

Neue Features

Sep 25, 2017

Neue Features in 12.7

Unterstützung für macOS 10.13 (High Sierra)

Dieses Release enthält Änderungen in der Art, wie Benutzer die generische USB-Umleitung für Citrix Receiver für Mac mit macOS 10.13 aktivieren. Informationen über das Konfigurieren der generischen USB-Umleitung mit macOS 10.13 finden Sie im Knowledge Center-Artikel [CTX228208](#).

Smartcard-Unterstützung mit StoreFront

Neben Citrix Receiver für Web unterstützt jetzt der native Citrix Receiver für Mac die Smartcard-Authentifizierung für Verbindungen mit NetScaler Gateway oder StoreFront.

Unterstützung für Servernamensanzeige (SNI)

Citrix Receiver für Mac unterstützt jetzt die NetScaler Gateway-Konfiguration mit Servernamensanzeige (SNI), sodass Benutzer Desktops und Anwendungen starten können. Weitere Informationen über SNI finden Sie im Knowledge Center-Artikel [CTX125798](#).

Behobene Probleme

Sep 25, 2017

Vergleich mit Citrix Receiver für Mac 12.6

Citrix Receiver für Mac 12.7 enthält alle Fixes, die in den Versionen 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5 und 12.6 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- Das Starten eines VDA mit einer Smartcard funktioniert möglicherweise nicht, wenn Sie NetScaler verwenden. Citrix Viewer reagiert nicht mehr und muss neu gestartet werden.

[#RFMAC-445]

- Wenn Sie sich bei XenApp Essentials anmelden und die zweistufige Authentifizierung verwenden, wird die Aufforderung für den Sicherheitscode möglicherweise nicht angezeigt.

[#RFMAC-976]

- Die Konfigurationsdatei für die USB-Umleitung wird möglicherweise beim Aktualisieren von Citrix Receiver für Mac nicht richtig gespeichert.

[#RFMAC-981]

- Veröffentlichte Anwendungen leiten interne URLs möglicherweise nicht um.

[#RFMAC-982]

- Citrix Viewer reagiert u. u. nicht mehr.

[#RFMAC-1050]

- Bei Wischgesten auf einem Mac mit High Sierra können grafische Störungen auftreten.

[#RFMAC-1073]

Vergleich mit Citrix Receiver für Mac 12.5

Citrix Receiver für Mac 12.6 enthält alle Fixes, die in den Versionen 12, 12.1, 12.1.100, 12.2, 12.3, 12.4 und 12.5 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- Beim Freigeben von Bildschirmen mit WebEx wird u. U. ein schwarzes Fenster auf dem freigegebenen Bildschirm angezeigt.

[#RFMAC-689, #LC6462]

- Nachdem die Bildschirmfreigabe mit WebEx beendet wurde, wird die Anwendung u. U. nicht im Vordergrund des Desktops angezeigt.

[#RFMAC-690, #LC6255]

- Unter macOS Sierra funktioniert möglicherweise die Tastenkombination Umschalt+Eingf nicht.

[#RFMAC-696]

- Wenn Sie nach dem Minimieren von WebEx die Anwendung wieder anzeigen, wird sie möglicherweise nicht richtig angezeigt.

[#RFMAC-742, #LC6840]

- Beim Starten einer Anwendung mit Citrix Receiver in Google Chrome wird das Statusfenster zum Anwendungsstart u. U. nicht angezeigt.

[#RFMAC-744]

- Beim Ausführen einer virtuellen Maschine werden XenDesktop-Sitzungen u. U. als schwarzer Bildschirm angezeigt.

[#RFMAC-808]

- Nach dem Start einer Anwendung wird das Popup zum Laden weiterhin angezeigt. Wenn Sie im Popup auf "Abbrechen" klicken, wird Citrix Receiver unerwartet beendet.

[#RFMAC-832, #LC7682]

- Bei der Verwendung von Server-zu-Client-URL-Umleitung werden u. U. URLs mit einem einmaligen, bereits abgelaufenen Zugriffstoken gestartet.

[#RFMAC-856]

- Bei der Verwendung von Safari unter den Builds macOS Sierra 10.12.6 Public Beta oder macOS High Sierra Developer Preview werden Apps und Desktops u. u. nicht gestartet.

[#RFMAC-869]

Vergleich mit Citrix Receiver für Mac 12.4

Citrix Receiver für Mac 12.5 enthält alle Fixes, die in den Versionen 12, 12.1, 12.1.100, 12.2, 12.3 und 12.4 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- Bei der Verwendung von Smartcards für die Anmeldung an einem Remotedesktopclient wird gelegentlich ein Fehler angezeigt, weil auf der Karte keine Zertifikate gefunden wurden.

[RFMAC-432, #650298]

- Die Storeerkennung schlägt fehl, wenn der Server eine Antwort sendet, die keine UTF-8-Antwort ist.

[#RFMAC-565]

- Beim Start einer SAML-Anwendung kann der Fehler "Ungültige Anforderung" auftreten.

[#RFMAC-598, #LC6558]

- ReceiverHelper wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn CEIPRegistry.json eine ungültige JSON-Datei enthält.

[#RFMAC-639]

- Wenn Sie nicht an Citrix Receiver angemeldet sind, schlägt das Starten einer veröffentlichten Anwendung vom Launchpad oder Finder aus fehl und folgende Fehlermeldung wird angezeigt: "Verbindung nicht möglich. Kommunikation mit dem Authentifizierungsmanager-Dienst nicht möglich."

[#RFMAC-648]

Vergleich mit Citrix Receiver für Mac 12.3

Citrix Receiver für Mac 12.4 enthält alle Fixes, die in den Versionen 12, 12.1, 12.1.100, 12.2 und 12.3 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- Citrix Viewer sendet nicht das richtige Tastaturlayout an den Server.

[#581829]

- Beim Verwenden der geteilten Ansicht mit Citrix Receiver für Mac 12.1 funktioniert das Ändern der Größe von gehosteten Desktops und das Wechseln zwischen ihnen möglicherweise nicht.

[#604943]

- Bei mehreren Anzeigefenstern in einer Konfiguration, in der die primäre Anzeige unten ist, flimmern die veröffentlichten Anwendungsfenster von Citrix Receiver für Mac möglicherweise.

[#652254]

- Benutzer können Dateien auf einem Netzlaufwerk u. U. nicht bearbeiten oder speichern, wenn sie veröffentlichte Anwendungen verwenden.

[#660657]

- Beim Speichern einer Datei auf einem Netzlaufwerk wird die VDA-Sitzung möglicherweise unterbrochen.

[#660661]

- Beim Verwenden einer externen Tastatur in einer VDA-Sitzung oder einer veröffentlichten Anwendung funktioniert die EINFÜG-Taste u. U. nicht.

[#660669]

- Drucker, die in einer Sitzung nicht angezeigt werden, sind trotzdem vorhanden und verfügbar.

[#667462]

Vergleich mit Citrix Receiver für Mac 12.2

Citrix Receiver für Mac 12.3 enthält alle Fixes, die in den Versionen 12, 12.1, 12.1.100 und 12.2 enthalten waren, und darüber hinaus folgenden neuen Fix:

- Wenn Citrix Receiver für Mac für die Verwendung eines Proxyservers konfiguriert wird, schlagen SSL-Verbindungen (Secure Socket Layer) u. U. fehl.

[#640652]

Vergleich mit Citrix Receiver für Mac 12.1.100

Citrix Receiver für Mac 12.2 enthält alle Fixes, die in den Versionen 12, 12.1 und 12.1.100 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- Das Problem, dass die Alt-Taste auf deutschen Tastaturen nach Eingabe von Alt-I nicht freigegeben wurde, wurde behoben.

[#LC3796]

- Ein Problem wurde behoben, das einen Fehler bei der Server-zu-Client-Inhaltsumleitung verursachte, wenn die umgeleitete URL nicht-ASCII-Zeichen enthielt.

[#LC4470]

- In einem HDX-App-Fenster wurden gelegentlich Zeichenartefakte angezeigt, wenn das Fenster minimiert oder maximiert worden war. Dieses Problem wurde behoben.

[#LC4668]

- Ein Problem, das Fehler bei der Smartcard-Passthrough-Authentifizierung verursachte, wurde behoben.

[#LC4907]

- Audio, das von einem Mikrofon remote über den Server übermittelt wurde, klang u. U. sehr abgehackt. Dieses Problem wurde behoben.

[#LC5157]

- Das Problem, dass Strg-Tab-Tastenkombinationen nicht an aktive Desktopsitzungen weitergeleitet wurde, wurde behoben.

[#LC5367]

- Bei der Wiederverbindung mit einer vorhandenen Sitzung war die Tastaturzuordnung der Sitzung u. U. falsch. Dieses Problem wurde behoben.

[#LC5395]

- Ein Problem, bei dem ein Microsoft Remote Desktop Client, der in einer HDX-Sitzung ausgeführt wird, keinen Zugriff auf Smartcards hatte, wurde behoben.

[#LC5454]

- Wenn die Benutzerzertifikatauthentifizierung auf NetScaler Gateway konfiguriert war, schlug die Verbindung von Sitzungen fehl. Dieses Problem wurde behoben.

[#LC5455]

- Ein Problem wurde behoben, bei dem Receiver für Mac eine Sitzung im Vollbildmodus startete, wenn der Parameter "ScreenPercent" in der ICA-Datei angegeben war.

[#605353]

- Ein Problem wurde behoben, das den Absturz von Receiver für Mac verursachte, wenn eine Sitzung getrennt wurde, während eine Webcam remote in einer aktiven Sitzung verwendet wurde.

[#612051]

- Dieses Release behob ein Problem, bei dem Receiver für Mac beim Herunterladen von Zertifikatssperrlisten nicht die Proxykonfiguration des Systems verwendete.

[#638176]

Vergleich mit Citrix Receiver für Mac 12.1

Citrix Receiver für Mac 12.1.100 enthält alle Fixes, die in den Versionen 12 und 12.1 enthalten waren, und darüber hinaus die

folgenden neuen Fixes:

- 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 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 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 das Fehlschlagen von IPv6-Verbindungen zu NetScaler Gateway verursachte.

[#LC4512]

- Ein Problem wurde behoben, das beim Eingeben eines einzelnen japanischen oder chinesischen Zeichens dazu führte, dass kein Zeichen auf dem Sitzungsdesktop angezeigt wurde.

[#603635]

Vergleich mit Citrix Receiver für Mac 12

Citrix Receiver für Mac 12.1 enthält alle Fixes, die in Version 12 enthalten waren, und darüber hinaus die folgenden neuen Fixes:

- 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]

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]

Bekannte Probleme

Sep 25, 2017

In diesem Release bestehen die folgenden bekannten Probleme:

- Ist die Desktopgestaltungsumleitung in einer Sitzung im Vollbildmodus aktiviert, können in Citrix Viewer grafische Störungen auftreten.

[#RFMAC-1078]

- Citrix Viewer wird möglicherweise unerwartet beendet, wenn mit dem lokalen koreanischen IME-Modul Zeichen an eine ICA-Sitzung gesendet werden.

[#RFMAC-1079]

- Auf einem Mac mit einem französisch-kanadischen Tastaturlayout wird bei Verbindungen mit einem Windows 7 VDA das Zirkumflexzeichen (^) nicht wie erwartet zugeordnet.

[#RFMAC 1107]

- In den Geräteeinstellungen sind Benutzeroberflächenelemente in anderen Sprachen möglicherweise abgeschnitten.

[#RFMAC-1113]

In diesem Release bestehen die folgenden bekannten Probleme:

- Bei einer Proxyverbindung schlägt die Kommunikation per EDT-Protokoll fehl.

[#664725, #RFMAC-464]

- Unter macOS x 10.12 wird Citrix Viewer u. U. unerwartet beendet, wenn ein Desktop über die Menüleiste getrennt wird. Das Problem tritt auch auf, wenn der Modus "Alle Displays in Vollbild verwenden" aktiviert ist, während die Desktopsitzung abgemeldet wird.

