



Citrix Workspace-App für Mac

Contents

Info zu diesem Release	3
Systemanforderungen und Kompatibilität	24
Installieren, Deinstallieren und Aktualisieren	30
Aktualisieren	32
Konfigurieren	39
Authentifizierung	78
Sichere Kommunikation	81

Info zu diesem Release

February 21, 2022

Wichtig

Ab macOS Catalina hat Apple zusätzliche Anforderungen für Stammzertifikate und Zwischenzertifikate erzwungen, die Administratoren konfigurieren müssen. Weitere Informationen finden Sie im Apple Support-Artikel [HT210176](#).

Neue Features in Release 2201

Migration von StoreFront zu Workspace [Technical Preview]

Wenn Ihre Organisation von On-Premises-StoreFront zu Workspace wechselt, müssen Benutzer die neue Workspace-URL der Workspace-App manuell hinzufügen. Dieses Feature ermöglicht es Administratoren, Benutzer nahtlos von einem StoreFront-Store zu einem Workspace-Store unter minimaler Benutzerinteraktion zu migrieren.

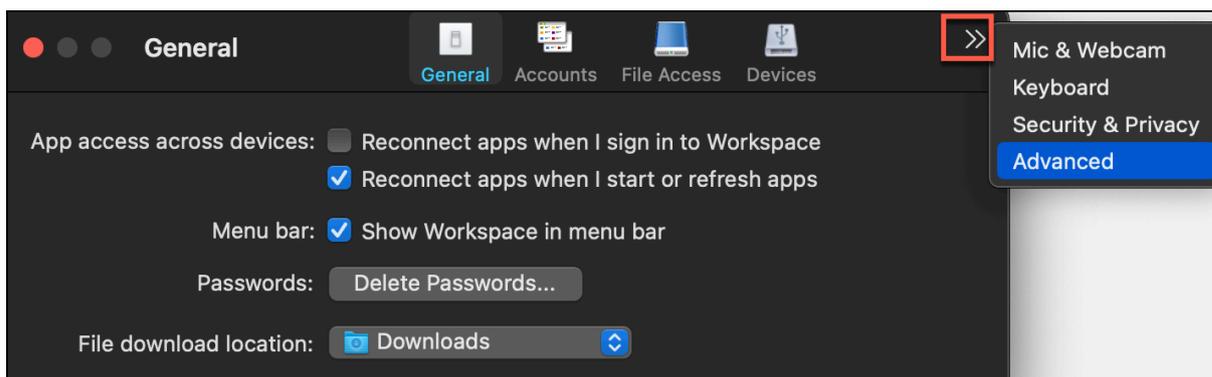
Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Preview-Features, begrüßt jedoch [Feedback](#) zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

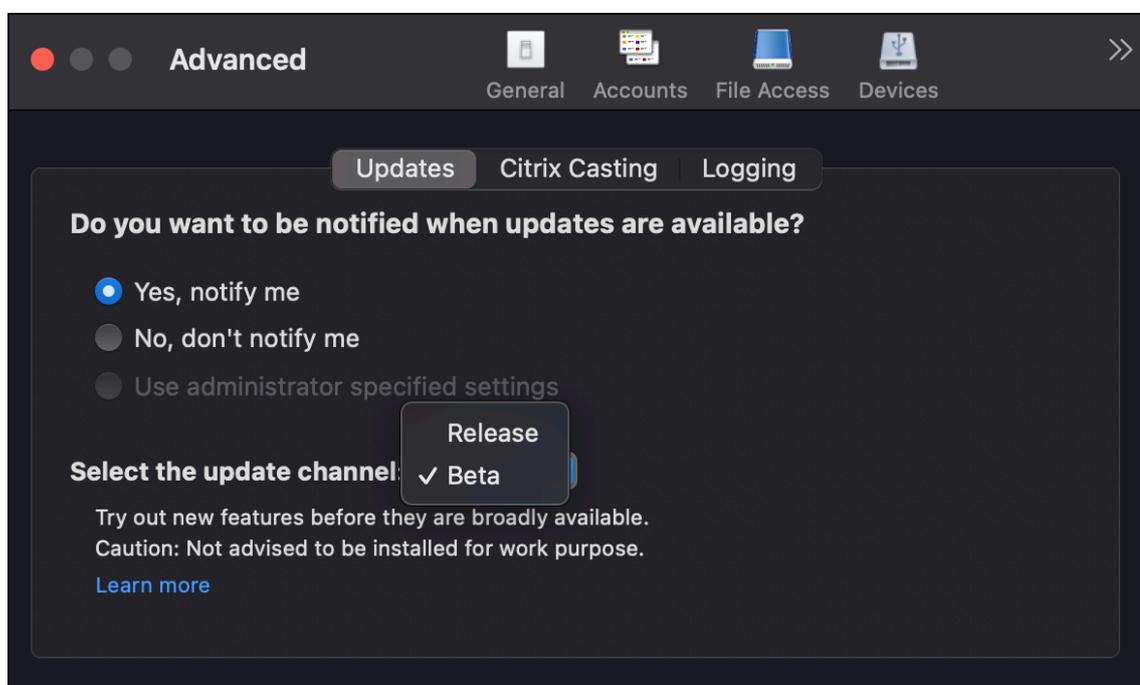
Beta-Programm für Citrix Workspace-App

Ab diesem Release können Sie vorhandene Installationen von Citrix Workspace-Apps automatisch auf die neuesten Beta Builds aktualisieren und diese testen. Beta Builds sind Early Access-Versionen, die vor der allgemeinen Verfügbarkeit eines vollständig unterstützten stabilen Releaseupdates veröffentlicht werden. Sie erhalten eine Updatebenachrichtigung, wenn die Citrix Workspace-App für automatische Updates konfiguriert ist.

Um auf die Beta-Builds zuzugreifen, öffnen Sie die Workspace-App, klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und klicken Sie dann auf **Einstellungen > Erweitert**. Um auf Beta Builds zu aktualisieren, wählen Sie den **Beta-Kanal** in der Dropdownliste aus.



- **Beta:** Early Access Release zum einfachen Testen und Melden von Problemen vor der allgemeinen Verfügbarkeit.
- **Release:** Vollständig unterstütztes stabiles Releaseupdate.



Weitere Informationen zur Verwendung dieser Funktion finden Sie unter [Aktualisierung](#).

Vollbildmodus auf mehreren Monitoren [Technical Preview]

Sie können jetzt auf zwei oder mehr Monitoren gleichzeitig in den Vollbildmodus wechseln. Führen Sie die folgenden Schritte aus, um diese Funktion zu verwenden:

1. Öffnen Sie den Citrix Viewer.
2. Um den Vollbildmodus auf den anderen angeschlossenen Monitoren zu verwenden, ziehen Sie das Fenster von Ihrem primären Monitor, sodass es sich auf die angeschlossenen Monitore aus-

dehnt. Wählen Sie in der Citrix Viewer-Symbolleiste die Option **Zu Vollbild wechseln**. Das Fenster wechselt auf diesen Monitoren in den Vollbildmodus.

Hinweis:

Wenn Sie zuvor die Option **Alle Displays in Vollbild verwenden** ausgewählt haben, heben Sie die Auswahl auf, da diese Auswahl auf allen angeschlossenen Monitoren den Vollbildmodus festlegt.

3. Ziehen Sie das Citrix Virtual Desktop-Fenster auf einen Monitor, um in den Vollbildmodus zu wechseln.

Citrix empfiehlt die Verwendung von maximal 3 Monitoren, einschließlich des primären Monitors.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Preview-Features, begrüßt jedoch [Feedback](#) zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Behobene Probleme in Release 2201

- Beim Auswählen des Kandidatentexts aus dem Kompositionsfenster des Eingabemethoden-Editors mit den Pfeilen nach links oder rechts auf der Tastatur bewegt sich der Eingabecursor nicht entsprechend. Dieses Problem tritt auf, wenn Sie einen Desktop starten und das Kontrollkästchen **Lokales Tastaturlayout statt des Remoteserver-Tastaturlayouts verwenden** im Fenster **Einstellungen > Tastatur** der Citrix Workspace-App aktiviert ist. Dieses Problem tritt nur in chinesischer und japanischer Sprache auf. [HDX-34956]
- Der Mauszeiger verschwindet zeitweise in Workspace-App-Sitzungen und Sie können nichts anklicken. [HDX-36820]
- Die Desktopsitzung wird unerwartet geschlossen, wenn Sie in einem Excel-Arbeitsblatt eine Zelle in einer PivotTable ziehen. [HDX-37178]
- Wenn Richtlinien für verlustfreien Codec oder Vollbild-H.264-Codec angewendet werden, treten nach der Aktualisierung auf Version 2112 manchmal Probleme mit Grafiken in Ihrer Desktopsitzung auf. [HDX-37272]
- Nach dem Upgrade der Workspace-App von Version 2010 auf Version 2112 können Sie keine Verbindung zu Desktops oder Apps herstellen. [RFMAC-10811]

Bekannte Probleme in Release 2201

- Der Clientname wird im Citrix Brokerdienst und in Citrix Director mit zufälligen Zeichen angezeigt, wenn Sie die Workspace-App im Offlinemodus (Intranetmodus) verwenden. [RFMAC-10842]

Frühere Releases

In diesem Abschnitt werden Features in früheren Releases zusammen mit behobenen und bekannten Problemen aufgeführt. Releases erreichen 18 Monate nach Veröffentlichung das Ende des Lebenszyklus (EOL). Einzelheiten zu den Lebenszyklusdaten für die unterstützten Versionen finden Sie unter [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

2112

Neue Features

Unterstützung für benutzerdefinierte Webstores

Sie können jetzt über die Citrix Workspace-App für Mac auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Zuvor konnten Sie nur über den Browser auf die benutzerdefinierten Stores zugreifen.

Die Citrix Workspace-App für Mac lädt die benutzerdefinierten Webstores ähnlich wie ein Browser und erweitert die Funktionen des App-Schutzes auf benutzerdefinierte Webstores. Durch den Zugriff auf das benutzerdefinierte Portal über die native Workspace-App werden Benutzern umfassende Funktionen und eine gute Benutzererfahrung für dieses Feature geboten. Weitere Informationen zum Global App Configuration Service finden Sie unter [Erste Schritte](#).

Weitere Informationen zum Konfigurieren eines benutzerdefinierten Webstores finden Sie unter [Benutzerdefinierter Webstore](#).

Anfordern der Steuerung in Microsoft Teams

Ab diesem Release können Sie bei einem Microsoft Teams-Anruf die Steuerung anfordern, wenn ein Teilnehmer den Bildschirm freigibt. Wenn Sie die Steuerung übernommen haben, können Sie auf dem freigegebenen Bildschirm auswählen, bearbeiten und andere Änderungen vornehmen.

Zum Übernehmen der Steuerung bei Freigabe eines Bildschirms klicken Sie oben im Microsoft Teams-Bildschirm auf **Steuerung anfordern**. Der Teilnehmer des Meetings, der den Bildschirm freigibt, kann die Anforderung akzeptieren oder ablehnen. Wenn Sie fertig sind, klicken Sie auf **Steuerung freigeben**.

Einschränkung:

Während Peer-zu-Peer-Anrufen zwischen einem optimierten Benutzer und einem Benutzer mit dem nativen Microsoft Teams-Desktopclient, der auf dem Endpunkt ausgeführt wird, ist die Option **Steuerung anfordern** nicht verfügbar. Als Workaround können Benutzer einem Meeting beitreten, um die Option **Steuerung anfordern** zu erhalten.

Dynamisches e911

Ab diesem Release unterstützt die Citrix Workspace-App den dynamischen Notruf. Wenn Sie Microsoft-Anrufpläne, Operator Connect und Direct Routing verwenden, haben Sie folgende Möglichkeiten:

- Konfigurieren und Übermitteln von Notrufen
- Benachrichtigen von Sicherheitspersonal

Die Benachrichtigung erfolgt basierend auf dem aktuellen Standort der Citrix Workspace-App auf dem Endpunkt anstelle des Microsoft Teams-Clients, der auf dem VDA ausgeführt wird. Der Ray Baum Act schreibt vor, dass der Aufenthaltsort des 911-Anrufers an die entsprechende Notrufleitstelle (Public Safety Answering Point, PSAP) übertragen wird. Ab Citrix Workspace-App 2112.1 für Windows erfüllt die Microsoft Teams-Optimierung mit HDX die Bestimmungen von Ray Baum's Law. Weitere Informationen zu diesem Feature finden Sie unter [Unterstützung für dynamisches e911](#) im Abschnitt **Microsoft-Telefonsystem**.

PDF Universal Printing (Technical Preview)

Das Feature PDF Universal Printing ist mit Citrix Virtual Apps and Desktops 2112 verfügbar. Diese Funktion ist in der Standardeinstellung deaktiviert. Um das Feature nutzen zu können, müssen Sie sich mit diesem [Webformular](#) registrieren. Sobald wir Ihre Informationen erhalten haben, wird das Feature für Sie aktiviert. Sie erhalten außerdem Anweisungen zur Verwendung des Features und zu den Druckrichtlinien, die aktiviert sein müssen.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Preview-Features, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Servicekontinuität

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Benutzer können so ihre virtuellen Apps und

Desktops unabhängig vom Integritätsstatus der Cloud-Dienste starten. Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen.

Die Workspace-App und die Workspace Web-Erweiterung verwenden gemeinsam Workspace-Verbindungsleases, um bei Ausfällen den Zugriff auf Apps und Desktops über einen Browser zu ermöglichen. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Citrix Workspace Browser

Dieses Release des Workspace Browser basiert auf Chromium Version 95. Informationen zu Features oder Bugfixes in Citrix Workspace Browser finden Sie unter [Neue Features](#) in der Dokumentation zu Citrix Workspace Browser.

Behobene Probleme

- Der Fehler “Verbindung zum Server nicht möglich” wird angezeigt, wenn das Transportprotokoll von Enlightened Data Transport (EDT) zu TCP wechselt. [CVADHELP-18310]
- Wenn eine geschützte Progressive Web App (PWA) unter macOS geöffnet wird, werden die **App-Schutzrichtlinien** nicht erzwungen. [RFMAC-10128]

2111

Neue Features

- Mit diesem Release können Benutzer die Citrix Workspace-App für Mac nicht manuell auf eine Version zurücksetzen, die niedriger ist als die auf ihren Systemen installierte Version. Wenn auf einem Mac-Gerät beispielsweise die Citrix Workspace-App Version 2109 installiert ist, können Sie die App nicht manuell auf Version 2108 oder niedriger zurücksetzen.
- Starten Sie die Remotedesktopsitzung mit einer dauerhaften Lizenz, wenn Sie Clientzugriffslizenzen (CAL) für den Zugriff auf Remotedesktops ausführen. Sie können die Remotedesktopsitzung starten, wenn die Client-ID länger als 15 Zeichen ist.
- Um das Citrix Virtual Channel SDK auf einen Mac zu laden, auf dem die Citrix Workspace-App 2111 ausgeführt wird, müssen Sie Ihre benutzerdefinierten virtuellen Kanäle neu kompilieren. Einzelheiten finden Sie unter [Update Custom Virtual Channels on Citrix Workspace app for Mac](#).

Unterstützung für benutzerdefinierte Webstores [Technical Preview]

Ab diesem Release können Sie über die Citrix Workspace-App für macOS auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Administratoren müssen den benutzerdefinierten Webstore

der Liste der zulässigen URLs im Global App Configuration Service hinzufügen, um dieses Feature verwenden zu können. Nach dem Hinzufügen der URLs können Sie die URL des benutzerdefinierten Webstores unter “Konto hinzufügen” in der Citrix Workspace-App angeben. Der benutzerdefinierte Webstore wird im nativen Workspace-App-Fenster für macOS geöffnet.

Hinweis:

Kunden haben die Möglichkeit, Technical Previews in Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu testen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Preview-Features, begrüßt jedoch [Feedback](#) zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Citrix Workspace Browser - Informationen zu Features oder Bugfixes in Citrix Workspace Browser finden Sie unter [Neue Features](#) in der Dokumentation zu Citrix Workspace Browser.

Behobene Probleme

- Auf Geräten mit macOS wird Advanced Audio Coding (AAC) nicht unterstützt. [CTXBR-1844]
- Wenn Sie die Workspace-App mit der Datei `.cr` konfigurieren und sich dann mit Ihren Anmeldeinformationen anmelden, wird die Homepage verzögert angezeigt. [RFMAC-9990]
- Öffnen Sie eine geschützte SaaS-App, öffnen Sie eine neue Registerkarte und trennen Sie die neue Registerkarte, indem Sie sie aus der Registerkartenleiste in ein neues Fenster ziehen. Ordnen Sie nun zwei Fenster nebeneinander an und öffnen Sie eine neue Registerkarte im zweiten Fenster, um einen Screenshot zu erstellen. Sie können auch den Screenshot für die geschützte SaaS-App erfassen. [RFMAC-10060]
- Wenn Sie von einem Store zum anderen wechseln, werden Sie möglicherweise vom ersten Store abgemeldet. [RFMAC-10137]
- Wenn Sie bei der Anmeldung an der Workspace-App falsche Anmeldeinformationen eingeben, wird die Fehlermeldung “Falsche Anmeldeinformationen” nicht angezeigt. Es wird erneut eine Authentifizierungsaufforderung angezeigt. Manchmal wird **Domäne\Benutzer** in der Authentifizierungsaufforderung anstelle von **Benutzername** angezeigt. [RFMAC-10210]
- Anrufe schlagen fehl, wenn ein optimierter Microsoft Teams P2P-Anruf von der Citrix Workspace-App für Mac 2109 zur Citrix Workspace-App für Windows 2109 getätigt wird. [HDX-35223]

2109.1

Neue Features

macOS Monterey-Unterstützung

Die Citrix Workspace-App für Mac wird auf macOS Monterey (12.0.1) unterstützt.

Behobene Probleme

- Wenn Sie eine geschützte App, eine nicht geschützte SaaS-App und eine geschützte Desktopsitzung geöffnet haben, wird der Browser unerwartet beendet. Dieses Problem tritt auf, wenn Sie vom Fenster der geschützten Desktopsitzung zu der nicht geschützten SaaS-App wechseln. [CTXBR-2087]
- Wenn vom Administrator externe Erweiterungen in Google Chrome installiert wurden, stürzt der Citrix Workspace-Browser beim Öffnen ab. [CTXBR-2135]

2109

Neue Features

Hinweis:

Bei aktivierter Servicekontinuität werden beim Upgrade auf Version 2109 die Verbindungslease-dateien aktualisiert. Alle vorhandenen Leases werden gelöscht und neue Leases werden im Rahmen von Funktionsverbesserungen abgerufen.

Citrix Workspace-App für Mac auf macOS Monterey Beta

Die Citrix Workspace-App 2109 für Mac wurde auf macOS Monterey Beta 7 getestet. Verwenden Sie dieses Setup in einer Testumgebung und geben Sie uns Feedback.

Achtung:

Verwenden Sie die Citrix Workspace-App für Mac unter macOS Monterey Beta-Versionen nicht in Produktionsumgebungen.

