator können Sie eine URL erstellen, die Kontoinformationen enthält. 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.

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 URL für den StoreFront-Store oder die XenApp Services-Site, der bzw. die Ressourcen hostet. Beispiel: https://servername.example.com
- Für den Zugriff mit NetScaler Gateway oder Access Gateway wird die NetScaler Gateway- oder Access Gateway-Adresse, die Produktedition und die erforderliche Authentifizierungsmethode benötigt.
  Weitere Informationen zur Konfiguration von NetScaler Gateway oder Access Gateway finden Sie in der Dokumentation für NetScaler Gateway oder Access 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.

Optimieren der Citrix Receiver für Mac-Umgebung

Oct 28, 2015

Sie können die Umgebung mit Folgendem optimieren, um die beste Receiver-Leistung zu erhalten:

- Automatische Wiederverbindung von Benutzern
- Bereitstellen von HDX Broadcast-Sitzungszuverlässigkeit
- Kontinuität für mobile Benutzer
- Zuweisen von Clientgeräten

Wiederverbinden von Benutzern

Automatische Wiederverbindung von Benutzern

Benutzer können von ICA-Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit der automatischen HDX Broadcast-Wiederverbindung von Clients kann Receiver unabsichtlich getrennte Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden.

Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können. Receiver versucht, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Wenn eine Benutzerauthentifizierung erforderlich ist, wird dem Benutzer bei der automatischen Wiederverbindung ein Dialogfeld zur Eingabe der Anmeldeinformationen angezeigt. Die automatische Wiederverbindung findet nicht statt, wenn Benutzer Anwendungen beenden, ohne sich abzumelden.

Sie konfigurieren die automatische HDX Broadcast Wiederverbindung von Clients mit Richtlinieneinstellungen auf dem Server. Weitere Informationen finden Sie in der Dokumentation von XenApp und XenDesktop .

Neustarten von Desktops

Benutzer können einen virtuellen Desktop neu starten, wenn er nicht startet, beschädigt wird oder das Herstellen der Verbindung zu lange dauert. Sie konfigurieren dieses Feature in XenDesktop.

Das Kontextmenü-Element Neu starten ist auf allen Desktops verfügbar, die Benutzer abonniert haben, und auf der App-Seite der Benutzer. Das Menüelement ist deaktiviert, wenn der Neustart nicht für den Desktop aktiviert ist. Wenn der Benutzer Neu starten auswählt, fährt Receiver den Desktop herunter und startet ihn dann neu.

Wichtig: Teilen Sie Benutzern mit, dass der Neustart von Desktops zu einem Verlust der Daten führen kann.

Bereitstellen von HDX Broadcast-Sitzungszuverlässigkeit

Mit der HDX Broadcast-Sitzungszuverlässigkeit werden den Benutzern die Fenster einer gehosteten Anwendung und eines Desktops angezeigt, wenn die Verbindung unterbrochen ist. Beispiel: Benutzer, die eine drahtlose Verbindung verwenden und in einen Tunnel fahren, können die Verbindung im Tunnel verlieren. Die Verbindung wird bei der Ausfahrt aus dem Tunnel wiederhergestellt. Während die Verbindung unterbrochen ist, wird das Sitzungsfenster mit der Sitzungszuverlässigkeit weiterhin angezeigt, bis die Verbindung wiederhergestellt wird.

Sie können Ihr System so konfigurieren, dass Benutzern eine Warnungsmeldung angezeigt wird, wenn die Verbindung nicht verfügbar ist.

Sie konfigurieren die HDX Broadcast-Sitzungszuverlässigkeit mit Richtlinieneinstellungen auf dem Server. Weitere Informationen finden Sie in der XenDesktop- und XenApp-Dokumentation .

Receiver-Benutzer können die Servereinstellungen für die HDX Broadcast-Sitzungszuverlässigkeit nicht überschreiben.

Wichtig: Wenn die HDX Broadcast-Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

Kontinuität für mobile Benutzer

Mit Workspace Control folgen Desktops und Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Workstation zu einer anderen gehen, ohne ihre Desktops und Anwendungen auf jedem einzelnen Gerät neu starten zu müssen.

Die Richtlinien und die Clientlaufwerkzuordnung ändern sich entsprechend, wenn Benutzer zu einem anderen Benutzergerät wechseln. Die angewendeten Richtlinien und Zuordnungen hängen vom Benutzergerät ab, an dem Sie momentan an einer Sitzung angemeldet sind. Wenn sich Pflegepersonal z. B. von einem Benutzergerät in der Notaufnahme des Krankenhauses abmeldet und dann an einer Arbeitsstation in der Röntgenabteilung anmeldet, gelten für die Sitzung die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen der Röntgenabteilung, solange der Benutzer am Benutzergerät der Röntgenabteilung angemeldet ist.

Konfigurieren der Workspace Control-Einstellungen

1. Klicken Sie im Receiver-Fenster auf das Pfeil-unten-Symbol und wählen Sie Einstellungen.
2. Klicken Sie auf die Registerkarte Allgemein.
3. Wählen Sie eine der folgenden Optionen:
   - Verbindungen zu Anwendungen wiederherstellen, wenn ich Receiver starte: Benutzer können eine Verbindung mit getrennten Anwendungen wiederherstellen, wenn Sie Receiver starten.
   - Verbindungen zu Anwendungen wiederherstellen, wenn ich Anwendungen starte oder aktualisiere: Benutzer können eine Verbindung mit getrennten Apps wiederherstellen, wenn sie die Apps starten oder im Citrix Receiver-Menü Apps aktualisieren auswählen.