[#RFMAC-618]

In diesem Release bestehen die folgenden bekannten Probleme:

- Bei einer Proxyverbindung schlägt die Kommunikation per EDT-Protokoll (Enlightened Data Transport) fehl.

[#664725]

- Bei der Verwendung von NetScaler Gateway, das mit VDA-Version 7.11 oder früher für EDT konfiguriert wurde, schlägt die Verbindung zu TCP fehl, weil der Fallbackmechanismus auf TCP nicht funktioniert.

[#665617]

In diesem Release bestehen die folgenden bekannten Probleme:

- Wenn auf einem Benutzergerät ein Proxyserver konfiguriert ist, schlägt das Feature zur automatischen Wiederverbindung von Clients bei einem VDA für Desktopbetriebssystem u. U. fehl.

[#659683]

- In einer IPv6-Umgebung schlägt das Starten einer Sitzung u. U. fehl, wenn Secure Socket Layer (SSL) aktiviert ist.

[#659700]

In diesem Release bestehen die folgenden bekannten Probleme:

- Wenn beim Umleiten von Smartcards mehrere gleichzeitige Sitzungen ausgeführt werden, bleibt Receiver u. U. hängen.

[#511140]

- Benutzer können in OS X u. U. nicht die geteilte Ansicht mit HDX-App-Fenstern verwenden.

[#637963]

- Beim Umleiten eines über USB verbundenen CD/DVD-Laufwerks mit der generischen USB-Umleitung wird das Laufwerk u. U. ausgeworfen.

[#645484]

- Einige USB-Geräte funktionieren in einer Sitzung möglicherweise nicht, wenn die Richtlinie für die USB-Optimierung auf "Erfassung" festgelegt ist.

[#649082]

- In einigen Fällen wird der neue Benachrichtigungsbildschirm für USB-Geräte nicht richtig angezeigt, wenn ein USB-Gerät während der automatischen Wiederverbindung des Clients angeschlossen wird.

[#649714]

- Benutzer erhalten u. U. eine Schlüsselbundaufforderung, wenn sie nach dem Upgrade auf Receiver für Mac 12.2 eine Verbindung zu einem Konto herstellen.

[#649885]

- Auf Systemen mit Mac OS X 10.9 hat der Microsoft Remote Desktop Client, der in einer HDX-Sitzung ausgeführt wird, u. U. keinen Zugriff auf Smartcards.

[#650298]

- Tastatureingaben, die während eines Wiederverbindungs Vorgangs der Sitzungszuverlässigkeit ausgeführt werden, werden u. U. nicht wiedergegeben, wenn die Sitzung wiederverbunden ist.

[#652154]

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]

In diesem Release bestehen die folgenden bekannten Probleme:

- Wenn eine veröffentlichte Eingabeaufforderung beim Trennen einer Sitzung minimiert wird, wird die Eingabeaufforderung ggf. nicht bei einer erneuten Verbindung angezeigt.

[#411702]

- 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]

- 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]

- Bei einer Konfiguration mit mehreren Monitoren werden Seamless-Anwendungen u. U. auf die primäre Anzeige verschoben, wenn eine Anzeige neu konfiguriert wird.

[#506532]

- Wenn für den Viewer der Vollbildmodus eingestellt wird, während DirectX oder OpenGL ausgeführt werden, verschwindet möglicherweise der Cursor.

[#510745]

- 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]

- Wenn die Serversprache 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]

- In Receiver angezeigte Anwendungsamen 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]

- Das Starten von Sitzungen schlägt fehl, wenn eine Gemalto .NET-Smartcard zum Authentifizieren bei XenDesktop 5.6 verwendet wird.

[#550781]

- Bei Verwendung einer PIV-Smartcard kann Receiver die Verbindung mit einer XenDesktop 5.6-Sitzung nicht wiederherstellen.

[#550986]

- 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]

- Unter OS X El Capitan (10.11) werden virtuelle Desktops und Apps in der geteilten Ansicht nicht normal angezeigt.

[#582397]

- In OS X Yosemite (10.10) blockiert u. U. die aktualisierte Version von Safari Citrix Receiver als Pop-upfenster. Sie lösen dieses Problem, indem Sie das Öffnen von Pop-upfenstern für Apps/Desktops zulassen.

Systemanforderungen

Sep 25, 2017

Citrix Receiver für Mac unterstützt folgende Betriebssysteme:

- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Mac OS X El Capitan (10.11)
- Mac OS X Yosemite (10.10)

Hinweis

Mac OS X-Releases vor Mac OS X Yosemite werden nicht unterstützt.

Kompatible Citrix Produkte

Citrix Receiver für Mac ist kompatibel mit allen zurzeit unterstützten Versionen der folgenden Citrix Produkte. Weitere Informationen zum Citrix Produktlebenszyklus und wann Citrix die Unterstützung bestimmter Produktversionen beendet, finden Sie unter [Citrix Product Lifecycle Matrix](#).

Citrix Receiver für Mac ist mit den folgenden Browsern kompatibel:

- Safari 7.0 (und höher)
- Mozilla Firefox 22.x und höher
- Google Chrome 28.x (und höher)

Hardwareanforderungen

- 140.7 MB freier Datenträgerspeicher
- Eine funktionierende Netzwerk- oder Internetverbindung für die Verbindung mit Servern
- Webinterface:
 - Webinterface 5.4 für Windows mit XenApp Services-Sites (auch PNAgent Services genannt) für den Zugriff auf Anwendungen nativ von Citrix Receiver für Mac statt über einen Webbrowser.
- Bereit von Citrix Receiver für Mac:
 - Citrix Receiver für Web 2.1, 2.5 und 2.6
 - Citrix Webinterface 5.4
- StoreFront:
StoreFront 2.x oder höher für den Zugriff auf Anwendungen nativ von Citrix Receiver für Mac oder von einem Webbrowser aus.

Wenn Benutzer Citrix Receiver für Mac auf OS X El Capitan ausführen und Probleme beim Herstellen von Verbindungen

haben, aktualisieren Sie das NetScaler Gateway-Plug-In. 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 folgende Verbindungen mit XenApp oder XenDesktop:

- HTTP
- HTTPS
- ICA-über-TLS

Citrix Receiver für Mac unterstützt folgende Konfigurationen:

Für LAN-Verbindungen	Für sichere Remote- oder lokale Verbindungen
• StoreFront mit StoreFront Services- oder Citrix Receiver für Mac für Web-Site • Webinterface 5.4 für Windows mit XenApp Services-Sites	Citrix NetScaler Gateway: • 12.0 einschließlich VPX • 11.1 einschließlich VPX • 11.0 einschließlich VPX • 10.5 einschließlich VPX • Enterprise Edition 10.x einschließlich VPX • Enterprise Edition 9.x einschließlich VPX • VPX Citrix Secure Gateway 3.x (nur für die Verwendung mit Webinterface)

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

Für Verbindungen mit StoreFront unterstützt Citrix Receiver für Mac 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				Ja*	Ja*

(Domäne mit Sicherheitstoken) SMS	Receiver für Web mit Browsern	StoreFront Services-Site (nativ)	StoreFront XenApp Services-Site (nativ)	NetScaler bei Receiver für Web (Browser) Ja*	NetScaler bei StoreFront Services-Site (nativ) Ja*
Smartcard**	Ja	Ja		Ja*	Ja
Benutzerzertifikat				Ja	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 Citrix Receiver für Mac 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	
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.

Citrix Receiver für Mac unterstützt die Smartcardauthentifizierung für die folgenden Konfigurationen:

- Smartcardauthentifizierung bei Receiver für Web/StoreFront 2.x und höher, XenDesktop 7.1 und höher sowie XenApp 6.5 und höher.
- 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: Citrix 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 für Mac.
- In Double-Hop-Sitzungen: Wenn ein Double Hop benötigt wird, wird eine weitere Verbindung zwischen Citrix Receiver für Mac und dem virtuellen Desktop des Benutzers hergestellt.

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 für Mac Sie auf, ein Zertifikat auszuwählen. Nach der Auswahl des Zertifikats werden Sie von Citrix Receiver für Mac aufgefordert, das Smartcardkennwort einzugeben. Nach erfolgreicher Authentifizierung wird die Sitzung gestartet.

Wenn auf der Smartcard nur ein passendes Zertifikat ist, verwendet Citrix Receiver für Mac 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

Hinweis: Die Installation des PKCS#11-Moduls ist nicht obligatorisch.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung

1. Wählen Sie in Citrix Receiver **Einstellungen**.
2. Klicken Sie auf **Sicherheit und Datenschutz**.
3. Klicken Sie im Bereich "Sicherheit und Datenschutz" auf **Smartcard**.
4. 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.
5. Wählen Sie das entsprechende Modul aus und klicken Sie auf **Hinzufügen**.

Unterstützte Leser, Middleware und Smartcardprofile

Citrix 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)
- Gemalto .NET-Karten

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.
- Citrix Receiver für Mac speichert nicht die Zertifikatauswahl des Benutzers.
- Citrix Receiver für Mac speichert nicht die Smartcard-PIN des Benutzers. PIN-Abfragen werden vom Betriebssystem gehandhabt, das möglicherweise seinen eigenen Zwischenspeicherungsmechanismus hat.
- Citrix 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:

- [Configuring Citrix XenDesktop 7.6 and NetScaler 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](#)

Anforderungen für die Smartcardauthentifizierung

Sep 25, 2017

Citrix Receiver für Mac unterstützt die Smartcardauthentifizierung für die folgenden Konfigurationen:

- Smartcardauthentifizierung bei Receiver für Web/StoreFront 2.x und höher, XenDesktop 7.1 und höher sowie XenApp 6.5 und höher.
- 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: Citrix 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 für Mac.
- In Double-Hop-Sitzungen: Wenn ein Double Hop benötigt wird, wird eine weitere Verbindung zwischen Citrix Receiver für Mac und dem virtuellen Desktop des Benutzers hergestellt.

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 für Mac Sie auf, ein Zertifikat auszuwählen. Nach der Auswahl des Zertifikats werden Sie von Citrix Receiver für Mac aufgefordert, das Smartcardkennwort einzugeben. Nach erfolgter Authentifizierung wird die Sitzung gestartet.

Wenn auf der Smartcard nur ein passendes Zertifikat ist, verwendet Citrix Receiver für Mac 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

Hinweis: Die Installation des PKCS#11-Moduls ist nicht obligatorisch. Dieser Abschnitt gilt nur für ICA-Sitzungen. Die Beschreibung gilt nicht für Citrix Receiver-Zugriff auf NetScaler Gateway oder StoreFront, wenn eine Smartcard erforderlich ist.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung:

1. Wählen Sie in Citrix Receiver **Einstellungen**.
2. Klicken Sie auf **Sicherheit und Datenschutz**.
3. Klicken Sie im Bereich **Sicherheit und Datenschutz** auf **Smartcard**.
4. 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.
5. Wählen Sie das entsprechende Modul aus und klicken Sie auf **Hinzufügen**.

Citrix Receiver für Mac unterstützt die meisten, mit macOS 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)
- Gemalto .NET-Karten

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

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Citrix Receiver für Mac speichert nicht die Zertifikatauswahl des Benutzers.
- Citrix Receiver für Mac speichert nicht die Smartcard-PIN des Benutzers. PIN-Abfragen werden vom Betriebssystem gehandhabt, das möglicherweise seinen eigenen Zwischenspeicherungsmechanismus hat.
- Citrix 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 finden Sie unter:

- [Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2](#)

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

Sep 25, 2017

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

Dieser Abschnitt enthält folgende Themen:

- [Installation](#)
- [Manuelle Installation von Receiver für Mac](#)
- [Upgrade auf Receiver für Mac](#)
- [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](#)

Citrix Receiver für Mac kann von Benutzern auf folgende Weise installiert werden: von der Citrix Website, automatisch von Receiver für Web oder vom Webinterface, oder mit einem ESD-Tool (Electronic Software Distribution).