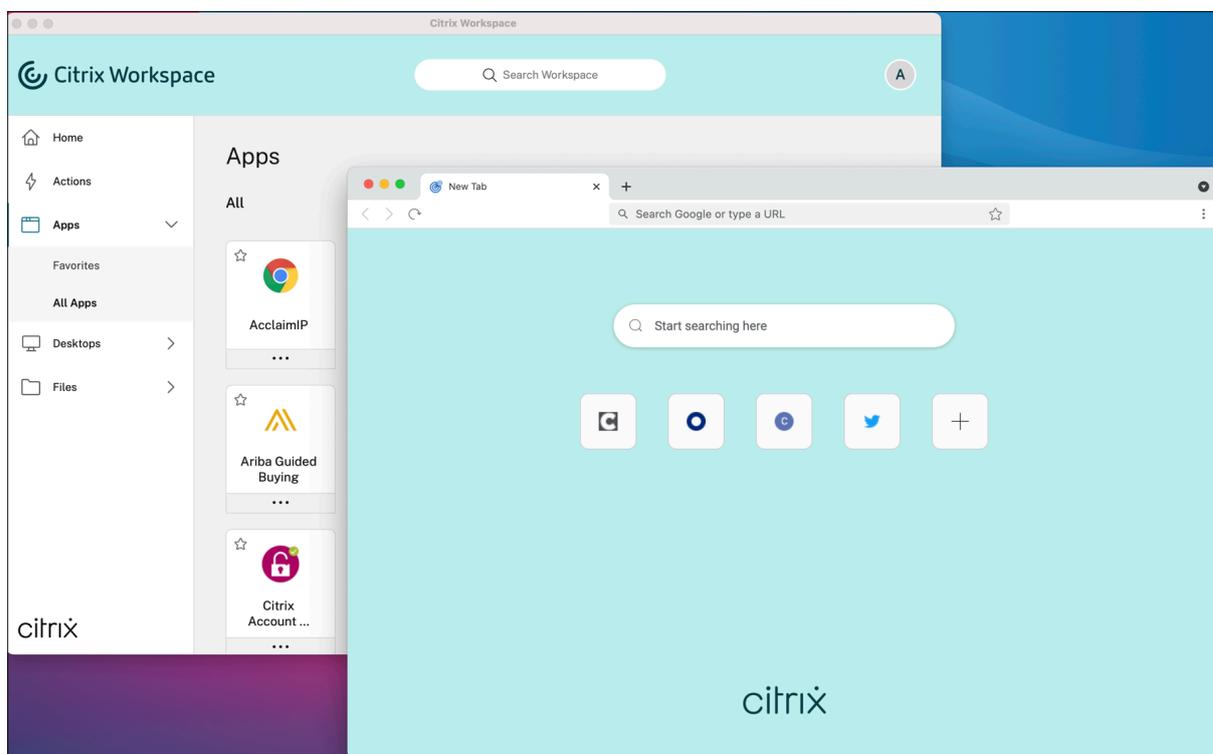
Automatische Storesuche per E-Mail-Adresse

Sie können jetzt Ihre E-Mail-Adresse in der Citrix Workspace-App für Mac eingeben, um automatisch den zugehörigen Store zu ermitteln. Wenn einer Domäne mehrere Stores zugeordnet sind, wird standardmäßig der erste vom Global App Configuration Service zurückgegebene Store als bevorzugter Store hinzugefügt. Benutzer können bei Bedarf stets zu einem anderen Store wechseln.

Citrix Workspace Browser

Citrix Workspace Browser ist ein systemeigener Browser, der auf dem Clientcomputer ausgeführt wird. Damit können Benutzer Web- oder SaaS-Apps in der Citrix Workspace-App sicher öffnen. Der Browser gewährleistet eine konsistente Benutzeroberfläche beim Zugriff auf verschiedene Web- oder

SaaS-Apps. Gleichzeitig verbessern Sie Ihre Produktivität und erzielen eine gute Leistung bei der Wiedergabe der Apps.



Der neue Workspace Browser ermöglicht eine verbesserte Benutzererfahrung im Stil eines systemeigenen Browsers und bietet folgende Features:

- Zugriff ohne VPN auf interne Webseiten
- Unterstützung für Mikrofon und Webcam
- Browsing mit Registerkarten
- Mehrfensteransichten
- Bearbeitbare Omnibox
- Lesezeichen
- Verknüpfungen auf der neuen Registerkarte
- Anpassbare Einstellungen
- Analytics

Administratoren können Secure Workspace Access- (SWA) oder App-Schutzrichtlinien wie Anti-Keylogging, Anti-Screenshot, Download, Drucken, Zwischenablagebeschränkungen und Wasserzeichen in unterschiedlichen Kombinationen pro URL aktivieren.

Weitere Informationen finden Sie in der Dokumentation zu [Citrix Workspace Browser](#).

Verbesserung der Endpunktanalyse (EPA)

Ab diesem Release unterstützt die Citrix Workspace-App für macOS End Point Analysis (EPA). Die Endpunktanalyse scannt das Gerät auf Endpunktsicherheitsanforderungen, die auf dem Citrix Gateway konfiguriert sind. Wenn der Scan erfolgreich abgeschlossen wurde, erhält ein Benutzer Zugriff.

Hinweis:

Dieses Feature funktioniert nur, wenn Sie die mehrstufige Authentifizierung (nFactor) in der Umgebung konfiguriert haben.

Weitere Informationen zum EPA-Scan finden Sie unter [Advanced Endpoint Analysis scans](#).

Adaptives Audio

Bei adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht konfigurieren. Damit optimiert adaptives Audio die Einstellungen für Ihre Umgebung und ersetzt veraltete Audiokomprimierungsformate für mehr Benutzerkomfort. Weitere Informationen finden Sie unter [Adaptives Audio](#).

Unterstützung für H.264 Advanced Video Coding (MPEG-4 AVC) mit Microsoft Teams

Dieses Release unterstützt die hardwarebeschleunigte H.264-Videocodierung/-decodierung. Dies verringert die CPU-Auslastung und verbessert die Qualität von Videokonferenzen. Die Multimediaengine von Citrix HDX-optimiertem Microsoft Teams (HdxRtcEngine.exe) verwendet jetzt Apples Video Toolbox Framework zur Codierung und Decodierung. Dieses Framework komprimiert und dekomprimiert Video schneller und in Echtzeit. Darüber hinaus wird das Auslagern von Codierung und Decodierung an die GPU optimiert. Die hardwarebeschleunigte Videodecodierung und -codierung ist standardmäßig aktiviert, wenn ein Gerät sie unterstützt. Durch diese Verbesserung wird die CPU-Auslastung bei Multimedianoutzung reduziert, wenn Microsoft Teams mit HDX optimiert ist.

Behobene Probleme

- Nach der Anmeldung bei der Workspace-App für Mac werden Sie nach einigen Stunden zur Authentifizierung aufgefordert. [RFMAC-10032]
- Wenn Sie einen Store in der Workspace-App hinzufügen, die Authentifizierungsdomäne in der Serverkonsole ändern, die App einige Minuten lang inaktiv lassen und dann eine beliebige App oder Desktopsitzung öffnen, stürzt die Workspace-App möglicherweise ab. [RFMAC-10133]
- Wenn bereits eine virtuelle App oder ein virtueller Desktop ausgeführt wird und Sie eine weitere virtuelle App oder einen virtuellen Desktop starten, wird Citrix Viewer angezeigt, aber die virtuelle App wird nicht geöffnet. Dieses Problem tritt auf Geräten mit macOS 11.6 auf. [RFMAC-10134]

2108.1

Neue Features

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

Behobene Probleme

Wenn bereits eine virtuelle App oder ein virtueller Desktop ausgeführt wird und Sie eine weitere virtuelle App oder einen virtuellen Desktop starten, wird Citrix Viewer angezeigt, aber die virtuelle App wird nicht geöffnet. Dieses Problem tritt auf Geräten mit macOS 11.6 auf. [RFMAC-10134]

2108

Neue Features

Die Citrix Workspace-App für Mac unterstützt nun MTU-Discovery (Maximum Transmission Unit = maximale Übertragungseinheit) für Enlightened Data Transport (EDT). Das Feature erhöht die Zuverlässigkeit und Kompatibilität des EDT-Protokolls und bietet eine verbesserte Benutzererfahrung.

Hinweis:

MTU-Discovery für EDT wird unter macOS Big Sur und höher unterstützt.

Behobene Probleme

- Es kommt zu einer Videoverzögerung bei Konferenzgesprächen in Microsoft Teams. [HDX-32603]
- Auf Mac-Clients, auf denen macOS Big Sur ausgeführt wird, kann ein interner HTTP 404- oder HTTP/1.1-Serverfehler auftreten. Das Problem tritt auf, wenn versucht wird, die Verbindung zu Sitzungen wiederherzustellen. [RFMAC-9448]

2107

Neue Features

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

Behobene Probleme

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

2106

Neue Features

Unterstützung für benutzerdefinierte URLs für 301-Weiterleitungen

Sie können URLs für HTTP 301-Weiterleitungen von StoreFront oder Citrix Gateway an Citrix Workspace hinzufügen.

Bei der Migration von StoreFront zu Citrix Workspace können Sie die StoreFront-URL per HTTP 301-Weiterleitung an eine Citrix Workspace-URL weiterleiten. Beim Hinzufügen einer alten StoreFront-URL erfolgt dann automatisch eine Weiterleitung an Citrix Workspace.

Beispiel einer Weiterleitung:

Die StoreFront-URL `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` kann an die Citrix Workspace-URL `https://<Citrix Workspace url>/Citrix/Roaming/Accounts` umgeleitet werden.

Hinweis:

- Die Citrix Workspace-App für Mac unterstützt nicht das Mehrfrequenzwahlverfahren (Dual Tone Multi Frequency, DTMF) für Microsoft Teams aufgrund ausstehender Änderungen von Microsoft.
- Ab dieser Version stimmen die Versionsnummer des Citrix Viewers und die Versionsnummer der Citrix Workspace-App möglicherweise nicht überein. Diese Änderung hat keinen Einfluss auf Ihre Benutzererfahrung.

Servicekontinuität

Das Servicekontinuität-Feature beseitigt oder minimiert die Abhängigkeit von bestimmten am Verbindungsprozess beteiligten Komponenten. Benutzer können so ihre virtuellen Apps und Desktops unabhängig vom Integritätsstatus der Cloud-Dienste starten.

Weitere Informationen finden Sie unter [Servicekontinuität](#) in der Dokumentation zu Citrix Workspace.

Behobene Probleme

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

2104

Neue Features

Die Citrix Workspace-App für Mac unterstützt die manuelle Anmeldung von Benutzern bei Netzwerkfreigaben, es sei denn, Ihre Organisation aktiviert Single Sign-On. Um auf freigegebene Netzwerkspeicherorte zuzugreifen, öffnen Sie die Citrix Workspace-App, navigieren Sie zu **Dateien > Netzwerkfreigaben** und geben Sie Ihre Anmeldeinformationen ein. Weitere Informationen zum Einrichten von Netzwerkfreigaben finden Sie unter [Create and manage storage zone connectors](#).

Behobene Probleme

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

2102

Neue Features

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

Behobene Probleme

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

2101

Neue Features

Unterstützung für Apple M1-Chip

Die Citrix Workspace-App für Mac unterstützt jetzt Apple M1-Chips mit Rosetta 2 unter macOS Big Sur (11.0 und höher). Daher müssen alle virtuellen Kanäle von Drittanbietern Rosetta 2 verwenden. Andernfalls funktionieren diese virtuellen Kanäle möglicherweise nicht in der Citrix Workspace-App für Mac unter macOS Big Sur (11.0 und höher). Weitere Informationen über Rosetta finden Sie in diesem [Apple-Supportartikel](#).

Unterstützung der Microsoft Teams-Optimierung für nahtlose App-Sitzungen

Die Citrix Workspace-App für Mac unterstützt jetzt die Microsoft Teams-Optimierung für nahtlose App-Sitzungen. Daher können Sie Microsoft Teams als Anwendung aus der Workspace-App starten. Weitere Informationen finden Sie in den folgenden Artikeln:

- [Optimierung für Microsoft Teams](#)
- [Microsoft Teams-Umleitung](#)

Unterstützung für Mehrfrequenzwahlverfahren (Dual Tone Multi Frequency, DTMF) mit Microsoft Teams

Die Citrix Workspace-App für Mac unterstützt das Mehrfrequenzwahlverfahren (DTMF) mit Telefonesystemen (z. B. PSTN) und Telefonkonferenzen in Microsoft Teams. Das Feature ist in der Standardeinstellung aktiviert.

Behobene Probleme

- Versuche, eine Microsoft Teams-Besprechung mit der OWA (Outlook Web-App) zu öffnen, schlagen möglicherweise fehl, wodurch alle zugehörigen Fenster unerwartet geschlossen werden. [CTXBR-1175]
- Wenn Sie einen Videoanruf starten, reagiert Microsoft Teams möglicherweise nicht mehr und zeigt den Fehler `Citrix HDX not connected` an. [RFMAC-6727]
- Unter macOS Big Sur (11.0.1) kann das Anschließen von USB-Geräten fehlschlagen, wodurch die Sitzung unerwartet beendet wird. [RFMAC-7079]
- Auf einem veröffentlichten Desktop wird für Dateien, die auf Ihrem lokalen Mac gespeichert sind, als Dateierstellungsdatum möglicherweise 30. November 1979 statt des aktuellen Datums angezeigt. [CVADHELP-16309]
- Manchmal wird der Anmeldebildschirm in veröffentlichten Apps möglicherweise nicht richtig angezeigt, was zu einer reduzierten Fenstergröße und einer roten Hintergrundfarbe führt. [CVADHELP-16027]
- Audioanrufe werden möglicherweise auf Ihrer Seite getrennt, wenn Sie Audiogeräte trennen und anschließen. [RFMAC-7371]
- Versuche, Text aus Office 365-Apps zu kopieren, sind u. U. auch dann erfolgreich, wenn die Richtlinie für die Einschränkung der Zwischenablage aktiviert ist. [CTXBR-1166]
- Versuche, Microsoft Teams zu starten, schlagen möglicherweise aufgrund von Problemen mit der HDX RealTime Connector Engine fehl und die folgende Fehlermeldung wird angezeigt.
`Sorry, we couldn't connect you`
[CVADHELP-16432]

2012

Neue Features

Apple M1-Chip - Preview

Die Citrix Workspace-App für Mac unterstützt jetzt Apple-Geräte mit M1-Chip auf Previewbasis.

Optimierung der Bildschirmfreigabe in Microsoft Teams

Die Citrix Workspace-App für Mac unterstützt jetzt die Optimierung der Bildschirmfreigabe in Microsoft Teams. Weitere Informationen:

- [Optimierung für Microsoft Teams](#)
- [Microsoft Teams-Umleitung](#)

Leistungsverbesserungen

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

Behobene Probleme

- Wenn Sie die Citrix Workspace-App für Mac 2008 oder höher verwenden, schlagen Versuche, mehrere Instanzen einer veröffentlichten Anwendung zu starten, möglicherweise fehl. [CVADHELP-16019]
- Versuche, die generische USB-Umleitung zu starten, schlagen möglicherweise fehl, wenn Sie eine USB-Dockingstation verwenden. [RFMAC-6687]
- Beim Öffnen eines Fensters mit STRG+O in veröffentlichten Desktops werden u. U. zwei Fenster geöffnet. [CVADHELP-15747]
- Wenn Sie die Citrix Workspace-App für Mac unter macOS Big Sur Beta verwenden, werden Audioanrufe möglicherweise getrennt. Das Problem tritt auf, wenn Sie Audiogeräte trennen und verschiedene Audiogeräte während eines Audioanrufs anschließen. [RFMAC-6112]
- Die HDX RealTime Connector-Engine wird möglicherweise unerwartet beendet, wenn Sie die Kamera in Microsoft Teams ein- und ausschalten. [RFMAC-6293]
- Das Starten von Citrix Files von der Workspace-App für Mac aus schlägt möglicherweise aufgrund von Problemen mit Single Sign-On fehl. [RFMAC-4477]

2010

Neue Features

Verbesserung der Authentifizierung

Um ein nahtloses Erlebnis zu ermöglichen, wird das Authentifizierungsdialogfeld jetzt in der Citrix Workspace-App angezeigt. Die Storedetails werden auf dem Anmeldebildschirm angezeigt. Authentifizierungstoken werden verschlüsselt und gespeichert, sodass Sie die Anmeldeinformationen bei einem Systemneustart oder Neustart der Sitzung nicht erneut eingeben müssen.

Hinweis:

Diese Verbesserung der Authentifizierung ist nur in Cloud-Bereitstellungen anwendbar.

Unterstützung für macOS Big Sur

Die Citrix Workspace-App für Mac wird unter macOS Big Sur (11.0.1) unterstützt.

Leistungsverbesserungen

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

Behobene Probleme

- Das Starten von veröffentlichten Desktops oder Anwendungen schlägt u. U. fehl und eine Fehlermeldung wird angezeigt. Das Problem tritt auf, wenn Ihr Computernamen Sonderzeichen enthält. [CVADHELP-15492]
- Anmeldeversuche bei veröffentlichten Anwendungen und Desktopsitzungen schlagen möglicherweise fehl. Das Problem tritt auf, wenn Sie mit der Maus auf **OK** klicken, um sich anzumelden. [CVADHELP-15300]

2009**Neue Features****Optimierung für Microsoft Teams (Vorschau)**

Citrix bietet eine Optimierung für die Verwendung der Desktopversion von Microsoft Teams in Citrix Virtual Apps and Desktops und der Citrix Workspace-App. Die Optimierung für Microsoft Teams ähnelt der Komponente HDX RealTime Optimization für Microsoft Skype for Business. Der Unterschied besteht darin, dass wir alle notwendigen Komponenten für die Optimierung von Microsoft Teams im VDA und in der Workspace-App für Mac bündeln. Mit der Optimierung für Microsoft Teams unterstützt die Citrix Workspace-App für Mac Audio und Video.

Weitere Informationen:

- [Optimierung für Microsoft Teams](#)
- [Microsoft Teams-Umleitung](#)

- Bekannte Probleme

Citrix Workspace-App für Mac unter macOS Big Sur Beta

Die Citrix Workspace-App 2009 für Mac wurde unter macOS Big Sur Beta 8 getestet. Bitte verwenden Sie dieses Setup in einer Testumgebung und geben Sie uns [Feedback](#). Im Abschnitt Bekannte Probleme finden Sie spezifische Probleme bei macOS Big Sur Beta.

Achtung:

Verwenden Sie die Citrix Workspace-App für Mac unter macOS Big Sur Beta-Versionen nicht in Produktionsumgebungen.

Kernelerweiterungen für USB-Umleitung

Die Citrix Workspace-App 2009 für Mac ist für die USB-Umleitung nicht mehr von Kernelerweiterungen (KEXT) abhängig.

Behobene Probleme

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

2008

Neue Features

Leistungsverbesserungen

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

Unterstützung für macOS-Versionen

Citrix Workspace-App 2008 für Mac ist das letzte Release, das die macOS-Versionen High Sierra (10.13) und Mojave (10.14) unterstützt.