Zuweisen von Clientgeräten

Receiver ordnet lokale Laufwerke und Geräte automatisch zu, damit sie in einer Sitzung verfügbar sind. Wenn die Clientgerätzuordnung auf dem Server aktiviert ist, kann eine auf dem Server ausgeführte Remoteanwendung oder ein Remotedesktop auf Geräte zugreifen, die an das lokale Benutzergerät angeschlossen sind. Sie haben folgende Möglichkeiten:

- Zugreifen auf lokale Laufwerke, COM-Ports und Drucker
- Wiedergeben von Audiodateien (Systemklänge und Audiodateien), die in der Sitzung abgespielt werden

Hinweis: Für die Clientaudiozuordnung und die Clientdruckerzuordnung ist keine Konfiguration auf dem Benutzergerät erforderlich.

Zuordnen von Clientlaufwerken

Mit der Clientlaufwerkzuordnung greifen Sie auf lokale Laufwerke auf dem Benutzergerät in Sitzungen zu, z. B. CD-Laufwerke, DVDs und Memory Stick (USB). Wenn ein Server für die Clientlaufwerkzuordnung konfiguriert ist, können Benutzer auf lokal gespeicherte Dateien zugreifen, diese in Sitzungen bearbeiten und dann entweder auf einem lokalen Laufwerk oder einem Laufwerk auf dem Server speichern.

Receiver überwacht die Verzeichnisse, in denen Hardwaregeräte wie CDs, DVDs und Memory Sticks (USB) normalerweise auf dem Benutzergerät bereitgestellt werden, und ordnet neue in der Sitzung automatisch dem nächsten verfügbaren Laufwerkbuchstabe auf dem Server zu.

Sie können den Lese- und Schreibzugriff für zugeordnete Laufwerke in den Receiver-Einstellungen konfigurieren.

Konfigurieren des Lese- und Schreibzugriffs für zugeordnete Laufwerke

1. Klicken Sie auf der Receiver-Homepage auf das Pfeil-nach-unten-Symbol und klicken Sie dann auf Einstellungen.
2. Klicken Sie auf Geräte.
3. Wählen Sie das Niveau für den Lese- und Schreibzugriff für zugeordnete Laufwerke unter den folgenden Optionen aus:
   - Lese-/Schreibrechte
   - Leserechte
   - Kein Zugriff
   - Immer fragen
4. Melden Sie sich von offenen Sitzungen ab und erneut an, um die Änderungen anzuwenden.

Zuordnen von COM-Ports für Clients

Mit der Client-COM-Portzuordnung können Geräte, die an COM-Ports des Benutzergeräts angeschlossen sind, in Sitzungen verwendet werden. Diese Zuordnungen können genau wie andere Netzwerkzuordnungen verwendet werden.

Die seriellen Macintosh-Ports stellen nicht alle Steuersignalleitungen bereit, die von Windows-Anwendungen verwendet werden. Die Leitungen DSR (Data Set Ready), DCD (Device Carrier Detect), RI (Ring Indicator) und RTS (Request To Send) sind nicht verfügbar. Windows-Anwendungen, die diese Signale für das Handshaking und die Flusssteuerung benötigen, funktionieren ggf. nicht. Die Macintosh-Implementierung der seriellen Kommunikation verlässt sich nur auf die Leitungen CTS (Clear To Send) und DTR (Data Terminal Ready) für das Eingabe- und Ausgabehardware-Handshaking.

Zuordnen eines Client-COM-Ports

1. Klicken Sie auf der Receiver-Homepage auf das Pfeil-nach-unten-Symbol und klicken Sie dann auf Einstellungen.
2. Klicken Sie auf Geräte.
3. Wählen Sie den gewünschten COM-Port aus der Liste Zugeordnete COM-Ports aus. Dies ist der virtuelle COM-Port, der in der Sitzung angezeigt wird, nicht der physische Port auf dem lokalen Computer.
4. Wählen Sie das Gerät, das Sie dem virtuellen COM-Port zuordnen möchten, im Kontextmenü Gerät aus.
5. Starten Sie Receiver und melden Sie sich an einem Server an.
6. Öffnen Sie eine Eingabeaufforderung. Geben Sie Folgendes ein:
   net use comx: \\client\comz:

   wobei x die Nummer des COM-Ports auf dem Server ist (für die Zuordnung stehen die Ports 1 bis 9 zur Verfügung) und z die Nummer des Client-COM-Ports (Port 1 bis 4 stehen zur Verfügung).

7. Geben Sie an der Eingabeaufforderung net use ein, um die Zuordnung zu bestätigen. Eine Liste der zugeordneten Laufwerke, LPT-Ports und zugeordneten COM-Ports wird angezeigt.