Von einem Benutzer von Citrix.com:

- Ein Erstbenutzer von Citrix Receiver für Mac, der Citrix Receiver für Mac von Citrix.com oder Ihrer eigenen Downloadsite herunterlädt, kann ein Konto durch Eingabe einer E-Mail-Adresse statt einer Server-URL einrichten. Citrix Receiver für Mac 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 Citrix Receiver für Mac nicht installiert ist.

- Die e-mail-basierte Kontenermittlung wird für einen Erstbenutzer nicht angewendet, wenn Citrix Receiver für Mac 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 Citrix Receiver für Mac kann ein Konto durch Eingabe einer Server-URL oder durch Download einer Provisioningdatei einrichten.

Mit einem ESD-Tool (Electronic Software Distribution)

- Ein Erstbenutzer von Citrix Receiver für Mac muss eine Server-URL für das Einrichten des Kontos eingeben.

Benutzer können Citrix Receiver für Mac 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 Citrix Receiver für Mac

1. Laden Sie die DMG-Datei für die gewünschte Version von Citrix Receiver für Mac von der Citrix Website herunter und öffnen Sie 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.

Upgrades werden von Version 11.x des Online Plug-Ins für Mac unterstützt. Sie können Citrix Receiver für Mac von allen Citrix Receiver für Mac-Vorversionen aus aktualisieren.

Important

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.

Bereitstellungen mit StoreFront:

- Sie sollten NetScaler Gateway und StoreFront 3.x so konfigurieren, wie es in der Dokumentation für [NetScaler Gateway](#) und [StoreFront](#) 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 Citrix Receiver für Mac 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 Citrix Receiver für Mac, 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 Citrix Receiver für Mac und teilen Sie den Benutzern mit, wie Citrix Receiver für Mac aktualisiert wird. Sie können beispielsweise Benutzern Installationsmeldungen auf dem Bildschirm "Meldungen" bereitstellen, damit Benutzer wissen, dass sie auf die aktuelle Version von Citrix Receiver für Mac aktualisieren müssen.

Sie können Citrix Receiver für Mac über Citrix Receiver für Web bereitstellen, um sicherzustellen, dass Citrix Receiver auf den Benutzergeräten installiert ist, bevor Benutzer versuchen, 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 Citrix Receiver für Web-Site erkennt, dass ein Benutzer keine kompatible Citrix Receiver für Mac-Version hat, wird der Benutzer zum Download und zur Installation von Citrix Receiver für Mac aufgefordert. Weitere Informationen finden Sie in der [StoreFront](#)-Dokumentation.

Dieses Feature ist nur für XenDesktop- und XenApp-Releases verfügbar, die das Webinterface unterstützen.

Sie können Citrix Receiver für Mac auf einer Webseite bereitstellen, um sicherzustellen, dass Citrix Receiver für Mac 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.

Weitere Informationen finden Sie unter [Konfigurieren der Clientbereitstellung](#) in der Webinterface-Dokumentation.

Sie können Citrix Receiver für Mac 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

Sep 25, 2017

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

- [Konfigurieren der USB-Umleitung](#)
- [Konfigurieren der Sitzungszuverlässigkeit](#)
- [Konfigurieren von CEIP](#)
- [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 Citrix Receiver für Mac 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.
- [Konfigurieren von automatischen Updates](#)
- 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](#).

Mit HDX USB-Geräteumleitung können USB-Geräte zum und vom Benutzergerät umgeleitet werden. Benutzer können beispielsweise eine Verbindung zum USB-Flashlaufwerk auf einem lokalen Computer herstellen und dann remote von einem virtuellen Desktop oder einer desktopgehosteten Anwendung darauf zugreifen. Während einer Sitzung können Benutzer die Geräte mit Plug & Play verwenden, einschließlich PTP-Geräte (Picture Transfer Protocol) wie digitale Kameras, MTP-Geräte (Media Transfer Protocol) wie digitale Audio Player oder tragbare Media Player, POS-Geräte (Point of Sale) und andere Geräte wie 3D-Mäuse, Scanner, Signaturpads usw.

Hinweis

Double-Hop-USB wird bei Sitzungen mit über Desktop gehosteten Anwendungen nicht unterstützt.

USB-Umleitung ist für folgende Citrix Receiver für Mac verfügbar:

- Windows
- Linux
- Macintosh

Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Sie können festlegen, welche USB-Geräte einem virtuellen Desktop verfügbar gemacht werden, indem Sie die Liste der unterstützten USB-Geräte für die Umleitung beschränken. Weiteres hierzu finden Sie weiter unten in diesem Abschnitt.

Tipp

In Umgebungen, in denen aus Sicherheitsgründen eine Trennung zwischen dem Benutzergerät und dem Server erforderlich ist, empfiehlt es sich, die Benutzer darüber zu informieren, welche Typen von USB-Geräten zu vermeiden sind.

Die beliebtesten USB-Geräte können über optimierte virtuelle Kanäle umgeleitet werden und liefern hervorragende Leistung und Bandbreiteneffizienz über ein WAN. Optimierte virtuelle Kanäle sind normalerweise die beste Option, insbesondere in Umgebungen mit hoher Latenz.

Hinweis

Für die Umleitung von USB-Geräten gilt Citrix Receiver für Mac behandelt ein SMART-Board ebenso wie eine Maus.

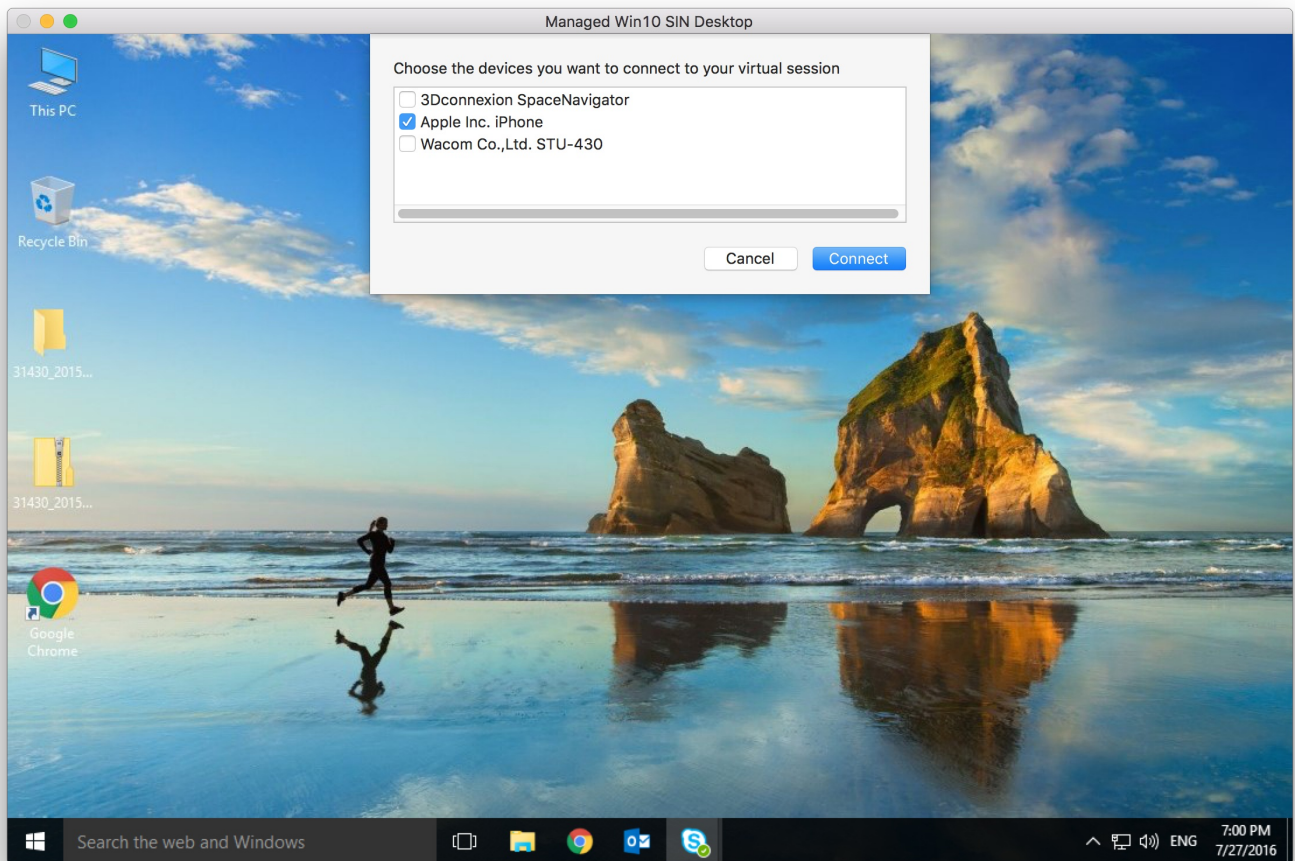
Das Produkt unterstützt die Verwendung von optimierten virtuellen Kanälen mit USB 3.0-Geräten und USB 3.0-Ports, wie ein virtueller CDM-Kanal, der zum Anzeigen von Dateien auf einer Kamera oder zur Audiowiedergabe über ein Headset verwendet wird. Das Produkt unterstützt zudem die generische USB-Umleitung von USB 3.0-Geräten, die mit einem USB 2.0-Port verbunden sind.

Einige erweiterte gerätespezifischen Features, z. B. HID-Schaltflächen (Human Interface Device) auf einer Webcam, funktionieren möglicherweise mit dem optimierten virtuellen Kanal nicht wie erwartet. Wenn dies ein Problem darstellt, können Sie den allgemeinen virtuellen Kanal für USB verwenden.

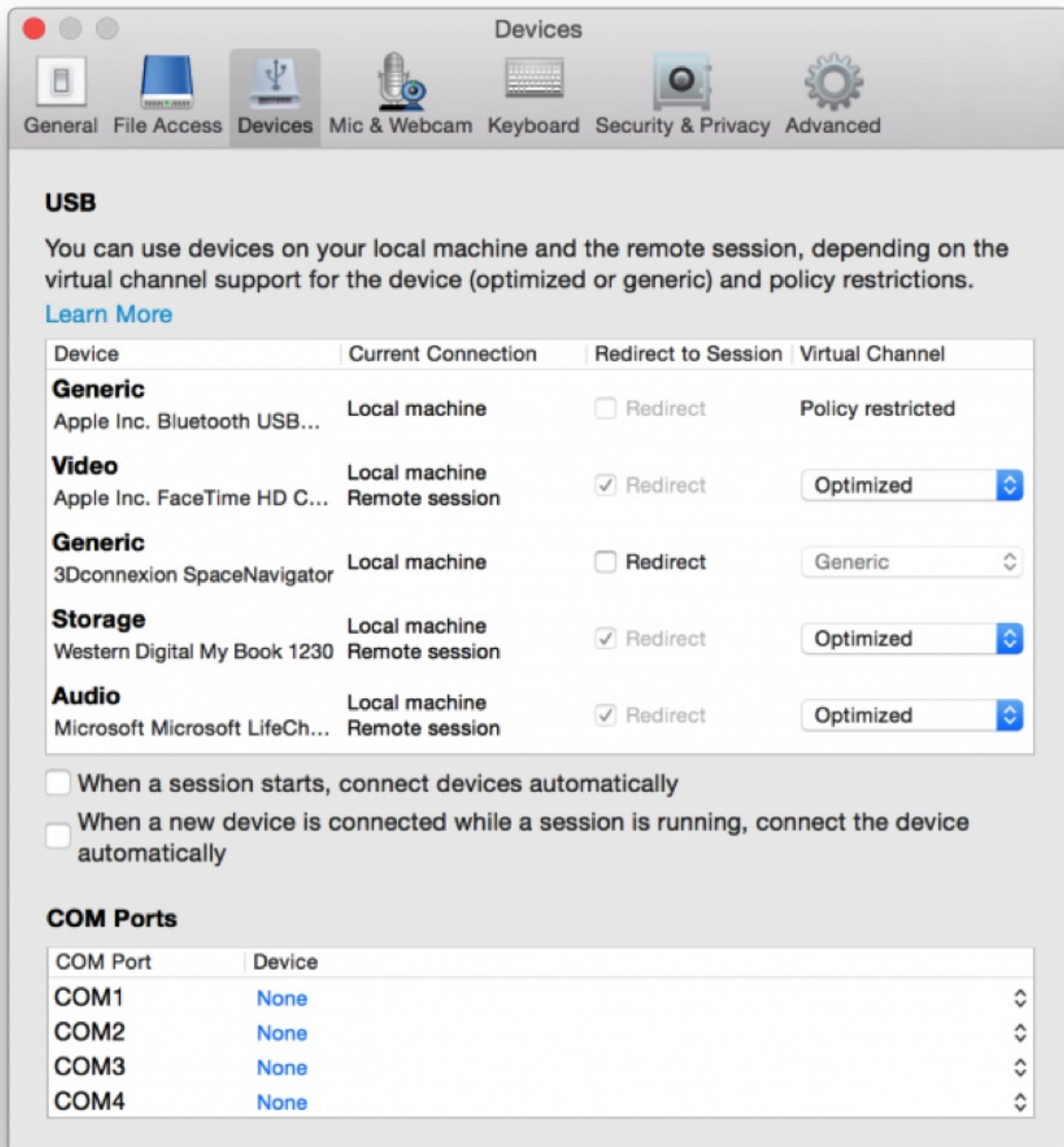
Einige Geräte werden standardmäßig nicht umgeleitet und sind nur in der lokalen Sitzung verfügbar. Es wäre beispielsweise nicht angemessen, eine über internes USB direkt angeschlossene Netzwerkkarte umzuleiten.