Behobene Probleme

Wenn Sie die EULA auf VDAs hinzufügen, führt das Starten von veröffentlichten Desktops zu einem grauen oder schwarzen Bildschirm. [CVADHELP-14986]

2007

Neue Features

Leistungsverbesserungen

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

Behobene Probleme

- Wenn ein Benutzer Enlightened Data Transport (EDT) auf Citrix Gateway aktiviert, können Probleme in den Clientaudioeinstellungen dazu führen, dass die Citrix Workspace-App für Mac unerwartet beendet wird. [CVADHELP-14686]
- Wenn das Intel SDK auf VDAs verwendet wird, auf denen die Richtlinie **Videocodec zur Komprimierung verwenden** aktiviert ist, führt das Starten von veröffentlichten Desktops möglicherweise zu einem grünen Bildschirm. [CVADHELP-13647]
- Versuche, die WMI-Latenzdaten (Windows Management Instrumentation) abzurufen, schlagen möglicherweise in den Versionen 2002 und 2005 der Citrix Workspace-App für Mac fehl. [RFMAC-4325]

2006

Neue Features

Aktualisieren auf den Citrix Analytics-Dienst

Die Citrix Workspace-App überträgt Daten von ICA-Sitzungen, die Sie über einen Browser starten, sicher an den Citrix Analytics-Dienst. Weitere Informationen dazu, wie Citrix Analytics diese Informationen verwendet, finden Sie unter [Self-Service für Leistung](#) und [Self-Service-Suche für Virtual Apps and Desktops](#).

H.264-Unterstützung für die Webcamumleitung

Die Citrix Workspace-App für Mac unterstützt jetzt den Videokomprimierungsstandard H.264 (auch MPEG-4 AVC genannt). Infolgedessen können veröffentlichte 64-Bit-Apps nun die Webcamumleitung verwenden.

Stabilitätsverbesserungen

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

Behobene Probleme

- Anmeldeversuche bei der Citrix Workspace-App für Mac schlagen u. U. fehl und eine nicht verwandte Benutzeroberfläche wird angezeigt. Als Workaround klicken Sie im Menü auf **Apps aktualisieren**, um den Store zu laden. [RFMAC-4063]

Bekannte Probleme

Bekannte Probleme in Release 2112

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2111

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2109.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2109

- Wenn Sie die Workspace-App mit der Datei `.cr` konfigurieren und sich dann mit Ihren Anmeldeinformationen anmelden, wird die Homepage verzögert angezeigt. [RFMAC-9990]
- Wenn eine geschützte Progressive Web App (PWA) unter macOS geöffnet wird, werden die *App-Schutzrichtlinien* nicht erzwungen. [RFMAC-10128]
- Wenn Sie Stores in der Workspace-App hinzufügen, die Einstellung **Aktueller Zeitraum für die erneute Authentifizierung** in **Neuauthentifizierungszeitraum für die Workspace-App** ändern und nach einigen Minuten vom On-Premises-Store zum Cloudstore wechseln, werden Sie vom Cloud-Store abgemeldet und müssen sich erneut authentifizieren. Wenn Sie sich in der Workspace-App anmelden, wird das Wartezeichen dauerhaft angezeigt und Sie können sich nicht anmelden. [RFMAC-10140]

Bekannte Probleme in Release 2108.1

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2108

Wenn Sie eine abonnierte SaaS-App starten, nachdem die Authentifizierungsdomäne in der Serverkonsole geändert wurde, wird die Sitzung nicht gestartet und die folgende Fehlermeldung angezeigt:

“Die Authentifizierungsdomäne hat sich geändert. Warten Sie etwas und melden Sie sich dann erneut an.” [RFMAC-9616]

Bekannte Probleme in Release 2107

Wenn Sie die Authentifizierungsdomäne in der Serverkonsole ändern und sich mit Ihren Anmeldeinformationen anmelden, wird die folgende Fehlermeldung angezeigt:

“Verbindung mit dem Server ist nicht möglich.”

Sie können auf den Store zugreifen, sobald Sie auf **OK** geklickt haben. [RFMAC-9494]

Bekannte Probleme in Release 2106

Wenn Sie Ihren Bildschirm freigeben, wird ein schwarzes Fenster angezeigt. [HDX-30083]

Bekannte Probleme in Release 2104

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2102

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2101

- Versuche, von der Workspace-App für Mac aus auf Dateien in Netzwerkfreigaben zuzugreifen, schlagen möglicherweise fehl, auch wenn die Option aktiviert ist. [RFMAC-7272]
- Unter macOS Big Sur schlagen Versuche, die SAML Single Sign-On-App in der Citrix Workspace-App für Mac zu starten, möglicherweise fehl und die folgende Fehlermeldung wird angezeigt.

Page could not load. Please **try** again later or contact your administrator **for** assistance. Incident ID:-202

[RFMAC-7282]

Bekannte Probleme in Release 2012

- Wenn Sie einen Videoanruf starten, reagiert Microsoft Teams möglicherweise nicht mehr und zeigt den Fehler `Citrix HDX not connected` an. Starten Sie als Workaround Microsoft Teams oder den VDA neu. [RFMAC-6727]
- Videoanrufe über Microsoft Skype for Business werden unter macOS Big Sur (11.0.1) nicht unterstützt.
- Unter macOS Big Sur (11.0.1) kann das Anschließen von USB-Geräten fehlschlagen, wodurch die Sitzung unerwartet beendet wird. Schließen Sie als Workaround das USB-Gerät erneut an. [RFMAC-7079]

Bekannte Probleme in Release 2010

- In Skype for Business unter macOS Big Sur (11.0.1) ist eingehendes Video nicht sichtbar.
- Wenn Sie die Citrix Workspace-App für Mac 2008 oder höher verwenden, schlagen Versuche, mehrere Instanzen einer veröffentlichten Anwendung zu starten, möglicherweise fehl. [CVADHELP-16019]
- Versuche, die generische USB-Umleitung zu starten, schlagen möglicherweise fehl, wenn Sie eine USB-Dockingstation verwenden. [RFMAC-6687]
- Wenn Sie ein MacBook Pro 2018 und höher und FaceTime verwenden, sehen Benutzer möglicherweise einen grünen, schwarzen oder verzerrten Balken am unteren Rand der Videovorschau. [RFMAC-2829]

Bekannte Probleme in Release 2009

- Wenn Sie die Bildschirmfreigabe in Microsoft Teams in der Citrix Workspace-App für Mac verwenden, können nur Anwendungen von Drittanbietern freigegeben werden, z. B. Microsoft PowerPoint. Eingehende Bildschirmfreigabe wird jedoch vollständig unterstützt. [RFMAC-3403]
- Wenn Sie die Citrix Workspace-App für Mac unter macOS Big Sur Beta verwenden, werden Audioanrufe möglicherweise getrennt. Das Problem tritt auf, wenn Sie Audiogeräte trennen und verschiedene Audiogeräte während eines Audioanrufs anschließen. [RFMAC-6112]
- Die HDX RealTime Connector-Engine wird möglicherweise unerwartet beendet, wenn Sie Kameras bei einem optimierten Videoanruf in Microsoft Teams wechseln. [RFMAC-6157]
- Audio- und Videoanrufe werden möglicherweise getrennt, wenn Sie Netzwerke in Microsoft Teams wechseln. [RFMAC-6292]
- In einer Cloud-Bereitstellung werden veröffentlichte Desktops möglicherweise mit einer nicht übereinstimmenden Hintergrundfarbe gestartet. Das Problem tritt gelegentlich bei einigen macOS Big Sur Beta-Versionen auf. [RFMAC-6343]

- Das Installersymbol für die Citrix Workspace-App für Mac fehlt möglicherweise, wenn Sie die Datei **CitrixWorkspaceApp.dmg** öffnen. Das Problem tritt gelegentlich bei einigen macOS Big Sur Beta-Versionen auf. [RFMAC-6378]
- Die HDX RealTime Connector-Engine wird möglicherweise unerwartet beendet, wenn Sie die Kamera in Microsoft Teams ein- und ausschalten. [RFMAC-6293]

Bekannte Probleme in Release 2008

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2007

In diesem Release wurden keine neuen Probleme festgestellt.

Bekannte Probleme in Release 2006

In diesem Release wurden keine neuen Probleme festgestellt.

Hinweise zu Drittanbietern

Die Citrix Workspace-App enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

[Citrix Workspace-App für Mac – Hinweise zu Drittanbietern](#)

Systemanforderungen und Kompatibilität

February 18, 2022

Unterstützte Betriebssysteme

Die Citrix Workspace-App für Mac unterstützt folgende Betriebssysteme:

- macOS Monterey (12.0.1)
- macOS Big Sur 11 (einschließlich Nebenversionen und Patchversionen)
- macOS Catalina (10.15)

Kompatible Citrix Produkte

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

Kompatible Browser

Die Citrix Workspace-App 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

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

Softwareanforderungen

- Bereitstellen der Citrix Workspace-App für Mac:
 - Citrix Workspace für Web 2.1, 2.5 und 2.6
- StoreFront:
StoreFront 2.x oder höher für den Zugriff auf Apps nativ von der Citrix Workspace-App für Mac oder von einem Webbrowser aus.

Verbindungen, Zertifikate und Authentifizierung

Verbindungen

Die Citrix Workspace-App für Mac unterstützt folgende Verbindungen mit Citrix Virtual Apps and Desktops:

- HTTPS
- ICA-über-TLS

Die Citrix Workspace-App für Mac unterstützt folgende Konfigurationen:

Für LAN-Verbindungen	Für sichere Remote- oder lokale Verbindungen
StoreFront mit StoreFront Services oder Citrix Receiver für Web-Site	Citrix Gateway 10.5 - 12.0, einschließlich VPX; Enterprise Edition 9.x - 10.x, einschließlich VPX; VPX

Zertifikate

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, muss das Stammzertifikat für die Zertifizierungsstelle des Unternehmens auf dem Benutzergerät installiert sein. Anschließend können Sie mit der Citrix Workspace-App für Mac erfolgreich auf Citrix-Ressourcen zugreifen.

Hinweis:

Wenn das Zertifikat des Remote-Gateways beim Herstellen der Verbindung nicht verifiziert werden kann, wird eine Warnung über ein nicht vertrauenswürdige Zertifikat angezeigt, da das Stammzertifikat nicht im lokalen Schlüsselspeicher vorhanden ist. Wenn ein Benutzer trotz Warnung fortfährt, wird eine Liste der Anwendungen angezeigt. Die Anwendungen können jedoch nicht gestartet werden.

Importieren von Stammzertifikaten auf Geräten mit Citrix Workspace-App für Mac

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. Die Citrix Workspace-App für Mac unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate mit Citrix Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat zugeordnet werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu [Citrix Gateway](#). Weitere Informationen zum Installieren, Verknüpfen und Aktualisieren von Zertifikaten finden Sie unter [How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway](#).

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

Die Citrix Workspace-App für Mac hat eine strenge Validierungsrichtlinie für Serverzertifikate.

Wichtig

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

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

Beim Validieren eines Serverzertifikats verwendet die Citrix Workspace-App für Mac jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases der Citrix Workspace-App 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 mit der Citrix Workspace-App 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 die Citrix Workspace-App für Mac verwendet:

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

Die Citrix Workspace-App für Mac überprüft, ob alle Zertifikate gültig sind. Die Citrix Workspace-App für Mac überprüft ebenfalls, ob dem “Beispielstammzertifikat” bereits vertraut wird. Wenn die Citrix Workspace-App für Mac dem “Beispielstammzertifikat” nicht vertraut, schlägt die Verbindung fehl.

Wichtig

Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet. Beispielsweise gibt es derzeit zwei Zertifikate (“DigiCert”/“GTE CyberTrust Global Root” und “DigiCert Baltimore Root”/“Baltimore CyberTrust Root”), mit

denen die gleichen Serverzertifikate validiert werden können. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar (“DigiCert Baltimore Root”/”Baltimore CyberTrust Root”). Wenn Sie “GTE CyberTrust Global Root” auf dem Gateway konfigurieren, schlagen die Citrix Workspace-App für Mac-Verbindungen auf diesen Benutzergeräten fehl. Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist. Stammzertifikate laufen wie alle Zertifikate irgendwann ab.

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”

Die Citrix Workspace-App für Mac verwendet dann die beiden Zertifikate. Dann sucht die App nach einem Stammzertifikat auf dem Benutzergerät. Wird ein vertrauenswürdigen Zertifikat gefunden, das korrekt validiert wird, z. B. “Beispielstammzertifikat”, ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl. Diese Konfiguration stellt das von der Citrix Workspace-App für Mac benötigte Zwischenzertifikat zur Verfügung, ermöglicht der Citrix Workspace-App für Mac aber auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

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

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat”
- “Falsches Stammzertifikat”

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Die Citrix Workspace-App 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:

- “Beispielserverzertifikat”
- “Beispielzwischenzertifikat 1”
- “Beispielzwischenzertifikat 2”

Wichtig

Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat, das für Situationen gedacht ist, in denen es mehr als ein Stammzertifikat gibt. Ein früher ausgestelltes Stammzertifikat wird gleichzeitig mit einem später ausgestellten Stammzertifikat verwendet. In

diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden. Beispielsweise hat das früher ausgestellte Stammzertifikat "Class 3 Public Primary Certification Authority" das entsprechende übergreifende Zwischenzertifikat "Verisign Class 3 Public Primary Certification Authority - G5". Ein entsprechendes später ausgestelltes Stammzertifikat "Verisign Class 3 Public Primary Certification Authority - G5" ist ebenfalls verfügbar und es ersetzt "Class 3 Public Primary Certification Authority". Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.

Hinweis

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

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

- "Beispielserverzertifikat"
- "Beispielzwischenzertifikat"

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

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

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

- "Beispielserverzertifikat"

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

Authentifizierung

Für Verbindungen mit StoreFront unterstützt die Citrix Workspace-App für Mac die folgenden Authentifizierungsmethoden:

	Workspace für Web mit Browsern	StoreFront Services-Site (nativ)	StoreFront XenApp Services-Site (nativ)	Citrix Gateway bei Workspace für Web (Browser)	Citrix Gateway bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja		Ja*	Ja*
Domänen-Passthrough					
Sicherheitstoken				Ja*	Ja*
Zweistufige Authentifizierung (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Ja*
Smartcard	Ja	Ja		Ja*	Ja
Benutzerzertifikat				Ja	Ja (Citrix Gateway Plug-In)

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

Installieren, Deinstallieren und Aktualisieren

February 18, 2022

Citrix Workspace-App für Mac enthält ein Installationspaket und unterstützt Remotezugriff über Citrix Gateway und Secure Web Gateway.

Sie können die Citrix Workspace-App für Mac auf folgende Weise installieren:

- Über die Citrix Website
- Automatisch aus Workspace für Web

- Mit einem ESD-Tool (Electronic Software Distribution)

Manuelle Installation

Von einem Benutzer von Citrix.com

Erstbenutzer können die Citrix Workspace-App für Mac von Citrix.com oder der eigenen Downloadsite herunterladen. Sie können dann ein Konto durch Eingabe einer E-Mail-Adresse anstelle einer Server-URL einrichten. Die Citrix Workspace-App für Mac ermittelt das Citrix Gateway oder den StoreFront-Server, der der E-Mail-Adresse zugeordnet ist. Anschließend wird der Benutzer aufgefordert, sich anzumelden und die Installation fortzusetzen. Dieses Feature wird als e-mail-basierte Kontenermittlung bezeichnet.

Hinweis:

Ein Erstbenutzer ist ein Benutzer, auf dessen Gerät die Citrix Workspace-App für Mac nicht installiert ist.

Die e-mail-basierte Kontenermittlung wird für einen Erstbenutzer nicht angewendet, wenn Sie die Citrix Workspace-App für Mac von einem anderen Speicherort (d. h. nicht Citrix.com) heruntergeladen haben (z. B. von einer Citrix Receiver für Web-Site).

Wenn die Citrix Workspace-App für Mac für Ihre Site konfiguriert werden muss, verwenden Sie eine andere Bereitstellungsmethode.

Mit einem ESD-Tool (Electronic Software Distribution)

Ein Erstbenutzer der Citrix Workspace-App für Mac muss eine Server-URL für das Einrichten des Kontos eingeben.

Von der Citrix-Downloadseite

Sie können die Citrix Workspace-App für Mac von einer Netzwerkfreigabe oder direkt auf dem Benutzergerät installieren. Sie können die App installieren, wenn Sie die Datei von der Citrix-Website unter [Downloads](#) herunterladen.

Installieren der Citrix Workspace-App für Mac:

1. Laden Sie die DMG-Datei für die gewünschte Version der Citrix Workspace-App für Mac von der Citrix-Website herunter.
2. Öffnen Sie die heruntergeladene Datei.
3. Klicken Sie auf der Eröffnungsseite auf **Weiter**.
4. Klicken Sie auf der Seite **Lizenzierung** auf **Weiter**.
5. Klicken Sie auf **Akzeptieren**, um die Bedingungen der Lizenzvereinbarung zu akzeptieren.

6. Klicken Sie auf der Seite **Installationstyp** auf **Installieren**.
7. Wählen Sie auf der Seite **Konto hinzufügen** die Option **Konto hinzufügen** aus und klicken Sie dann auf **Weiter**.
8. Geben Sie den Benutzernamen und das Kennwort eines Administrators für das lokale Gerät ein.

Deinstallieren

Sie können die Citrix Workspace-App für Mac manuell deinstallieren, indem Sie die DMG-Datei öffnen. Wählen Sie **Citrix Workspace-App deinstallieren** und folgen Sie den Anweisungen auf dem Bildschirm. Die DMG-Datei ist die Datei, die bei der erstmaligen Installation der Citrix Workspace-App für Mac von Citrix heruntergeladen wird. Wenn sich die Datei nicht mehr auf Ihrem Computer befindet, laden Sie die Datei erneut von [Citrix Downloads](#) herunter, um die Anwendung zu deinstallieren.

Upgrade

Die Citrix Workspace-App für Mac sendet Ihnen Benachrichtigungen, wenn ein Update für eine vorhandene Version oder ein Upgrade auf eine neuere Version verfügbar ist.

Sie können die Citrix Workspace-App für Mac von allen Citrix Workspace-App für Mac-Vorversionen aus aktualisieren.

Wenn Sie ein Upgrade auf eine neuere Version der Citrix Workspace-App für Mac durchführen, wird die vorherige Version automatisch deinstalliert. Sie müssen Ihre Maschine nicht neu starten.

Aktualisieren

February 21, 2022

Manuelle Aktualisierung

Um die Citrix Workspace-App für Mac manuell zu aktualisieren, laden Sie die neueste Version der App von der [Citrix Downloadseite](#) herunter und installieren Sie sie.

Automatische Aktualisierung

Wenn eine neue Version der Citrix Workspace-App veröffentlicht wird, sendet Citrix das Update an das System, auf dem die Citrix Workspace-App installiert ist. Sie werden über das verfügbare Update informiert.