Verbessern der Benutzererfahrung in Citrix Receiver für Mac

Oct 28, 2015

Sie können die Erfahrung der Benutzer mit den folgenden unterstützten Features verbessern:

- ClearType-Schriftartenglättung
- Clientseitige Mikrofoneingabe
- Windows-Sondertasten
- Windows-Tastenkombinationen
- Verwenden eines Eingabemethoden-Editors (IME) und internationaler Tastaturlayouts
- Verwenden mehrerer Monitore
- Verwenden der Desktopsymbolleiste

ClearType-Schriftartenglättung

Mit ClearType-Schriftartenglättung (auch Subpixel-Rendering von Schriftarten genannt) wird eine höhere Qualität der Schriftartenanzeige erzielt als bei traditioneller Schriftartenglättung oder Anti-Aliasing.

Wenn Sie die ClearType-Schriftartglättung auf dem Server aktivieren, werden Benutzergeräte nicht gezwungen, die ClearType-Schriftartglättung zu verwenden. Sie ermöglichen die serverseitige Unterstützung der ClearType-Schriftartglättung auf Benutzergeräten, auf denen diese Funktion lokal aktiviert ist, und die Receiver verwenden.

Receiver erkennt automatisch die Einstellung für Schriftartglättung auf dem Benutzergerät und sendet diese Informationen an den Server. Die Sitzungsverbindung wird mit dieser Einstellung hergestellt. Wenn die Sitzung getrennt oder beendet wird, nimmt der Server die ursprüngliche Einstellung wieder an.

Clientseitige Mikrofoneingabe

Receiver unterstützt die mehrfache clientseitige Mikrofoneingabe. Lokal installierte Mikrofone können für Folgendes verwendet werden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Unterstützung für digitale Diktate ist mit Receiver verfügbar. Weitere Informationen zur Konfiguration dieses Features finden Sie in der Dokumentation für XenApp und XenDesktop.

Sie können wählen, ob Mikrofone, die an das Benutzergerät angeschlossen sind, in Sitzungen verwendet werden. Wählen Sie hierfür eine der folgenden Optionen in den Receiver-Einstellungen auf der Registerkarte "Mikrofon und Webcam" aus:

- Mikrofon und Webcam verwenden
- Mikrofon und Webcam nicht verwenden
- Immer fragen

Wenn Sie Jedes Mal fragen auswählen, werden Sie bei jedem Herstellen einer Verbindung zu gehosteten Anwendungen oder Desktops in einem Dialogfeld gefragt, ob Sie das Mikrofon in dieser Sitzung verwenden möchten.

Windows-Sondertasten

Receiver stellt zahlreiche zusätzliche Optionen und vereinfachte Methoden für den Ersatz von Sondertasten bereit, u. a.

Ersatz von Funktionstasten in Windows-Anwendungen durch Mac-Tasten. Auf der Registerkarte Tastatur konfigurieren Sie die gewünschten Optionen wie folgt:

- Mit "Control-Zeichen senden mit" können Sie auswählen, ob Sie die Befehl-Zeichentaste-Tastenkombinationen als Strg+-Zeichentaste-Tastenkombinationen in einer Sitzung senden. Wenn Sie "Befehl oder Control" im Kontextmenü auswählen, können Sie bekannte Befehl-Zeichentaste- oder Strg-Zeichentaste-Tastenkombinationen auf dem MAC als Strg+Zeichentaste-Tastenkombinationen an den PC senden. Wenn Sie Befehl auswählen, müssen Sie Strg+Zeichentastekombinationen verwenden.
- Mit "Alt-Zeichen senden mit" können Sie auswählen, wie die Alt-Taste in einer Sitzung repliziert wird. Wenn Sie die Befehl-Option auswählen, können Sie Befehl-Option-Tastenkombinationen als Alt-Tastenkombinationen in einer Sitzung senden. Sie können auch Befehl auswählen und die Befehl-Taste als Alt-Taste verwenden.
- Mit "Windows-Logo-Taste mit Befehl (rechts) senden" können Sie die Windows-Logo-Taste durch Druck der Befehl-Taste an der rechten Seite der Tastatur an Remotedesktops und Anwendungen senden. Wenn diese Option deaktiviert ist, hat die rechte Befehl-Taste dieselbe Funktion wie die linke Befehl-Taste gemäß den zwei obigen Einstellungen im Dialogfeld "Einstellungen". Sie können die Windows-Logo-Taste jedoch mit dem Menü "Tastatur" senden. Wählen Sie Tastatur > Windows-Tastenkombination senden > Start.
- Mit "Sondertasten unverändert senden" deaktivieren Sie die Konvertierung von Sondertasten. Beispiel: Die Kombination Option-1 (auf der Zehnertastatur) entspricht der Sondertaste F1. Sie können dieses Verhalten ändern und diese Sondertaste so einstellen, dass sie 1 (die Zahl 1 auf der Zehnertastatur) in der Sitzung darstellt, wenn Sie das Kontrollkästchen "Sondertasten unverändert senden" aktivieren. In der Standardeinstellung ist dieses Kontrollkästchen nicht aktiviert, d. h. Option-1 wird als F1 an die Sitzung gesendet.

Funktions- und andere Sondertasten werden mit dem Menü "Tastatur" an eine Sitzung gesendet.