Verwenden von USB-Umleitung

1. Verbinden Sie das USB-Gerät mit dem Gerät, auf dem Receiver installiert ist.
2. Sie werden aufgefordert, die auf dem lokalen System verfügbaren USB-Geräte auszuwählen.



3. Wählen Sie das Gerät aus, das Sie verbinden möchten, und klicken Sie auf **Verbinden**. Schlägt die Verbindung fehl, wird eine Fehlermeldung angezeigt.
4. Im Fenster **Einstellungen** auf der Registerkarte **Geräte** wird das verbundene USB-Gerät im USB-Bereich angezeigt:



5. Wählen Sie für das USB-Gerät den virtuellen Kanaltyp aus: *Generisch* oder *Optimiert*.
6. Eine Meldung wird angezeigt. Klicken Sie, um das USB-Gerät mit Ihrer Sitzung zu verbinden:



USB Devices Detected

Click to connect the devices to your session.

Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen. Wenn Sie mit Citrix Receiver für Mac arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, erscheinen unmittelbar im USB-Menü von Desktop Viewer.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, kann das Problem u. U. dadurch behoben werden, dass das Gerät erst nach dem Beginn der virtuellen Sitzung angeschlossen wird.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Menü **Sicheres Entfernen**, bevor Sie das USB-Gerät entfernen.

Konfigurieren des EDT-Protokolls

Standardmäßig ist das EDT-Protokoll in Citrix Receiver für Mac aktiviert.

Citrix Receiver für Mac liest die EDT-Einstellungen in der Datei default.ica und wendet sie entsprechend an.

Um EDT zu deaktivieren, führen Sie den folgenden Befehl in einem Terminal aus:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Auf dem Client friert der Bildschirm ein, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Important

Benutzer von Citrix Receiver für Mac können die Servereinstellung nicht außer Kraft setzen.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden.

Hinweis

Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und NetScaler Gateway gesendet werden.

Verwenden von Sitzungszuverlässigkeitsrichtlinien

Mit der Richtlinieneinstellung **Sitzungszuverlässigkeit - Verbindungen** können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.

Der Standardwert für die Einstellung **Sitzungszuverlässigkeit - Timeout** ist 180 Sekunden (3 Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Benutzer nicht zu einer Neuauthentifizierung auffordert, um den Bedienkomfort zu erhöhen.

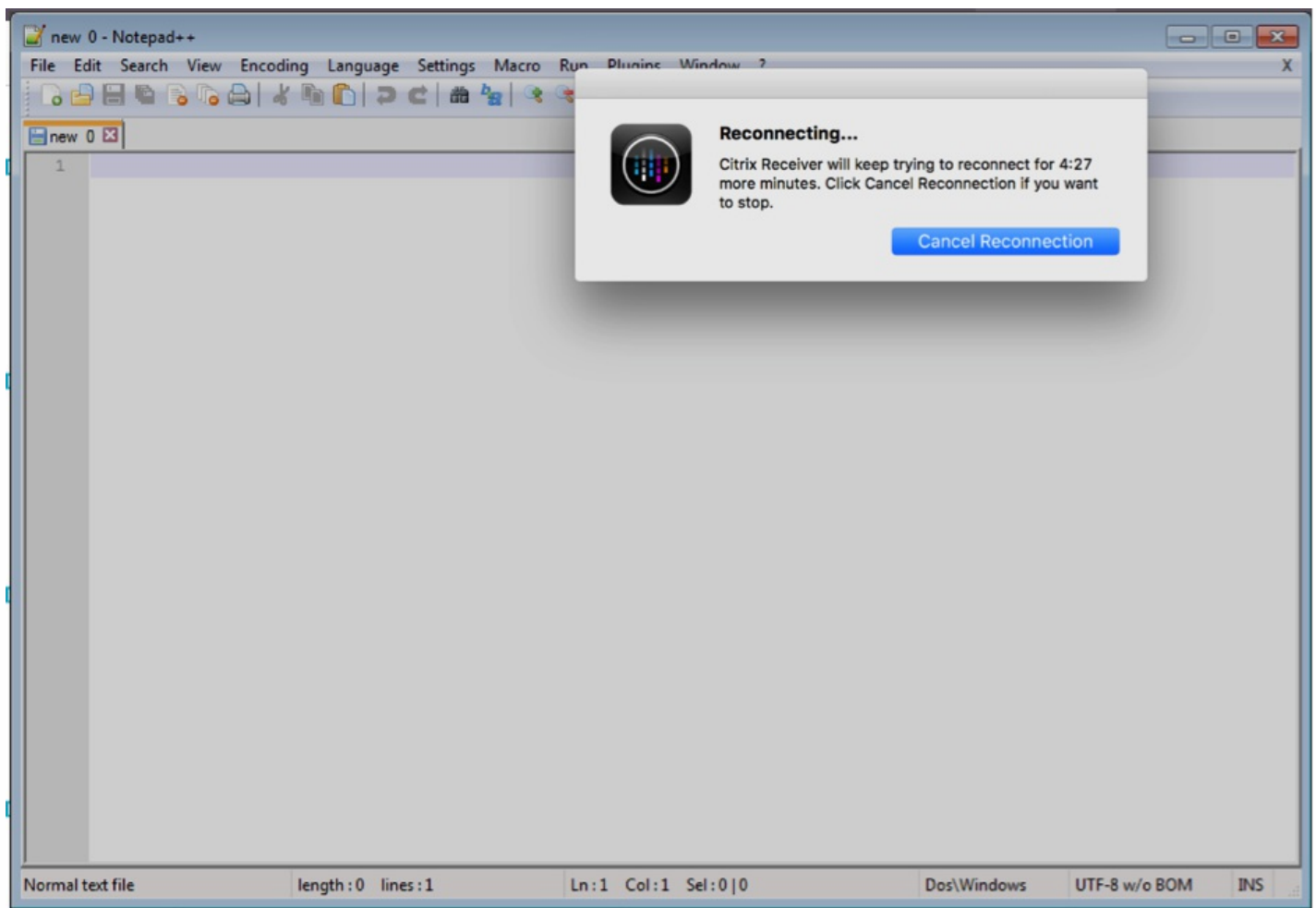
Tipp

Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.

Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer" geändert.

Verwenden Sie die Funktion zur automatischen Wiederverbindung von Clients, wenn Sie möchten, dass Benutzer eine Verbindung mit unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können. Sie können die Einstellung für die Citrix Richtlinie "Authentifizierung bei automatischer Wiederverbindung von Clients" so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wiederverbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option "Sitzungszuverlässigkeit - Timeout" festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, die Verbindung mit der unterbrochenen Sitzung wiederherzustellen.



Hinweis

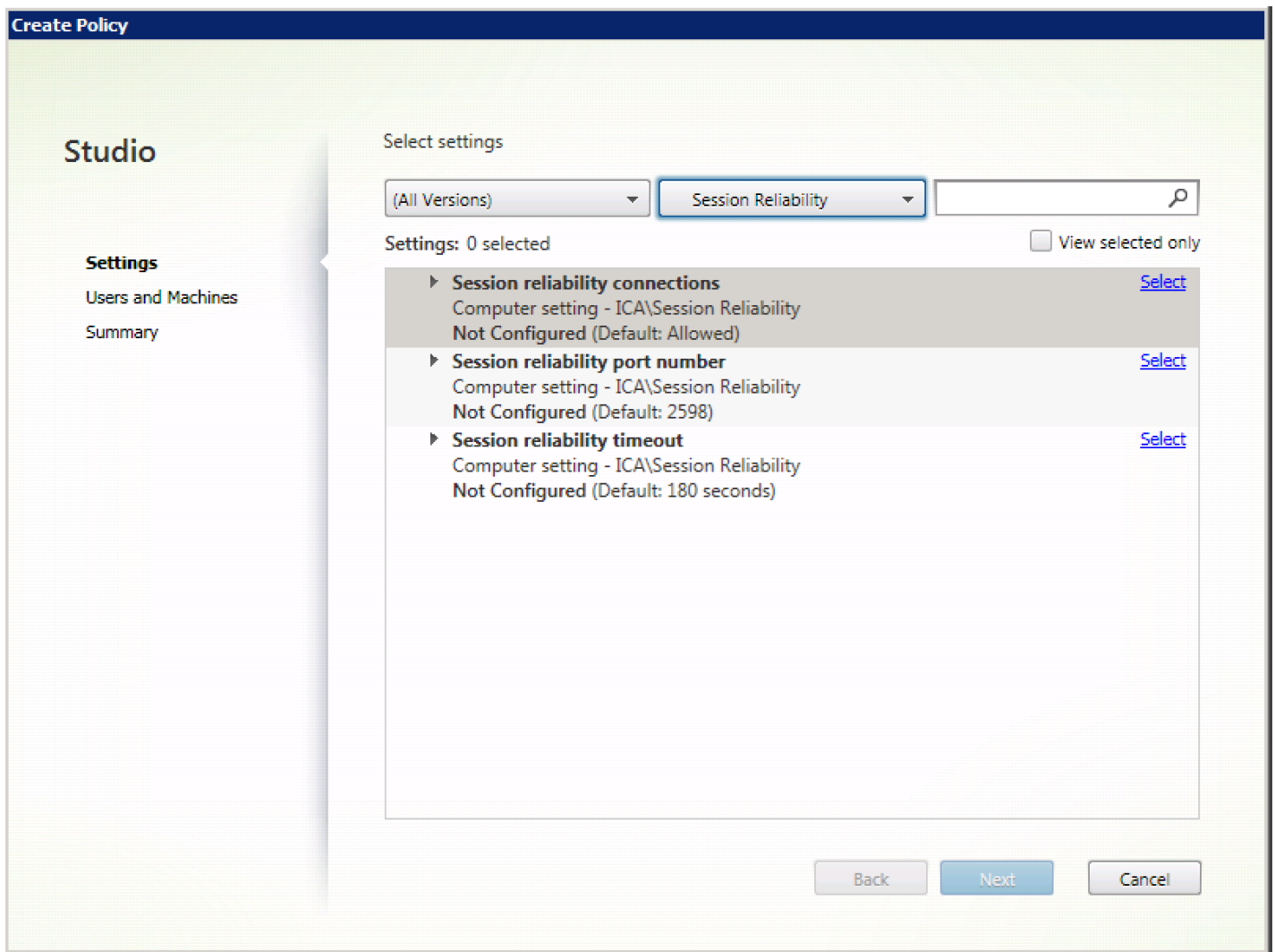
Die Sitzungszuverlässigkeit ist standardmäßig auf dem Server aktiviert. Sie deaktivieren dieses Feature, indem Sie die vom Server verwaltete Richtlinie konfigurieren.