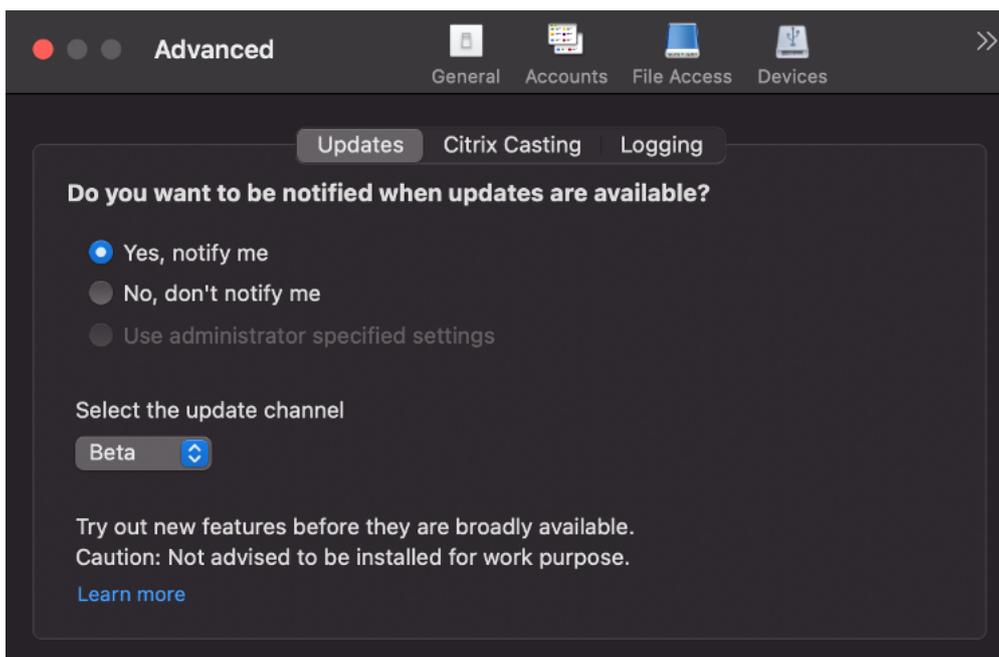
Hinweis:

- Wenn Sie einen ausgehenden Proxy mit SSL-Interception konfiguriert haben, fügen Sie eine Ausnahme zum Workspace-Signaturdienst für automatische Updates <https://citrixupdates.cloud.com/> und zum Downloadspeicherort <https://downloadplugins.citrix.com/> hinzu, damit Sie Updates von Citrix erhalten.
- Ihr System muss über eine Internetverbindung verfügen, um Updates zu erhalten.
- Workspace für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
- Citrix HDX RTME für macOS ist in Citrix Workspace-Updates enthalten. Sie werden über das verfügbare HDX RTME-Update in der Citrix Workspace-App informiert.
- Ab Version 2111 haben die Updateprotokolle für Citrix Workspace neue Pfade. Die Workspace-Updateprotokolle sind unter `/Library/Logs/Citrix Workspace Updater`. Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Installieren des Beta-Programms für die Citrix Workspace-App

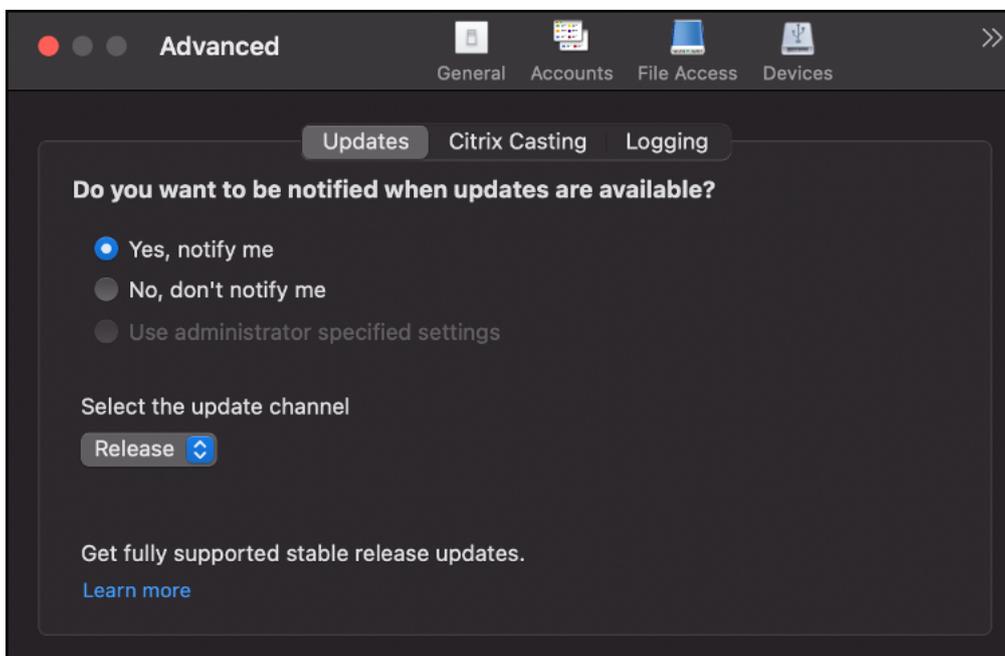
Sie erhalten eine Updatebenachrichtigung, wenn die Citrix Workspace-App für automatische Updates konfiguriert ist. Führen Sie die folgenden Schritte aus, um den Beta Build auf Ihrem System zu installieren:

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie in der Dropdownliste **Beta** aus, wenn der Beta Build verfügbar ist.



Um von einem Beta Build zu einem Releasebuild zu wechseln, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf "Citrix Workspace" und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie in der Dropdownliste **Updatekanal auswählen** die Option **Release** aus.



Hinweis:

Kunden können Beta Builds in ihren Umgebungen zu testen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, und Feedback hierzu geben. Citrix akzeptiert keine Supportanfragen für Beta Builds, begrüßt jedoch [Feedback](#) zur Verbesserung der Builds. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

Erweiterte Konfiguration für automatische Updates (Citrix Workspace-Updates)

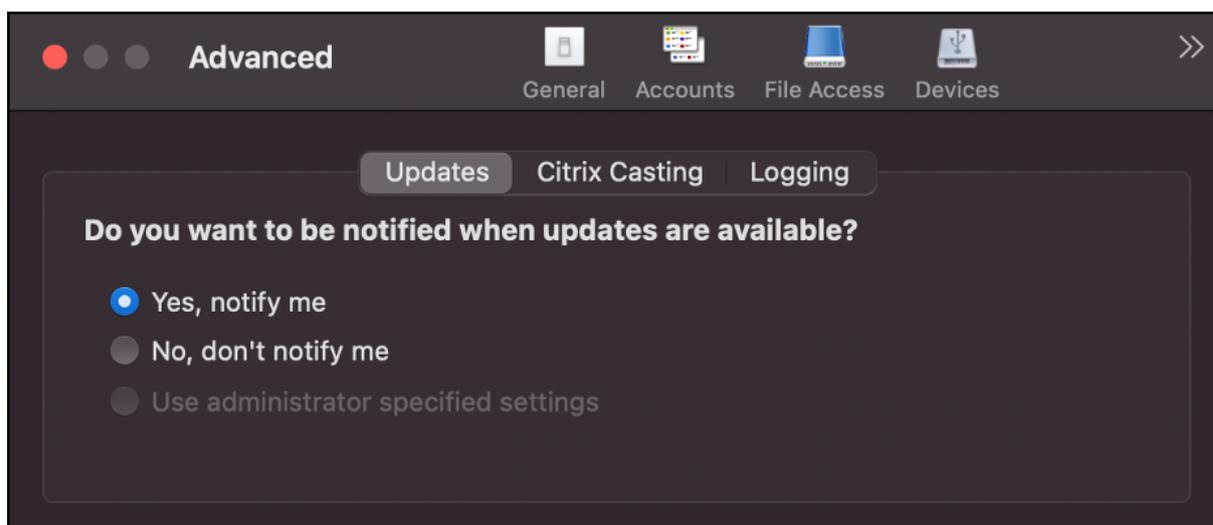
Sie können Citrix Workspace-Updates mit den folgenden Methoden konfigurieren:

1. Grafische Benutzeroberfläche (GUI)
2. StoreFront

Konfigurieren von Citrix Workspace-Updates mit der GUI

Benutzer können die Einstellung für Citrix Workspace-Updates im Dialogfeld **Erweiterte Einstellungen** außer Kraft setzen. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet. Um das Update über die GUI zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie das Hilfssymbol der Citrix Workspace-App auf Ihrem Mac aus.
2. Wählen Sie in der Dropdownliste **Einstellungen > Erweitert** aus.
3. Wählen Sie die Einstellungen für die Updatebenachrichtigungen und schließen Sie das Fenster.



Konfigurieren von Citrix Workspace-Updates mit StoreFront

1. Öffnen Sie die Datei `web.config` mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkonto-Element in der Datei (Store ist der Kontoname Ihrer Bereitstellung).

Beispiel: `<account id=... name="Store">`

Vor dem Tag `</account>` navigieren Sie zu den Eigenschaften des Benutzerkontos:

```
1 <properties>
2     <clear />
3 </properties>
4 <!--NeedCopy-->
```

3. Fügen Sie das Tag für automatische Updates nach dem Tag `<clear />` ein.

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
7         description="" published="true" updaterType="Citrix"
8         remoteAccessType="None">
9
10    <annotatedServices>
11
12        <clear />
13
14        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
15
16            <metadata>
17
18                <plugins>
19
20                    <clear />
21
22                </plugins>
23
24            <trustSettings>
```

```
24
25     <clear />
26
27 </trustSettings>
28
29 <properties>
30
31     <property name="Auto-Update-Check" value="auto" />
32
33     <property name="Auto-Update-DeferUpdate-Count" value
34         ="1" />
35
36     <property name="Auto-Update-Rollout-Priority" value=
37         "fast" />
38
39 </properties>
40
41 </metadata>
42
43 </annotatedServiceRecord>
44
45 </annotatedServices>
46
47 <metadata>
48
49     <plugins>
50
51         <clear />
52
53     </plugins>
54
55     <trustSettings>
56
57         <clear />
58
59     </trustSettings>
60
61     <properties>
62
63         <clear />
64
65     </properties>
66
67 </metadata>
```