Wenn die Tastatur eine Zehnertastatur enthält, können Sie die folgenden Tastaturanschläge verwenden:

PC-Taste oder Aktion	**Mac-Optionen**
Einfügen	0 (die Zahl 0) auf der Zehnertastatur. Die Num-Taste muss deaktiviert sein. Sie können sie mit der Pause-Taste ein- und ausschalten. Option-Hilfe
Löschen	Dezimalstelle auf der Zehnertastatur. Die Num-Taste muss deaktiviert sein. Sie können sie mit der Pause-Taste ein- und ausschalten. Entfernen
F1 bis F9	Option-1 bis -9 (die Zahlen 1 bis 9) auf der Zehnertastatur
F10	Option-0 (die Zahl 0) auf der Zehnertastatur
F11	Option-Minuszeichen auf der Zehnertastatur
F12	Option-Pluszeichen auf der Zehnertastatur

Windows-Tastenkombinationen

In Remotesitzungen werden die meisten Mac-Tastaturkombinationen für die Texteingabe erkannt, wie z. B. Option-G für die Eingabe des Copyrightsymbols ©. Einige Tastaturanschläge in einer Sitzung werden jedoch nicht in der Remoteanwendung oder auf dem Remotedesktop angezeigt sondern vom Mac-Betriebssystem interpretiert. Dies kann dazu führen, dass Tasten Mac-Reaktionen auslösen.

Sie möchten vielleicht auch bestimmte Windows-Tasten verwenden, z. B. Einfügen, die auf vielen Mac-Tastaturen nicht vorhanden ist. Genauso zeigen einige Windows 8-Tastenkombinationen Charms und App-Befehle an und docken Apps an und wechseln sie. Diese Verknüpfungen werden von Mac-Tastaturen nicht nativ imitiert, können jedoch mit dem Menü "Tastatur" an den Remotedesktop oder die Remoteanwendung gesendet werden.

Tastaturen und die Konfiguration der Tasten können sich stark zwischen Computern unterscheiden. Receiver bietet daher mehrere Auswahlen an, um sicherzustellen, dass Tastaturanschläge richtig an gehostete Anwendungen und Desktops weitergeleitet werden. Diese Auswahlen werden in folgender Tabelle aufgelistet. Das Standardverhalten wird beschrieben. Wenn Sie die Standardwerte angepasst haben (mit Receiver oder anderen Einstellungen), werden möglicherweise andere Kombinationen von Tastaturanschlägen weitergeleitet, und der Remote-PC weist ein anderes Verhalten auf.

Wichtig: Bestimmte Tastenkombinationen, die in der Tabelle aufgelistet sind, sind nicht auf neueren Mac-Tastaturen verfügbar. In den meisten Fällen kann die Tastatureingabe mit dem Menü Tastatur zur Sitzung gesendet werden.
In der Tabelle verwendete Konventionen:

- Buchstabentasten sind großgeschrieben; dies gibt nicht an, dass die Umschalt-Taste gleichzeitig gedrückt werden soll.
- Bindestriche zwischen Tastaturanschlägen geben an, dass Tasten gleichzeitig gedrückt werden sollen (z. B. Strg-C).
- Zeichentasten erstellen die Texteingabe und umfassen alle Buchstaben, Zahlen und Satzzeichen; Sondertasten erstellen alleine keine Eingabe und fungieren als Modifikator oder Steuerelemente. Zu den Sondertasten gehören die Control-, Alt-, Umschalt-, Befehl- und Option-Taste sowie die Pfeiltasten und Funktionstasten.
- Menüanweisungen beziehen sich auf die Menüs in der Sitzung.
- Abhängig von der Konfiguration des Benutzergeräts funktionieren einige Tastenkombinationen nicht erwartungsgemäß und alternative Kombinationen sind aufgeführt.
- Fn bedeutet die Fn-Taste (Funktion) auf einer Mac-Tastatur; Funktionstasten sind F1 bis F12 auf einer PC- oder Mac-Tastatur.

Windows-Taste oder Tastenkombination	**Mac-Äquivalent**
Alt+Zeichentaste	Cmd-Option-Zeichen (z. B. zum Senden von Alt-C verwenden Sie Cmd-Option-C)
Alt+Sondertaste	Option-Sondertaste (z. B. Option-Tab) Cmd-Option-Sondertaste (z. B. Cmd-Option-Tab)
Strg+Zeichentaste	Cmd-Zeichentaste (z. B. Cmd-C) Ctrl-Zeichentaste (z. B. Ctrl-C)
Strg+Sondertaste	Ctrl-Sondertaste (z. B. Ctrl-F4)

Windows-Taste oder Tastenkombination	Mac-Äquivalent
	Cmd-Zeichentaste (z. B. Cmd-F4)
Strg/Alt/Umschalt/Windows-Logo + Funktionstaste	Wählen Sie Tastatur > Funktionstaste senden > Ctrl/Alt/Umschalt/Cmd-Funktionstaste
Strg+Alt	Ctrl-Option-Cmd
Strg+Alt+Entf	Ctrl-Option-Vorwärts entfernen Ctrl-Option-Fn-Entfernen (auf MacBook-Tastaturen) Wählen Sie Tastatur > senden Sie Ctrl-Alt-Entf
Delete	Delete Wählen Sie Tastatur > Taste senden > Entfernen Fn-Rücktaste
Ende	Ende Fn-Rechtspfeil
Esc	Esc Wählen Sie Tastatur > Taste senden > Esc
F1 bis F12	F1 bis F12 Wählen Sie Tastatur > Funktionstaste senden > F1 bis F12
Pos1	Pos1 Fn–Linkspfeil
Einfg	Wählen Sie Tastatur > Taste senden > Einfügen
Num	Entfernen
Bild ab	Bild ab Fn–Abwärtspfeil
Bild auf	Bild auf

Windows-Taste oder Tastenkombination	Mac-Äquivalent
	Fn–Aufwärtspfeil
Leertaste	Wählen Sie Tastatur > Taste senden > Leertaste
Registerkarte	Wählen Sie Tastatur > Taste senden > Tab
Windows-Logo	Rechte Cmd-Taste (eine standardmäßig aktivierte Tastatureinstellung) Wählen Sie Tastatur > Windows-Tastenkombination senden > Start
Tastenkombinationen zum Anzeigen von Charms	Wählen Sie Tastatur > Windows-Tastenkombination senden > Charms
Tastenkombinationen zum Anzeigen von App-Befehlen	Wählen Sie Tastatur > Windows-Tastenkombination senden > App-Befehle
Tastenkombinationen zum Andocken von Apps	Wählen Sie Tastatur > Windows-Tastenkombination senden > Andocken
Tastenkombinationen zum Wechseln von Apps	Wählen Sie Tastatur > Windows-Tastenkombination senden > Apps wechseln

Verwenden eines Eingabemethoden-Editors (IME) und internationaler Tastaturlayouts

Mit Receiver können Sie einen Eingabemethoden-Editor (IME) auf dem Benutzergerät oder dem Server verwenden.

Wenn der clientseitige Eingabemethoden-Editor (IME) aktiviert ist, können Benutzer an der Einfügemarke statt in einem Fenster Text eingeben.

Mit Receiver können Benutzer auch das gewünschte Tastaturlayout angeben.

Aktivieren des clientseitigen Eingabemethoden-Editors

1. Klicken Sie auf der Menüleiste Citrix Viewer auf Tastatur > International > Client-IME verwenden.
2. Stellen Sie sicher, dass der serverseitige IME auf direkte Eingabe oder den alphanumerischen Modus eingestellt ist.
3. Geben Sie mit dem Mac-IME Text ein.

Explizites Angeben des Anfangspunkts für die Texteingabe

- Klicken Sie auf der Menüleiste Citrix Viewer auf Tastatur > International > Kompositionszeichen verwenden.

Verwenden des serverseitigen Eingabemethoden-Editors

- Stellen Sie sicher, dass der clientseitige IME auf den alphanumerischen Modus eingestellt ist.

Zugeordnete serverseitige IME-Eingabemodustasten

Receiver stellt Tastaturzuordnungen für serverseitige Windows-IME-Eingabemodustasten bereit, die nicht auf Mac-

Tastaturen verfügbar sind. Auf Mac-Tastaturen ist die Optionstaste den folgenden serverseitigen IME-Eingabemodustasten zugeordnet, abhängig vom serverseitigen Gebietsschema:

Serverseitiges Systemgebietsschema	**Serverseitige IME-Eingabemodustaste**
Japanisch	**Kanji-Taste** (Alt + Hankaku/Zenkaku auf der japanischen Tastatur)
Koreanisch	**Rechte Alt-Taste** (Umschalten Hangul/English auf der koreanischen Tastatur)

Verwenden internationaler Tastaturlayouts

- Stellen Sie sicher, dass die Tastaturlayouts auf der Client- und Serverseite auf dasselbe Gebietsschema wie die Standardeingabesprache auf der Serverseite eingestellt sind.

Verwenden mehrerer Monitore

Mit der Menüoption **Alle Displays in Vollbild verwenden** können Benutzer Receiver für Mac im Vollbildmodus über mehrere Monitore hinweg ausführen.

Bekannte Einschränkungen

Der Vollbildmodus wird nur auf einem Monitor oder auf allen Monitoren unterstützt. Diese Funktion kann über ein Menüelement festgelegt werden.

Verwenden der Desktopsymbolleiste

Benutzer können jetzt im Fenstermodus und im Vollbildmodus auf die Desktopsymbolleiste zugreifen. Zuvor konnte die Symbolleiste nur im Vollbildmodus angezeigt werden. Darüber hinaus wurden folgende Änderungen an der Symbolleiste vorgenommen:

- Die Schaltfläche **Home** wurde von der Symbolleiste entfernt. Diese Funktion kann mit den folgenden Befehlen ausgeführt werden:
  - Cmd-Taste+Tab: Wechseln zur vorherigen aktiven Anwendung.
  - Ctrl+Linkspfeil: Wechseln zum vorherigen Bereich.
  - Sie können mit dem integrierten Trackpad oder den Magic Mouse-Gesten zu einem anderen Bereich wechseln.
  - Wenn Sie den Cursor im Vollbildmodus an den Rand des Bildschirms bewegen, wird ein Dock angezeigt, in dem Sie Anwendungen aktivieren können.
- Die Schaltfläche für den Fenstermodus wurde von der Symbolleiste entfernt. Mit den folgenden Methoden können Sie vom Vollbildmodus in den Fenstermodus wechseln:
  - In OS X 10.10 klicken Sie in der Dropdown-Menüleiste auf die grüne Fensterschaltfläche.  oder 
  - In OS X 10.7, 10.8 und 10.9 klicken Sie in der Dropdown-Menüleiste auf die blaue Menüschaltfläche. 
  - In allen Versionen von OS X können Sie in der Dropdown-Menüleiste im Menü **Ansicht** die Option **Vollbildmodus beenden** auswählen.
- Das Verhalten der Symbolleiste beim Ziehen wurde aktualisiert und unterstützt bei mehreren Monitoren im Vollbildmodus das Ziehen zwischen Fenstern.

Sichern der Citrix Receiver-Kommunikation

Feb 16, 2016

Dieser Abschnitt enthält folgende Themen:

- Informationen zu Zertifikaten
- Verbinden mit NetScaler Gateway oder Access Gateway Enterprise Edition
- Verbinden mit Secure Gateway
- Herstellen von Verbindungen über Proxyserver
- Herstellen einer Verbindung durch eine Firewall
- Verbinden mit dem SSL-Relay
  - Informationen zu SSL-Richtlinien
  - Konfigurieren und Aktivieren von Receiver für TLS
  - Installieren von Stammzertifikaten auf Benutzergeräten
  - Konfigurieren von SSL-Richtlinien

Zum Sichern der Kommunikation zwischen der Serverfarm und Receiver können Sie Citrix Receiver-Verbindungen zur Serverfarm mit zahlreichen Sicherheitsverfahren integrieren, u. a.:

- Citrix NetScaler Gateway oder Citrix Access Gateway. Weitere Informationen zur Konfiguration dieser Programme mit Citrix StoreFront finden Sie in der StoreFront-Dokumentation.
  Hinweis: Citrix empfiehlt, die Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit NetScaler Gateway zu sichern.
- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das und vom Netzwerk ein und handhaben Verbindungen zwischen Citrix Receiver und Servern. Citrix Receiver unterstützt die Protokolle SOCKS und Secure Proxy.
- Secure Gateway: Secure Gateway stellt zusammen mit dem Webinterface einen einzigen sicheren, verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit.
- SSL-Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie Receiver mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.

Informationen zu Zertifikaten

Private (selbstsignierte) Zertifikate

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

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

Importieren von Stammzertifikaten auf Receiver für Mac-Geräten

Rufen Sie das Stammzertifikat des Zertifikatausstellers ab und senden Sie es an ein 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 Mac unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate mit Access Gateway oder NetScaler Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Access Gateway- oder NetScaler Gateway-Serverzertifikat zugeordnet werden. Weitere Informationen hierzu finden Sie in der NetScaler Gateway-Dokumentation. Die äquivalenten Informationen zu Access Gateway finden Sie im entsprechenden Knowledge Base-Artikel für Ihre Edition des Produkts:

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

Verbinden mit NetScaler Gateway oder Access Gateway Enterprise Edition

Damit Remotebenutzer sich mit der CloudGateway-Bereitstellung über NetScaler Gateway oder Access Gateway verbinden können, konfigurieren Sie diese für StoreFront (beide Komponenten von CloudGateway). 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 NetScaler Gateway oder Access Gateway zu, indem Sie NetScaler Gateway oder Access Gateway mit 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 mit NetScaler Gateway finden Sie im Abschnitt Configuring NetScaler Gateway Settings with the Remote Access Wizard. Weitere Informationen zur Konfiguration dieser Verbindungen mit Access Gateway finden Sie im Abschnitt Integrating Access Gateway with CloudGateway.

Damit Remotebenutzer über Access Gateway eine Verbindung mit der Webinterface-Bereitstellung herstellen können, konfigurieren Sie Access Gateway für das Webinterface, wie im Abschnitt Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface und in den anderen Themen in diesem Abschnitt beschrieben.

Verbinden mit Secure Gateway

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Secure Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen Receiver und dem Server bereitzustellen. Receiver muss nicht konfiguriert werden, wenn Sie Secure Gateway im Normalmodus verwenden und Benutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Secure Gateway-Servern verwendet Receiver Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Informationen zum Konfigurieren der Proxyservereinstellungen für Receiver finden Sie in der Dokumentation für das Webinterface.

Wenn Secure Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie Secure Gateway Proxy im Relaymodus verwenden. Weitere Informationen zum Relaismodus finden Sie in der Dokumentation für XenApp (Secure Gateway).

Wenn Sie den Relaymodus verwenden, fungiert der Secure Gateway-Server als Proxy und Sie müssen Receiver für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Secure Gateway-Servers.
- Portnummer des Secure Gateway-Servers. Der Relaymodus wird von Secure Gateway, Version 2.0 nicht unterstützt.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:
- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

Beispiel: Eigener_Computer.Beispiel.com ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (eigener_Computer), eine Second-Level-Domäne (Beispiel) und eine Top-Level-Domäne (com) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (Bespiel.com) wird im Allgemeinen als Domänenname bezeichnet.

Herstellen von Verbindungen über Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und Verbindungen zwischen Receiver und Servern gehandhabt. Receiver unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem XenApp- oder XenDesktop-Server verwendet Receiver die Proxyservereinstellungen, die remote auf dem Webinterface-Server konfiguriert sind. Informationen zum Konfigurieren der Proxyservereinstellungen für Receiver finden Sie in der Webinterface-Dokumentation.

Für die Kommunikation mit dem Webserver verwendet Receiver die Proxyservereinstellungen, die für den Standardwebbrowser auf dem Benutzergerät konfiguriert sind. Sie müssen die Proxyservereinstellungen für den Standardwebbrowser entsprechend auf dem Benutzergerät konfigurieren.

Herstellen einer Verbindung durch eine Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss Receiver über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können. Die Firewall muss HTTP-Datenübertragungen für die Kommunikation zwischen Benutzergerät und Webserver zulassen (meist über den HTTP-Standardport 80 oder 443, wenn ein sicherer Webserver verwendet wird). Für die Kommunikation zwischen Receiver und dem Citrix Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

Wenn die Firewall für die Netzwerkadressenübersetzung konfiguriert ist, verwenden, können Sie im Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports definieren. Beispiel: Wenn XenApp Server oder XenDesktop Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface Receiver eine alternative Adresse bereitstellen. Receiver stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her. Weitere Informationen finden Sie in der Dokumentation zum Webinterface.

Verbinden mit dem SSL-Relay

Sie können Receiver mit dem SSL-Relaydienst mit Receiver für Mac 12.0 integrieren, der TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen für TLS-Verbindungen zwischen Citrix Receiver und XenApp/XenDesktop unterstützt:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS (Transport Layer Security) ist die neueste, standardisierte Version des SSL-Protokolls. Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von SSL als offenem Standard übernahm.

TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie z. B. FIPS 140. FIPS 140 ist ein Standard für die Kryptografie.

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

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

- Verbindung zwischen einem TLS-fähigen Receiver und einem Server.
- Bei einem Webinterface-Server die Kommunikation zwischen dem XenApp-Server und dem Webserver.

Weitere Informationen zum Konfigurieren und Verwenden von SSL-Relay zum Sichern der Installation oder zum Konfigurieren des Webinterface-Servers für die TLS-Verschlüsselung finden Sie in der Dokumentation für XenApp und für das Webinterface.

> **Hinweis**
>
> Citrix Receiver für Mac verwendet plattformeigene Kryptografie (OS X) für Verbindungen zwischen Receiver und StoreFront.

Konfigurieren und Aktivieren von Receiver für TLS

Das Setup von TLS besteht aus zwei Hauptschritten:

1. Setup von SSL-Relay auf dem XenApp- oder XenDesktop-Server und dem Webinterface-Server und abrufen und installieren des benötigten Serverzertifikats. Weitere Informationen finden Sie in der Dokumentation für XenApp und für das Webinterface.
2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Installieren von Stammzertifikaten auf Benutzergeräten

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

Mac OS X hat ungefähr 100 installierte kommerzielle Stammzertifikate; wenn Sie ein anderes Zertifikat verwenden möchten, können sie es von einer Zertifizierungsstelle abrufen und auf jedem Benutzergerät installieren.

Abhängig von den Richtlinien und Abläufen in Ihrem Unternehmen möchten Sie das Stammzertifikat ggf. auf jedem

Benutzergerät installieren und die Installation nicht den Benutzern überlassen. Am einfachsten und sichersten ist es, wenn Sie die Stammzertifikate der Mac OS X-Schlüsselkette hinzufügen.

Hinzufügen eines Stammzertifikats zur Schlüsselkette

1. Doppelklicken Sie auf die Datei, die das Zertifikat enthält. Die Anwendung für den Schlüsselkettenzugriff wird automatisch gestartet.
2. Wählen Sie im Dialogfeld "Add Certificates" eine Option im Popupmenü "Keychain":
   - "login" (das Zertifikat gilt nur für den aktuellen Benutzer.)
   - "System" (das Zertifikat gilt für alle Benutzer eines Geräts.)
3. Klicken Sie auf "OK".
4. Geben Sie Ihr Kennwort in das Dialogfeld "Authenticate" ein und klicken Sie auf "OK".

Das Stammzertifikat ist installiert und kann von SSL-fähigen Clients und anderen Anwendungen, die SSL einsetzen, verwendet werden.

Informationen zu SSL-Richtlinien

In diesem Abschnitt finden Sie Informationen zur Konfiguration von Sicherheitsrichtlinien für ICA-Sitzungen über SSL in Citrix Receiver für Mac, Version 12.0. Sie können bestimmte SSL-Einstellungen, die für ICA-Verbindungen verwendet werden, in Citrix Receiver konfigurieren. Diese Einstellungen werden nicht auf der Benutzeroberfläche angezeigt. Für das Ändern müssen Sie einen Befehl auf dem Receiver-Gerät ausführen.

> ### Hinweis
>
> SSL-Richtlinien können mit anderen Methoden verwaltet werden, z. B. wenn Geräte von OS X-Server oder einer anderen Mobilgeräteverwaltungslösung gesteuert werden.

SSL-Richtlinien enthalten die folgenden Einstellungen:

SecurityComplianceMode: Stellt den Sicherheitskompatibilitätsmodus für die Richtlinie ein. Wenn Sie "SecurityComplianceMode" nicht konfigurieren, wird standardmäßig FIPS verwendet. Gültige Werte für diese Einstellung sind u. a.:

- **Keine**: Kein Kompatibilitätsmodus wird erzwungen
- **FIPS**: FIPS-Kryptografiemodule werden verwendet
- **SP800-52**: NIST SP800-52r1-Kompatibilität wird erzwungen

Einstellen von "SecurityComplianceMode" auf SP800-52: KOPIEREN

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions: Mit dieser Einstellung geben Sie die TLS-Protokollversionen an, die bei der Protokollaushandlung akzeptiert werden. Diese Informationen werden als Array dargestellt; jede Kombination der

möglichen Werte wird unterstützt. Wenn diese Einstellung nicht konfiguriert ist, werden als Standardwerte TLS10, TLS11 und TLS12 verwendet. Gültige Werte für diese Einstellung sind u. a.:

- **TLS10**: Gibt an, dass das TLS 1.0-Protokoll zugelassen ist.
- **TLS11**: Gibt an, dass das TLS 1.1-Protokoll zugelassen ist.
- **TLS12**: Gibt an, dass das TLS 1.2-Protokoll zugelassen ist.

Einstellen von "SecurityAllowedTLSVersions" auf TLS 1.1 und TLS 1.2: KOPIEREN

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy: Dieses Feature verbessert die kryptografische Authentifizierung des Citrix Servers und die allgemeine Sicherheit der SSL/TLS-Verbindungen zwischen einem Client und einem Server. Diese Einstellung steuert, wie eine bestimmte vertrauenswürdige Stammzertifizierungsstelle bei dem Versuch behandelt wird, eine Remotesitzung über SSL mit dem Client für OS X zu öffnen.

Wenn diese Einstellung aktiviert ist, prüft der Client, ob das Zertifikat des Servers widerrufen wurde. Es gibt mehrere Prüfstufen für die Zertifikatsperrliste.Der Client kann beispielsweise so konfiguriert werden, dass er nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft. Außerdem können Sie die Überprüfung der Zertifikate so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Das Prüfen der Zertifikatsperrliste ist ein fortschrittliches Feature, das von einigen Zertifikatausstellern unterstützt wird. Der Administrator kann Sicherheitszertifikate widerrufen (d. h. vor dem Ablaufdatum ungültig machen), wenn der private Schlüssel des Zertifikats kryptografisch kompromittiert oder der DNS-Name unerwartet geändert werden muss.

Gültige Werte für diese Einstellung sind u. a.:

- **NoCheck**: Es wird keine Überprüfung der Zertifikatsperrliste durchgeführt.
- **CheckWithNoNetworkAccess**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Es werden nur lokale Zertifikatsperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Secure Gateway-Server vorgelegt wird, nicht wichtig.
- **FullAccessCheck**: Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Secure Gateway-Server vorgelegt wird, nicht wichtig.
- **FullAccessCheckAndCRLRequired**: Die Zertifikatsperrliste wird überprüft; die Stamm-CA ist ausgeschlossen. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
- **FullAccessCheckAndCRLRequiredAll**: Die Zertifikatsperrliste und die Stamm-CA werden überprüft. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.

> ### Hinweis
>
> Wenn Sie "SSLCertificateRevocationCheckPolicy" nicht festlegen, wird standardmäßig "FullAccessCheck" verwendet.

Einstellen von "SSLCertificateRevocationCheckPolicy" auf "FullAccessCheckAndCRLRequred": KOPIEREN

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

Konfigurieren von SSL-Richtlinien

Führen Sie zum Konfigurieren von SSL-Einstellungen auf einem nicht verwalteten Computer den Befehl **defaults** in Terminal.app aus.

defaults ist eine Befehlszeilenanwendung, mit der Sie App-Einstellungen in einer Plistdatei der OS X-Einstellungen hinzufügen, bearbeiten und löschen können.

Ändern der Einstellungen

1. Öffnen Sie "Applications" > "Utilities" > "Terminal".
2. Führen Sie in "Terminal" folgenden Befehl aus:

   defaults write com.citrix.receiver.nomas

Ort:

: Der Name der Einstellung, wie oben beschrieben.

: Eine Option zum Identifizieren des Typs der Einstellung, entweder -string oder -array. Wenn der Einstellungstyp "string" ist kann dies ausgelassen werden.

: Der Wert für die Einstellung. Wenn der Wert ein Array ist und Sie mehrere Werte eingeben, müssen die Werte durch eine Leerstelle getrennt werden.

Beispiel: KOPIEREN

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

Wiederherstellen der Standardkonfiguration

Zurücksetzen einer Einstellung auf den Standard

1. Öffnen Sie "Applications" > "Utilities" > "Terminal".
2. Führen Sie in "Terminal" folgenden Befehl aus:

   defaults delete com.citrix.receiver.nomas

Ort:

: Der Name der Einstellung, wie oben beschrieben.

Beispiel: KOPIEREN

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```