Konfigurieren der Sitzungszuverlässigkeit

Standardmäßig ist die Sitzungszuverlässigkeit aktiviert.

Deaktivieren der Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Verbindungen**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Konfigurieren des Timeouts für die Sitzungszuverlässigkeit

Die Standardeinstellung für das Sitzungszuverlässigkeitstimeout ist 180 Sekunden.

Hinweis: Die Richtlinie für das Sitzungszuverlässigkeitstimeout kann nur mit XenApp/XenDesktop 7.11 und höher festgelegt werden.

Ändern des Timeouts für die Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Timeout**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

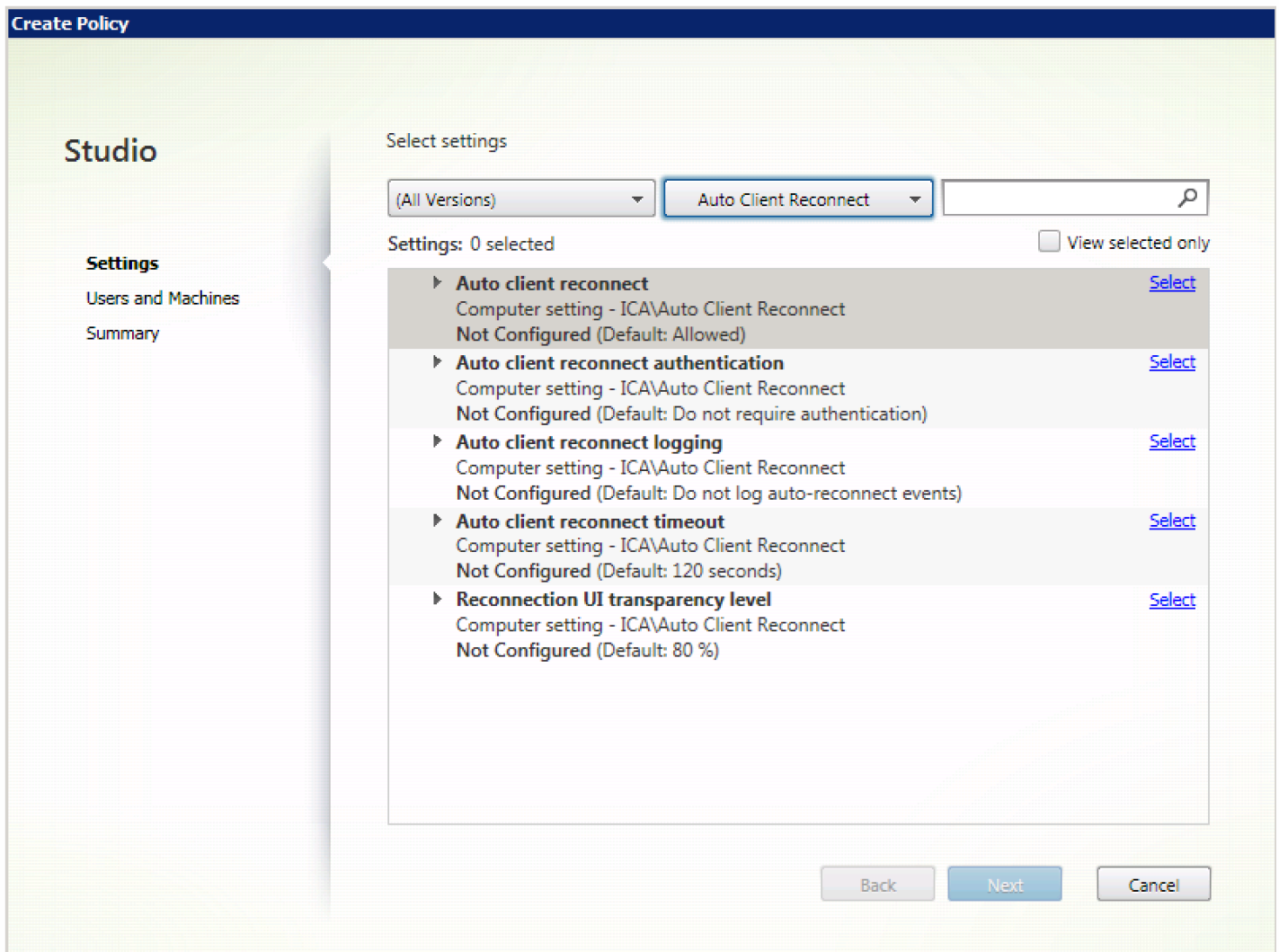
Konfigurieren der automatischen Wiederverbindung von Clients

Die automatische Wiederverbindung von Clients ist standardmäßig aktiviert.

Deaktivieren der automatischen Wiederverbindung von Clients

1. Starten Sie Citrix Studio.

2. Öffnen Sie die Richtlinie **Automatische Wiederverbindung von Clients**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Konfigurieren des Timeouts für die automatische Wiederverbindung von Clients

Die Standardeinstellung für das Timeout für die automatische Wiederverbindung von Clients ist 120 Sekunden.

Hinweis: Die Richtlinie für das Timeout für die automatische Wiederverbindung von Clients kann nur mit XenApp/XenDesktop 7.11 und höher festgelegt werden.

Ändern des Timeouts beim automatischen Wiederverbinden von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Automatische Wiederverbindung von Clients**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Einschränkungen:

Auf einem Terminalserver-VDA verwendet Citrix Receiver für Mac unabhängig von den Benutzereinstellungen 120 Sekunden als Timeoutwert.

Konfigurieren der Transparenzstufe für die Benutzeroberfläche beim Wiederverbinden

Bei Verbindungen mit Sitzungszuverlässigkeit und bei der automatischen Wiederverbindung von Clients wird die Sitzungsbenutzeroberfläche angezeigt. Die Transparenzstufe der Benutzeroberfläche kann mit einer Richtlinie in Citrix Studio angepasst werden.

Standardmäßig ist die Transparenz der Benutzeroberfläche beim Wiederverbinden auf 80 % festgelegt.

Ändern der Transparenzstufe für die Benutzeroberfläche beim Wiederverbinden

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Transparenzstufe für Benutzeroberfläche bei Wiederverbindung**.
3. Bearbeiten Sie den Wert.
4. Klicken Sie auf **OK**.

Interaktion zwischen automatischer Wiederverbindung von Clients und Sitzungszuverlässigkeit

Beim Erhalten der Verbindungsintegrität für aktive Citrix Receiver-Sitzungen können Mobilitätsprobleme im Zusammenhang mit dem Wechsel zwischen verschiedenen Zugriffspunkten, Netzwerkunterbrechungen und Anzeigetimeouts aufgrund von Latenz in Umgebungen eine echte Herausforderung darstellen. Um dieses Problem zu lösen hat Citrix die Technologien für Sitzungszuverlässigkeit und automatische Wiederverbindung in dieser Receiver für Mac-Version verbessert.

Die automatische Wiederverbindung von Clients ermöglicht Benutzern zusammen mit der Sitzungszuverlässigkeit, nach einer Netzwerkunterbrechung automatisch wieder eine Verbindung mit ihren Citrix Receiver-Sitzungen herzustellen. Diese über Richtlinien in Citrix Studio aktivierten Features können die Benutzererfahrung erheblich verbessern.

Hinweis

Timeoutwerte für die automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit können mit der Datei **default.ica** in StoreFront geändert werden.

Automatische Wiederverbindung von Clients

Die automatische Wiederverbindung von Clients kann mit einer Richtlinie in Citrix Studio aktiviert oder deaktiviert werden. Standardmäßig ist dieses Feature aktiviert. Informationen zum Ändern dieser Richtlinie finden Sie im Abschnitt zum automatischen Wiederverbinden von Clients weiter oben in diesem Artikel.

In StoreFront können Sie mit der Datei **default.ica** das Verbindungs timeout für **AutoClientReconnect** ändern. Dieses Timeout ist standardmäßig auf 120 Sekunden (2 Minuten) festgelegt.

Einstellung	Beispiel	Standard
TransportReconnectRetryMaxTimeSeconds	TransportReconnectRetryMaxTimeSeconds=60	120

Sitzungszuverlässigkeit

Die Sitzungszuverlässigkeit kann mit einer Richtlinie in Citrix Studio aktiviert oder deaktiviert werden. Standardmäßig ist dieses Feature aktiviert.

In StoreFront können Sie mit der Datei **default.ica** das Verbindungstimeout für die Sitzungszuverlässigkeit ändern. Dieses Timeout ist standardmäßig auf 180 Sekunden (3 Minuten) festgelegt.

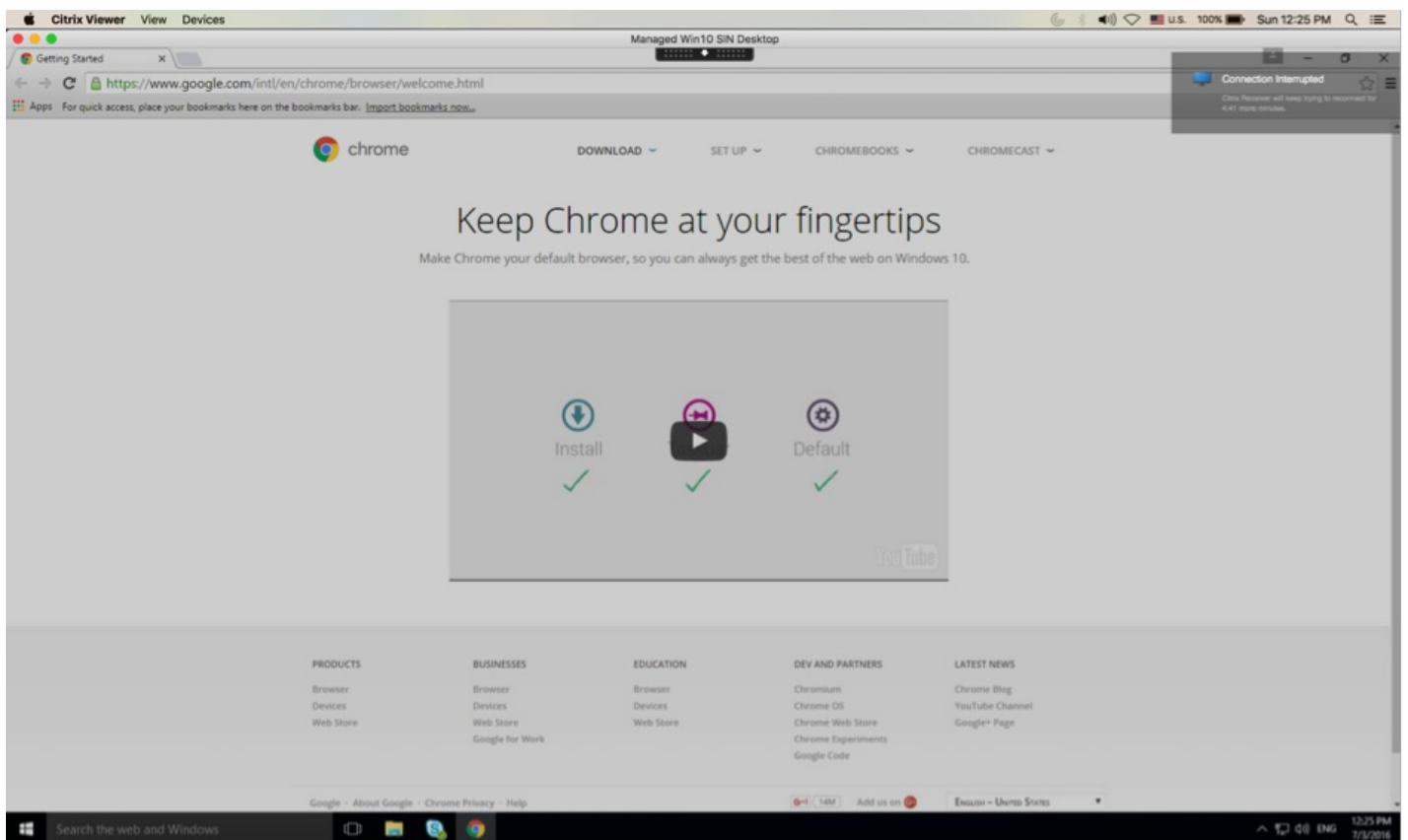
Einstellung	Beispiel	Standard
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Funktionsweise von Sitzungszuverlässigkeit und automatischer Wiederverbindung von Clients

Wenn automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit für Citrix Receiver für Mac aktiviert sind, berücksichtigen Sie Folgendes:

- Beim Wiederverbinden wird ein Sitzungsfenster ausgegraut. Ein Countdowntimer zeigt die verbleibende Zeit bis zur Wiederverbindung der Sitzung an. Wenn der Countdowntimer für die Sitzung abläuft, wird die Sitzung getrennt.