```
67     </account>
68
69 <!--NeedCopy-->
```

Nachfolgend sind die Bedeutungen der Eigenschaften und ihre möglichen Werte aufgeführt:

- **Auto-update-Check:** Gibt an, dass die Citrix Workspace-App ein Update automatisch erkennt, wenn es verfügbar ist.
- **Auto-update-Rollout-Priority:** Gibt den Bereitstellungszeitraum an, in dem Sie das Update erhalten können.
- **Auto-update-DeferUpdate-Count:** Gibt an, wie oft Sie die Benachrichtigungen für die Release-Updates ignorieren können.

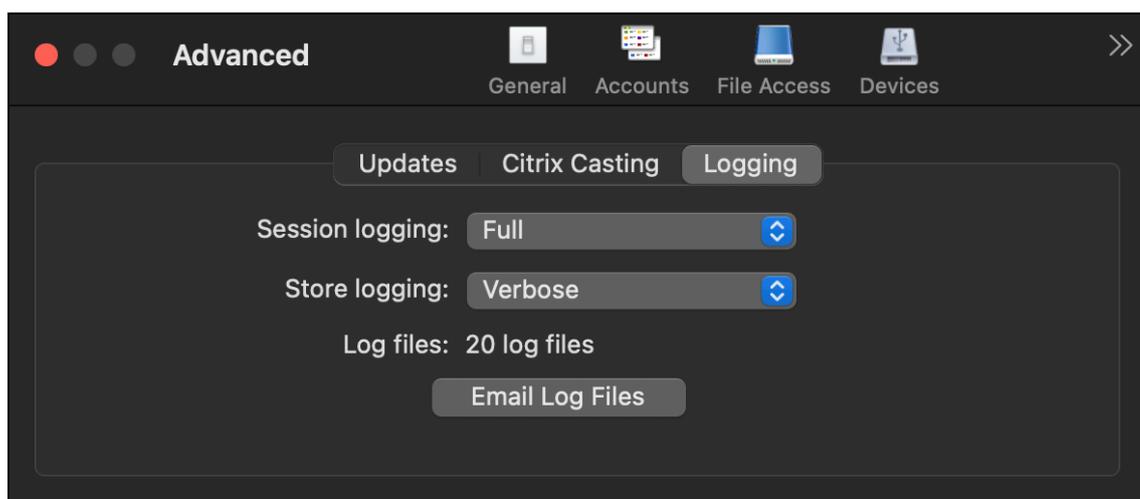
Protokollsammlung

Protokollsammlung vereinfacht das Sammeln von Protokollen für die Citrix Workspace-App. Die Protokolle helfen Citrix bei der Problembehandlung und erleichtern bei komplizierten Problemen den Support.

Sie können Protokolle über die GUI sammeln.

Sammeln von Protokollen:

1. Öffnen Sie die Citrix Workspace-App.
2. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf “Citrix Workspace” und wählen Sie **Einstellungen > Erweitert**.
3. Wählen Sie **Protokollierung**.



4. Wählen Sie eine der folgenden Sitzungsprotokollebenen aus:
 - **Deaktiviert (Standard):** Für die einfache Problembehandlung wird ein Minimum an Protokollen gesammelt.

- **Verbindungsdiagnose:** Identifiziert Fehler beim Verbinden. Die gesamte Protokollierung ist bis zu dem Zeitpunkt aktiviert, an dem die Sitzung als erfolgreich erkannt wird.
- **Vollständig:** Erfasst alles, einschließlich der Verbindungsdiagnose. Nach der Aktivierung speichert die Citrix Workspace-App bis zu 10 Sitzungsprotokolle. Danach werden sie gelöscht, beginnend mit den ältesten, um bei 10 Protokollen zu bleiben.

Hinweis:

Die Protokollierungsoption **Vollständig** kann sich auf die Leistung auswirken und sollte aufgrund der Datenmenge nur zur Problembehandlung verwendet werden. Aktivieren Sie die vollständige Protokollierung nicht für den Normalbetrieb. Wenn Sie diese Protokollierungsstufe aktivieren, wird eine Warnung angezeigt, die Sie bestätigen müssen, damit Sie fortfahren können.

5. Wählen Sie eine der folgenden Storeprotokollebenen aus:
 - **Deaktiviert (Standard):** Für die einfache Problembehandlung wird ein Minimum an Protokollen gesammelt.
 - **Normal:** Es werden nur Storekommunikationsprotokolle gesammelt
 - **Ausführlich:** Detaillierte Authentifizierungs- und Storekommunikationsprotokolle werden gesammelt.
6. Klicken Sie auf **Protokolldateien per E-Mail senden**, um Protokolle als ZIP-Datei zu sammeln und freizugeben.

Konfigurieren

February 18, 2022

Nach der Installation der Citrix Workspace-App für Mac-Software sind die folgenden Konfigurationsschritte erforderlich, damit Benutzer auf ihre gehosteten Anwendungen und Desktops zugreifen können.

Benutzer stellen Verbindungen u. a. über das Internet oder von einem Remotestandort her. Konfigurieren Sie für solche Benutzer die Authentifizierung über Citrix Gateway.

Administratortaufgaben und -überlegungen

In diesem Artikel werden Aufgaben und Überlegungen beschrieben, die für Administratoren der Citrix Workspace-App für Mac relevant sind.

Wichtig:

Wenn Sie macOS 10.15 ausführen, stellen Sie sicher, dass Ihr System mit den [Anforderungen für vertrauenswürdige Zertifikate von Apple in macOS 10.15](#) kompatibel ist. Überprüfen Sie dies, bevor Sie das Upgrade auf die Citrix Workspace-App für Mac Version 2106 durchführen.

Verwalten von Featureflags

Wenn ein Problem mit der Citrix Workspace-App in der Produktion auftritt, können wir ein betroffenes Feature dynamisch in der Citrix Workspace-App deaktivieren, auch nachdem das Feature bereitgestellt wurde. Hierfür verwenden wir Featureflags und den Drittanbieterdienst "LaunchDarkly".

Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen.

Sie können den Datenaustausch und die Kommunikation mit LaunchDarkly wie folgt ermöglichen:

Datenverkehr für folgende URLs zulassen

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- mobile.launchdarkly.com

IP-Adressen in einer Positivliste auflisten

Wenn Sie IP-Adressen in einer Positivliste auflisten müssen, konsultieren Sie die Liste der aktuellen IP-Adressbereiche unter [Liste öffentlicher IP-Adressen von LaunchDarkly](#). Mithilfe dieser Liste können Sie sicherstellen, dass Ihre Firewallkonfigurationen automatisch anhand der Infrastrukturupdates aktualisiert werden. Einzelheiten zum Status der Änderungen der Infrastruktur finden Sie auf der [Statusseite von LaunchDarkly](#).

LaunchDarkly-Systemanforderungen

Stellen Sie sicher, dass die Apps mit den folgenden Diensten kommunizieren können, wenn Sie Split-Tunneling in Citrix ADC für die folgenden Dienste auf **OFF** festgelegt haben:

- LaunchDarkly-Dienst.
- APNs-Listenerdienst

Integration des Content Collaboration-Diensts

Citrix Content Collaboration ermöglicht Ihnen den einfachen und sicheren Austausch von Dokumenten, das Senden umfangreicher Dokumente per E-Mail, die sichere Übertragung von Dokumenten an Dritte und den Zugriff auf einen Bereich für die Zusammenarbeit.

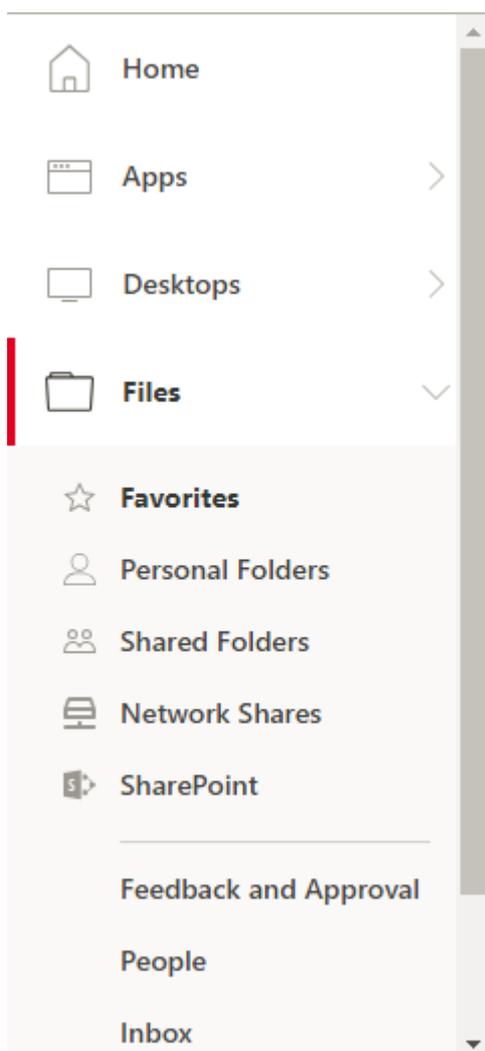
Citrix Content Collaboration bietet viele Möglichkeiten zum Arbeiten, darunter eine webbasierte Benutzeroberfläche, mobile Clients, Desktop-Apps und die Integration in Microsoft Outlook und Gmail.

Sie können Citrix Content Collaboration-Funktionen über die Registerkarte **Dateien** der Citrix Workspace-App aufrufen. Die Registerkarte **Dateien** wird nur angezeigt, wenn der Content Collaboration Service in der Workspacekonfiguration der Citrix Cloud-Konsole aktiviert ist.

Hinweis:

Windows Server 2012 und Windows Server 2016 bieten keine Unterstützung für die Citrix Content Collaboration-Integration. Grund ist eine im Betriebssystem festgelegte Sicherheitsoption.

In der folgenden Abbildung sehen Sie ein Beispiel für den Inhalt der Registerkarte **Dateien** der neuen Citrix Workspace-App:



Einschränkungen

- Beim Zurücksetzen der Citrix Workspace-App wird Citrix Content Collaboration nicht abgemeldet.
- Durch das Wechseln von Stores in der Citrix Workspace-App wird Citrix Content Collaboration nicht abgemeldet.

USB-Umleitung

Mit HDX USB-Geräteumleitung können USB-Geräte zum und vom Benutzergerät umgeleitet werden. Benutzer können eine Verbindung zum USB-Speicherstick auf einem lokalen Computer herstellen und dann remote von einem virtuellen Desktop oder einer desktopgehosteten Anwendung darauf zugreifen.

In einer Sitzung können Benutzer Plug-and-Play-Geräte, einschließlich PTP-Geräte (Picture Transfer

Protocol), verwenden. Beispiel:

- Digitalkameras, MTP-Geräte (Media Transfer Protocol) wie digitale Audio-Player und tragbare Medienplayer
- POS-Geräte und andere Geräte wie 3D SpaceMouse, Scanner, Unterschriftenfelder und so weiter.

Hinweis:

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

USB-Umleitung ist auf folgenden Clients verfügbar:

- Windows
- Linux
- Mac

Standardmäßig ist die USB-Umleitung für bestimmte Klassen von USB-Geräten zulässig bzw. nicht zulässig. Um festzulegen, welche USB-Geräte einem virtuellen Desktop verfügbar gemacht werden, aktualisieren Sie die Liste der für die Umleitung unterstützten USB-Geräte. Weitere Informationen finden Sie weiter unten.

Tipp

Wenn aus Sicherheitsgründen eine Trennung zwischen Benutzergerät und Server erforderlich ist, informieren Sie die Benutzer darüber, 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: die Citrix Workspace-App für Mac behandelt ein SMART-Board ebenso wie eine Maus.

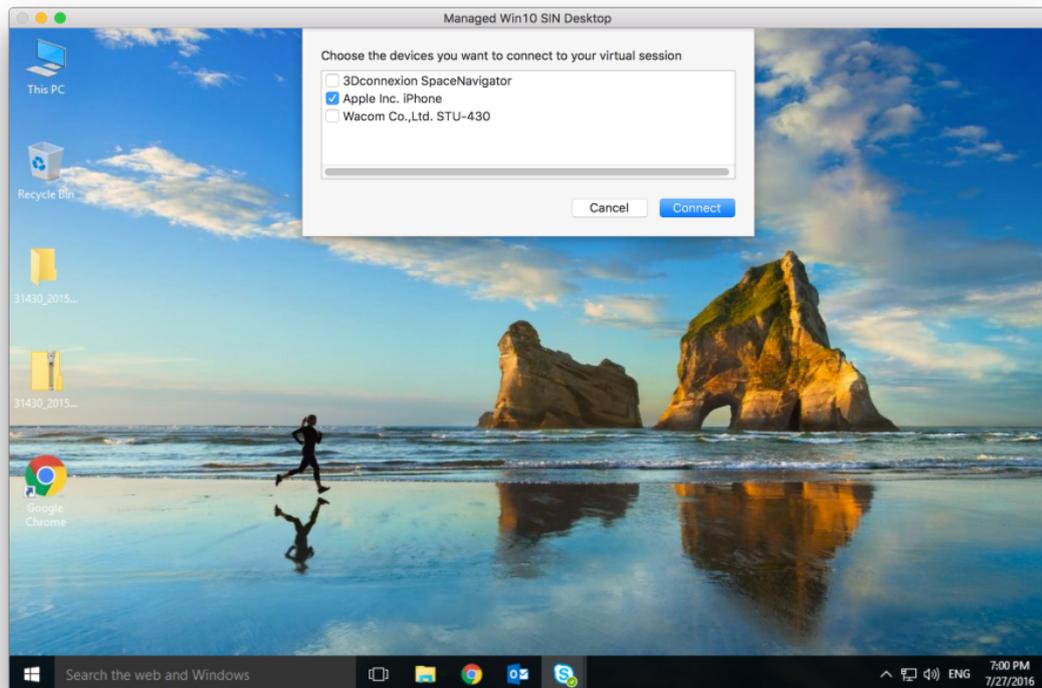
Das Produkt unterstützt optimierte virtuelle Kanäle mit USB 3.0-Geräten und USB 3.0-Anschlüssen. Beispielsweise wird ein virtueller CDM-Kanal zur Anzeige von Dateien in einer Kamera und zur Bereitstellung von Audio für ein Headset verwendet. Das Produkt unterstützt zudem die generische USB-Umleitung 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. Verwenden Sie den virtuellen Kanal für generisches USB als Alternative.

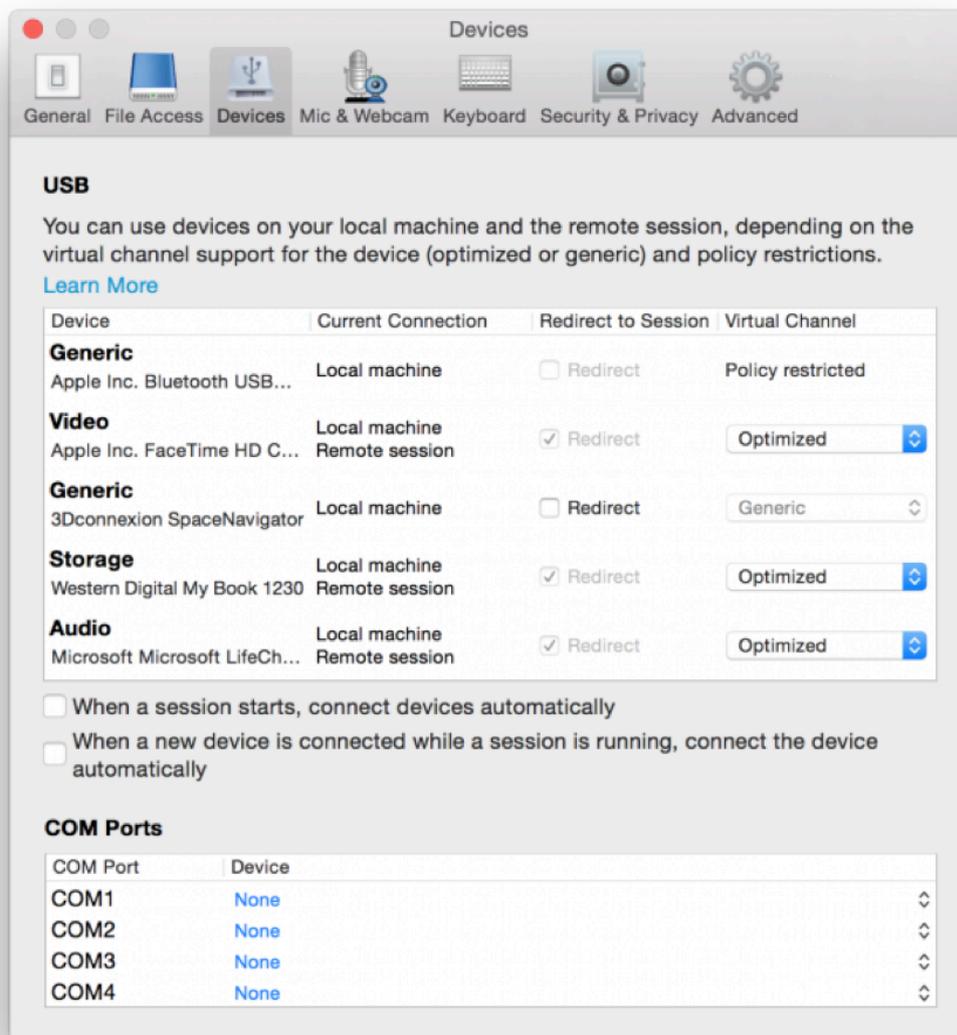
Einige Geräte werden standardmäßig nicht umgeleitet und sind nur in der lokalen Sitzung verfügbar. Es wäre beispielsweise nicht angemessen, eine über internes USB direkt angeschlossene Netzwerkkarte umzuleiten.

Verwenden von USB-Umleitung

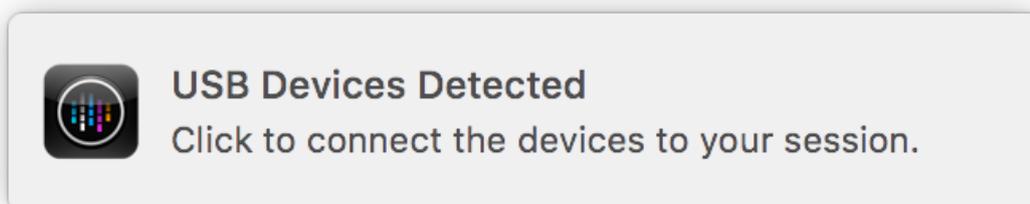
1. Verbinden Sie das USB-Gerät mit dem Gerät, auf dem die Citrix Workspace-App für Mac installiert ist.
2. Sie werden aufgefordert, die auf dem lokalen System verfügbaren USB-Geräte auszuwählen.



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 (Generisch oder Optimiert) aus.
6. Eine Meldung wird angezeigt. Klicken Sie, um das USB-Gerät mit Ihrer Sitzung zu verbinden:



Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen. Wenn Sie mit der Citrix Workspace-App 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.

Unterstützte USB-Geräte

Da Apple die Einstellung von Kernel Extensions (KEXT) angekündigt hat, wurde die Citrix Workspace-App für Mac auf das neue von Apple bereitgestellte USB-Framework für den Benutzermodus `IOUSBHost` migriert. In diesem Artikel werden die unterstützten USB-Geräte aufgeführt.

USB-Geräte, die mit der USB-Umleitung kompatibel sind

Die folgenden USB-Geräte funktionieren nahtlos mit der USB-Umleitung:

- 3DConnexion SpaceMouse
- Massenspeichergeräte
- Kingson DataTraveler USB-Speicherstick
- Externe HDD von Seagate
- Speicherstick von Kingston/Transcend, 32 GB/64 GB
- NIST PIV-Smartcard/-Lesegerät
- YubiKey

USB-Geräte, bei denen die USB-Umleitung fehlschlägt

Das folgende Gerät ist nicht mit der USB-Umleitung kompatibel:

- Externe SSD von Transcend

Nicht verifizierte USB-Geräte

Es gibt viele Geräte, von Citrix nicht verifiziert, für eine erfolgreiche USB-Umleitung mit der Citrix Workspace-App für Mac. Hier sind einige dieser Geräte:

- Andere Festplatten
- Spezielle Tasten auf der Tastatur und an Headsets, die ein benutzerdefiniertes HID-Protokoll verwenden

Unterstützung für Massenspeichergeräte

Wir haben festgestellt, dass nicht alle Arten von Massenspeichergeräten erfolgreich umgeleitet werden können. Für Geräte, die nicht umgeleitet werden können, gibt es einen optimierten virtuellen Kanal namens Clientlaufwerkzuordnung. Mit der Clientlaufwerkzuordnung kann der Zugriff auf die Massenspeichergeräte durch die Richtlinien auf dem Delivery Controller gesteuert werden.

Unterstützung für isochrone Geräte

Die generische USB-Umleitung bietet keine Unterstützung für die isochrone Klasse von USB-Geräten in der Citrix Workspace-App für Mac. Der isochrone Modus der Datenübertragung in einer USB-Spezifikation zeigt Geräte an, die die Zeitstempeldaten mit konstanter Geschwindigkeit streamen. Zum Beispiel: WebCams, USB-Kopfhörer und so weiter

Unterstützung für Verbundgeräte

Ein USB-Verbundgerät ist ein einzelnes Gadget, das mehr als eine Funktion ausführen kann. Zum Beispiel: Multifunktionsdrucker, iPhone usw. Derzeit unterstützt die Citrix Workspace-App für Mac keine Umleitung von Verbundgeräten in die Citrix Virtual Apps and Desktops-Sitzung.

Alternativen für nicht unterstützte USB-Geräte

Es gibt optimierte virtuelle Kanäle für Geräte, die nicht durch die generische USB-Umleitung unterstützt werden. Diese virtuellen Kanäle sind im Vergleich zur generischen USB-Umleitung auf Geschwindigkeit optimiert. Hier sind einige Beispiele:

- **Webcamumleitung:** Optimiert für rohen Webcamdatenverkehr. Das Microsoft Teams Optimization Pack hat eine eigene Methode zur Webcamumleitung. Daher fällt es nicht unter den virtuellen Kanal der Webcamumleitung.
- **Audioumleitung:** Optimiert für die Übertragung von Audiostreams.
- **Clientlaufwerkzuordnung:** Optimiert für die Umleitung von Massenspeichergeräten in die Citrix Virtual Apps and Desktops-Sitzung. Zum Beispiel: Speichersticks, Festplatten, DVD ROM/RW und so weiter.

Enlightened Data Transport (EDT)

Standardmäßig ist das EDT-Protokoll in der Citrix Workspace-App für Mac aktiviert.

Die Citrix Workspace-App 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
```

Sitzungszuverlässigkeit und automatische Wiederverbindung von Clients

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. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Wichtig

- Benutzer der Citrix Workspace-App für Mac können die Servereinstellung nicht außer Kraft setzen.
- Wenn die Sitzungszuverlässigkeit aktiviert ist, ändert sich der Standardport für die Sitzungskommunikation von 1494 zu 2598.

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

Hinweis

Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und Citrix 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 (drei Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Bedienkomfort erhöhen soll. Daher wird der Benutzer nicht zur erneuten Authentifizierung aufgefordert.

Tipp

Eine Verlängerung des Timeouts für die Sitzungszuverlässigkeit kann dazu führen, dass ein Benutzer abgelenkt wird und sich vom Gerät entfernt. Dann besteht das Risiko, dass unbefugte Benutzer Zugang zu der Sitzung erhalten.

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

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 wieder verbinden.

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

Hinweis

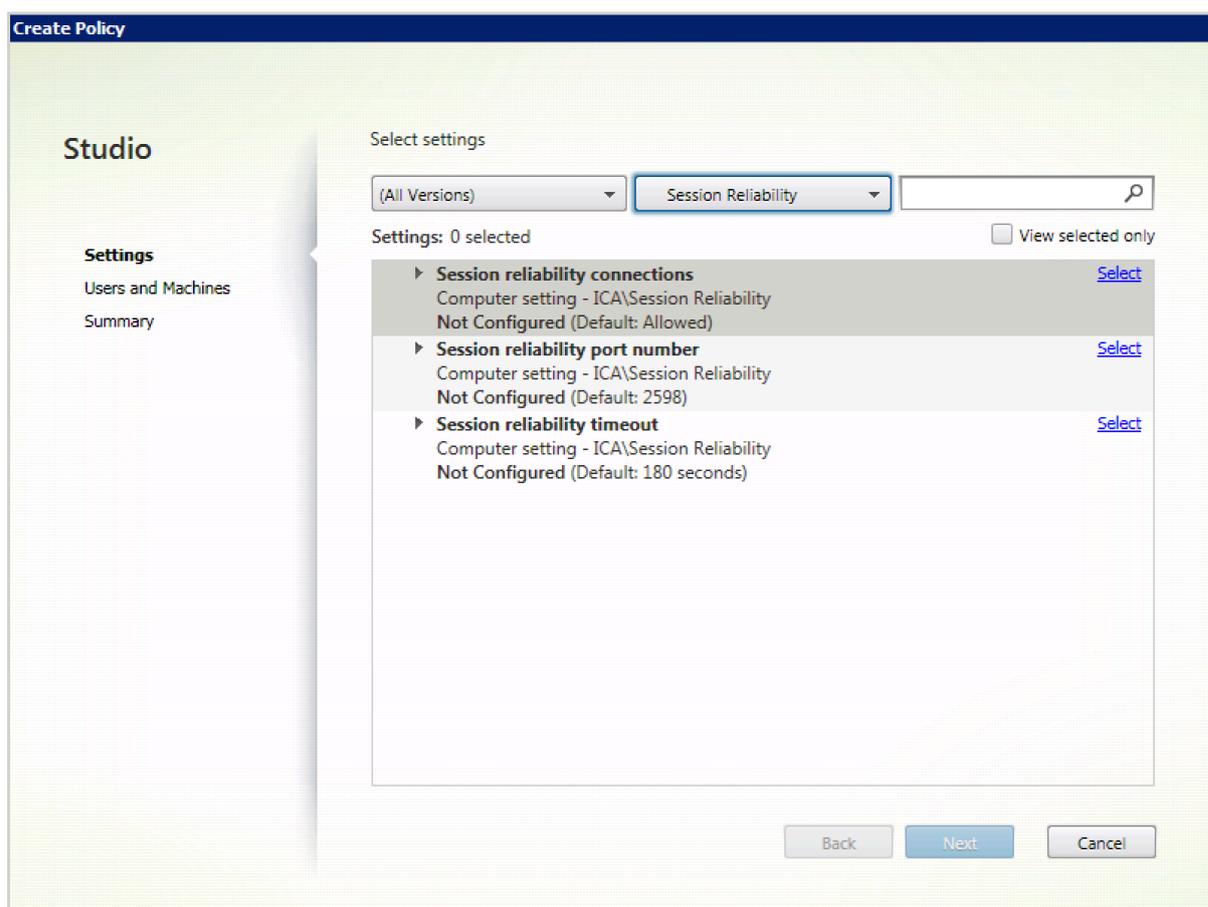
Die Sitzungszuverlässigkeit ist standardmäßig auf dem Server aktiviert. Sie deaktivieren dieses Feature, indem Sie die vom Server verwaltete Richtlinie konfigurieren.

Konfigurieren der Sitzungszuverlässigkeit in Citrix Studio

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 und XenDesktop 7.11 und höher festgelegt werden.