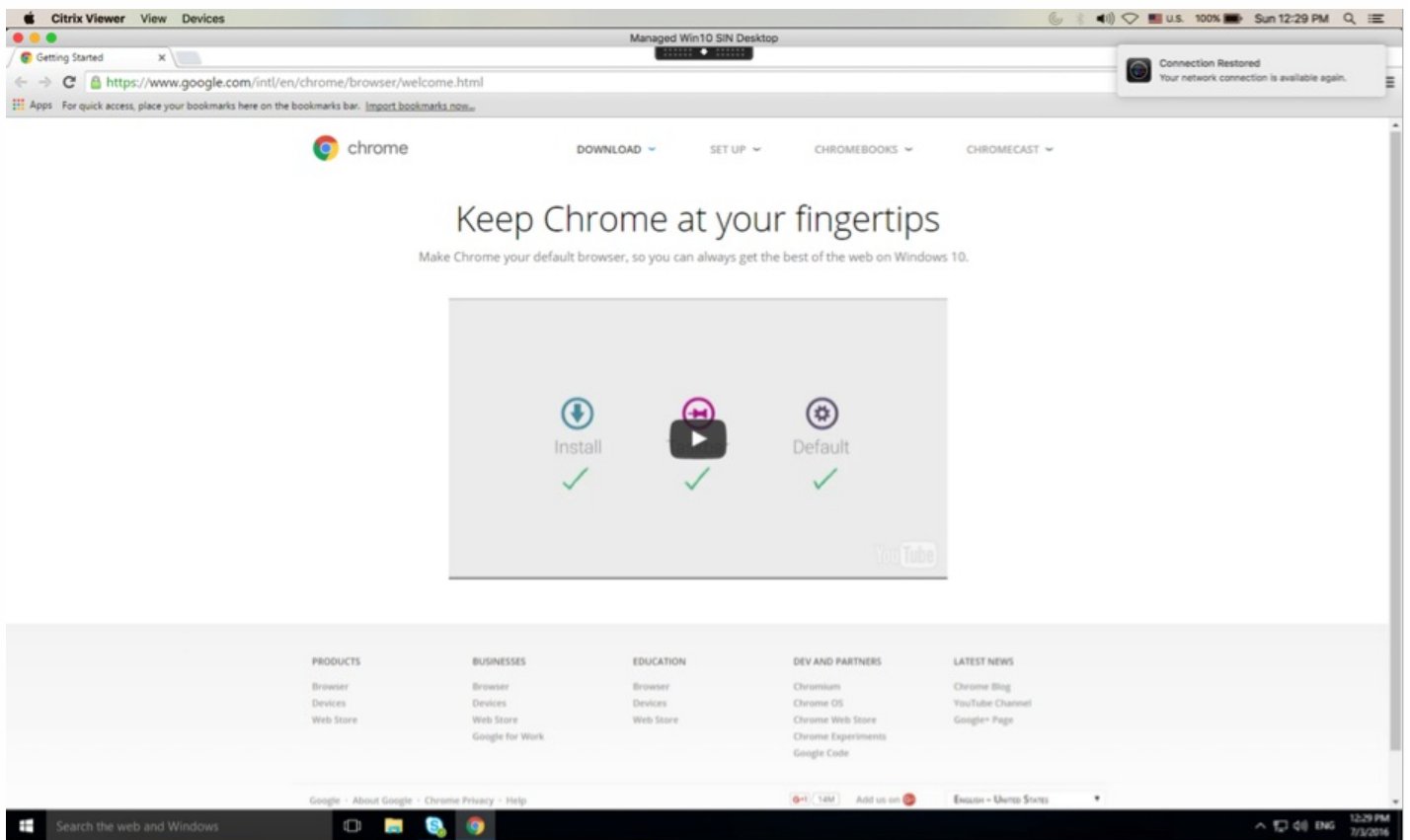
Standardmäßig beginnt der Wiederverbindungscountdown bei 5 Minuten. In diesem Zeitwert sind die Werte der beiden Timer für automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit, 2 und 3 Minuten, zusammengefasst. In der Abbildung unten sehen Sie die Meldung mit dem Countdowntimer, die oben rechts im Sitzungsfenster angezeigt wird:



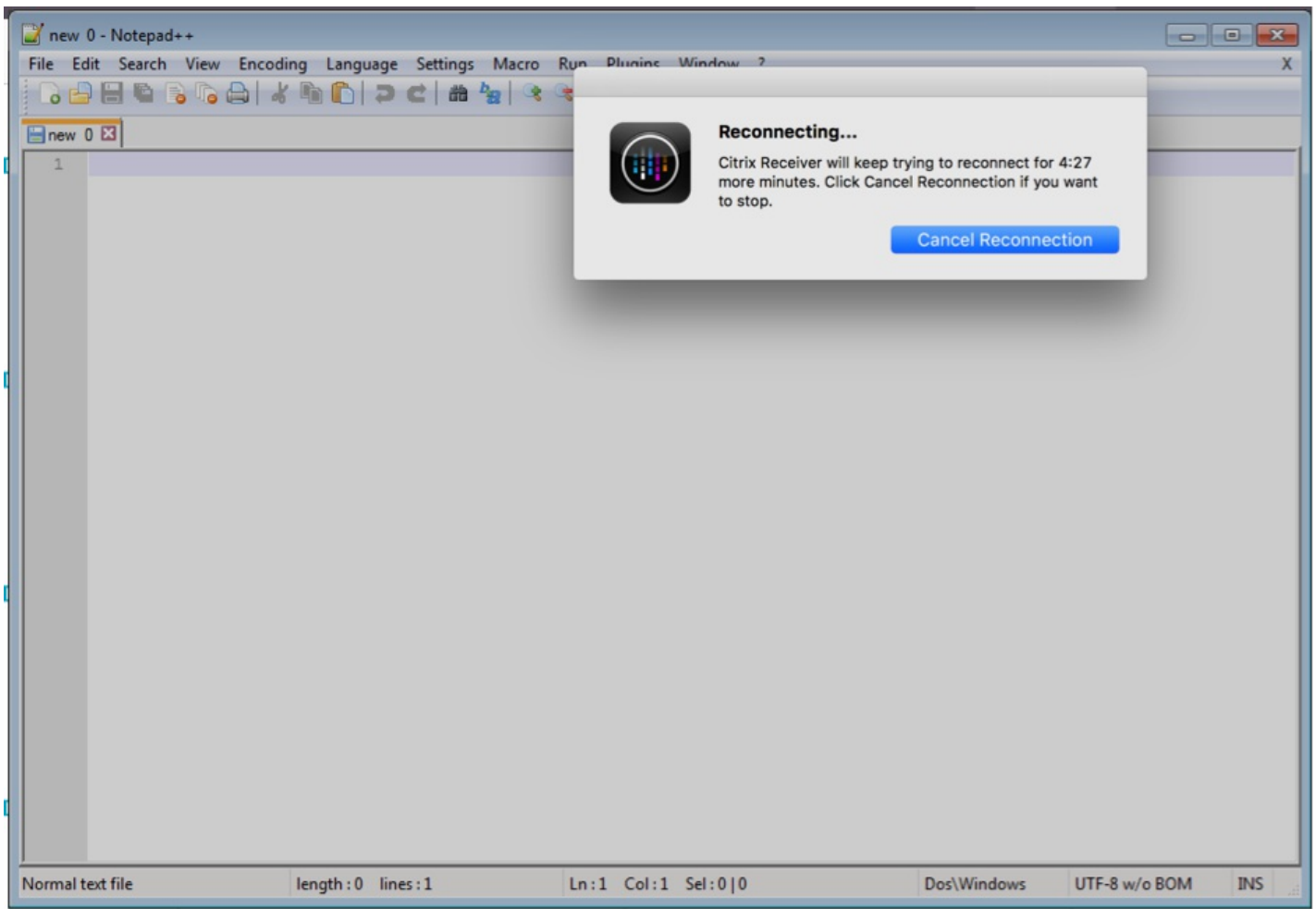
Tipp

Sie können die für eine inaktive Sitzung verwendete Graustufe mit einer Befehlszeile ändern. Beispiel: `com.citrix.receiver.nomas NetDisruptBrightness 80`. Der Standardwert ist 80. Der Höchstwert ist 100 (transparentes Fenster) und der Mindestwert kann 0 sein (schwarzes Fenster).

- Bei der erfolgreichen Wiederverbindung einer Sitzung (oder wenn eine Sitzung getrennt wird) werden Benutzer benachrichtigt. Die Benachrichtigung wird oben rechts im Sitzungsfenster angezeigt:



- In einem Sitzungsfenster, das durch Sitzungszuverlässigkeit und automatische Wiederverbindung von Clients gesteuert wird, wird eine Informationsmeldung zum Status der Sitzungsverbindung angezeigt. Klicken Sie auf **Wiederverbindung abbrechen**, um zu einer aktiven Sitzung zu wechseln.



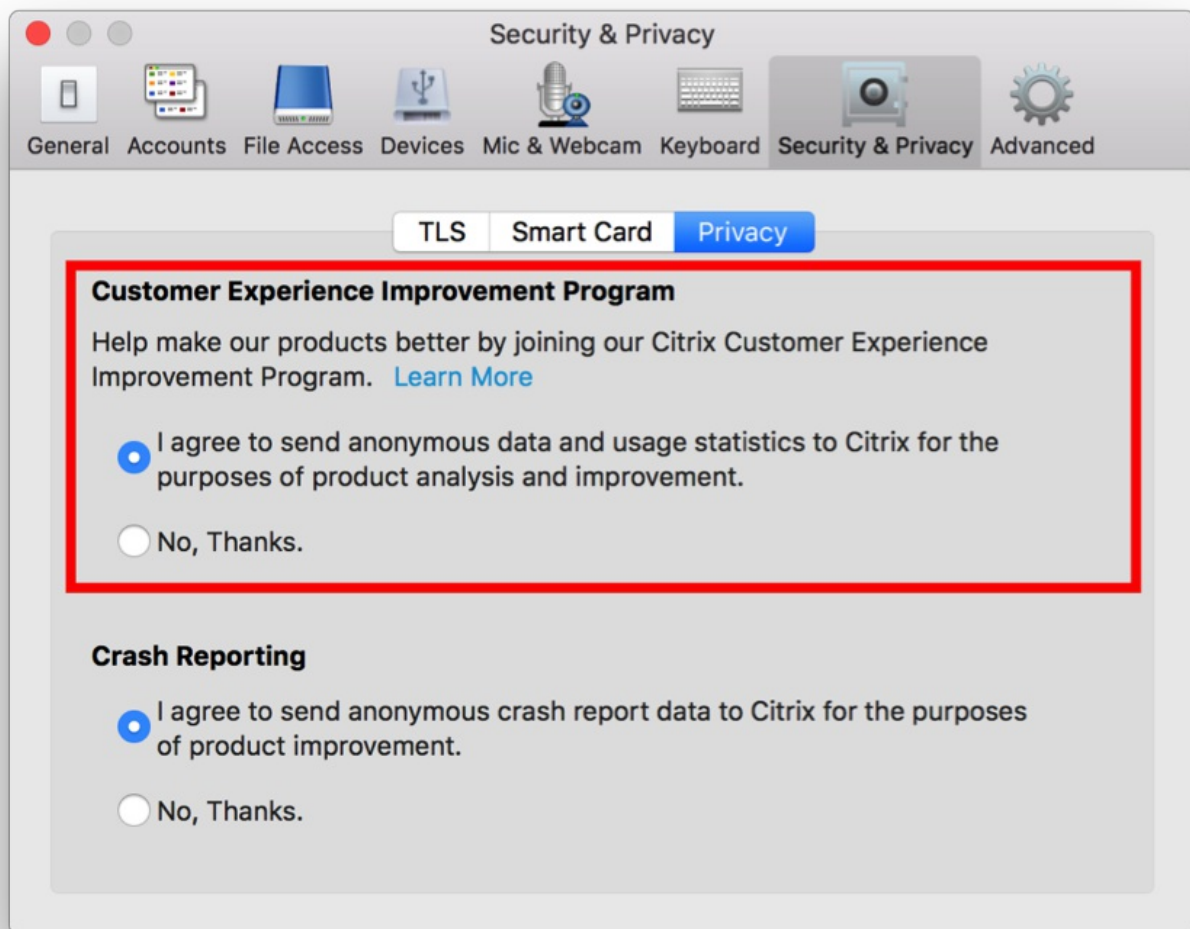
Entsprechend den Standardeinstellungen sammelt das Programm zur Verbesserung der Benutzerfreundlichkeit Daten und lädt sie alle 7 Tage nach Citrix hoch. Sie können die Einstellung zur Teilnahme am CEIP jederzeit in Citrix Receiver für Mac unter **Sicherheit > Einstellungen** ändern.

Tipp

Wenn das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) deaktiviert wird, werden nur ein Mal minimale Informationen (die installierte Version von Citrix Receiver für Mac) hochgeladen. Mit dieser Information kann die Verteilung der verschiedenen, von Kunden verwendeten Versionen festgestellt werden, daher ist sie für Citrix sehr wichtig. Die Übermittlung dieser Information erfolgt nur das eine Mal, wenn CEIP deaktiviert wird.

Deaktivieren von CEIP oder Ablehnen der Teilnahme

1. Wählen Sie im Fenster **Einstellungen** die Option **Sicherheit und Datenschutz**.
2. Wählen Sie die Registerkarte **Datenschutz**.
3. Nehmen Sie für das entsprechende Optionsfeld die gewünschte Einstellung vor. Beispielsweise klicken Sie zum Deaktivieren von CEIP auf **Nein, danke**.
4. Klicken Sie auf **OK**.



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 Citrix 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 Citrix Receiver für Mac oder durch Verweisen von Citrix Receiver für Mac auf eine StoreFront-Site. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über Citrix Receiver für Mac. 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 Citrix Receiver für Mac Tech Preview-Benutzererfahrung. Weitere Informationen zur Benutzererfahrung mit Citrix Receiver für Mac 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 für Mac sind diese Beschreibungen für Benutzer sichtbar.

Wie schon erwähnt konfigurieren Sie den Self-Service-Modus durch Hinzufügen eines StoreFront-Kontos zu Citrix Receiver für Mac oder durch Verweisen von Citrix Receiver für Mac auf eine StoreFront-Site. Auf diese Weise ermöglichen Sie Benutzern das Abonnieren von Anwendungen über die Benutzeroberfläche von Citrix Receiver für Mac. 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 von Citrix Receiver für Mac 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](#).

Mit StoreFront bestehen die erstellten Stores aus Diensten, die eine Authentifizierungs- und Ressourcenbereitstellungsinfrastruktur für Citrix Receiver für Mac 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 Dokumentation für [StoreFront](#).

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

2. Stores für CloudGateway konfigurieren Sie genauso wie für andere XenApp- und XenDesktop-Anwendungen. Für Citrix Receiver für Mac ist keine spezielle Konfiguration erforderlich. Weitere Informationen finden Sie unter *— Konfigurieren von Stores* in der [StoreFront](#)-Dokumentation.

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 Kontenermittlung mit der E-Mail-Adresse

Sie können Citrix Receiver für Mac für die e-mail-basierte Kontenermittlung konfigurieren. Nach der Konfiguration geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration von Citrix Receiver für Mac ein. Citrix Receiver für Mac ermittelt den NetScaler 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 die gehosteten 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, sodass Benutzerverbindungen angenommen werden und die e-mail-basierte Ermittlung der StoreFront- oder NetScaler Gateway-URL durchgeführt wird, finden Sie unter *— Connecting to StoreFront by Using Email-Based Discovery* in der NetScaler 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 Installation von Citrix Receiver für Mac öffnen Benutzer die Datei, um Citrix Receiver für Mac zu konfigurieren. Wenn Sie Receiver für Web-Sites konfigurieren, können Benutzer Citrix Receiver für Mac-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 Citrix Receiver für Mac 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 wird die NetScaler Gateway-Adresse, die Produktedition und die erforderliche Authentifizierungsmethode benötigt.

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

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

Konfigurieren von automatischen Updates

Ein Benutzer kann die Einstellung für Citrix Receiver-Updates im Dialogfeld **Einstellungen** überschreiben. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet.

1. Navigieren Sie in Citrix Receiver für Mac zum Dialogfeld **Einstellungen**.
2. Klicken Sie im Bereich **Erweitert** auf **Automatische Updates**. Das Dialogfeld "Citrix Receiver-Updates" wird angezeigt.
3. Wählen Sie eine der folgenden Optionen:
 - Ja, benachrichtigen Sie mich
 - Nein, nicht benachrichtigen
 - Vom Administrator festgelegte Einstellungen verwenden
4. Schließen Sie das Dialogfeld, um die Änderungen zu speichern.

Administratoren können Citrix Receiver-Updates mit StoreFront konfigurieren. Citrix Receiver verwendet diese Konfiguration nur für Benutzer, die "Vom Administrator festgelegte Einstellungen verwenden" ausgewählt haben. Mit den folgenden Schritten führen Sie die manuelle Konfiguration durch.

1. Öffnen Sie die Datei web.config in einem Text-Editor. Der Standardspeicherort ist
C:\inetpub\wwwroot\Citrix\Roaming\web.config
2. Suchen Sie das Benutzerkonto-Element in der Datei. Der Kontoname Ihrer Bereitstellung ist "Store".

Beispiel:

Vor dem Tag navigieren Sie zu den Eigenschaften des Benutzerkontos:

3. Fügen Sie das Tag für automatische Updates nach dem Tag ein.

auto-update-Check

Legt fest, dass Citrix Receiver ermitteln kann, ob Updates verfügbar sind.

Gültige Werte:

- Auto: Bei Verwendung dieser Option erhalten Benutzer Benachrichtigungen, wenn Updates verfügbar sind.
- Manual: Bei Verwendung dieser Option erhalten Benutzer keine Benachrichtigungen, wenn Updates verfügbar sind. Benutzer müssen manuell nach Updates suchen, indem sie **Nach Updates suchen** wählen.
- Disabled: Mit dieser Option werden Citrix Receiver-Updates deaktiviert.

auto-update-DeferUpdate-Count

Legt fest, wie oft Endbenutzer zum Update aufgefordert werden, bevor das Update auf die aktuelle Version von Citrix Receiver erzwungen wird. Der Standardwert ist 7.

Gültige Werte:

- -1: Der Endbenutzer kann das verfügbare Update beliebig oft verschieben.
- 0: Sobald das Update verfügbar ist, wird der Endbenutzer gezwungen, das Update auf die aktuelle Version von Citrix Receiver auszuführen.
- Positive Ganzzahl: Male, die der Endbenutzer an das Update erinnert wird, bevor das Update erzwungen wird. Citrix empfiehlt, diesen Wert höchstens auf 7 festzulegen.

auto-update-Rollout-Priority

Legt fest, wie schnell ein Gerät erkennt, dass ein Update verfügbar ist.

Gültige Werte:

- Auto: Citrix Receiver-Updates entscheidet, wann Benutzern verfügbare Updates bereitgestellt werden.
- Fast: Verfügbare Updates werden Benutzern mit der von Citrix Receiver festgelegten hohen Priorität zur Verfügung gestellt.
- Medium: Verfügbare Updates werden Benutzern mit der von Citrix Receiver festgelegten mittleren Priorität zur Verfügung gestellt.
- Slow: Verfügbare Updates werden Benutzern mit der von Citrix Receiver festgelegten niedrigen Priorität zur Verfügung gestellt.

Optimieren der Citrix Receiver für Mac-Umgebung

Sep 25, 2017

Sie können die Citrix Receiver für Mac-Umgebung wie folgt optimieren:

- [Automatische Wiederverbindung von Benutzern](#)
- [Neustarten von Desktops](#)
- [Aktivieren der Sitzungszuverlässigkeit](#)
- [Kontinuität für mobile Benutzer](#)
- [Zuweisen von Clientgeräten](#)
- [Zuordnen von Clientlaufwerken](#)
- [Zuordnen von COM-Ports für Clients](#)

Benutzer können von ICA-Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Mit dem Feature zur automatischen Wiederverbindung von Clients kann Citrix Receiver für Mac unabsichtlich getrennte ICA-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. Citrix Receiver für Mac 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 Wiederverbindung von Clients mit Richtlinien Einstellungen auf dem Server. Weitere Informationen finden Sie in der Dokumentation von [XenApp](#) und [XenDesktop](#).

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 Citrix Receiver für Mac den Desktop herunter und startet ihn neu.

Important

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

Mit dem Feature für Sitzungszuverlässigkeit werden Benutzern die Fenster einer gehosteten Anwendung und eines Desktops weiterhin 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 Sitzungszuverlässigkeit mit Richtlinieneinstellungen auf dem Server. Weitere Informationen über Sitzungszuverlässigkeit und die Interaktion mit Receiver finden Sie im [Dokument über das Sicherstellen höchster Dienstqualität und Zuverlässigkeit](#).

Weitere Informationen zu Richtlinien finden Sie unter [Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients"](#) und [Einstellungen der Richtlinie "Sitzungszuverlässigkeit"](#).

Tipp

Benutzer von Citrix Receiver für Mac können die Servereinstellungen für die Sitzungszuverlässigkeit nicht überschreiben.

Important

Wenn die Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

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 Fenster von Citrix Receiver für Mac auf den Abwärtspfeil ▼ 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.

Citrix Receiver für Mac ordnet lokale Laufwerke und Geräte automatisch zu, damit sie in einer Sitzung verfügbar sind. Wenn die Clientgerätozuordnung 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.

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.

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

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

Konfigurieren des Lese- und Schreibzugriffs für zugeordnete Laufwerke

1. Klicken Sie auf der Homepage von Citrix Receiver für Mac auf den Abwärtspfeil ▼ 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.

Mit der Client-COM-Portzuordnung können Geräte, die an COM-Ports des Benutzergeräts angeschlossen sind, in Sitzungen verwendet werden. Diese Zuordnungen können in gleicher Weise 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 Homepage von Citrix Receiver für Mac auf den Abwärtspfeil  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 Citrix Receiver für Mac 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

Sep 25, 2017

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

- [Programm zur Verbesserung der Benutzerfreundlichkeit \(CEIP\)](#)
- [ClearType-Schriftartenglättung](#)
- [Clientseitige Mikrofoneingabe](#)
- [Windows-Sondertasten](#)
- [Windows-Tastenkombinationen](#)
- [Verwenden eines Eingabemethoden-Editors \(IME\) und internationaler Tastaturlayouts](#)
- [Verwenden mehrerer Monitore](#)
- [Verwenden der Desktopsymbolleiste](#)

Das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt anonyme Konfigurations- und Verwendungsdaten in Citrix Receiver für Mac und sendet die Daten automatisch an Citrix. Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung von Citrix Receiver für Mac zu verbessern. Weitere Informationen finden Sie unter [Konfigurieren von CEIP](#).