Ändern des Timeouts für die Sitzungszuverlässigkeit:

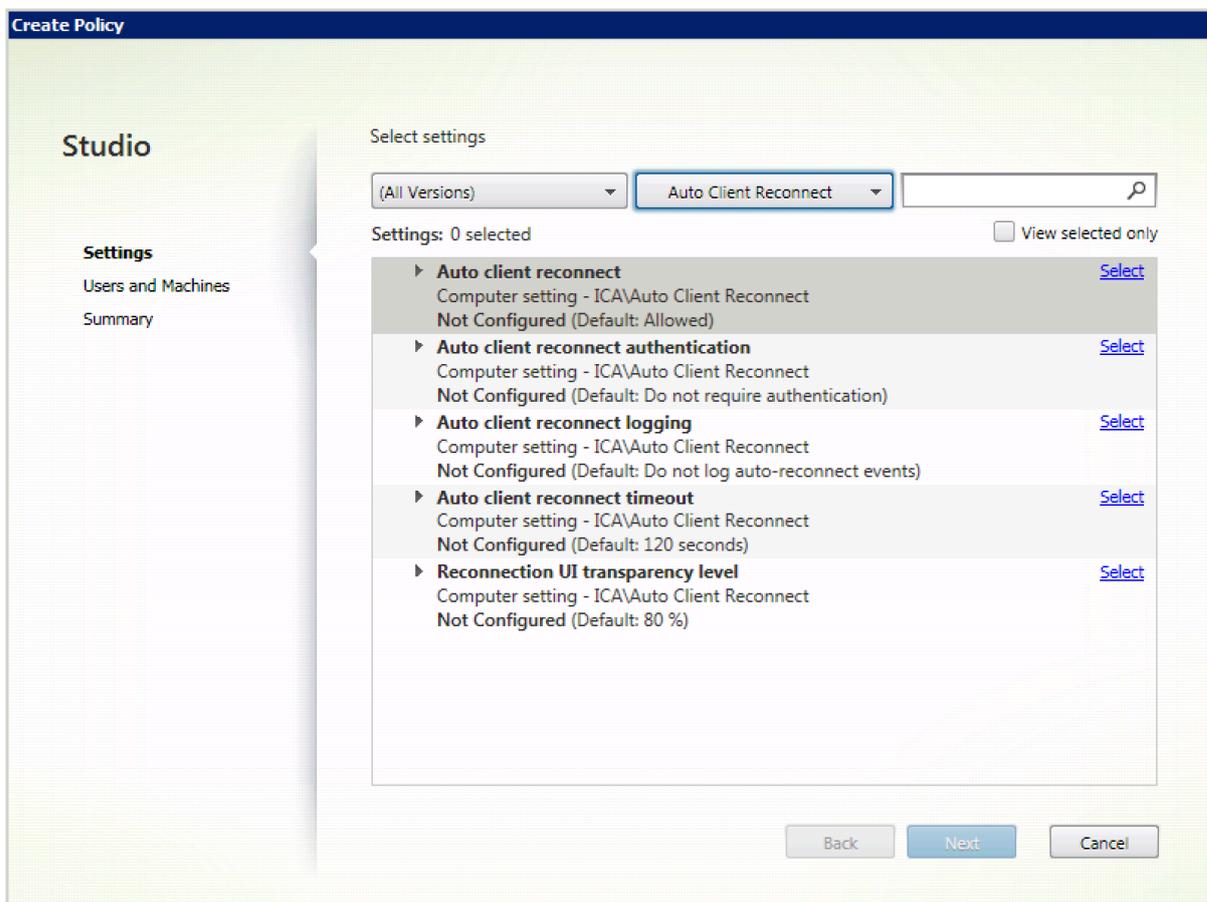
1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Timeout**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Konfigurieren der automatischen Wiederverbindung von Clients mit Citrix Studio

Die automatische Wiederverbindung von Clients ist standardmäßig aktiviert.

Deaktivieren der automatischen Wiederverbindung von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Client automatisch wieder verbinden**.
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 und 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 **Client automatisch wieder verbinden**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Einschränkungen:

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

Konfigurieren der Transparenz 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

Es gibt Herausforderungen rund um die Mobilität im Zusammenhang mit dem Wechsel zwischen Zugriffspunkten, Netzwerkunterbrechungen und Anzeigetimeouts aufgrund von Latenz. Sie erschweren die Aufrechterhaltung der Verbindungsintegrität für aktive Citrix Workspace-App für Mac-Sitzungen. Mit den verbesserten Technologien für Sitzungszuverlässigkeit und automatische Wiederverbindung von Citrix wird dieses Problem behoben.

Mit diesem Feature können Benutzer nach Netzwerkunterbrechungen die Verbindung zu Sitzungen automatisch wiederherstellen. Diese über Richtlinien in Citrix Studio aktivierten Features können die Benutzererfahrung 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 Verbindungstimeout für die automatische Wiederverbindung von Clients ändern. Die Standardeinstellung des Timeouts ist 120 Sekunden (zwei Minuten).

Einstellung	Beispiel	Standard
TransportReconnectRetryMaxT:	TransportReconnectRetryMaxT:	120

Sitzungszuverlässigkeit

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

Verwenden Sie die Datei **default.ica** in StoreFront, um das Verbindungstimeout für die Sitzungszuverlässigkeit zu ändern. Die Standardeinstellung des Timeouts ist 180 Sekunden (drei Minuten).

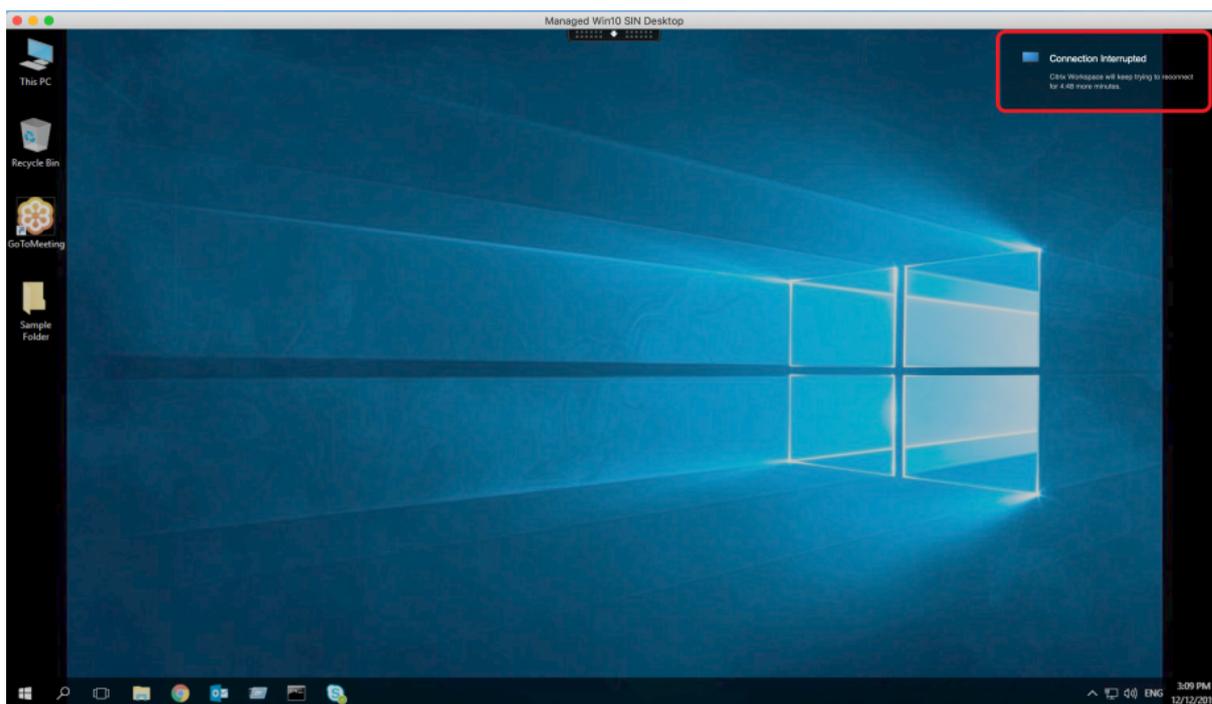
Einstellung	Beispiel	Standard
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Funktionsweise von Sitzungszuverlässigkeit und automatischer Wiederverbindung von Clients

Wenn automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit für die Citrix Workspace-App für Mac aktiviert sind, berücksichtigen Sie Folgendes:

- Wenn eine Wiederverbindung erfolgt, ist das 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.

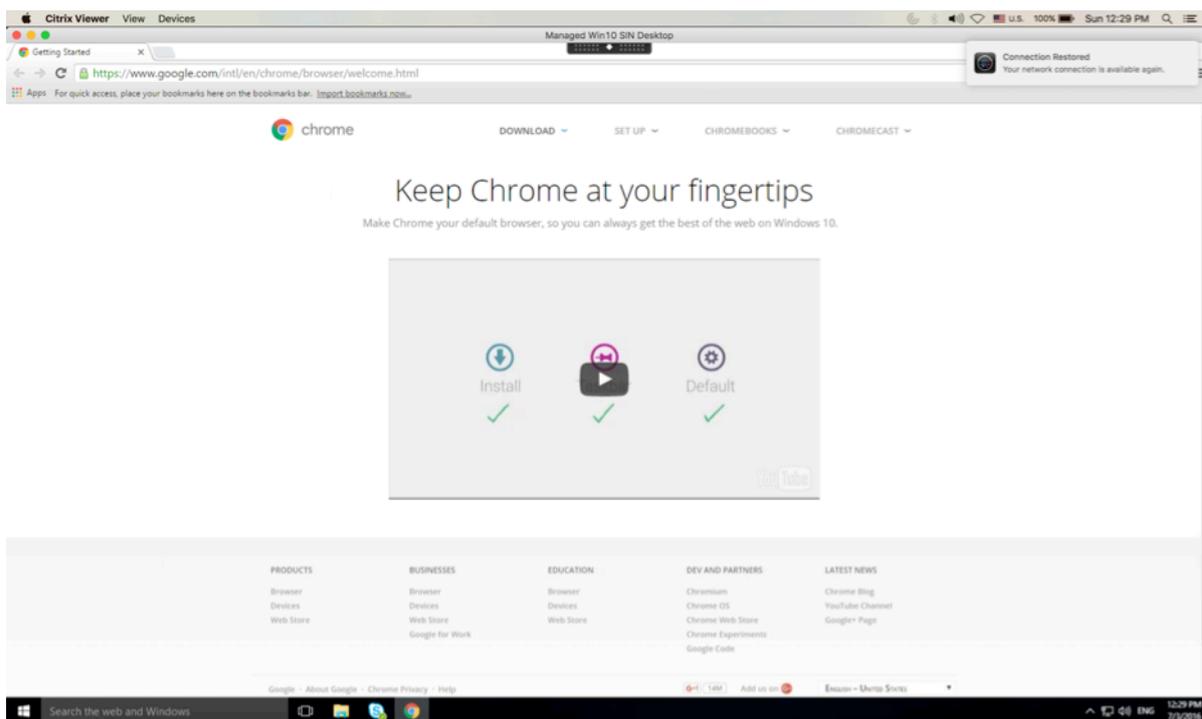
Standardmäßig beginnt die Anzeige des Wiederverbindungscountdowns bei 5 Minuten. In diesem Zeitwert sind die Werte der beiden Timer für automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit, 2 und 3 Minuten, zusammengefasst. In der Abbildung unten sehen Sie die Meldung mit dem Countdowntimer, 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.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Workspace-App für Mac und sendet die Daten automatisch an Citrix und Google Analytics.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Workspace-App zu verbessern.

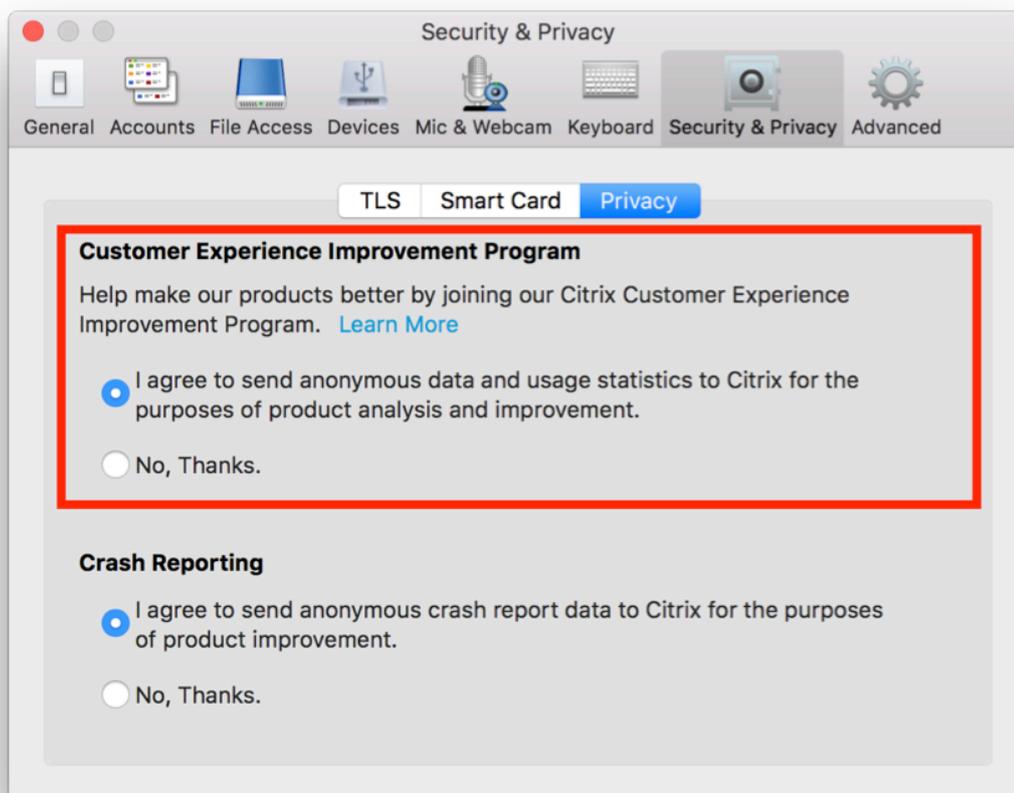
Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix. Ihre Daten sind gemäß dem [Citrix Services Security Exhibit](#), verfügbar im [Citrix Trust Center](#), geschützt.

Citrix verwendet Google Analytics, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu sammeln. Sie können prüfen, wie Google die für [Google Analytics gesammelten Daten verwendet](#).

Führen Sie die folgenden Schritte aus, um das Senden von CEIP-Daten an Citrix und Google Analytics zu deaktivieren:

1. Wählen Sie im Fenster **Einstellungen** die Option **Sicherheit und Datenschutz**.
2. Wählen Sie die Registerkarte **Datenschutz**.
3. Wählen Sie **Nein, danke**, um CEIP zu deaktivieren und die Teilnahme abzulehnen.
4. Klicken Sie auf **OK**.



Alternativ können Sie CEIP deaktivieren, indem Sie folgenden Terminalbefehl ausführen:

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```

Folgende Datenelemente werden von Google Analytics erfasst:

Betriebssystemversion	Sitzungsstart	Verwendung der generischen USB-Umleitung
-----------------------	---------------	--

Anwendungsbereitstellung

Berücksichtigen Sie die folgenden Optionen bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops, um die Benutzerfreundlichkeit beim Zugreifen auf Anwendungen zu erhöhen:

Webzugriffsmodus

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

Self-Service-Modus

Fügen Sie der Citrix Workspace-App für Mac ein StoreFront-Konto hinzu, oder legen Sie fest, dass die Citrix Workspace-App auf eine StoreFront-Site verweist. Anschließend können Sie den Self-Service-Modus konfigurieren, mit dem die Benutzer die Anwendungen über die Citrix Workspace-App für Mac abonnieren. 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 Benutzer eine Anwendung auswählen, wird eine Verknüpfung für die Anwendung im App-Ordner auf dem Benutzergerät platziert.

Wenn Benutzer auf eine StoreFront 3.0-Site zugreifen, erhalten sie eine Vorschau der Citrix Workspace-App für Mac.

Wenn Sie Anwendungen auf einer Citrix Virtual Apps-Farm veröffentlichen, können Sie die Erfahrung für Benutzer verbessern, die auf diese Anwendungen über StoreFront-Stores zugreifen. Stellen Sie sicher, dass Sie aussagekräftige Beschreibungen für die veröffentlichten Apps angeben. In Citrix Workspace-App für Mac sind diese Beschreibungen für Benutzer sichtbar.

Konfigurieren des Self-Service-Modus

Wie bereits erwähnt, fügen Sie der Citrix Workspace-App für Mac ein StoreFront-Konto hinzu oder Sie legen fest, dass die Citrix Workspace-App für Mac auf eine StoreFront-Site verweist. So können Sie den

Self-Service-Modus konfigurieren, mit dem die Benutzer die Anwendungen über die Benutzeroberfläche der Citrix Workspace-App für Mac abonnieren. 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 App für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge ****KEYWORDS: Auto**** an die Beschreibung anhängen, während Sie die App in Citrix Virtual Apps veröffentlichen. Wenn Benutzer sich bei dem Store anmelden, wird die App automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Anwendungen werden den Benutzern angekündigt bzw. häufig verwendete Anwendungen sind leichter zu finden, wenn Sie sie in der Citrix Workspace-App für Mac unter "Highlights" auführen. Um Apps für Mac in der Liste "Highlights" aufzuführen, hängen Sie die Zeichenfolge ****KEYWORDS: Featured**** an die App-Beschreibung an.

Weitere Informationen finden Sie in der Dokumentation zu [StoreFront](#).

Citrix Workspace-Updates

Konfigurieren mit der GUI

Ein Benutzer kann die Einstellung für **Citrix Workspace-Updates** im Dialogfeld **Einstellungen** außer Kraft setzen. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur auf den aktuellen Benutzer angewendet.

1. Navigieren Sie in der Citrix Workspace-App für Mac zum Dialogfeld **Einstellungen**.
2. Klicken Sie im Bereich **Erweitert** auf **Updates**. Das Dialogfeld "Citrix Workspace-App-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.

Konfigurieren von Citrix Workspace-Updates mit StoreFront

Administratoren können Citrix Workspace-App-Updates mit StoreFront konfigurieren. Die Citrix Workspace-App für Mac 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 Texteditor. 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: `<account id=... name="Store">`

Vor dem Tag `</account>` navigieren Sie zu den Eigenschaften des Benutzerkontos:

`<properties>`

`<clear />`

`</properties>`

3. Fügen Sie das Tag für automatische Updates nach dem Tag `<clear />` ein.

auto-update-Check

Die Funktion "auto-update-Check" legt fest, dass die Citrix Workspace-App für Mac ermitteln kann, ob Updates verfügbar sind.

Gültige Werte:

- Auto: Benutzer erhalten Benachrichtigungen, wenn Updates verfügbar sind.
- Manual: Benutzer erhalten keine Benachrichtigungen, wenn Updates verfügbar sind. Die Benutzer müssen manuell nach Updates suchen, indem sie **Nach Updates suchen** wählen.
- Disabled: Citrix Workspace-Updates werden deaktiviert.

auto-update-DeferUpdate-Count

Legt fest, wie oft Benutzer zum Update aufgefordert werden, bevor das Update auf die aktuelle Version der Citrix Workspace-App für Mac erzwungen wird. Der Standardwert ist 7.

Gültige Werte:

- -1 – Der Benutzer wird später erinnert, wenn ein Update verfügbar ist.
- 0 – Der Benutzer wird gezwungen, auf die aktuelle Version der Citrix Workspace-App für Mac zu aktualisieren, wenn das Update verfügbar ist.
- Positive Ganzzahl – Male, die der Benutzer 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 – Das Citrix Workspace-Updates-System entscheidet, wann Benutzern verfügbare Updates bereitgestellt werden.
- Fast – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten hohen Priorität zur Verfügung gestellt.
- Medium – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten mittleren Priorität zur Verfügung gestellt.
- Slow – Verfügbare Updates werden Benutzern mit der von Citrix Workspace-App für Mac festgelegten niedrigen Priorität zur Verfügung gestellt.

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung ermöglicht es Benutzern, bei der Verwendung eines Windows VDA oder Linux VDA zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist in der Standardeinstellung deaktiviert.

Um die Tastaturlayoutsynchronisierung zu aktivieren, gehen Sie zu **Einstellungen > Tastatur** und wählen Sie “Lokales Tastaturlayout statt des Remoteserver-Tastaturlayouts verwenden”.

Hinweis:

1. Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Benutzer, die in der japanischen, chinesischen oder koreanischen Sprache arbeiten, können den IME des Servers verwenden. Sie müssen die Option für das lokale Tastaturlayout deaktivieren, indem sie die entsprechende Option unter **Einstellungen > Tastatur** deaktivieren. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.
2. Das Feature funktioniert in Sitzungen nur dann, wenn der Umschalter im Client aktiviert und das entsprechende Feature auf dem VDA aktiviert ist. Das Menüelement **Clienttastaturlayout verwenden** wird unter **Geräte > Tastatur > International** hinzugefügt, um den aktivierten Status anzuzeigen.

Einschränkungen

- Die Verwendung der unter **Unterstützte Tastaturlayouts in Mac** aufgeführten Tastaturlayouts funktioniert, während das Feature aktiviert ist. Wenn Sie für das Clienttastaturlayout ein nicht kompatibles Layout wählen, wird das Layout möglicherweise auf dem VDA synchronisiert, die Funktionalität kann jedoch nicht bestätigt werden.
- Bei Remote-Apps, die mit erhöhten Rechten ausgeführt werden, kann keine Synchronisierung mit dem Clienttastaturlayout erfolgen. Um dieses Problem zu umgehen, ändern Sie das Tastaturlayout manuell auf dem VDA oder deaktivieren Sie die Benutzerkontensteuerung (UAC).

- Wenn ein Benutzer in einer RDP-Sitzung arbeitet, kann das Tastaturlayout nicht mit den **Alt** + **Shift**-Tastenkombinationen geändert werden, wenn RDP als App bereitgestellt wird. Als Workaround können Benutzer das Tastaturlayout mit der Sprachenleiste in der RDP-Sitzung ändern.

Tastaturlayoutunterstützung für Windows VDA

Supported keyboard layouts on Mac	
Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
	Dutch
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

Tastaturlayoutunterstützung für Linux VDA

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

Der erweiterte Client hängt von dem Feature für die Tastaturlayoutsynchronisierung ab. Standardmäßig ist das erweiterte Feature aktiviert, wenn das Feature für die Tastaturlayoutsynchronisierung aktiviert ist. Um nur dieses Feature zu steuern, öffnen Sie die Datei **Config** im Ordner **~/Library/Application Support/Citrix Receiver/**, suchen Sie die Einstellung **EnableIMEEnhancement** und aktivieren oder deaktivieren Sie das Feature, indem Sie den Wert auf “true” oder “false” festlegen.

Hinweis:

Die Einstellungsänderung wird nach einem Neustart der Sitzung wirksam.

Sprachenleiste

Sie können die Anzeige der Remotesprachenleiste in Anwendungssitzungen über die grafische Benutzeroberfläche ein- und ausblenden. Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt. In früheren Releases konnten Sie diese Einstellung nur über Registrierungsschlüssel auf dem VDA ändern. Ab der Citrix Workspace-App für Mac Version 1808 können Sie die Einstellungen im Dialogfeld **Einstellungen** ändern. Die Sprachenleiste wird in Sitzungen standardmäßig angezeigt.

Hinweis:

Das Feature ist in Sitzungen verfügbar, die unter einem VDA der Version 7.17 und höher ausgeführt werden.

Anzeigen/Ausblenden der Remotesprachenleiste

1. Öffnen Sie “Einstellungen”.
2. Klicken Sie auf “Tastatur”.
3. Aktivieren oder deaktivieren Sie “Remotesprachenleiste für die veröffentlichten Anwendungen anzeigen”.

Hinweis:

Die Änderungen werden sofort wirksam. Sie können die Einstellungen in einer aktiven Sitzung ändern. Die Remote-Sprachenleiste wird in Sitzungen mit nur einer Eingabesprache nicht angezeigt.

Citrix Casting

Mit Citrix Casting können Sie Ihren Mac-Bildschirm an Citrix Ready Workspace Hub-Geräte in der Nähe übertragen. Die Citrix Workspace-App für Mac unterstützt das Spiegeln Ihres Mac-Bildschirms per Citrix Casting auf Monitoren, die mit einem Workspace Hub verbunden sind.

Weitere Informationen finden Sie in der Dokumentation zu [Citrix Ready Workspace Hub](#).

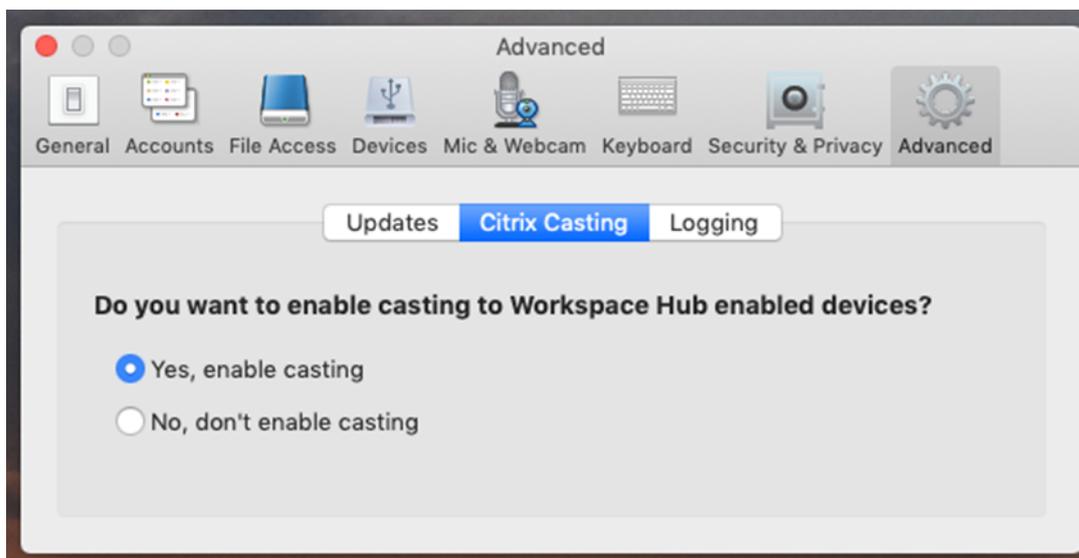
Voraussetzungen

- Citrix Workspace-App 1812 für Mac oder höher.
- Bluetooth ist zur Hub-Erkennung auf dem Gerät aktiviert.
- Citrix Ready Workspace Hub und Citrix Workspace-App müssen sich im selben Netzwerk befinden.
- Stellen Sie sicher, dass Port 55555 zwischen dem Gerät mit ausgeführter Citrix Workspace-App und dem Citrix Ready Workspace Hub nicht blockiert ist.
- Port 55556 ist der Standardport für SSL-Verbindungen zwischen Mobilgeräten und dem Citrix Ready Workspace Hub. Sie können in den Einstellungen von Raspberry Pi einen anderen SSL-Port konfigurieren. Wenn der SSL-Port blockiert ist, können die Benutzer keine SSL-Verbindungen zum Workspace Hub herstellen.
- Stellen Sie für Citrix Casting sicher, dass Port 1494 nicht blockiert ist.

Citrix Casting aktivieren

Citrix Casting ist standardmäßig deaktiviert. Aktivieren von Citrix Casting mit der Citrix Workspace-App für Mac:

1. Gehen Sie zu **Einstellungen**.
2. Wählen Sie **Erweitert** und anschließend **Citrix Casting**.
3. Wählen Sie **Ja, Casting aktivieren**.



Beim Start von Citrix Casting wird eine Benachrichtigung angezeigt und in der Menüleiste erscheint ein Citrix Casting-Symbol.

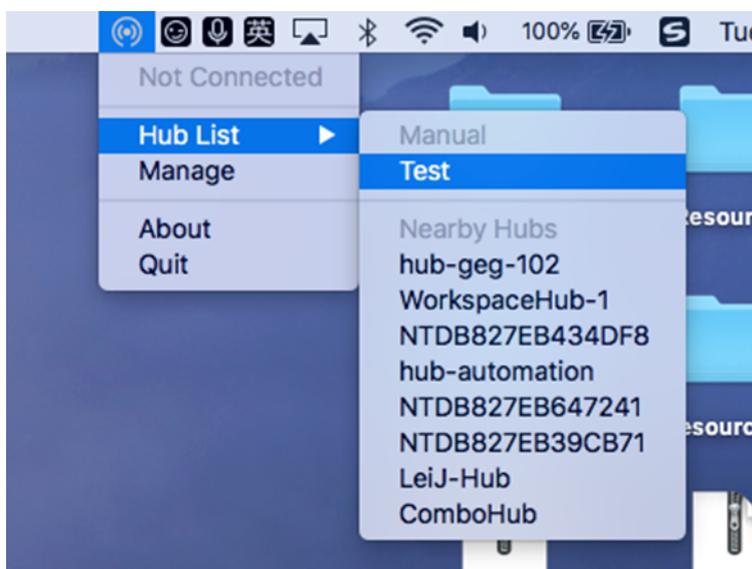
Hinweis:

Nach dem Aktivieren wird Citrix Casting stets automatisch mit der Citrix Workspace-App für Mac gestartet. Sie können das Feature jedoch unter **Einstellungen > Erweitert > Citrix Casting** mit **Nein, Casting nicht aktivieren** wieder deaktivieren.

Automatisches Ermitteln von Workspace-Hub-Geräten

Automatisches Verbinden mit Workspace Hubs:

1. Melden Sie sich auf Ihrem Mac bei der Citrix Workspace-App an und stellen Sie sicher, dass Bluetooth eingeschaltet ist. Bluetooth wird verwendet, um nahegelegene Workspace Hubs zu erkennen.
2. Wählen Sie in der Menüleiste das Symbol für **Citrix Casting**. Alle Citrix Casting-Funktionen werden über dieses Menü verwendet.
3. Im Untermenü **Hub-Liste** werden alle in der Nähe befindlichen Workspace Hubs angezeigt, die sich im selben Netzwerk befinden. Hubs werden in absteigender Reihenfolge gemäß ihrer Nähe zum Mac und mit dem konfigurierten Workspace Hub-Namen aufgelistet. Alle automatisch ermittelten Hubs werden unter **Hubs in der Nähe** angezeigt.
4. Wählen Sie den Namen des Hubs aus, mit dem Sie sich verbinden möchten.



Um die Auswahl eines Workspace Hubs während der Verbindung abbrechen, wählen Sie **Abbrechen**. Sie können **Abbrechen** auch verwenden, wenn die Netzwerkverbindung schlecht ist und der Verbindungsaufbau ungewöhnlich lange dauert.

Hinweis:

Es kann vorkommen, dass der gewünschte Hub nicht im Menü angezeigt wird. Prüfen Sie

das Menü **Hub-Liste** nach einen Moment erneut oder fügen Sie den Hub manuell hinzu. Die Workspace Hub-Daten werden periodisch an Citrix Casting übertragen.

Manuelles Ermitteln von Workspace-Hub-Geräten

Wenn Sie das Citrix Ready Workspace Hub-Gerät im Menü **Hubliste** nicht finden können, fügen Sie die IP-Adresse des Workspace-Hubs hinzu, um manuell darauf zuzugreifen. Workspace Hub hinzufügen:

1. Melden Sie sich auf Ihrem Mac bei der Citrix Workspace-App an und stellen Sie sicher, dass Bluetooth eingeschaltet ist. Bluetooth wird verwendet, um nahegelegene Workspace Hubs zu erkennen.
2. Wählen Sie in der Menüleiste das Symbol für **Citrix Casting**.
3. Wählen Sie die Menüoption **Verwalten**. Das Fenster **Hubs verwalten** wird angezeigt.
4. Klicken Sie auf **Hinzufügen**, um die IP-Adresse Ihres Hubs einzugeben.
5. Nachdem das Gerät hinzugefügt wurde, wird in der Spalte **Hubname** der Anzeigename des Hubs angezeigt. Verwenden Sie diesen Namen, um den Hub im Bereich **Manuell** des Untermenüs **Hubliste** zu identifizieren.

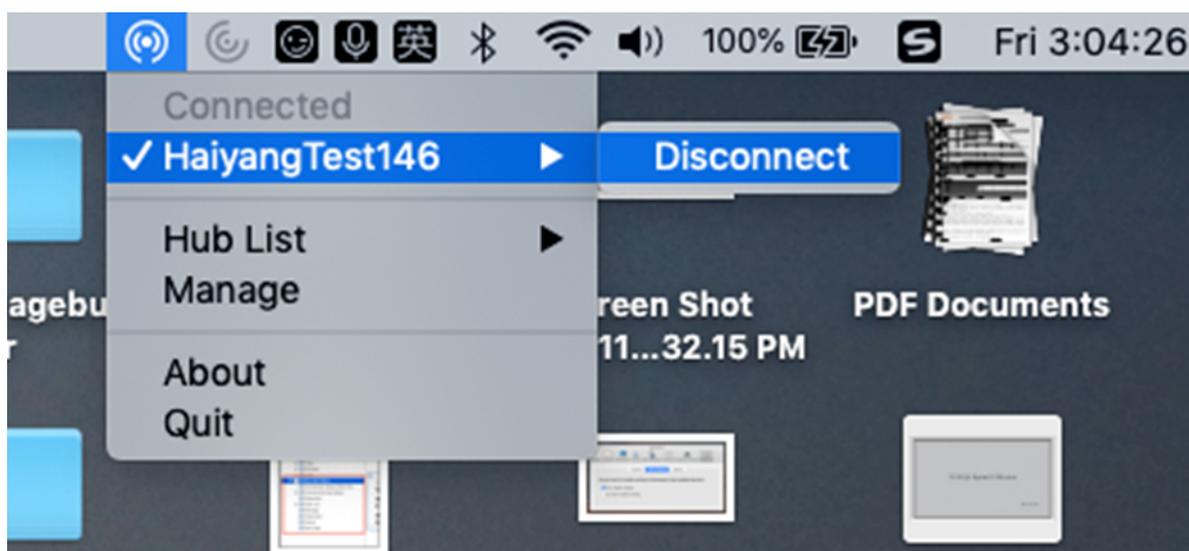
Hinweis:

Derzeit wird nur der Modus **Spiegeln** unterstützt. **Spiegeln** ist die einzige verfügbare Option in der Spalte **Anzeigemodus**.

Trennen des Workspace Hub-Geräts

Sie können die aktuelle Sitzung trennen und den Citrix Ready Workspace Hub automatisch oder manuell beenden.

- Schließen Sie den Laptop, um die Bildschirmcasting-Sitzung automatisch zu trennen.
- Bildschirmcasting-Sitzung manuell trennen:
 1. Wählen Sie das Symbol für **Citrix Casting**.
 2. Wählen Sie in der Liste der Hubs den Namen Ihres Workspace Hubs aus. Auf der rechten Seite wird die Option **Trennen** angezeigt.
 3. Wählen Sie **Trennen**, um den Hub zu beenden.



Bekannte Probleme

- Es gibt geringe Latenzprobleme beim Anzeigen des gespiegelten Bildschirms. Schlechte Netzwerkbedingungen können die Latenz noch verstärken.
- Wenn SSL in einem Citrix Ready Workspace Hub aktiviert ist und das Zertifikat des Hubs nicht vertrauenswürdig ist, wird eine Warnmeldung angezeigt. Um das Problem zu beheben, fügen Sie das Zertifikat mit dem Schlüsselbundtool zur Liste der vertrauenswürdigen Zertifikate hinzu.

Clientseitige Mikrofoneingabe

Die Citrix Workspace-App 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

Die Citrix Workspace-App für Mac bietet Unterstützung für digitale Diktate.

Sie können Mikrofone, die an das Gerät angeschlossen sind, verwenden. Wählen Sie hierfür eine der folgenden Optionen in den Einstellungen für **Mikrofon und Webcam** unter **Citrix Workspace-App für Mac > Einstellungen** aus:

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

Wenn Sie **Immer fragen** auswählen, müssen Sie jedes Mal beim Herstellen einer Verbindung in einem Dialogfeld bestätigen, dass Sie das Mikrofon in dieser Sitzung verwenden möchten.

Windows-Sondertasten

Die Citrix Workspace-App für Mac stellt diverse 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.
- “Windows-Logo-Taste mit  Befehl (rechts) senden”. Ermöglicht das Senden der Windows-Logo-Taste an Remote-Desktops und -anwendungen, wenn Sie die Befehlstaste auf der rechten Seite der Tastatur drücken. 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. Aktivieren Sie dazu das Kontrollkästchen “Sondertasten unverändert senden”. Standardmäßig ist dieses Kontrollkästchen nicht aktiviert, daher wird Option-1 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 Clear -Taste ein- und ausschalten; Option-Hilfe

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

Windows-Tastenkombinationen

In Remotesitzungen werden die meisten Mac-Tastaturkombinationen für die Texteingabe erkannt, 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. Sie werden 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. Mac-Tastaturen imitieren diese Tastenkombinationen nicht. Diese können jedoch über das Menü **Tastatur** an den Remote-Desktop oder die Remoteanwendung gesendet werden.

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

Wichtig

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

In der Tabelle verwendete Konventionen:

- Buchstabentasten sind großgeschrieben; dies gibt nicht an, dass die Umschalt-Taste gleichzeitig gedrückt werden soll.
- Bindestriche zwischen Tastaturanschlügen geben an, dass Tasten gleichzeitig gedrückt werden müssen (z. B. Strg-C).
- Mit Zeichentasten werden Texteingaben erzeugt. Dazu gehören alle Buchstaben, Zahlen und Satzzeichen. Sondertasten erzeugen keine Eingabe, sondern dienen als Modifikator oder Steuertaste. 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” bezieht sich auf die Fn-Taste (Funktion) der Mac-Tastatur. Funktionstaste bezieht sich auf die Tasten F1 bis F12 auf der 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	Strg-Option-Fn-Cmd-Löschen; Wählen Sie Tastatur > Strg+Alt+Entf senden
Löschen	Delete; Wählen Sie Tastatur > Taste senden > Entfernen; Fn-Rücktaste (Fn-Delete auf einigen US-Tastaturen)
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

Windows-Taste oder Tastenkombination	Mac-Äquivalent
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
Tabulatortaste	Wählen Sie Tastatur > Taste senden > Tabulator
Windows-Logo	Rechte Cmd-Taste (eine standardmäßig aktivierte Tastatureinstellung); Wählen Sie Tastatur > Windows-Tastenkombination senden > Start
Tastenkombinationen zum Anzeigen von Charms	Wählen Sie Tastatur > Windows-Tastenkombination senden > Charms
Tastenkombinationen zum Anzeigen von App-Befehlen	Wählen Sie Tastatur > Windows-Tastenkombination senden > App-Befehle
Tastenkombinationen zum Andocken von Apps	Wählen Sie Tastatur > Windows-Tastenkombination senden > Andocken
Tastenkombinationen zum Wechseln von Apps	Wählen Sie Tastatur > Windows-Tastenkombination senden > Apps wechseln

Verwenden eines Eingabemethoden-Editors (IME) und internationaler Tastaturlayouts

Mit der Citrix Workspace-App 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 Einfüge-
marke statt in einem Fenster Text eingeben.

Mit der Citrix Workspace-App 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

Die Citrix Workspace-App 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.

Mehrere Monitore

Benutzer können die Citrix Workspace-App für Mac im Vollbildmodus über mehrere Monitore hinweg ausführen.

1. Öffnen Sie den Citrix Viewer.
2. Wählen Sie in der Citrix Viewer-Symbolleiste je nach Anforderung eine der folgenden Optionen aus:
 - **Zu Vollbild wechseln** - Vollbild nur auf dem Hauptmonitor.
 - **Alle Displays in Vollbild verwenden** - Vollbild auf allen angeschlossenen Monitoren.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die Monitore.

Der Bildschirm ist nun auf alle Monitore erweitert.

Bekannte Einschränkungen

- Der Vollbildmodus wird nur auf einem Monitor oder auf allen Monitoren unterstützt. Diese Funktion kann über ein Menüelement festgelegt werden.
- Citrix empfiehlt die Verwendung von maximal 2 Monitoren. Die Verwendung von mehr als 2 Monitoren kann die Sitzungsleistung beeinträchtigen oder Probleme mit der Benutzerfreundlichkeit verursachen.

Desktopsymbolleiste

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

- Die Schaltfläche **Home** wurde von der Symbolleiste entfernt. Diese Funktion kann mit den folgenden Befehlen ausgeführt werden:
 - Cmd-Taste+Tab: Wechseln zur vorherigen aktiven Anwendung.
 - Ctrl+Linkspfeil: Wechseln zum vorherigen Bereich.
 - Sie können mit dem integrierten Trackpad oder den Magic Mouse-Gesten zu einem anderen Bereich wechseln.
 - Wenn Sie den Cursor im Vollbildmodus an den Rand des Bildschirms bewegen, wird ein Dock angezeigt, in dem Sie Anwendungen aktivieren können.
- Die Schaltfläche für den **Fenstermodus** wurde von der Symbolleiste entfernt. Wenden Sie eine dieser Methoden an, um vom Vollbildmodus in den Fenstermodus zu wechseln:
 - In OS X 10.10 klicken Sie in der Dropdown-Menüleiste auf die grüne Fensterschaltfläche.
 - 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.
- Unterstützung für das Ziehen zwischen Fenstern im Vollbildmodus mit mehreren Monitoren.

Workspace Control

Mit Workspace Control folgen Desktops und Anwendungen dem Benutzer, wenn er das Gerät wechselt. So können etwa Krankenhausärzte von einer Arbeitsstation 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. Beispielsweise kann sich ein Mitarbeiter im Gesundheitswesen von einem Gerät in der Notaufnahme abmelden und sich bei einer Arbeitsstation im Röntgenlabor anmelden. Die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen, die für die Sitzung im Röntgenlabor geeignet sind, werden für die Sitzung im Röntgenlabor wirksam.

Konfigurieren der Workspace Control-Einstellungen

1. Klicken Sie im Fenster der Citrix Workspace-App für Mac auf den Abwärtspfeil  und wählen Sie **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Allgemein**.
3. Wählen Sie eine der folgenden Optionen:
 - Beim Anmelden an Citrix Workspace Anwendungen wiederverbinden. Benutzer können eine Verbindung mit getrennten Anwendungen wiederherstellen, wenn sie Citrix Workspace 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 Menü der Citrix Workspace-App für Mac "Apps aktualisieren" auswählen.

Zuordnen von Clientlaufwerken

Mit der Clientlaufwerkzuordnung greifen Sie auf lokale Laufwerke auf dem Benutzergerät in Sitzungen zu, z. B. CD-Laufwerke, DVDs und USB-Sticks. Wenn eine Serverkonfiguration die Clientlaufwerkzuordnung zulässt, können Benutzer auf lokal gespeicherte Dateien zugreifen und diese in Sitzungen bearbeiten. Benutzer können sie auch speichern, entweder auf einem lokalen Laufwerk oder auf einem Laufwerk auf dem Server.

Die Citrix Workspace-App 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 Laufwerksbuchstaben auf dem Server zu.

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

Konfigurieren des Lese- und Schreibzugriffs für zugeordnete Laufwerke

1. Klicken Sie auf der Homepage der Citrix Workspace-App für Mac auf den Abwärtspfeil  und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf **Dateizugriff**.
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.

Benutzerdefinierter Webstore

Sie können über die Citrix Workspace-App für Mac auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Um dieses Feature verwenden zu können, muss der Administrator den benutzerdefinierten Webstore der Liste der zulässigen URLs in der Eigenschaft `allowedWebStoreURLs` im Global App Configuration Service hinzufügen.

Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter [Global App Configuration Service](#).

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Webstore-URL hinzuzufügen:

1. Öffnen Sie die Workspace-App und navigieren Sie zu **Konten**.
2. Klicken Sie im Fenster **Konten** auf das Symbol **+** und geben Sie die URL ein.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Webstore-URL zu löschen:

1. Öffnen Sie die Workspace-App und navigieren Sie zu **Konten**.
2. Wählen Sie im Fenster **Konten** das Konto aus, das Sie löschen möchten, und klicken Sie auf das Symbol **-**.

Authentifizierung

February 18, 2022

Smartcard

Die Citrix Workspace-App für Mac unterstützt die Smartcardauthentifizierung für die folgenden Konfigurationen:

- Smartcardauthentifizierung bei Workspace für Web oder StoreFront 2.x und höher
- Citrix Virtual Apps and Desktops 7 1808 und höher
- XenDesktop 7.1 und höher oder 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.
- Die Citrix Workspace-App 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 der Citrix Workspace-App für Mac.
- In Double-Hop-Sitzungen wird eine weitere Verbindung zwischen der Citrix Workspace-App für Mac und dem virtuellen Desktop des Benutzers hergestellt.

Info zur Smartcardauthentifizierung an Citrix Gateway

Es stehen mehrere Zertifikate zur Verfügung, wenn Sie eine Verbindung per Smartcard authentifizieren. Die Citrix Workspace-App für Mac fordert Sie auf, ein Zertifikat auszuwählen. Nach der Auswahl des Zertifikats werden Sie von der Citrix Workspace-App für Mac aufgefordert, das Smartcardkennwort einzugeben. Nach der Authentifizierung wird die Sitzung gestartet.

Wenn auf der Smartcard nur ein passendes Zertifikat ist, verwendet die Citrix Workspace-App 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 Workspace-Zugriff auf Citrix Gateway oder StoreFront, wenn eine Smartcard erforderlich ist.

Angeben eines PKCS#11-Moduls für die Smartcardauthentifizierung:

1. Wählen Sie in der Citrix Workspace-App für Mac **Einstellungen**.
2. Klicken Sie auf **Sicherheit und Datenschutz**.
3. Klicken Sie im Bereich **Sicherheit und Datenschutz** auf **Smartcard**.

4. Wählen Sie im Feld **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

Die Citrix Workspace-App 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:

- Clarify
- ActivIdentity (Clientversion)
- Charismathics (Clientversion)

Unterstützte Smartcards:

- PIV-Karten
- Common Access Card (CAC)
- Gemalto .NET-Karten

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

Einschränkungen

- Zertifikate müssen auf einer Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Citrix Workspace-App für Mac speichert nicht die Zertifikatauswahl des Benutzers.
- Die Citrix Workspace-App für Mac speichert nicht die Smartcard-PIN des Benutzers. PIN-Abfragen werden vom Betriebssystem gehandhabt, das möglicherweise seinen eigenen Cachingmechanismus hat.
- Die Citrix Workspace-App für Mac stellt die Verbindung mit Sitzungen nicht wieder her, wenn eine Smartcard eingesteckt ist.
- Für die Verwendung von VPN-Tunneln mit der Smartcardauthentifizierung müssen Sie das Citrix Gateway Plug-In installieren und sich über eine Webseite anmelden. Verwenden Sie Ihre Smartcards und PINs zur Authentifizierung bei jedem Schritt. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.

Sichere Kommunikation

February 18, 2022

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

Hinweis:

Citrix empfiehlt das Schützen der Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit Citrix Gateway.

- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das Netzwerk und vom Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App für Mac unterstützt die Protokolle SOCKS und Secure Proxy.
- Citrix Secure Web Gateway. Citrix Secure Web Gateway stellt 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 eine Firewall verwenden, die die interne IP-Adresse des Servers einer externen Internetadresse wie der Netzwerkadressübersetzung (NAT) zuweist, konfigurieren Sie die externe Adresse.

Hinweis:

Ab macOS Catalina hat Apple zusätzliche Anforderungen für Stammzertifikate und Zwischenzertifikate erzwungen, die Administratoren konfigurieren müssen. Weitere Informationen finden Sie im Apple Support-Artikel [HT210176](#).

Citrix Gateway

Damit Remotebenutzer sich über Citrix Gateway mit der XenMobile-Bereitstellung verbinden können, können Sie Citrix Gateway für StoreFront konfigurieren. 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 Citrix Gateway zu, indem Sie Citrix 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 die Citrix Workspace-App für Mac her.

Verbinden mit Citrix Secure Web Gateway

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

Wenn Sie den Relaymodus verwenden, fungiert der Citrix Secure Web Gateway-Server als Proxy und Sie müssen die Citrix Workspace-App für Mac für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Citrix Secure Web Gateway-Servers.
- Portnummer des Citrix Secure Web Gateway-Servers. Citrix Secure Web Gateway Version 2.0 unterstützt den Relaymodus nicht.

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 (example.com) wird als Domänenname bezeichnet.

Herstellen von Verbindungen über Proxyserver

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

Für die Kommunikation mit dem Webserver verwendet die Workspace-App für Mac die Proxyservereinstellungen, die für den Standardwebbrowser auf dem Benutzergerät konfiguriert sind. Konfigurieren Sie die Proxyservereinstellungen für den Standardwebbrowser entsprechend auf dem Benutzergerät.

Herstellen einer Verbindung durch eine Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Die Citrix Workspace-App für Mac muss 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 für einen sicheren Webserver). Für die Kommunikation zwischen Citrix Workspace und dem Citrix-Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

TLS

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 FIPS 140. FIPS 140 ist ein Standard für die Kryptografie.

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

Hinweis

Die Citrix Workspace-App für Mac verwendet plattformeigene Kryptografie (OS X) für Verbindungen zwischen der Citrix Workspace-App für Mac und StoreFront.

Die folgenden Verschlüsselungssammlungen sind aus Sicherheitsgründen veraltet:

- Verschlüsselungssammlungen mit dem Präfix "TLS_RSA_**"
- Verschlüsselungssammlungen RC4 und 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Die Citrix Workspace-App für Mac unterstützt nur die folgenden Verschlüsselungssammlungen:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Für Benutzer von DTLS 1.0 unterstützt die Citrix Workspace-App für Mac 1910 und höher nur die folgende Verschlüsselungssammlung:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Aktualisieren Sie Citrix Gateway auf Version 12.1 oder höher, wenn Sie DTLS 1.0 verwenden möchten. Andernfalls greift es basierend auf der DDC-Richtlinie auf TLS zurück.

Die folgenden Matrizen enthalten Einzelheiten zu internen und externen Netzwerkverbindungen:

Client cipher set	VDA cipher set	Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

Hinweis:

- Verwenden Sie Citrix Gateway 12.1 oder höher, damit EDT ordnungsgemäß funktioniert. Ältere Versionen unterstützen keine ECDHE-Verschlüsselungssammlungen im DTLS-Modus.
- Citrix Gateway unterstützt kein DTLS 1.2. `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` und `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` werden also nicht unterstützt. Citrix Gateway muss für die Verwendung von `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` konfiguriert sein, damit es in DTLS 1.0 ordnungsgemäß funktioniert.

Konfigurieren und Aktivieren der Citrix Workspace-App für TLS

Das Setup von TLS besteht aus zwei Hauptschritten:

1. Setup von SSL-Relay auf dem Citrix Virtual Apps and Desktops-Server und Abrufen und Installieren des benötigten Serverzertifikats.

2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Installieren von Stammzertifikaten auf Benutzergeräten

Für das Sichern der Kommunikation mit TLS zwischen TLS-aktivierter Citrix Workspace-App für Mac und der Serverfarm muss auf dem Clientgerät ein Stammzertifikat vorhanden sein. Das Stammzertifikat überprüft die Signatur der Zertifizierungsstelle im Serverzertifikat.

In macOS X sind ca. 100 kommerzielle Stammzertifikate vorinstalliert. Wenn Sie jedoch ein anderes Zertifikat verwenden möchten, können Sie eines von der Zertifizierungsstelle abrufen und auf jedem Benutzergerät installieren.

Installieren Sie das Stammzertifikat je nach den Richtlinien und Verfahren Ihres Unternehmens auf jedem Gerät, anstatt die Benutzer zur Installation aufzufordern. Am einfachsten und sichersten ist es, wenn Sie die Stammzertifikate der macOS X-Schlüsselkette hinzufügen.

Hinzufügen eines Stammzertifikats zur Schlüsselkette

1. Doppelklicken Sie auf die Datei, die das Zertifikat enthält. Durch diese Aktion wird die Anwendung für die Schlüsselbundverwaltung automatisch gestartet.
2. Wählen Sie im Dialogfeld "Add Certificates" eine Option im Pop-upmenü "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 wird von TLS-fähigen Clients und anderen Anwendungen, die TLS einsetzen, verwendet.

Informationen über TLS-Richtlinien

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

Hinweis

TLS-Richtlinien werden mit anderen Methoden verwaltet – von Geräten, die von einem 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.:

- **Ohne.** 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. Gibt 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. Verbessert die kryptografische Authentifizierung des Citrix Servers und die allgemeine Sicherheit der SSL/TLS-Verbindungen zwischen einem Client und einem Server. Diese Einstellung regelt den Umgang mit einer vertrauenswürdigen Stammzertifizierungsstelle beim Öffnen einer Remotesitzung über SSL mit dem Client für OS X.

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. Administratoren können Sicherheitszertifikate widerrufen (d. h. vor dem Ablaufdatum ungültig machen), wenn private Schlüssel von Zertifikaten kryptografisch kompromittiert sind oder der DNS-Name unerwartet geändert werden muss.

Gültige Werte für diese Einstellung sind u. a.:

- **NoCheck.** Es wird keine Überprüfung der Zertifikatsperrliste durchgeführt.
- **CheckWithNoNetworkAccess.** Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Es werden nur lokale Zertifikatsperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay oder Citrix Secure Web Gateway-Server vorgelegt wird, nicht wichtig.

- **FullAccessCheck.** Es wird eine Überprüfung der Zertifikatsperrliste durchgeführt. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden einer Zertifikatsperrliste ist für die Überprüfung des Serverzertifikats, das vom Ziel-SSL-Relay oder Citrix Secure Web Gateway-Server vorgelegt wird, nicht wichtig.
- **FullAccessCheckAndCRLRequired.** Die Prüfung der Zertifikatsperrliste wird durchgeführt, mit Ausnahme der Root-Zertifizierungsstelle. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.
- **FullAccessCheckAndCRLRequiredAll.** Die Prüfung der Zertifikatsperrliste wird durchgeführt, einschließlich der Stammzertifizierungsstelle. Lokale Zertifikatsperrlisten-Stores und alle Verteilungspunkte werden verwendet. Das Finden aller erforderlichen Zertifikatsperrlisten ist für die Überprüfung wichtig.

Hinweis

Wenn Sie “SSLCertificateRevocationCheckPolicy” nicht festlegen, wird standardmäßig “FullAccessCheck” verwendet.

```
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 OSX-Einstellungslistendatei 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 <name> <type> <value>
```

Wobei:

<name>: Der Name der Einstellung, wie oben beschrieben.

<type>: Eine Option zum Identifizieren des Typs der Einstellung, entweder -string oder -array. Wenn der Einstellungstyp “string” ist, kann diese Einstellung ausgelassen werden.

<value>: Der Wert für die Einstellung. Wenn der Wert ein Array ist und mehrere Werte angegeben werden müssen, trennen Sie die Werte durch ein Leerzeichen.

```
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 <name>
```

Wobei:

<name>: Der Name der Einstellung, wie oben beschrieben.

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

Sicherheitseinstellungen

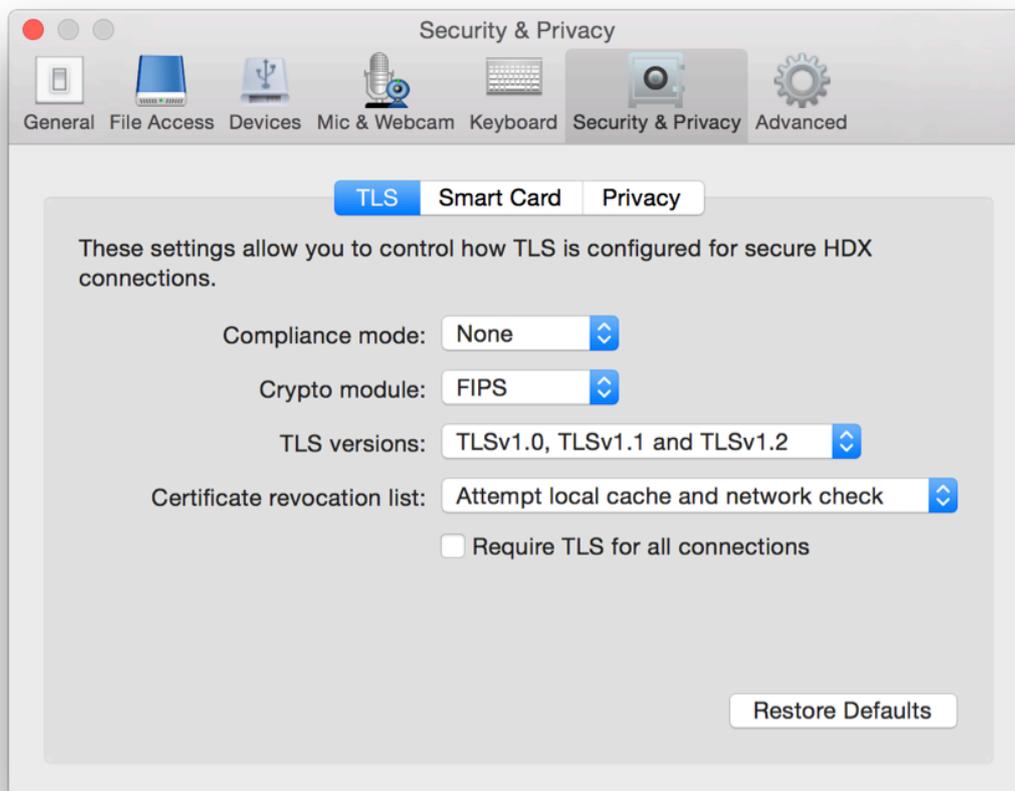
Mit Citrix Receiver für Mac-Version 12.3 wurden Sicherheitsverbesserungen eingeführt, u. a.:

- Verbesserte Benutzeroberfläche für die Sicherheitskonfiguration: In älteren Versionen war die Befehlszeile die bevorzugte Methode, um sicherheitsrelevante Änderungen vorzunehmen. Jetzt 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: Sie können Verbindungen überprüfen, die eine bestimmte TLS-Version verwenden, sowie Verschlüsselungsalgorithmen, den Modus, die Schlüsselgröße und den SecureICA-Status. 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:



**Locations**

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

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).