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 Citrix Receiver für Mac verwenden.

Citrix Receiver für Mac 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.

Citrix Receiver für Mac 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

Citrix Receiver für Mac bietet Unterstützung für digitale Diktate. Weitere Informationen zum Konfigurieren dieses Features finden Sie unter [Audiofeatures](#) auf der Website mit der Produktdokumentation.

Sie können wählen, ob Mikrofone, die an das Benutzergerät angeschlossen sind, in Sitzungen verwendet werden. Wählen Sie hierfür eine der folgenden Optionen in den Citrix Receiver für Mac-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.

Citrix Receiver für Mac 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 PC-Taste oder Aktion	Option-1 bis -9 (die Zahlen 1 bis 9) auf der Zehnertastatur Mac-Optionen
F10	Option-0 (die Zahl 0) auf der Zehnertastatur
F11	Option-Minuszeichen auf der Zehnertastatur
F12	Option-Pluszeichen auf der Zehnertastatur

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. Citrix Receiver für Mac 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 Citrix Receiver für Mac oder anderen Einstellungen), werden möglicherweise andere Kombinationen von Tastaturanschlägen weitergeleitet, und der Remote-PC weist ein anderes Verhalten auf.

Important

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) 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
Löschen	Löschen 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 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

Mit Citrix Receiver für Mac 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 Citrix Receiver für Mac 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

Citrix Receiver für Mac 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.

Mit der Menüoption **Alle Displays in Vollbild verwenden** können Benutzer Citrix 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.

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 10.9 klicken Sie in der Dropdown-Menüleiste auf die blaue Menüschtfläche. 
 - 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 für Mac-Kommunikation

Sep 25, 2017

Dieser Abschnitt enthält Informationen zum Sichern der Kommunikation in Citrix Receiver für Mac.

- [Informationen zu Zertifikaten](#)
- [Verbindungen mit NetScaler Gateway](#)
- [Verbinden mit Secure Gateway](#)
- [Herstellen von Verbindungen über Proxyserver](#)
- [Herstellen einer Verbindung durch eine Firewall](#)
- [Verbinden mit TLS-Relay](#)
 - [Informationen über TLS-Richtlinien](#)
 - [Konfigurieren und Aktivieren von Receiver für TLS](#)
 - [Installieren von Stammzertifikaten auf Benutzergeräten](#)
 - [Konfigurieren von TLS-Richtlinien](#)
- [Konfigurieren von Sicherheitseinstellungen mit der Benutzeroberfläche](#)

Zum Sichern der Kommunikation zwischen der Serverfarm und Citrix Receiver für Mac können Sie Verbindungen zur Serverfarm mit zahlreichen Sicherheitsverfahren integrieren, einschließlich Citrix NetScaler Gateway. Weitere Informationen zur Konfiguration mit Citrix StoreFront finden Sie in der [StoreFront-Dokumentation](#).

Hinweis

Citrix empfiehlt, dass die Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit NetScaler Gateway gesichert wird.

- 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 für Mac 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 Citrix Receiver für Mac 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.

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 Citrix Receiver für Mac 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. Citrix Receiver für Mac unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate mit NetScaler Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem NetScaler Gateway-Serverzertifikat zugeordnet werden. Weitere Informationen hierzu finden Sie in der [NetScaler Gateway-Dokumentation](#). Weitere Informationen zum Installieren und Verknüpfen eines Zwischenzertifikats mit einer primären ZS auf einem NetScaler Gateway-Gerät finden Sie im folgenden Artikel: [How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway](#).

Richtlinie für gemeinsame Serverzertifikatvalidierung

Citrix Receiver für Mac hat eine strenge Validierungsrichtlinie für Serverzertifikate.

Important

Bestätigen Sie vor der Installation dieser Version von Citrix Receiver für Mac, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:

- die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
- die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
- die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder ungültiges Zwischenzertifikat
- die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

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

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

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"
- "Beispielstammzertifikat"

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

Important

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

Hinweis

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

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

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

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

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

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall ist das Gateway normalerweise wie

folgt mit allen Zwischenzertifikaten konfiguriert, jedoch nicht mit dem Stammzertifikat:

- "Beispielserversertifikat"
- "Beispielzwischenzertifikat 1"
- "Beispielzwischenzertifikat 2"

Important

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

Hinweis

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

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

- "Beispielserversertifikat"
- "Beispielzwischenzertifikat"

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

- "Beispielserversertifikat"
- "Beispielzwischenzertifikat"
- "Übergreifendes Beispielzwischenzertifikat" [nicht empfohlen]

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

- "Beispielserversertifikat"

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

Damit Remotebenutzer sich mit der XenMobile-Bereitstellung über NetScaler Gateway verbinden können, konfigurieren Sie diese für StoreFront. Die Methode für das Aktivieren des Zugriffs hängt von der in der Bereitstellung verwendeten XenMobile-Edition ab.

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

Weitere Informationen zum Konfigurieren dieser Verbindungen mit NetScaler Gateway finden Sie unter [Integrating with NetScaler Gateway and NetScaler](#).

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Secure Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen Citrix Receiver für Mac und dem Server bereitzustellen. Citrix Receiver für Mac 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 Citrix Receiver für Mac Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden. Weitere Informationen zum Konfigurieren der Proxyservereinstellungen für Citrix Receiver für Mac finden Sie in der [Webinterface](#)-Dokumentation.

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

Wenn Sie den Relaymodus verwenden, fungiert der Secure Gateway-Server als Proxy und Sie müssen Citrix Receiver für Mac 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 (Beispiel.com) wird im Allgemeinen als Domänenname bezeichnet.

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

Für die Kommunikation mit dem XenApp- oder XenDesktop-Server verwendet Citrix Receiver für Mac 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 Citrix Receiver für Mac die Proxyservereinstellungen, die für den Standardwebbrowser auf dem Benutzergerät konfiguriert sind. Sie müssen die Proxyservereinstellungen für den Standardwebbrowser entsprechend auf dem Benutzergerät konfigurieren.

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss Citrix Receiver für Mac 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 der XenApp-Server oder XenDesktop-Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface Citrix Receiver für Mac eine alternative Adresse bereitstellen. Citrix Receiver für Mac stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her. Weitere Informationen finden Sie in der Dokumentation zum [Webinterface](#).

Citrix Receiver für Mac 12.3 unterstützt TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen für TLS-Verbindungen mit XenApp/XenDesktop:

- 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

Hinweis: Citrix Receiver für Mac, das auf Mac OS Sierra ausgeführt wird, unterstützt nicht die folgenden TLS-Verschlüsselungssammlungen:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

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

Citrix Receiver für Mac unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

Weitere Informationen zur Konfiguration und Sicherung der Installation mit TLS-Relay finden Sie in der Dokumentation für [XenDesktop](#) und StoreFront.

Hinweis

Citrix Receiver für Mac verwendet plattformeigene Kryptografie (OS X) für Verbindungen zwischen Citrix Receiver für Mac und

Konfigurieren und Aktivieren von Citrix Receiver für Mac 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-aktiviertem Citrix Receiver für Mac und der Serverfarm muss auf dem Clientgerät 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 TLS-fähigen Clients und anderen Anwendungen, die TLS einsetzen, verwendet werden.

Informationen über TLS-Richtlinien

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

Hinweis

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

TLS-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

```
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.

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

Hinweis

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

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

Konfigurieren von TLS-Richtlinien

Führen Sie zum Konfigurieren von TLS-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:

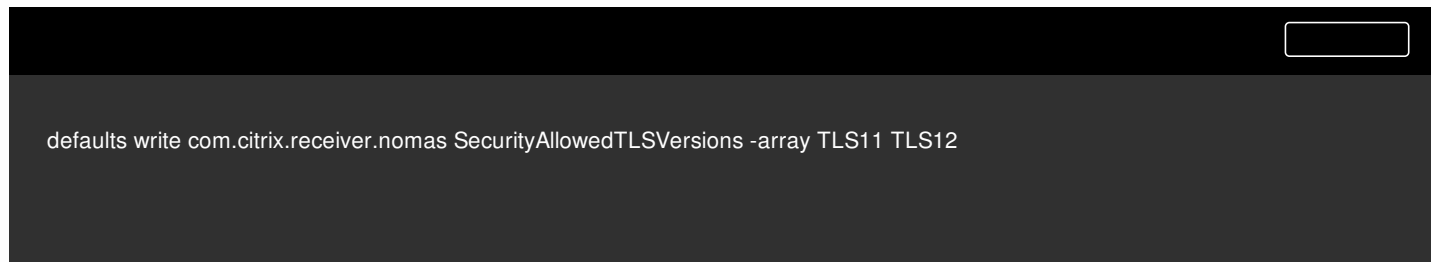
```
defaults write com.citrix.receiver.nomas
```

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.



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

Wiederherstellen der Standardkonfiguration

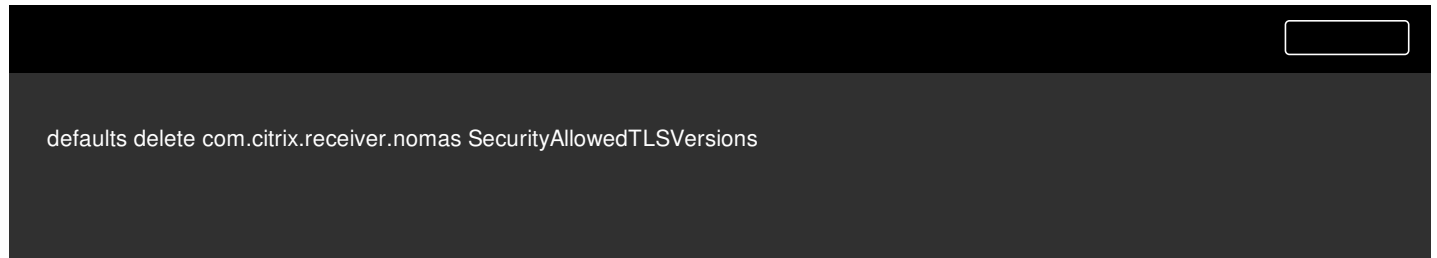
Zurücksetzen einer Einstellung auf den Standard

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.



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

Mit Citrix Receiver für Mac-Version 12.3 wurden zahlreiche Sicherheitsverbesserungen eingeführt, u. a.:

- Verbesserte Benutzeroberfläche für die Sicherheitskonfiguration: In vorherigen Releases war die Befehlszeile die bevorzugte Methode zum Vornehmen sicherheitsrelevanter Änderungen. Nun können Konfigurationseinstellungen für die Sitzungssicherheit einfach über die Benutzeroberfläche vorgenommen werden. Diese nahtlose Methode zum Festlegen von Sitzungseinstellungen führt zu einer besseren Benutzererfahrung.
- Anzeigen von TLS-Verbindungen: Mit Citrix Receiver für Mac können Sie Verbindungen mit Servern, die eine bestimmte TLS-Version verwenden, durch zusätzliche Informationen verifizieren, einschließlich dem für die Verbindung verwendeten Verschlüsselungsalgorithmus, Modus, Schlüsselgröße und Aktivierung von SecureICA. Darüber hinaus können Sie das Serverzertifikat für TLS-Verbindungen anzeigen.

Die neue Registerkarte **TLS** im erweiterten Bildschirm **Sicherheit und Datenschutz** enthält die folgenden neuen Optionen:

- Konformitätsmodus festlegen

- Kryptografiemodul konfigurieren
- Geeignete TLS-Version auswählen
- Zertifikatsperrliste auswählen
- Einstellungen für alle TLS-Verbindungen aktivieren

Im Bild unten sehen Sie die Einstellungen für Sicherheit und Datenschutz, auf die über die Benutzeroberfläche zugegriffen werden kann:

