Citrix Workspace™-App für iOS

Die Citrix Workspace-App für iOS ist eine Clientsoftware, die im Apple Store zum Download verfügbar ist. Sie ermöglicht Ihnen den Zugriff auf und die Ausführung von virtuellen Desktops und gehosteten Anwendungen, die von Citrix Virtual Apps and Desktops bereitgestellt werden.

iOS ist das Betriebssystem für mobile Apple-Geräte wie iPads und iPhones. Die Citrix Workspace-App für iOS läuft auf Geräten, die das iOS-Betriebssystem verwenden, wie z. B. iPhone X, iPad mini und iPad Pro.

Detaillierte Informationen zu den Funktionen, behobenen Problemen und bekannten Problemen finden Sie auf der Seite Informationen zu dieser Version.

Informationen zu veralteten Elementen finden Sie auf der Seite Veraltet.

Sprachunterstützung

Die Citrix Workspace-App für iOS ist für die Verwendung in anderen Sprachen als Englisch angepasst. Eine Liste der von der Citrix Workspace-App für iOS unterstützten Sprachen finden Sie unter Sprachunterstützung.

Referenzartikel

- Technischer Überblick: Citrix Workspace
- Globaler App-Konfigurationsdienst
- Workspace-Benutzeroberfläche (UI)
- Microsoft Teams-Optimierung in Citrix Virtual Apps and Desktops-Umgebungen
- Veröffentlichungszeitpläne der Citrix Workspace-App

Neuerungen in verwandten Produkten

- Citrix Workspace
- Citrix DaaS
- StoreFront

- Secure Private Access
- Citrix Workspace-App für Mac

Legacy-Dokumentation

Für Produktversionen, die das End of Life (EOL) erreicht haben, siehe Legacy-Dokumentation.

Über diese Version

Erfahren Sie mehr über neue Funktionen, Verbesserungen, behobene Probleme und bekannte Probleme.

> **Hinweis:**
>
> - Wir würden uns über Ihr wertvolles Feedback zu dieser Version freuen, das Sie unter **Einstellungen** > **Problem melden** geben können. Von hier aus können uns sowohl ausführliche Protokolle als auch Screenshots mitgeteilt werden.
> - Suchen Sie nach technischen Vorschauen? Wir haben eine Liste zusammengestellt, damit Sie sie an einem Ort finden können. Erkunden Sie unsere Seite Funktionen in der technischen Vorschau.

Neuerungen in 26.9.0

Unterstützung für OS 27

Die Citrix Workspace-App für iOS unterstützt jetzt iOS/iPadOS 27.

Erweiterte Anti-Screen-Capture-Abdeckung für Multi-Fenster-Layouts

Anti-Screen-Capture in App Protection-fähigen Sitzungen erstreckt sich jetzt auf den schwebenden Fenstermodus. Der Schutz wird überall dort erzwungen, wo die geschützte Sitzung präsentiert wird – Vollbild, Split View, Slide Over, schwebendes Fenster und Stage Manager – und bleibt im Hintergrund und im App-Switcher-Snapshot erhalten, wenn Sie von der Citrix Workspace-App wegwechseln.

Behobene Probleme in 26.9.0

- Nach dem Upgrade auf Citrix Workspace-App Version 25.9.0.36 auf iPads liefern Barcode-Scans in der Novatek-Anwendung zeitweise falsche oder unvollständige Daten.

- Veröffentlichte App wird nicht angezeigt, wenn die Citrix Workspace-App im Hintergrund/Vollbildmodus ist und über Safari gestartet wird.
- Geschützte App-Ressource wird möglicherweise nicht mit der Citrix Workspace-App für iOS 2511 gestartet, wenn der Store über den Web Interface-Modus hinzugefügt wird.

Neuerungen in 26.7.0

Verbesserte Audioleistung (Wiedergabe) über EDT Lossy

Ab Version 2607 verbessert die Citrix Workspace-App für iOS die Audio-Wiedergabe in der Sitzung durch die Nutzung von EDT Lossy, einem UDP-basierten Transport, der für Echtzeit-Audio-Streaming optimiert ist.

Im Vergleich zu Standard-EDT und Transmission Control Protocol (TCP) bietet der verlustbehaftete EDT-Modus eine flüssigere Audiowiedergabe in mobilen Netzwerken mit hoher Latenz, variabler Bandbreite oder Paketverlust. Dieses Update reduziert Audio-Stottern und -Aussetzer und sorgt für ein konsistenteres und hochwertigeres Hörerlebnis bei virtuellen Sitzungen, Medienwiedergabe und Online-Meetings.

Scroll-Unterstützung für Maus, Trackpad und Touch

Diese Funktion unterstützt horizontales und diagonales Scrollen für die folgenden Eingabemethoden:

- **Mausrad-Scrollen:** Verwenden Sie ein physisches Mausrad, um vertikal und horizontal zu scrollen.
- **Trackpad-Zwei-Finger-Schwenken (Apple und Drittanbieter):** Verwenden Sie eine Zwei-Finger-Schwenkgeste, um vertikal und horizontal zu scrollen.
- **Touch auf dem Bildschirm (Ein-Finger-Scrollen):** Verwenden Sie einen einzelnen Finger auf einem iPhone- oder iPad-Bildschirm, um vertikal und horizontal zu scrollen.

VDA-Betriebssystemerkennung und Tastenkombinationsunterstützung

Ab Version 2607 erkennt die Citrix Workspace™-App für iOS nun das Betriebssystem des verbundenen VDA und sendet entsprechende Tastenkombinationen:

- **VDA-Betriebssystemerkennung:** Erkennt, ob der verbundene VDA Windows, Linux oder macOS ausführt.
- **Automatischer Eingabemodus für macOS VDA:** Wenn Sie eine Verbindung zu einem macOS VDA herstellen, schaltet die App den Eingabemodus auf **Scancode** um. Die App

sendet außerdem Diagnosedaten und zeichnet einen Telemetrie-Datenpunkt für diese Einstellung auf.

- **Erweiterte Tastatur-Symbolleisten-Verknüpfungen:** Ordnet gängige Verknüpfungen dem Modell der Citrix Workspace-App für ChromeOS zu:
  - Kopieren (Strg+C oder Befehl+C)
  - Einfügen (Strg+V oder Befehl+V)
  - Ausschneiden (Strg+X oder Befehl+X)
  - Alles auswählen (Strg+A oder Befehl+A)
  - Rückgängig (Strg+Z oder Befehlstaste+Z)
  - Suchen (Strg+F oder Befehlstaste+F)
  - Speichern (Strg+S oder Befehlstaste+S)

Verbesserte In-Session-Symbolleiste

Die Sitzungssymbolleiste wurde mit einem einheitlichen Design für iPhone und iPad aktualisiert, einschließlich aktualisierter Notch- und Tastatur-Assets. Die Symbolleiste verhält sich jetzt konsistent über alle iPad-Ausrichtungen hinweg, und die Interaktion zwischen der In-Session-Tastatur und der Symbolleiste wurde verbessert, um eine reibungslosere Benutzererfahrung zu bieten.

Automatische Synchronisierung der Grafikeinstellungen mit nativen iOS-Einstellungen

Ab Citrix Workspace-App für iOS 2607 wird die alte Auflösungsauswahl unter **Einstellungen > Anzeigeoptionen > Auflösung** durch vereinfachte, absichtsbasierte Optionen ersetzt, die die Anzeigeskalierung an die nativen iOS-Einstellungen anpassen. Dies erleichtert das Erreichen einer DPI-Anpassung auf externen Monitoren, indem virtuelle Desktopsitzungen dynamisch an die Auflösung des angeschlossenen Displays (bis zu 4K) angepasst werden, um optimale Klarheit und Lesbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Automatische Synchronisierung der Grafikeinstellungen mit nativen iOS-Einstellungen

Schnellerer und widerstandsfähigerer Sitzungsstart mit parallelen EDT- und TCP-Verbindungsversuchen

Die Citrix Workspace-App für iOS verbessert jetzt den Sitzungsstart, indem sie EDT- und TCP-Verbindungen parallel versucht. Zuvor basierte der Sitzungsaufbau auf einem einzigen Transportpfad gleichzeitig, was die Verbindungsaufbauzeit erhöhen konnte, wenn der bevorzugte

Pfad langsam reagierte oder nicht verfügbar war. Mit dieser Verbesserung kann die App den Transport fortsetzen, der zuerst verfügbar wird, was dazu beiträgt, die Startlatenz zu reduzieren und die Verbindungszuverlässigkeit unter verschiedenen Netzwerkbedingungen zu verbessern.

Hinweis zur Einstellung

- Ab Version 27.3.0 ist die Einstellung **EDT zulassen** nicht mehr in der App-Benutzeroberfläche verfügbar. Zuvor war diese Einstellung unter **Einstellungen > Erweitert > Adaptive Transport-Einstellungen > EDT zulassen** verfügbar.

  EDT bleibt als administratorgesteuerte Einstellung verfügbar. Dieses Update vereinfacht die App-Erfahrung und bietet eine konsistente EDT-Konfiguration durch administrative Richtlinien.
- Ab Version 26.11.0 werden die Methoden zur Store-Hinzufügung **Automatische Konfiguration**, **XenApp Services** und **Access Gateway** eingestellt. Die Option **Manuelle Einrichtung** wird entfernt. Die Option **Webinterface** wird entsprechend auf den Begrüßungsbildschirm verschoben und in **Als benutzerdefinierten Webstore hinzufügen** umbenannt.

Informationen zu eingestellten Elementen finden Sie auf der Seite Einstellung.

Behobene Probleme in 26.7.0

- Nach einer Zeit der Inaktivität kann die Citrix Workspace-App den Bildschirm **Erste Schritte** anzeigen. Dies geschieht auch dann, wenn der Benutzer bereits bei einem Store angemeldet ist.
- Wenn Sie die Citrix Workspace-App für iOS Version 2509 verwenden, können Sitzungsstarts mit der Fehlermeldung **Der Sitzungsstart wurde beendet; entweder war die Sitzung für den Benutzer nicht sichtbar, oder die ICA-Engine wurde nicht ordnungsgemäß geladen** fehlschlagen.
- Wenn Sie versuchen, eine veröffentlichte App über die Citrix Workspace-App zu starten, wobei die Startmethode auf Webbrowser eingestellt ist, kann der Start mit der Fehlermeldung **ICA konnte nicht abgerufen werden** fehlschlagen.
- Möglicherweise können Sie keine Doppelbyte-Zeichen in einer VDA-Sitzung einfügen, wenn Sie die Citrix Workspace-App für iOS verwenden.
- Auf dem iPad mit der Citrix Workspace-App für iOS 26.3.0 kann die App einfrieren, wenn Sie Store-Anmeldeinformationen eingeben, und der Enumerationsbildschirm wird möglicherweise nicht angezeigt.

- Wenn Sie ein externes Display im Präsentationsmodus verwenden, kann der Cursor auf dem iPad nach lokaler Interaktion nicht mehr reagieren und möglicherweise nicht auf den externen Bildschirm zurückkehren.
- Möglicherweise wird die Fehlermeldung **Sitzungsfehler, ICA konnte nicht abgerufen werden** angezeigt, wenn Sie eine geschützte Ressource von einem Store starten, der im Web-Interface-Modus in der Citrix Workspace-App für iOS 25.11 hinzugefügt wurde.

Bekannte Probleme in 26.7.0

Wenn Sie eine geschützte Sitzung auf einem iPhone starten, kann ein weißer Bereich am oberen Bildschirmrand erscheinen, wodurch die Windows-Taskleiste verschwindet. Um dieses Problem zu umgehen, ändern Sie die Geräteausrichtung auf Querformat.

Neuerungen in 26.3.10

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Behobene Probleme in 26.3.10

- Das Hinzufügen eines Stores kann fehlschlagen, wenn Citrix Gateway über *http* mit StoreFront verbunden ist.

Bekannte Probleme in 26.3.10

Es gibt keine neuen bekannten Probleme.

Neuerungen in 26.3.0

Verbessertes Audio-Einheiten-Management

Ab Version 26.3.0 wurde die Stereo-Audioverarbeitung für eine verbesserte Kompatibilität mit iOS 26 verfeinert. Sie bietet verbesserte Stabilität, Klarheit und eine höhere Klangqualität.

Verbesserte Sitzungswiederherstellung (Technical Preview)

Ab Version 26.3.0 wurden die folgenden Verbesserungen an der in der Version 25.11.0 angekündigten Funktion „Verbesserte Sitzungs-Timeout-Erfahrung (Technical Preview)“ vorgenommen:

- Anzeige spezifischer Gründe für Sitzungs-Timeouts, z. B. **Gerätesperre** oder **App im Hintergrund** oder **Netzwerkunterbrechung**.

- Die Einstellung für die Sitzungswiederherstellung kann entweder über GACS durch Aktivieren der Option **Manuelle Sitzungswiederherstellung** unter **Sitzungserfahrung > Konnektivität** oder über MDM konfiguriert werden.

IdP-Abmeldung bei WSP Inaktivitätstimeout

Ab Version 26.3.0 führt die Citrix Workspace-App eine Einstellung **Identitätsanbieter nach Inaktivitätstimeout** im Workspace-Portal ein. Diese Einstellung ermöglicht es Administratoren, Benutzer vom Identitätsanbieter (z. B. Microsoft Entra ID) abzumelden, wenn sich Benutzer von der Citrix Workspace-App abmelden. Diese Funktion funktioniert mit Stores, für die die Multi-Faktor-Authentifizierung (MFA) konfiguriert ist.

Unterstützung des EDT-Lossy-Modus für SecureHDX-Verbindungen

Ab Version 26.3.0 funktioniert der EDT (Enlightened Data Transport) Lossy-Modus (unzuverlässiger Subkanal) auch über SecureHDX-Verbindungen (SecureICA 2.0). Zuvor funktionierte EDT Lossy nur mit DTLS-verschlüsselten Verbindungen. Diese Verbesserung erweitert die Unterstützung für unzuverlässige Subkanäle auf SecureHDX-Verbindungen. Sie verbessert die Echtzeitleistung für latenzempfindliche Protokolle wie Audio und Video, wenn SecureICA 2.0 aktiviert ist. Weitere Informationen finden Sie unter EDT Lossy-Modus unterstützt jetzt SecureHDX

Unterstützung dynamischer Tastatureinstellungen während einer aktiven HDX-Sitzung

Ab Version 26.3.0 werden Tastatureinstellungen, die während einer aktiven HDX-Sitzung geändert werden, sofort wirksam. Dadurch entfällt die Notwendigkeit, die bestehende Sitzung zu trennen und erneut zu verbinden, was bisher der Fall war.

Always On Tracing (AOT)

Ab Version 26.3.0 führt die Citrix Workspace-App für iOS Always On Tracing (AOT) ein, ein modernes Diagnosesystem von Citrix. AOT sammelt kontinuierlich relevante Protokolldaten in der gesamten Citrix Virtual Apps and Desktops (CVAD)-Umgebung. Es basiert auf Citrix Diagnostic Facility (CDF)-Traces und fügt Komponentenprotokolle hinzu, um die Fehlerbehebung bei häufigen Problemen wie VDA-Registrierungsfehlern und Problemen beim Starten von Apps oder Desktops zu unterstützen. AOT läuft automatisch im Hintergrund und stellt sicher, dass wichtige Diagnosedaten verfügbar sind, wenn Probleme auftreten, selbst wenn Sie das Problem nicht reproduzieren können.

AOT vereinfacht die Fehlerbehebung für IT-Administratoren und Citrix Support-Teams durch:

- Automatisches Erfassen von Sitzungs- und Systemprotokollen ohne manuelle Schritte.
- Bereitstellung von leicht zugänglichen, lesbaren Protokollen.
- Ermöglichung von Self-Service-Diagnosen.
- Reduzierung der Abhängigkeit vom Citrix Support und Sicherstellung einer schnelleren mittleren Reparaturzeit (MTTR).
- Erleichterung der Eskalation durch vollständigen Diagnosekontext.
- Sichere Handhabung von Protokollen mit Schwärzung sensibler Daten.

Voraussetzungen und detaillierte Konfigurationsinformationen finden Sie in der Citrix Always On Tracing-Dokumentation.

Verbesserte Stabilität für Menüleisten- und Bildschirmtastaturfunktionen

Release 26.3.0 enthält die folgenden Verbesserungen, die an die Plattformänderungen in iPadOS 26 angepasst sind:

- Die App blendet die erweiterte Tastatur aus, wenn Sie die Geräteausrichtung ändern.
- Tastatur und Maus funktionieren möglicherweise in einer Multi-Monitor-Einrichtung nicht, wenn Sie **Erweiterte Anzeige** unter **Geräteeinstellungen > Anzeige & Helligkeit** aktivieren und dann in den **Citrix Workspace-App-Einstellungen** deaktivieren.

Behobene Probleme in 2603

- Wenn Sie über die Citrix Workspace-App eine Verbindung zu einem Linux-VDA herstellen, wird die Clientkamera möglicherweise nicht erkannt oder ist nicht verwendbar, während sie auf einem Windows-VDA funktioniert.
- Nachdem Sie die Citrix Workspace-App beendet haben, während Sie sich auf der Seite des sekundären Stores befanden, und sie erneut starten, wird die Enumerationsseite des primären Stores geöffnet.
- Möglicherweise wird der Fehlercode „Error code: 403“ angezeigt, wenn Sie versuchen, eine Store-URL in der Citrix Workspace-App für iOS Version 25.7.0 hinzuzufügen.
- Wenn das schwebende Fenster aktiviert ist, wird die benutzerdefinierte Auflösungseinstellung möglicherweise nicht beibehalten, nachdem Sie zu einer anderen App wechseln und zur Citrix Workspace-App zurückkehren.
- Änderungen, die Sie an den Anzeigeoptionen im Web-Interface-Modus vornehmen, werden beim Neustart der Citrix Workspace-App auf die Standardwerte zurückgesetzt.

- Nach dem Upgrade der Citrix Workspace-App auf Version 25.11.0- können Fehler beim Starten von Sitzungen auftreten.
- Möglicherweise erhalten Sie den Fehler *Der Sitzungsstart wurde beendet; entweder war die Sitzung für den Benutzer nicht sichtbar, oder die ICA-Engine wurde nicht richtig geladen*, wenn Sie VDA-Sitzungen in der Citrix Workspace-App Version 25.9.0 starten.

Bekannte Probleme in 2603

Es gibt keine neuen bekannten Probleme.

Neuerungen in 25.11.0

Nahtlose Integration von deviceTRUST® in die Citrix Workspace™-App für iOS

Ab Version 25.11.0 enthält die Citrix Workspace-App für iOS deviceTRUST, das die Sicherheit durch kontinuierliche Überprüfung der Gerätehaltung innerhalb der Sitzung verbessert. deviceTRUST ist für eine einheitliche Bereitstellung in die Citrix Workspace-App integriert. Weitere Informationen finden Sie unter deviceTRUST.

Wichtige Details:

- **Integrierte Funktionalität:** Ab Version 25.11.0 oder höher wird die deviceTRUST Client Extension standardmäßig als Teil der Citrix Workspace-App für iOS installiert, was die Bereitstellung und Verwaltung vereinfacht.
- **Kontinuierliche Haltungsprüfungen:** Diese Funktion verbessert die Sicherheit, indem sie kontinuierliche Prüfungen des Kontexts und der Sicherheitshaltung des Endgeräts innerhalb der Sitzung durchführt und so zur Implementierung eines Zero-Trust-Sicherheitsmodells beiträgt.
- **Kompatibilität:** Die Integration wird auf iOS-Versionen 17, 18 und 26 unterstützt.
- **Administration:** Administratoren können die deviceTRUST-Konsole verwenden, um Richtlinien zu konfigurieren und Gerätezustandseinstellungen zu verwalten. Weitere Informationen zur Konfiguration finden Sie unter Erste Schritte für Lokal

Verbesserte Bildschirmtastatur-Erfahrung

Ab Version 25.11.0 hat Citrix die Erfahrung mit der Bildschirmtastatur durch Verbesserungen des automatischen Tastaturanzeigeverhaltens beim Verbinden mit Windows Virtual Desktop Agent (VDA) 25.11.0 Desktops verbessert.

Diese Verbesserungen erhöhen die Benutzerfreundlichkeit bei der Interaktion mit Eingabefeldern und Taskleistenelementen, die am unteren Rand der Desktopsitzung erscheinen, während die Bildschirmtastatur verwendet wird.

Verbesserte Sitzungs-Timeout-Erfahrung (Technische Vorschau)

Diese Initiative zielt darauf ab, die Endbenutzererfahrung bei Sitzungs-Timeouts, die durch Inaktivität oder Netzwerkunterbrechungen verursacht werden, zu verbessern. Benutzern von Cloud- und On-Premises-Stores wird die Möglichkeit geboten, sich direkt vom Timeout-Bildschirm aus wieder zu verbinden, wodurch das erneute Starten von Sitzungen über die Client-Benutzeroberfläche entfällt.

Hauptmerkmale:

- Der Timeout-Bildschirm zeigt spezifische Gründe für Sitzungs-Timeouts an, wie z. B. **Gerät ging in den Ruhezustand** oder **Netzwerkunterbrechung**.
- Benutzer können sich nahtlos wieder mit der Sitzung verbinden, sei es eine neue Sitzung oder eine Fortsetzung der vorherigen Sitzung, basierend auf der Administratorkonfiguration.
- Die Lösung unterstützt Wiederverbindungsszenarien, bei denen die automatische Wiederverbindung fehlschlagen könnte, wie z. B. bei Netzwerkwechseln (zum Beispiel Wi-Fi zu LAN).

> **Hinweis:**
>
> Diese Funktion wird derzeit nicht für Sitzungen unterstützt, die über den Browser gestartet werden, oder für Stores, die als Web Interface hinzugefügt wurden.

> Weitere Informationen zum Aktivieren dieser vom Administrator gesteuerten Funktion finden Sie in der HDX-Dokumentation für Citrix Virtual Apps and Desktops.

Unterstützung für Anti-Screen-Capture und Anti-Keylogging in benutzerdefinierten Web-Stores

Ab Version 25.11.0 werden App Protection **Anti-Screen-Capture** und **Anti-Keylogging** nun in benutzerdefinierten Web-Stores unterstützt.

User-Agent für Web Interface

Ab Version 25.11.0 enthält der User-Agent-String, der bei einigen über Web Interface initiierten Netzwerkanfragen verwendet wird, standardmäßig den Bezeichner der Citrix Workspace-App.

Vor der Änderung war der User-Agent: `Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148`

Nach der Änderung ist der User-Agent:

`Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148`

`CWA/25.11.0 iOS/26.2 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad`

Nahtloses Single Sign-On für Entra ID-verbundene VDAs unter iOS

Ab Version 25.11.0 unterstützt die Citrix Workspace-App für iOS nahtloses Single Sign-On (SSO) mit Microsoft Entra ID-verbundenen VDAs in Cloud-Bereitstellungen. Zuvor wurden Benutzer beim Starten von HDX-Sitzungen mit Microsoft Entra ID-verbundenen VDAs zur Eingabe von Anmeldeinformationen aufgefordert, da SSO für dieses Szenario nicht verfügbar war. Diese Änderung bietet Administratoren die Möglichkeit, SSO zu konfigurieren – die Notwendigkeit, Anmeldeinformationen beim Start der Sitzung einzugeben, kann entfallen, wodurch die Authentifizierung für Organisationen, die Entra ID als primären Identitätsanbieter verwenden, optimiert wird.

Mit dieser Funktion können Benutzer, die von Active Directory zu Entra ID migrieren, Sitzungen ohne manuelle Eingabe von Anmeldeinformationen starten, was eine verbesserte und vereinfachte Authentifizierungserfahrung bietet. Informationen zur Systemkompatibilität und den End-to-End-Konfigurationsschritten finden Sie unter Microsoft Entra Single Sign-On.

Behobene Probleme in 25.11.0

- Es kann vorkommen, dass die Citrix Workspace-App während eines Teams-Anrufs abstürzt, wenn ein USB-C-auf-3,5-mm-Kopfhörerbuchsenadapter an Ihr Gerät angeschlossen ist.
- Es kann vorkommen, dass die Citrix Workspace-App abstürzt, wenn Sie auf die von SPA bereitgestellte Visma Web-App zugreifen.
- Die Citrix Workspace-App für iOS bleibt möglicherweise nach der Eingabe der Store-Anmeldeinformationen im Dialogfeld „Ihre Dienste werden abgerufen“ hängen.

- Möglicherweise sind Probleme bei der Authentifizierung mit FIDO2 über den Systemauthentifizierungsbrowser in einem lokalen Store aufgetreten, der mit GACS konfiguriert ist.
- Möglicherweise treten Probleme auf, wenn Sie versuchen, ein Konto in der Citrix Workspace-App für iOS 24.9.0 mithilfe abgeleiteter Anmeldeinformationen hinzuzufügen.
- Möglicherweise treten Inkonsistenzen bei der Pinch-&-Zoom-Funktionalität in der Citrix Workspace-App 25.7.2 nach dem Upgrade von Version 25.3.1 auf.
- Möglicherweise haben Sie in früheren Versionen der Citrix Workspace-App für iOS inkonsistente Transporte beim Wiederverbinden von EDT-Sitzungen nach einer Netzwerkunterbrechung erlebt. Die aktualisierte Version behält nun das zuletzt erfolgreiche Protokoll bei, verwendet EDT, wenn verfügbar, und greift nur dann auf TCP zurück, wenn EDT nicht verfügbar ist.

Bekannte Probleme in 25.11.0

Es gibt keine neuen bekannten Probleme.

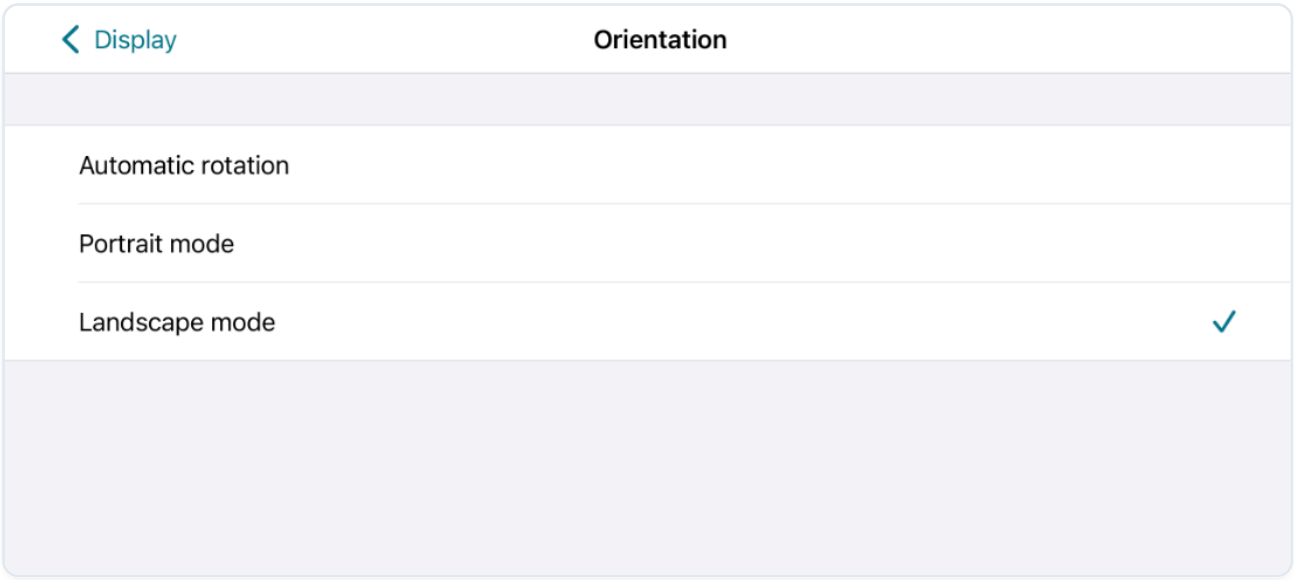
Neuerungen in 25.9.0

Verbesserte Fehlerbehebung mit Citrix Troubleshoot Connection

Bisher erforderte die Behebung von Problemen beim Starten virtueller Apps oder Desktops traditionell IT-Support. Mit der erweiterten Funktion „Citrix Troubleshoot Connection“ ermöglicht die Citrix Workspace-App Benutzern über eine überarbeitete Benutzeroberfläche, Startprobleme selbst zu beheben und zu beheben, indem sie klare Fehlermeldungen und Schritt-für-Schritt-Empfehlungen bereitstellt. Benutzer sehen den detaillierten Fehler und eine Schaltfläche zur Behebung des Problems. Sie können häufige Probleme wie Netzwerkprobleme oder nicht verfügbare Ressourcen mit Ein-Klick-Wiederherstellungsaktionen beheben. Dies reduziert Ihren Bedarf an IT-Support und hilft Ihnen, schneller wieder an die Arbeit zu gehen. Weitere Informationen finden Sie unter Citrix Troubleshoot Connection.

Unterstützung des Querformatmodus auf dem iPhone

Die Funktion umfasst auch die Unterstützung des Querformatmodus auf dem iPhone für eine bessere Fehlerbehebung auf Ihrem Gerät. Diese Einstellung ermöglicht es Ihnen, die Ausrichtung der App für eine optimale Anzeige von Desktop-Inhalten und datenintensiven Bildschirmen auszuwählen. Mit Version 2509 ist die Standardausrichtung **automatische Drehung**.



Verbessertes Desktop-Start-Erlebnis

Ab Version 2509 gewährleistet die Citrix Workspace-App für iOS ein verbessertes Desktop-Start-Erlebnis. Benutzer erleben einen nahtlosen, flimmerfreien Übergang zum Desktop ohne Zwischenbildschirme. Die App eliminiert außerdem schwarze Bildschirme und Flimmern beim Ändern der Größe oder Strecken und bietet so eine stabile und moderne Benutzeroberfläche. Diese Funktion ist standardmäßig aktiviert.

Verbesserte Feststelltasten-Synchronisierung für externe Tastaturen

Ab Version 2509 verbessert die Citrix Workspace-App für iOS die Handhabung der Feststelltasten-Synchronisierung, wenn Sie externe Tastaturen verwenden. Die App stellt sicher, dass der Feststelltasten-Status zwischen dem iOS-Client und dem Virtual Delivery Agent (VDA) konsistent bleibt und bietet Ihnen ein nahtloses Tipperlebnis. Das Wechseln zwischen lokalen iOS-Apps und Citrix-Sitzungen führt nicht mehr zu inkonsistenten Groß- oder Kleinbuchstabeneingaben.

Verbesserungen bei der Synchronisierung von Audiogeräten und Lautstärke

Wir haben verbessert, wie Audiogeräte und Lautstärke in Ihren virtuellen Sitzungen verwaltet werden:

Verbesserte Audiogeräte-Synchronisierung: Nur Ihr aktuell ausgewähltes System-Audiogerät wird jetzt dem Virtual Delivery Agent (VDA) zugeordnet, wodurch eine unnötige Gerätezordnung verhindert wird. Der tatsächliche Name des Geräts bleibt erhalten, was die Identifizierung innerhalb Ihrer Sitzung erleichtert.

Verbesserte Audio-Lautstärke-Synchronisierung: Die Lautstärke des Lautsprechers wird jetzt unidirektional von Ihrem System zum VDA synchronisiert. Außerdem können Sie jetzt die

Mikrofonverstärkung direkt im VDA anpassen, und die Citrix Workspace-App speichert diese Einstellung zur Verwendung in zukünftigen Sitzungen.

Abkündigungsbenachrichtigungen für veraltete Funktionen

Ab Version 26.3.0 unterstützt die Citrix Workspace-App für iOS die folgenden veralteten Funktionen nicht mehr. Die Unterstützung für die folgenden Funktionen wird eingestellt:

- Citrix X1 Mouse
- Citrix Casting

Weitere Informationen finden Sie unter Abkündigung der Citrix Workspace-App für iOS

Behobene Probleme in Version 25.9.0

- Möglicherweise stellen Sie fest, dass die erweiterte Symbolleisten-Benutzeroberfläche auf iOS 26-Geräten angezeigt wird, wenn die Sitzung in den Fenstermodus wechselt.
- Möglicherweise stellen Sie fest, dass die Bildschirmtastatur auf iOS 26-Geräten verschwindet, wenn Sie das Fenster der Citrix Workspace-App in der Größe ändern.
- Beim Starten einer Sitzung erkennt die Citrix Workspace-App möglicherweise keine auf dem Yubikey vorhandenen Zertifikate auf dem Sitzungsstartbildschirm.
- Auf iPhone-Geräten können Sie sich möglicherweise nicht im Store anmelden, wenn Sie die Citrix Workspace-App für iOS verwenden.
- Auf iPad-Geräten wird Audio möglicherweise nicht an den 2203 VDA umgeleitet, wenn Sie die Citrix Workspace-App für iOS verwenden.
- Bei der Verwendung von AirPods mit der Citrix Workspace-App für iOS hören Sie möglicherweise keine Klingeltöne in einer Sitzung.
- Über einen USB-C-Hub angeschlossene Audiogeräte funktionieren möglicherweise nicht mit Skype in der Citrix Workspace-App für iOS.
- Möglicherweise stellen Sie fest, dass die Lautstärke einer in Windows Media Player innerhalb einer Sitzung abgespielten Audiodatei nicht mit den Lautstärketasten des Geräts erhöht oder verringert werden kann.
- Die Audiowiedergabe kann nach dem Fortsetzen der Aufnahme über Audacity stoppen.
- Möglicherweise stellen Sie fest, dass die Citrix Workspace-App abstürzt, wenn Sie versuchen, sich vom Store abzumelden, während die Netzwerkverbindung deaktiviert ist.

- Auf iPad-Geräten kann die Citrix Workspace-App abstürzen, wenn sie mit einem externen Monitor verbunden ist, während ein Sitzungsstart läuft.

Bekannte Probleme in 25.9.0

- Es kann vorkommen, dass die Citrix Workspace-App während eines Teams-Anrufs abstürzt, wenn ein USB-C-auf-3,5-mm-Kopfhörerbuchsenadapter an Ihr Gerät angeschlossen ist.
- Beim Entsperren des Geräts, nachdem es für einige Zeit gesperrt war, kann es zu einer Verkürzung des Sitzungsbildes kommen.

Frühere Versionen

Dieser Abschnitt enthält Informationen zu neuen Funktionen und behobenen Problemen in den früheren Releases, die wir unterstützen. Weitere Informationen zum Lebenszyklus dieser Releases finden Sie unter Lebenszyklus-Meilensteine für Citrix Workspace-App und Citrix Receiver.

25.7.2

Neuigkeiten

Unterstützung für iOS 26

Die Citrix Workspace-App für iOS unterstützt jetzt iOS 26. Weitere Informationen zu iOS 26 finden Sie im Blog iOS26

Verbesserte Anzeige der Verbindungsstärke

Die Anzeige der Verbindungsstärke bietet Echtzeit-Einblicke in Ihre Verbindungsqualität und hilft bei der Selbstbehebung von Verbindungsproblemen. Diese Funktion ist über die Symbolleiste zugänglich und standardmäßig aktiviert. Ab Version 25.7.2 haben wir die Anzeige verbessert und bieten Einblicke in:

- **Echtzeit-CPU-, Arbeitsspeicher- und Festplattenauslastung** auf Ihrem lokalen Gerät. Dies gibt Benutzern Aufschluss darüber, ob eine verminderte Leistung auf eine überlastete Endpunkt-Rechenleistung zurückzuführen ist.
- **Verbindungsverlauf**, der Einblicke in die Aktivitäten der letzten 15 Minuten bietet und anzeigt, ob die Verbindung durchweg stabil war oder zeitweise Unterbrechungen aufwies.

- **Echtzeit-Empfehlung** – Die Anzeige der Verbindungsstärke versucht, dem Benutzer potenzielle Empfehlungen zu geben, die ihm helfen können, das Verbindungsproblem zu lösen, bevor er ein Support-Ticket erstellt.

Weitere Informationen finden Sie unter Verbesserte Anzeige der Verbindungsstärke.

Desktops und Apps automatisch starten

Ab Version 25.7.2 startet die Citrix Workspace-App für iOS automatisch einen Desktop oder eine App, die von Administratoren in Citrix Studio mit `KEYWORDS: AutoStartPrimaryApp` gekennzeichnet wurde. Diese Funktionalität funktioniert sowohl in Cloud- als auch in On-Premises-Stores. Weitere Informationen finden Sie unter Desktops und Apps automatisch starten

Unterstützung für iPad und iPhone im Sperrmodus

Ab Version 25.7.2 unterstützt die Citrix Workspace-App für iOS den Sperrmodus auf iPad und iPhone. Wenn der Sperrmodus aktiviert ist, sind bestimmte Gerätefunktionen absichtlich eingeschränkt.

Behobene Probleme in 25.7.2

Es gibt keine neuen behobenen Probleme.

25.5.10

Neuigkeiten

Diese Version enthält kleinere Fehlerbehebungen, und die Citrix Workspace-App für iOS unterstützt jetzt iOS 26.

Behobene Probleme

In dieser Version gibt es keine behobenen Probleme.

25.5.0

Neuigkeiten

Verbesserte Zeigermodus-Erfahrung

Ab Version 25.5.0 unterstützt die Citrix Workspace-App für iOS das Scrollen und Zoomen innerhalb einer Sitzung bei Verwendung des Zeigermodus. Im Zeigermodus kann der Benutzer jetzt:

- Mit einer Zwei-Finger-Wischbewegung (vertikal oder horizontal) in die entsprechende Richtung scrollen.
- Den Sitzungsinhalt durch Tippen und Halten mit zwei Fingern und anschließendem Auf- oder Zuziehen zoomen.

Hinweis:

Standardmäßig führt ein Zwei-Finger-Auf- oder Zuziehen einen lokalen Zoom aus. Um einen Remote-Zoom auszuführen, tippen und halten Sie zwei Finger für einige Sekunden, bis die Meldung „Remote-Zoom aktiviert“ angezeigt wird, und fahren Sie dann mit dem Zoomen fort.

Update zur Sichtbarkeit der Tastatureinstellungen

Ab Version 25.5.0 der Citrix Workspace-App für iOS sind die Tastatureinstellungen jetzt auch sichtbar, wenn kein Store konfiguriert ist. Zuvor war die Tastaturoption in der Citrix Workspace-App erst nach dem Hinzufügen eines Stores sichtbar. In der Kundenumgebung funktionierte diese Funktionalität wie erwartet, und die Synchronisierung war nach dem Hinzufügen des Stores erfolgreich. Der Kunde hat jedoch angegeben, dass er den Store aufgrund von Sicherheitseinschränkungen nicht zur Citrix Workspace-App hinzufügen kann.

Dieses Update stellt sicher, dass Benutzer, die aufgrund von Sicherheitsrichtlinien keinen Store hinzufügen können, weiterhin auf die Tastatureinstellungen zugreifen und diese bei Bedarf ändern können.

Reibungslose Desktop-Größenänderung

Bei der Größenänderung des Bildschirms oder bei Änderungen des Fenstermodus können schwarze Bildschirme oder Flackern auftreten. Diese Funktion verbessert die Benutzererfahrung, indem sie diese Probleme beseitigt und einen reibungslosen und nahtlosen Übergang beim Ändern der Größe oder Strecken des Bildschirms bietet.

Unterstützung für schwebende Sitzungsfenster

Beim Wechseln zwischen Apps in einer VDA-Sitzung auf Mobilgeräten kann es zu Unterbrechungen oder Verbindungsabbrüchen kommen. Dieses Problem tritt häufig beim Multitasking auf, z. B. bei der Teilnahme an Besprechungen oder der Durchführung einer MFA-Authentifizierung. Diese Funktion verbessert die Benutzererfahrung, indem sie eine unterbrechungsfreie Sitzungsleistung, z. B. bei Audio und Grafik, gewährleistet, selbst wenn die App im Hintergrund ausgeführt wird. Sie ermöglicht Benutzern, nahtlos Multitasking zu betreiben,

ohne sich Gedanken über Sitzungs-Timeouts oder den Verlust der Sichtbarkeit machen zu müssen. Diese Funktion bietet einen zuverlässigeren und effizienteren Workflow für Geräte, die den Stage Manager nicht unterstützen.

Einschränkung

Diese Funktion funktioniert unter iOS 18.0 und höher.

- Die Multitasking-Kamera wird aufgrund unterschiedlicher Geräte-Chip-Fähigkeiten möglicherweise nicht unterstützt.
- Multi-Monitor-Szenarien werden nicht unterstützt.

Behobene Probleme

- Möglicherweise können Sie sich nicht mit der Azure Multi-Faktor-Authentifizierung authentifizieren.
- Wenn die Konfiguration der Citrix Workspace™-App unter iOS über Intune bereitgestellt wird, stellen Sie möglicherweise fest, dass mehrere Stores angezeigt werden, obwohl nur ein lokaler Store als sichtbar konfiguriert ist.

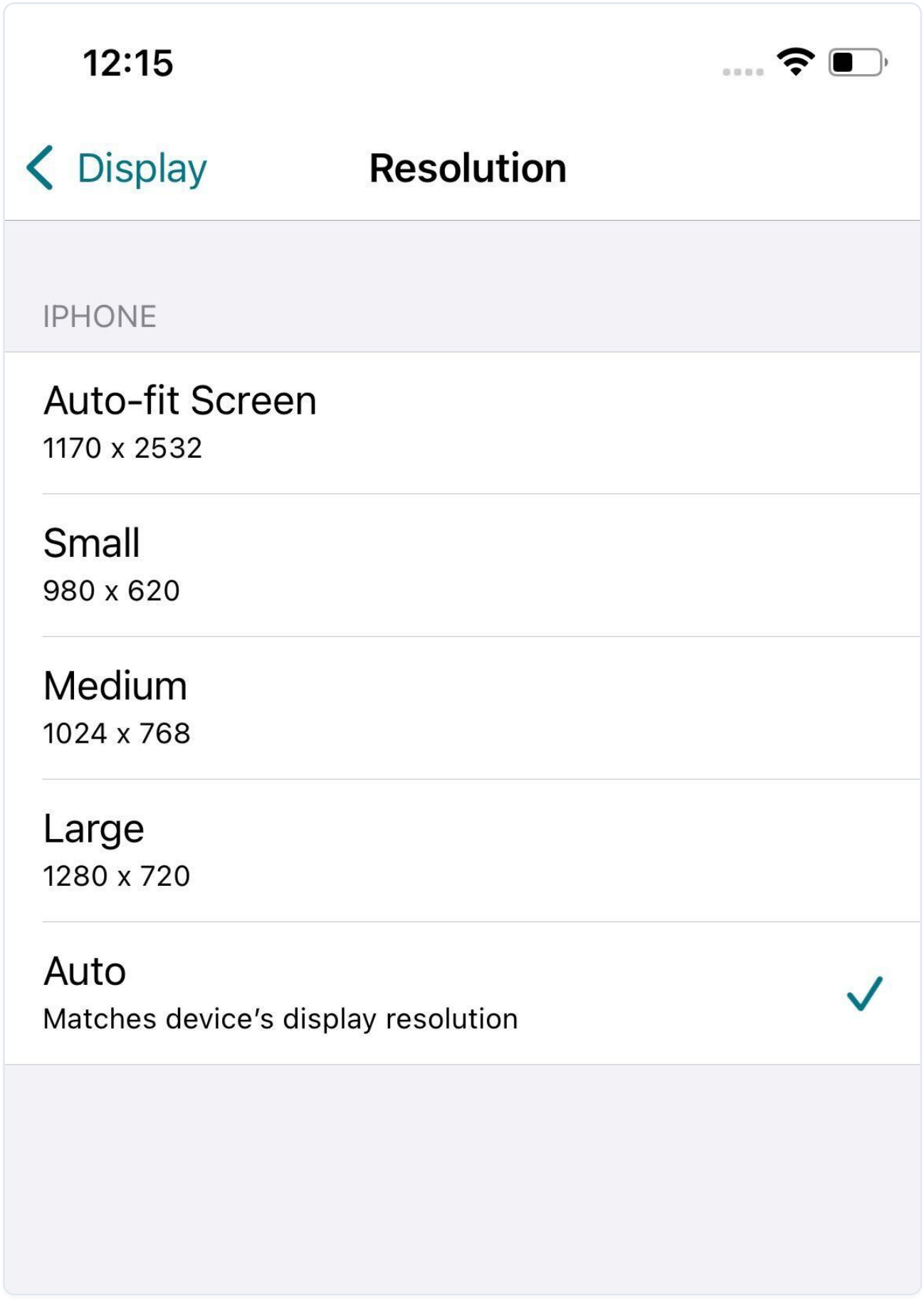
25.3.4

Neuigkeiten

Verbesserte Sitzungsauflösung

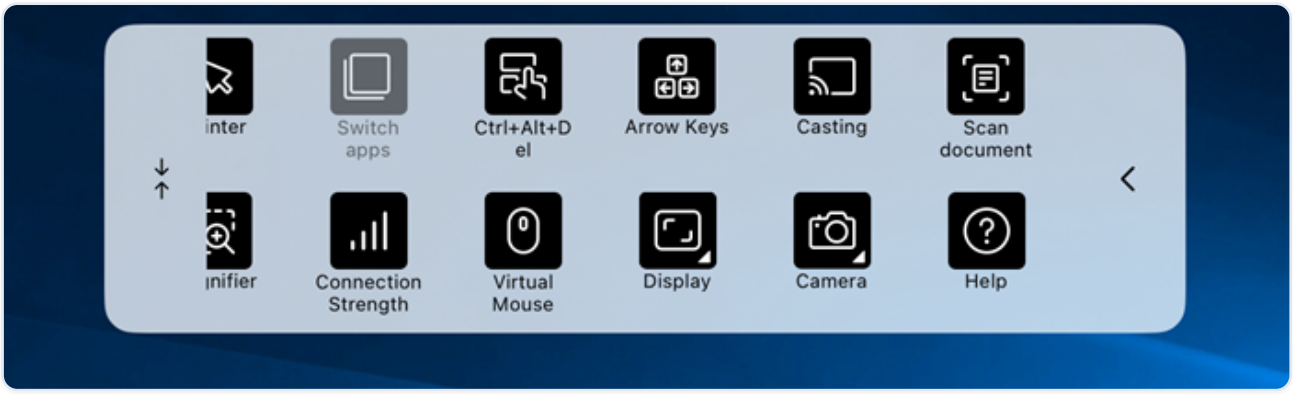
Ab Version 25.3.4 bietet die Citrix Workspace-App für iOS Verbesserungen bei der Sitzungsauflösung für eine nahtlosere Benutzererfahrung. Die **DPI**-Einstellungen, die standardmäßig auf „Auto“ stehen, passen sich automatisch an, sobald ein Benutzer eine Sitzung startet, was die gesamte Erfahrung verbessert.

Um eine konsistente und benutzerfreundliche Erfahrung zu gewährleisten, starten virtuelle Desktops standardmäßig im Querformat. Dies berücksichtigt Breitbildanwendungen und Multitasking-Anforderungen. Diese Funktion ist standardmäßig aktiviert.


12:15
Display
Resolution
IPHONE
Auto-fit Screen
1170 x 2532
Small
980 x 620
Medium
1024 x 768
Large
1280 x 720
Auto
Matches device's display resolution

Neue In-Session-Symbolleiste

Ab Version 25.3.4 ist die neue Symbolleiste standardmäßig aktiviert, wenn keine Administratoreinstellung über den Global App Configuration Service (GACS) und Mobile Device Management (MDM) konfiguriert ist.



Behobene Probleme

- Nach dem Upgrade auf Citrix Workspace-App für iOS Version 25.3.4 kann bei einigen Benutzern der folgende Fehler auftreten, wenn sie versuchen, Sitzungen zu starten: The operation couldn’t be completed (HDXSDKErrorDomain_Session Error 8).
- Einige iPad-Benutzer auf VDA 2402 und 2402 CU1 können andere während Anrufen in Apps wie Skype oder Webex nicht hören. Betroffene Benutzer können die Medienwiedergabe aus der Sitzung hören, aber nicht die Person am anderen Ende. Das Trennen und erneute Verbinden des Audios kann eine vorübergehende Problemumgehung darstellen.
- Es kann vorkommen, dass der Zeiger in der Symbolleiste aktiviert wird, wenn das Batteriesymbol in der Taskleiste in einem Windows-VDA angeklickt wird.
- Wenn eine physische Maus an einem iPad-Gerät angeschlossen ist, kann es vorkommen, dass die Symbole für Lupe und Zeiger nicht automatisch deaktiviert werden.
- iPadOS: Firebase-Foundation _userInfoForFileAndLine-AppSwitcher.

25.1.2

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Behobene Probleme

Die Citrix Workspace-App für iOS stellt möglicherweise keine Sitzung her, wenn ein Benutzer mit einem bestimmten VPN verbunden ist.

25.1.1

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

> **Wichtig:**
>
> Die Version 25.1.0 wurde aufgrund von Stabilitätsproblemen zurückgezogen. Die neue verfügbare Version ist 25.1.1. Dies bedeutet, dass der neueste Build 25.1.1 die Funktionen der Version 25.1.0 nicht enthält. Wir arbeiten an einem neuen stabilen Build, der alle Funktionen der Version 25.1.0 zusammen mit den notwendigen Korrekturen enthalten wird.

Behobene Probleme

Ähnlich dem vorherigen stabilen Build.

25.1.0

Neuigkeiten

- Verbesserte Citrix-Sicherheit mit vorausgefülltem Benutzernamen
- Unterstützt GACS-authentifizierte Microservices (On-Premises)
- Verbesserung des Cross-Multi-Screen-Erlebnisses
- DPI-Anpassung
- Standardmäßige Querformatausrichtung für virtuelle Desktops
- Verbessertes gesichertes ICA
- Verbesserter Mauszeigermodus

Verbesserter Mauszeigermodus

Ab Version 25.1.0 führt die Citrix Workspace-App für iOS Verbesserungen am Mauszeigermodus ein. Mit dieser Funktion werden die folgenden Verbesserungen eingeführt, die eine reibungslosere und konsistentere Erfahrung bieten:

- Der Mauszeiger bewegt sich jetzt natürlicher, indem die Wischgeschwindigkeit verwendet wird.
- Der Mauszeigermodus ist jetzt auf iPhones verfügbar, ähnlich wie auf iPads.

Hinweis:

Ab dieser Version werden Sitzungen auf iPhones standardmäßig im Multitouch-Modus gestartet, sodass Sie den In-Session-Zoom mit einer Pinch-Geste ausführen können. Um den clientseitigen (Viewport-)Zoom zu verwenden, muss der Zeigermodus aktiviert werden.

Verbesserte Citrix®-Sicherheit mit vorausgefülltem Benutzernamen

Ab Version 25.1.0 können Sie Unified Endpoint Management (UEM) verwenden, um den Benutzernamen in einem bestimmten Format an verwaltete Geräte zu übertragen. Unter iOS liest die Citrix Workspace-App diese Konfiguration, ruft den Benutzernamen ab und füllt ihn im Authentifizierungsdialogfeld voraus, wodurch er schreibgeschützt wird. Weitere Informationen finden Sie unter Verbesserte Citrix-Sicherheit mit vorausgefülltem Benutzernamen.

Unterstützt GACS-authentifizierte Microservices (On-Premises)

Ab Version 25.1.0 unterstützt die Citrix Workspace-App für iOS authentifizierte Microservices, wodurch GACS Benutzergruppen verwalten kann. Diese Funktion bietet Administratoren eine verbesserte Kontrolle für lokale Umgebungen. Weitere Informationen finden Sie unter Unterstützt GACS-authentifizierte Microservices (On-Premises).

Verbesserung der geräteübergreifenden Multi-Screen-Erfahrung

Ab Version 25.1.0 verbessert die Citrix Workspace-App für iOS die Benutzererfahrung für iPads, die an externe Monitore oder Docks angeschlossen sind. Diese Updates umfassen die Möglichkeit, Anwendungen über mehrere Bildschirme zu verteilen, um das Multitasking zu verbessern. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Verbesserung der geräteübergreifenden Multi-Screen-Erfahrung.

DPI-Anpassung

Die DPI-Anpassungsfunktion stellt sicher, dass die virtuelle Sitzung entsprechend der DPI des Geräts gerendert wird. Ab Version 25.1.0 verbessert eine neue Anzeigeeinstellung die DPI-Anpassungsfunktionen. Weitere Informationen finden Sie unter DPI-Anpassung.

Standard-Querformatausrichtung für virtuelle Desktops

Ab Version 25.1.0 erzwingt die Citrix Workspace-App standardmäßig die Querformatausrichtung, wenn ein virtueller Desktop auf iPhone-Geräten gestartet wird. Dies gewährleistet eine optimale und konsistente Benutzererfahrung für Breitbildanwendungen und Multitasking. Weitere Informationen finden Sie unter Standard-Querformatausrichtung für virtuelle Desktops.

Verbessertes gesichertes ICA®

Ab Version 25.1.0 verbessert die neue ICA-Verschlüsselungsfunktion die Sicherheit durch die Verwendung moderner Verschlüsselungsalgorithmen. Dies erhöht die Sicherheitslage unseres Produkts und bietet unseren Kunden anschließend eine Möglichkeit, die Sicherheitslage ihrer Umgebungen auf einfache und zuverlässige Weise zu verbessern. Weitere Informationen finden Sie unter Verbessertes gesichertes ICA.

Behobene Probleme in 25.1.0

Es gibt keine neuen behobenen Probleme in dieser Version.

24.12.0

Neuigkeiten

- Start der In-Memory-ICA-Lösung
- Schnelle Smartcard
- Unterstützung für lokale WSUI über Gateway
- Erzwingen des Citrix-Zugriffs mit der Citrix Workspace-App
- Unterstützung für Multi-Site-Store-Failover basierend auf dem geografischen Standort
- Zuordnung der rechten Optionstaste für die Alt-Taste
- Anzeige der Verbindungsstärke
- Verbesserte neue anpassbare Symbolleiste
- Veraltung des Betriebssystems iOS 15

Einführung der In-Memory-ICA-Lösung

Ab Version 24.12.0 verbessert die Citrix Workspace-App für iOS die Unterstützung für hybride In-Memory-Starts mithilfe des Citrix Workspace-Launchers. Diese Verbesserung ermöglicht eine effizientere und sicherere Benutzererfahrung, da das Herunterladen von ICA-Dateien entfällt. Weitere Informationen finden Sie unter Einführung der In-Memory-ICA-Lösung.

Schnelle Smartcard

Ab Version 24.12.0 führt die Citrix Workspace-App für iOS Smartcard-Verbesserungen für eine optimierte Authentifizierungsleistung und Benutzerfreundlichkeit ein. Dieses Update bringt erhebliche Verbesserungen bei der Smartcard-Unterstützung, wodurch die Benutzererfahrung reibungsloser und effizienter wird. Weitere Informationen finden Sie unter Schnelle Smartcard.

Unterstützung für WSUI On-Premises über Gateway

Ab Version 24.12.0 unterstützt die Citrix Workspace-App für iOS die Web-Benutzeroberfläche für den lokalen Store, der sich ebenfalls hinter dem Gateway befindet. Der Administrator muss diese Funktion konfigurieren, da sie standardmäßig nicht aktiviert ist. Weitere Informationen finden Sie unter Unterstützung für WSUI On-Premises über Gateway.

Erzwingen des Citrix-Zugriffs über die Citrix Workspace-App

Ab Version 24.12.0 können Administratoren Benutzer auf iOS-Geräten dazu verpflichten, ausschließlich über die native App auf Citrix Workspace zuzugreifen. Wenn diese Funktion aktiviert ist, werden Benutzer, die versuchen, auf die Store-URL und Browser von Drittanbietern zuzugreifen, automatisch zur Citrix Workspace-App umgeleitet. Dies stellt sicher, dass sie alle Funktionen der nativen App nutzen und eine nahtlose Benutzererfahrung genießen können. Weitere Informationen finden Sie unter Erzwingen des Citrix-Zugriffs über die Citrix Workspace-App.

Unterstützung für Multi-Site-Store-Failover basierend auf dem geografischen Standort

Ab Version 24.12.0 verbessert die Funktion zur Handhabung von Multi-Store-Failover die Multi-Store-Failover-Handhabung, indem Store-Adressprüfungen asynchron ausgeführt und veraltete Store-Einträge entfernt werden, wenn eine neue Failover-Store-Adresse erkannt wird. Weitere Informationen finden Sie unter Unterstützung für Multi-Site-Store-Failover basierend auf dem geografischen Standort.

Zuordnung der rechten Optionstaste zur Alt-Taste

Ab Version 24.12.0 führt die Citrix Workspace-App für iOS eine Verbesserung ein, die es Benutzern ermöglicht, die rechte Optionstaste in der Sitzung der Alt-Taste zuzuordnen. Weitere Informationen finden Sie unter Zuordnung der rechten Optionstaste zur Alt-Taste.

Anzeige der Verbindungsstärke

Ab Version 24.12.0 unterstützt die Citrix Workspace-App für iOS die Anzeige der Verbindungsstärke in der Symbolleiste des **Desktop Viewers**. Diese Funktion zeigt ein Symbol für die Netzwerkstärke an, das Sie auf Netzwerkprobleme aufmerksam macht. Weitere Informationen finden Sie unter Anzeige der Verbindungsstärke.

Verbesserte neue anpassbare Symbolleiste

Ab Version 24.12.0 führt die Citrix Workspace-App für iOS eine neue anpassbare Symbolleiste ein. Die überarbeitete Desktop Viewer-Symbolleiste verbessert die Benutzererfahrung und den Support

durch größere Flexibilität. Administratoren können die In-Session-Symbolleiste nun an die Anforderungen ihrer Organisation anpassen. Die Auswahl externer Webcams ist jetzt in der neuen Symbolleiste verfügbar. Weitere Informationen finden Sie unter Erweiterte neue anpassbare Symbolleiste.

Einstellung der Unterstützung für Betriebssystem iOS 15

Ab Version 24.12.0 wird die Unterstützung für das Betriebssystem iOS 15 eingestellt. Alternativ können Sie auf die neueste verfügbare iOS-Version aktualisieren. Weitere Informationen finden Sie unter Einstellung der Unterstützung.

Behobene Probleme in 24.12.0

- Es ist möglicherweise nicht möglich, ein Clientzertifikat zu löschen, wenn es in einer gelöschten Speichereinstellung installiert wurde.
- Es kann vorkommen, dass eine Sitzung auf dem sekundären Monitor aktiv bleibt, wenn ein Benutzer eine Sitzung über die Seitenleiste trennt.
- Beim Öffnen der Citrix Workspace-App auf dem iPad und bei Verwendung der Benutzeroberfläche der nächsten Generation von StoreFront™ 2402 LTSR kann ein Fehler mit der Meldung **Verbindung zum Server nicht möglich** auftreten.

24.10.0

Neuigkeiten

Verwaltung von Feature-Flags

Citrix ändert die Art und Weise, wie Feature-Flags verwaltet werden, um den Zugriff auf Vorschaufunktionen zu ermöglichen und die dynamische Verwaltung von Funktionen in der Produktion zu gewährleisten. Um die optimale Funktion von Funktionen, die unter Feature-Flags fallen, sicherzustellen, müssen Sie den Datenverkehr zur URL `features.netscalergateway.net` zulassen. Weitere Informationen finden Sie unter Verwaltung von Feature-Flags.

Behobene Probleme

Wenn mehrere Apps, die vom selben VDA veröffentlicht wurden, geöffnet sind, kann das Klicken auf die Schaltfläche **Wechseln** in der Sitzungssymbolleiste dazu führen, dass Benutzer nicht zwischen diesen Apps wechseln können und keine Reaktion erfolgt.

24.9.0

Neuigkeiten

- Unterstützung für iOS 18
- Unterstützung für Rapid Scan
- Unterstützung für Nachhaltigkeitsinitiative
- Erweiterte Verwaltung von Multi-App-Fenstern
- Biometrie-Eingabeaufforderung überspringen
- Abrufen von GACS-Endpunkten per E-Mail, Store-URL oder domänenbasierter Discovery-API
- Unterstützt GACS-authentifizierte Microservices (Cloud)
- Unterstützung für App Protection

Unterstützung für iOS 18

Die Citrix Workspace-App für iOS unterstützt jetzt iOS 18.

Unterstützung für Rapid Scan

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS die Rapid Scan-Funktion. Sie können diese Funktion verwenden, um mehrere Dokumente mit einem iOS-Gerät zu scannen und diese gescannten Dokumente dann mit der Citrix Workspace-App für Mac und iOS auf ein Mac-Gerät zu übertragen.

Weitere Informationen finden Sie unter Unterstützung für Rapid Scan

Unterstützung für Nachhaltigkeitsinitiative

Ab Version 24.9.0 wird Benutzern beim Schließen eines virtuellen Desktops eine Aufforderung angezeigt, sich von ihrer Desktopsitzung abzumelden. Diese Funktion hilft, Energie zu sparen, indem sie sich von VMs abmeldet, wenn sie nicht benötigt werden. Zuvor blieben diese Sitzungen in einem getrennten Zustand, was zu unnötigem Energieverbrauch führte.

Weitere Informationen finden Sie unter Unterstützung für Nachhaltigkeitsinitiative

Verbesserte Multi-App-Fensterverwaltung

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS eine nahtlose Multi-App-Fensterverwaltung für iPads, die an externe Monitore angeschlossen sind. Diese Funktion

verbessert Multitasking und Produktivität, indem sie native Multi-App-Erlebnisse ermöglicht. Sie kann auch aktiviert werden, wenn das iPad-Gerät nicht an externe Monitore angeschlossen ist.

Weitere Informationen finden Sie unter Verbesserte Multi-App-Fensterverwaltung

Aufforderung zur Biometrie-Aktivierung überspringen

Bisher wurden Endbenutzer aufgefordert zu wählen, ob sie Biometrie (Touch ID oder Face ID) zur Authentifizierung in der Citrix Workspace-App verwenden möchten. Ab Version 24.9.0 können Administratoren diese Aufforderung nun überspringen, wodurch der Anmeldevorgang für Benutzer optimiert wird.

Wenn die Biometrie aktiviert ist, werden Benutzerpasswörter sicher im Schlüsselbund gespeichert und durch biometrische Authentifizierung geschützt. Nach Ablauf des Authentifizierungstokens werden Benutzer automatisch zur biometrischen Verifizierung aufgefordert. Wenn die Biometrie auf dem Gerät nicht konfiguriert ist, müssen Benutzer ihre Anmeldeinformationen manuell eingeben, wenn das Token abläuft.

Diese Funktion wird derzeit nur für lokale Stores unterstützt, die LDAP-Authentifizierung verwenden.

Weitere Informationen finden Sie unter Aufforderung zur Biometrie-Aktivierung überspringen

Abrufen von GACS-Endpunkten per E-Mail, Store-URL oder domänenbasierter Discovery-API

Ab Version 24.9.0 können Administratoren einen Webstore basierend auf E-Mail-Adresse, Domäne und Store-URL konfigurieren, sodass der Global App Configuration Service (GACS) Benutzer identifizieren und zur entsprechenden benutzerdefinierten Web-URL leiten kann. Citrix Workspace-App für iOS-Geräte können GACS-Endpunkte nun über diese Discovery-API abrufen, wodurch die Notwendigkeit fest codierter Endpunkte entfällt und unnötige Aufrufe reduziert werden, wenn keine Konfiguration vorliegt.

Weitere Informationen finden Sie unter Abrufen von GACS-Endpunkten per E-Mail, Store-URL oder domänenbasierter Discovery-API

Unterstützt GACS-authentifizierte Microservices (Cloud)

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS authentifizierte Microservices, wodurch GACS Benutzergruppen für unsere Kunden verwalten kann. Dies bietet größere Flexibilität und Kontrolle und wird derzeit nur für Cloud-Stores unterstützt.

Weitere Informationen finden Sie unter Unterstützung für GACS-authentifizierte Microservices (Cloud)

Unterstützung für App Protection

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS die App Protection-Funktion.

App Protection ist eine Funktion der Citrix Workspace-App, die eine verbesserte Sicherheit bei der Verwendung von veröffentlichten Ressourcen von Citrix Virtual Apps and Desktops™ bietet. Diese Funktion schränkt die Möglichkeit ein, dass Clients durch Keylogging- und Bildschirmaufnahme-Malware kompromittiert werden. App Protection verhindert die Exfiltration vertraulicher Informationen wie Benutzeranmeldeinformationen und sensibler Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um sensible Informationen zu sammeln und auszunutzen.

Weitere Informationen finden Sie unter Unterstützung für App Protection

Behobene Probleme in 24.9.0

Es gibt keine neuen behobenen Probleme.

24.8.1

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Behobene Probleme in 24.8.1

Diese Version behebt Bereiche, die die Gesamtleistung und Stabilität verbessern.

24.8.0

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Behobene Probleme in 24.8.0

- Möglicherweise können Sie in der Smartcard-fähigen Einrichtung keine VDA-Sitzung starten und sich nicht erfolgreich am virtuellen Desktop anmelden.

24.7.0

Neuigkeiten

Unterstützung für DTLS 1.2

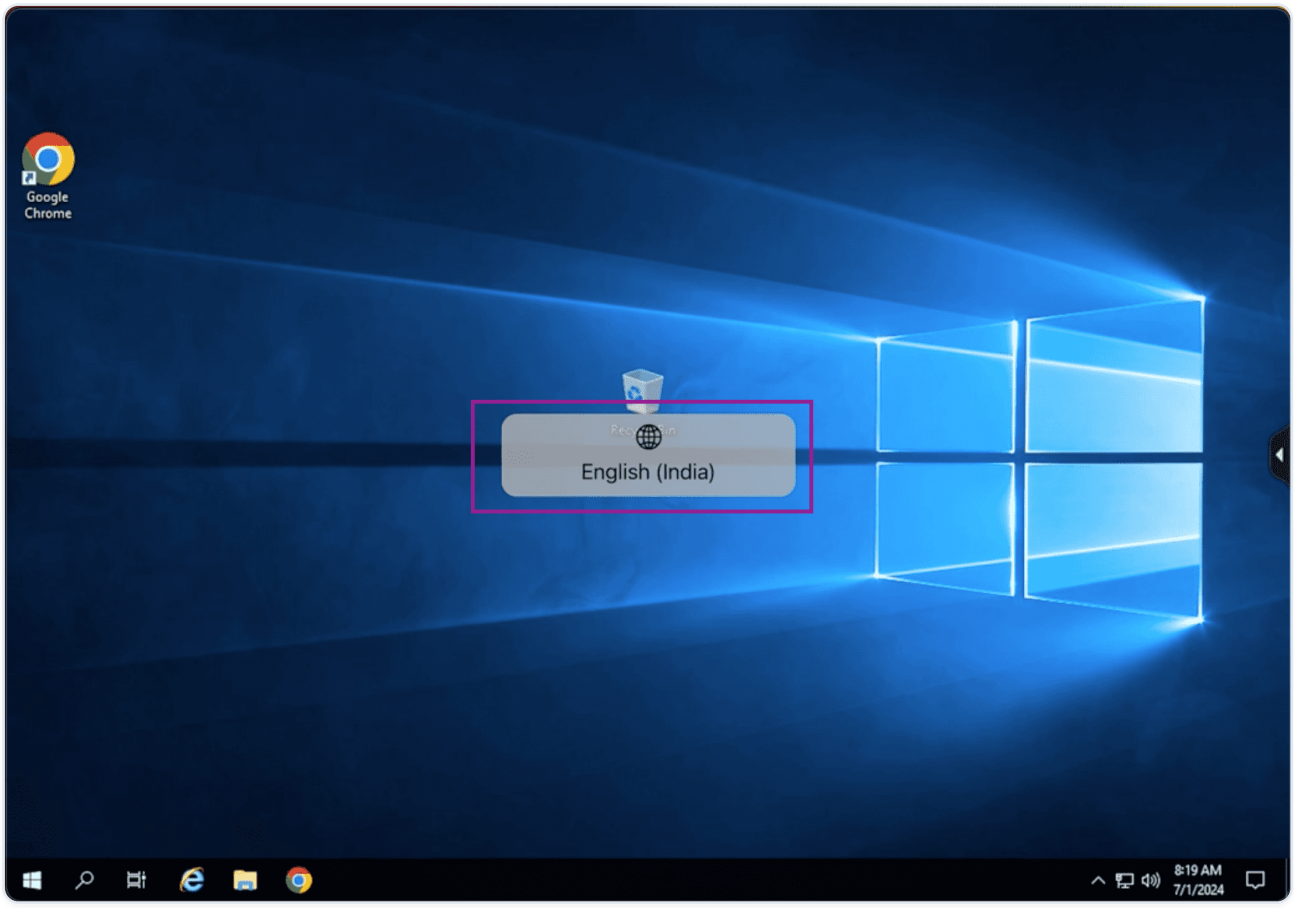
Ab Version 24.7.0 unterstützt die Citrix Workspace-App für iOS das DTLS-Protokoll Version 1.2. DTLS 1.2 bietet Erweiterungen und Verbesserungen gegenüber der vorherigen Version, darunter robuste Verschlüsselungsalgorithmen, bessere Handshake-Protokolle und Schutz vor verschiedenen Angriffen. Dieses Protokoll verbessert die allgemeine Sicherheit.

> **Hinweis:**
>
> Sollte es ein Problem mit DTLS-Protokoll Version 1.2 geben, greift die Citrix Workspace-App für iOS nahtlos auf die zuvor unterstützten Versionen zurück.

> Weitere Informationen finden Sie unter Unterstützung für DTLS 1.2.

Erkennung und Anzeige der Tastatursprachenänderung in der virtuellen Sitzung

Ab Version 24.7.0 erkennt die Citrix Workspace-App für iOS automatisch und zeigt eine Meldung in der virtuellen Sitzung an, wenn der Benutzer die Tastatursprache wechselt. Wenn Sie die Tastatursprache mit der Globus-Taste auf der Gerätetastatur oder einer externen Tastatur wechseln, erscheint eine Meldung auf dem Bildschirm, die über die aktuelle Tastatursprache informiert. Diese Funktion stellt sicher, dass Sie sich der aktuellen Tastatursprache innerhalb der virtuellen Sitzung bewusst sind.



Weitere Informationen finden Sie unter Erkennen und Anzeigen der Tastatursprachenänderung in der virtuellen Sitzung.

Unterstützung für adaptives Audio

Ab Version 24.7.0 unterstützt die Citrix Workspace-App für iOS HDX Adaptive Audio. Diese Funktion verbessert die Benutzererfahrung durch optimierte Audioqualität und geringe Latenz.

Weitere Informationen finden Sie im Artikel Audiopolicyeinstellung in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung für die Konfiguration von Citrix Workspace-App-Einstellungen über UEM

Bisher konnten Sie die Store-URL in der Citrix Workspace-App nur mit Unified Endpoint Management (UEM) konfigurieren.

Ab Version 24.7.0 können Sie die Einstellungen der Citrix Workspace-App auf den verwalteten Geräten auch mit jeder UEM-Lösung konfigurieren, die in Ihrer Infrastruktur bereitgestellt wird.

> **Hinweis:**

> Wenn Sie als Administrator die Möglichkeit haben, die Einstellungen der Citrix Workspace-App über UEM und den Global App Configuration Service (GACS) zu konfigurieren, haben die UEM-Einstellungen Vorrang vor GACS.

> Weitere Informationen finden Sie unter Unterstützung für die Konfiguration von Citrix Workspace-App-Einstellungen über UEM.

Technische Vorschau

- Unterstützung der Authentifizierung mit FIDO2 beim Herstellen einer Verbindung zu einem lokalen Store
- Unterstützung für mehrere Audiogeräte
- Unterstützung für App Protection

Eine vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Funktionen in der technischen Vorschau.

Behobene Probleme in 24.7.0

- Benutzer des NetScaler®-Stores der Citrix Workspace-App für iOS können sich möglicherweise nicht bei der neuen Benutzeroberfläche anmelden, wenn Secure Private Access mit clientlosen VPN (cVPN)-Richtlinien aktiviert ist.

24.6.0

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Behobene Probleme in 24.6.0

- Es kann vorkommen, dass das Trackpad der Magic Keyboard in der virtuellen Sitzung auf einem iPad Pro M4-Gerät nicht richtig funktioniert. Weitere Informationen finden Sie im Citrix Knowledge Center-Artikel – CTX677048.
- Wenn Sie ein Bild mit der Gerätekamera aus der virtuellen App-Sitzung aufnehmen, kann es vorkommen, dass das aufgenommene Bild auf dem Kopf steht.
- Bei der Verwendung von Skype in einer virtuellen Sitzung kann es vorkommen, dass der Bildschirm einfriert, wenn Sie die Citrix Workspace-App schließen und die Verbindung zur Sitzung wiederherstellen.

24.5.0

Neuigkeiten

Unterstützung der Authentifizierung mit FIDO2 bei der Verbindung mit einem Cloud Store

Ab Version 24.5.0 können Benutzer sich bei der Citrix Workspace-App mit FIDO2-basierter passwortloser Authentifizierung anmelden, wenn sie sich mit einem Cloud Store verbinden. FIDO2 bietet eine nahtlose Authentifizierungsmethode, die es Unternehmensmitarbeitern ermöglicht, auf Apps und Desktops innerhalb virtueller Sitzungen zuzugreifen, ohne Benutzernamen oder Passwort eingeben zu müssen. Diese Funktion unterstützt sowohl Roaming- (nur USB) als auch Plattform-Authentifikatoren (nur PIN-Code, Touch ID und Face ID). Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Unterstützung der Authentifizierung mit FIDO2 bei der Verbindung mit einem Cloud Store.

> **Hinweis:**
>
> Die FIDO2-Authentifizierung wird standardmäßig mit den Chrome Custom Tabs unterstützt. Wenn Sie die FIDO2-Authentifizierung mit WebView verwenden möchten, bekunden Sie Ihr Interesse per E-Mail an <ios_ear_support@cloud.com>.

Unterstützung für Dokumentenscanner

Ab Version 2405 unterstützt die Citrix Workspace-App für iOS die Dokumentenscanner-Funktion. Mit dieser Funktion können Sie jetzt mehrere Dokumente scannen und speichern, alles innerhalb der Desktopsitzung. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Unterstützung für Dokumentenscanner.

Technische Vorschau

- Unterstützung für Single Sign-On für Microsoft Entra ID-verbundene VMs
- Unterstützung für die Erzwingung der biometrischen Authentifizierung für den Zugriff auf die Citrix Workspace-App

Eine vollständige Liste der Technical Preview-Funktionen finden Sie auf der Seite Features in Technical Preview.

Behobene Probleme

- Möglicherweise stellen Sie fest, dass bei Verwendung des Barcode-Scanners in der virtuellen Sitzung der Text nicht korrekt gescannt werden kann.

24.4.0

Neuigkeiten

Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Ankündigung zur Einstellung der TLS 1.0- und TLS 1.1-Protokolle

Citrix plant, die Unterstützung für die TLS 1.0- und TLS 1.1-Protokolle in zukünftigen Versionen einzustellen. Die alternativen Protokolle sind TLS 1.2 oder TLS 1.3. Weitere Informationen finden Sie unter Deprecation.

Behobene Probleme

- Wenn Sie die Gerätekamera aus der virtuellen App-Sitzung öffnen, kann die Citrix Workspace-App für iOS unerwartet geschlossen werden.

24.3.5

Neuigkeiten

Unterstützung für das Twocanoes Smartcard-Dienstprogramm-Lesegerät

Ab Version 24.3.5 unterstützt die Citrix Workspace-App für iOS die Twocanoes Smartcard-Dienstprogramm-Lesegeräte. Weitere Informationen zu den unterstützten Smartcard-Lesegeräten und Konfigurationsdetails finden Sie unter Smart Cards.

> **Hinweis:**
>
> Das Twocanoes Smartcard-Dienstprogramm-USB-C-Lesegerät wird sowohl für die Anmeldung bei der Citrix Workspace-App als auch für die Anmeldung bei virtuellen Sitzungen unterstützt. Das Twocanoes Smartcard-Dienstprogramm-Bluetooth-Lesegerät wird jedoch nur für die Anmeldung bei der Citrix Workspace-App und nicht für die Anmeldung bei virtuellen Sitzungen unterstützt.

Unterstützung für die Konfiguration des Gerätenamens über UEM

Ab Version 24.3.5 ermöglicht die Citrix Workspace-App für iOS Administratoren, Gerätenamen basierend auf Benutzergruppen über Unified Endpoint Management (UEM) zuzuweisen und zu identifizieren. Weitere Informationen finden Sie unter Support for configuring device name through UEM.

Technische Vorschau

- Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen über UEM

Weitere Informationen zu dieser Technischen Vorschau finden Sie unter Features in Technical Preview.

Behobene Probleme

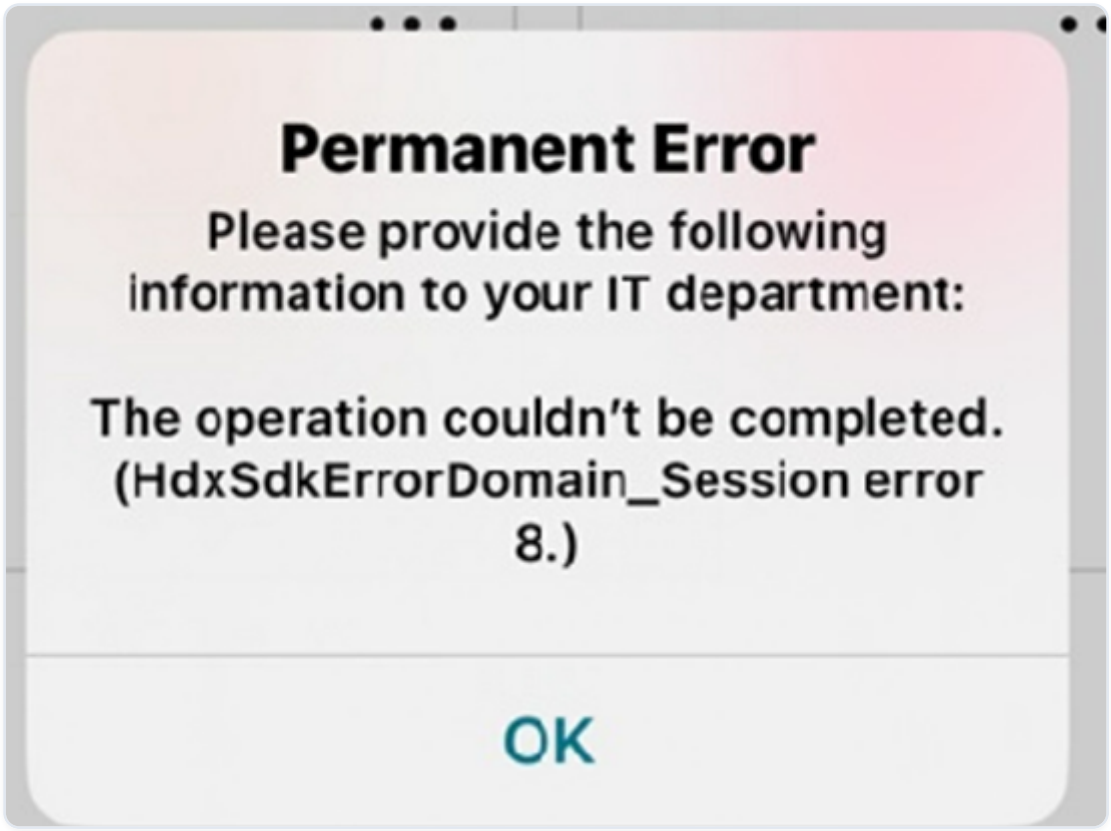
Diese Version befasst sich mit Bereichen, die die Gesamtleistung und Stabilität verbessern.

Bekannte Probleme

Bekannte Probleme in 25.7.2

- Sitzungsstarts können mit dem folgenden Fehler fehlschlagen, wenn das iOS-Gerät an eine Dockingstation angeschlossen ist:

  "Permanenter Fehler. Bitte geben Sie die folgenden Informationen an Ihre IT-Abteilung weiter. Der Vorgang konnte nicht abgeschlossen werden. (HdxSdkErrorDomain_session Fehler 8.)"



Dieses Problem tritt auf, wenn die Citrix Workspace-App gestartet wird, während das Gerät bereits an die Dockingstation angeschlossen ist. Als Problemumgehung starten Sie zuerst die Citrix Workspace-App, schließen Sie dann die Dockingstation an das Gerät an und starten Sie die Sitzung. Eine Korrektur ist für die Release-Version 25.9.0 (voraussichtlich Ende Oktober) geplant.

- Während iOS Version 26 den Fenstermodus unterstützen wird, ist die Citrix Workspace-App für iOS ab dieser Version auf ein einziges Fenster beschränkt. Dies bedeutet, dass jeweils nur eine Sitzung aktiv sein kann, und wenn Benutzer versuchen, ein anderes Fenster zu öffnen, werden sie zur aktuell aktiven Sitzung gewechselt.
- Der Lockdown-Modus schränkt bestimmte webbasierte Funktionen ein, wenn er auf Ihrem iPad oder iPhone aktiviert ist, wie unten erwähnt.
    - Der Lockdown-Modus vereinfacht die Anzeige von Rich-Media-Inhalten.
    - Möglicherweise treten auch eingeschränkte Authentifizierungsabläufe auf oder Sie haben eingeschränkte Netzwerkoperationen.

Bekannte Probleme in 25.5.0

Es gibt keine neuen bekannten Probleme.

Bekannte Probleme in 25.1.0

Das Symbolleistenmenü erweiterniert nicht, wenn Sie auf die neue Symbolleistenkerbe auf einem externen Monitor klicken.

Bekannte Probleme in 24.12.0

Die schnelle Smartcard unterstützt derzeit keine Smartcards mit Elliptic Curve Cryptography (ECC).

Bekannte Probleme in 24.9.0

Es gibt keine neuen bekannten Probleme.

Bekannte Probleme in 24.8.1

Es gibt keine neuen bekannten Probleme.

Bekannte Probleme in 24.8.0

Es gibt keine neuen bekannten Probleme.

Bekannte Probleme in 24.7.0

Es gibt keine neuen bekannten Probleme.

Bekannte Probleme in 24.5.0

Es kann vorkommen, dass das Trackpad der Magic Keyboard in der virtuellen Sitzung auf einem iPad Pro M4-Gerät nicht richtig funktioniert. Als Problemumgehung können Sie eine externe Maus (entweder mit kabelgebundenem USB-Typ-C-Anschluss oder Bluetooth) verwenden, um in der virtuellen Sitzung auf dem Bildschirm zu navigieren.

Bekannte Probleme in 24.1.0

Nach dem Upgrade der Citrix Workspace-App für iOS auf Version 24.1.0 kann die Tastatureingabe über die virtuelle Tastatur in der Sitzung für Anwendungen, die auf Oracle Java Web Start-Software basieren, fehlschlagen.

Bekannte Probleme in 24.10.0

Es gibt keine neuen bekannten Probleme.

Einschränkungen

- Wir empfehlen, zum Kopieren und Einfügen die Tasten **Strg + C** und **Strg + V** auf der Bildschirmtastatur Ihres Geräts zu verwenden. Die Tasten **Befehl + C** und **Befehl + V** auf einer externen Tastatur funktionieren möglicherweise nicht.
- Versuche, eine App durch Tippen auf die ICA-Datei im Download-Manager zu starten, schlagen bei Verwendung des Safari-Webbrowsers fehl. Um einen erfolgreichen App-Start von Safari aus zu gewährleisten, stellen Sie sicher, dass die neueste Version der Citrix Workspace-App oder von Citrix Receiver für iOS (aber nicht beide) auf dem Gerät vorhanden ist.
- Nach der Migration von StoreFront zu Citrix Workspace flackert der Bildschirm kurz, wenn Sie auf die Schaltfläche **Weiter** im Pendo-Leitfaden tippen.
- Beim Starten von Web- und SaaS-Apps innerhalb der Citrix Workspace-App schlägt die Authentifizierung mit der Fehlermeldung „Zugriff verweigert“ fehl, wenn die App Google IdP verwendet und der Benutzer sich anmelden muss.

Einstellung

Informationen zu veralteten Elementen finden Sie auf der Seite Veraltet.

Funktionen in der technischen Vorschau

Funktionen in der technischen Vorschau können in Nicht-Produktions- oder eingeschränkten Produktionsumgebungen verwendet werden und bieten Kunden die Möglichkeit, Feedback zu geben. Citrix® akzeptiert keine Supportfälle für Funktionen in der technischen Vorschau, begrüßt jedoch Feedback zur Verbesserung dieser Funktionen. Citrix kann auf Feedback basierend auf dessen Schweregrad, Kritikalität und Wichtigkeit reagieren.

Möchten Sie eine Funktion der technischen Vorschau ausprobieren? Senden Sie eine E-Mail an mailto:citrixappios@citrix.com und teilen Sie uns mit, welche Funktion Sie evaluieren möchten.

Liste der Funktionen in der technischen Vorschau

TITEL	VERFÜGBAR AB VERSION
Unterstützung für abgeleitete Anmeldeinformationen und Apple Token Extension	26.7.0

TITEL	VERFÜGBAR AB VERSION
Verbesserte Erfahrung bei der Sitzungswiederherstellung	26.3.0
Unterstützung für Single Sign-On für Microsoft Entra ID-verbundene VMs	24.5.0
Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen über UEM	24.3.5
Hinzufügen mehrerer Stores mithilfe von Unified Endpoint Management (UEM)	23.9.0
Löschen mehrerer Stores mithilfe von Unified Endpoint Management (UEM))	23.9.0
Verbessertes Webstore-Erlebnis	23.8.0
Unterstützung für ein verbessertes Single Sign-On (SSO)-Erlebnis für Web- und SaaS-Anwendungen	23.3.0

Abgeleitete Anmeldeinformationen und Unterstützung für Apple Token Extension

Die Citrix Workspace-App für iOS 26.7.0 unterstützt Apple Token Extension (CryptoTokenKit) sowohl in der App als auch in aktiven HDX-Sitzungen. Dies ermöglicht einer Drittanbieteranwendung für abgeleitete Anmeldeinformationen auf dem Gerät, digitale Zertifikate für die folgenden Anwendungsfälle bereitzustellen:

- **Citrix Gateway- oder StoreFront-Authentifizierung**: Authentifiziert Benutzer in der Citrix-Umgebung mithilfe eines abgeleiteten Zertifikats, ohne physischen Smartcard-Leser.
- **Anmeldung bei virtuellen Apps und Desktops**: Der Benutzerprinzipalname wird aus dem Zertifikat gelesen und beim Start an den VDA übergeben, sodass die Sitzung ohne erneute Aufforderung angemeldet wird.
- **Kryptografische Umleitung innerhalb der Sitzung**: Erweitert Anmeldeinformationen in die HDX-Sitzung, sodass virtualisierte Apps (z. B. Browser, E-Mail-Clients, PDF-Signaturtools und Unternehmens-Apps) kryptografische Anfragen über die Client-Token-Erweiterung stellen können.

Eine abgeleitete Anmeldeinformation ist ein Client-Zertifikat, das einem mobilen Gerät nach der Identitätsprüfung mit einer vorhandenen PIV- oder CAC-Karte während der Registrierung ausgestellt wird. Es bietet eine Smartcard-äquivalente Sicherheit auf Geräten ohne Kartenleser.

Verbessertes Sitzungswiederverbindungserlebnis

Ab Version 26.3.0 werden die folgenden Verbesserungen an der Funktion „Verbessertes Sitzungs-Timeout-Erlebnis (Technical Preview)“ vorgenommen, die in der Version 25.11.0 angekündigt wurde:

- Anzeige spezifischer Gründe für Sitzungs-Timeouts, wie z. B. **Gerätesperre**, **App im Hintergrund** oder **Netzwerkunterbrechung**.
- Sitzungswiederverbindungseinstellung konfigurierbar entweder über GACS durch Aktivieren der Option **Manuelle Sitzungswiederverbindung** unter **Sitzungserlebnis > Konnektivität** oder über MDM.

System- und Infrastrukturanforderungen

KOMPONENTE	ANFORDERUNG
Client-Betriebssystem	iOS oder iPadOS 17.0 oder höher
Citrix Client	Citrix Workspace-App für iOS 26.7.0 oder höher
Virtual Delivery Agent	Citrix VDA für Windows, mit aktivierten Smartcard-Umleitungsrichtlinien
Drittanbieter	Registrierte Anmeldeinformations-App, die eine iOS CryptoTokenKit-Token-Erweiterung implementiert
Infrastruktur	Citrix Gateway oder StoreFront für die Clientzertifikatauthentifizierung konfiguriert
Zertifikat	Muss einen UPN im Subject Alternative Name (SAN) für die Sitzungsanmeldung und die Verwendung innerhalb der Sitzung enthalten

Diese Funktion wird pro Kunde aktiviert. Wenden Sie sich an den Citrix Support, um sie für Ihre Stores zu aktivieren.

Konfigurationsschritte

1. Installieren Sie die App des Anbieters für abgeleitete Anmeldeinformationen und schließen Sie die Registrierung ab.
2. Gehen Sie in der Citrix Workspace-App zu **Einstellungen** > **Abgeleitete Anmeldeinformationen** und aktivieren Sie **Abgeleitete Anmeldeinformationen verwenden**.
3. Fügen Sie den Store hinzu. Wenn die Clientzertifikatauthentifizierung konfiguriert ist, präsentiert die Citrix Workspace-App die verfügbaren Anmeldeinformationen.
4. Starten Sie einen Desktop oder eine App und autorisieren Sie, wenn Sie dazu aufgefordert werden.

Administratoren können diese Einstellung über die MDM-Richtlinie für erweiterte Einstellungen sperren.

Unterstützung für Single Sign-On für Microsoft Entra ID-verbundene VMs

|Technische Vorschau ab Version 24.5.0|Aktivierungsformular|Feedback-Formular|

Ab Version 24.5.0 unterstützt die Citrix Workspace-App für iOS Benutzer, die sich mit Single Sign-On-Authentifizierung bei Azure AD-verbundenen VM-Geräten anmelden. Sie müssen Microsoft-Anmeldeinformationen angeben, wenn Sie sich zum ersten Mal bei einem Azure AD-verbundenen VM-Gerät anmelden. Bei nachfolgenden Anmeldungen sind Anmeldeinformationen erst erforderlich, wenn das Token abläuft.

> **Hinweis:**
>
> - Wenn der Benutzer **WKwebview** nicht zur Authentifizierung verwendet, müssen die Anmeldeinformationen zum ersten Mal eingegeben werden.
> - Diese Funktion ist nur für Cloud-Stores anwendbar.

Hinzufügen mehrerer Stores mit Unified Endpoint Management (UEM)

|Technische Vorschau ab Version 23.12.0|Aktivierungsformular|Feedback-Formular|

Administratoren können Unified Endpoint Management-Lösungen verwenden, um mehrere Stores für verwaltete iOS-Geräte zu konfigurieren und hinzuzufügen. Die Details für jeden Store können einer XML-Datei hinzugefügt werden. Diese XML-Datei kann dann beim Konfigurieren der App-Konfigurationsrichtlinie hochgeladen werden.

Hinweis:

Die XML-Datei muss im Schlüssel-Wert-Format vorliegen.

KONFIGURATIONSSCHLÜSSEL	WERTTYP	BESCHREIBUNG
URL	String	Die Store-URL. Zum Beispiel example.cloud.com
storeType (wahlweise)	Integer	Wenn auf **1** gesetzt, können Benutzer das Laden des nativen oder Standard-Stores sehen. Wenn auf **2** gesetzt, können Benutzer den Store in einer Weboberfläche anzeigen.
Anzeigename (optional)	String	Der Name des Stores.
Benutzerspeicheränderung einschränken (optional)	Boolesch	Wenn auf **true** gesetzt, können Benutzer den Store nicht ändern, d. h. hinzufügen, löschen oder bearbeiten. Wenn auf **false** gesetzt, können Benutzer den Store ändern, d. h. hinzufügen, löschen oder bearbeiten.

Wichtig

- Wenn das Flag **restrict_user_store_modification** auf **true** gesetzt ist, werden alle bestehenden Stores gelöscht, bevor ein neuer UEM-konfigurierter Store hinzugefügt wird.
- Wenn storeType nicht angegeben ist, wird die Standardschnittstelle als nativ behandelt.

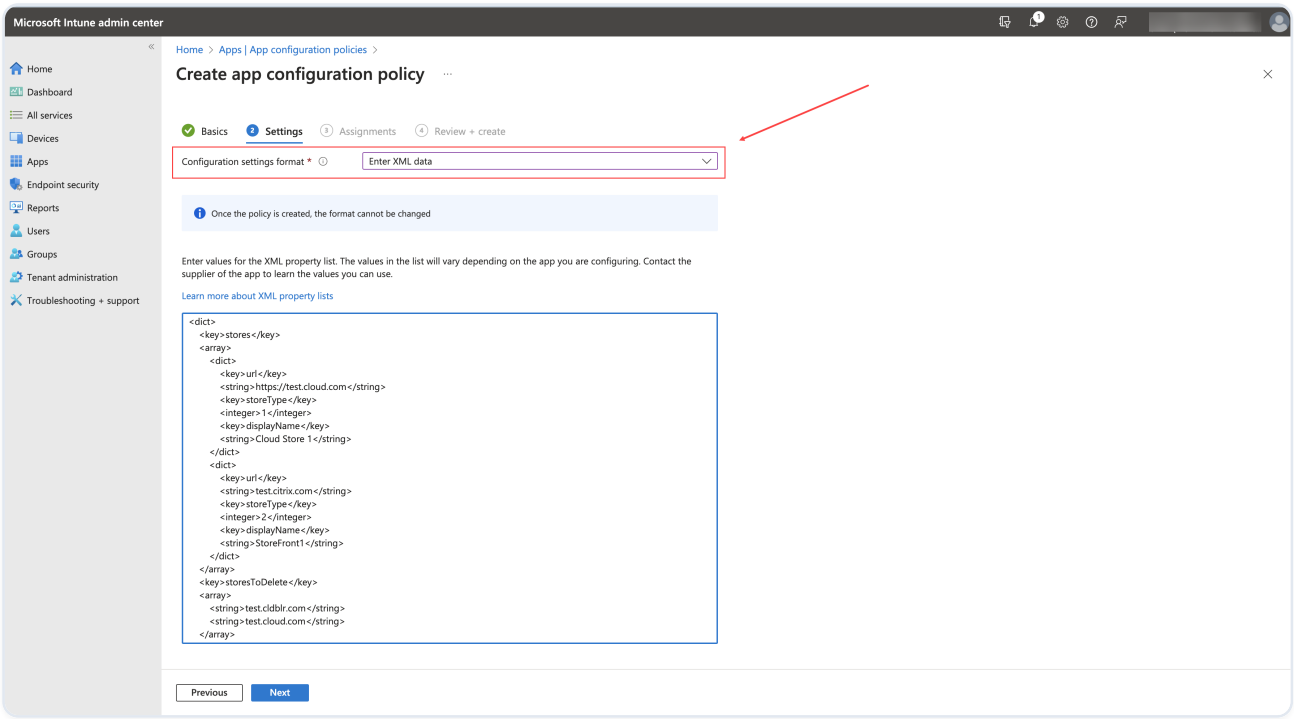
Beispiel-XML-Konfiguration zum Hinzufügen von Stores

Weitere Informationen finden Sie in dieser Beispiel-XML-Datei.

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>test.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store </string>
        </dict>
        <dict>
            <key>url</key>
            <string>test.citrix.com</string>
            <key>storeType</key>
            <integer>2</integer>
            <key>displayName</key>
            <string>StoreFront</string>
        </dict>
```

```
        </array>
            <key>restrict_user_store_modification</key>
        <true/>
    </dict>
```

Sobald die XML-Datei mit der Store-Konfiguration fertig ist, können Administratoren die Datei auf die Seite **App-Konfigurationsrichtlinie erstellen** hochladen. Zum Beispiel müssen Administratoren in Microsoft Intune die Option **XML-Daten eingeben** aus dem Dropdown-Menü **Format der Konfigurationseinstellungen** auswählen.



Mehrere Stores mithilfe von Unified Endpoint Management (UEM) löschen

|Technical Preview ab Version 23.12.0|Aktivierungsformular|Feedback-Formular|

Administratoren müssen eine Liste der zu löschenden Stores zu einer XML-Datei mit dem Schlüsselnamen **storesToDelete** hinzufügen, um einen oder mehrere Stores zu löschen.

Beispiel-XML-Konfiguration zum Löschen von Stores

Weitere Informationen finden Sie in dieser Beispiel-XML-Datei.

```
    <dict>
        <key>storesToDelete</key>
    <array>
        <string>test.cldblr.com</string>
        <string>test.onprem.com</string>
    </array>
   </dict>
```

Im Folgenden finden Sie eine Beispiel-XML-Konfigurationsdatei, die die Konfiguration für das Hinzufügen und Löschen von Stores enthält.

```
        <dict>
        <key>stores</key>
        <array>
            <dict>
                <key>url</key>
                <string>test.cloud.com</string>
                <key>storeType</key>
                <integer>1</integer>
                <key>displayName</key>
                <string>Cloud Store </string>
            </dict>
            <dict>
```

```
                <key>url</key>
                <string>test.citrix.com</string>
                <key>storeType</key>
                <integer>2</integer>
                <key>displayName</key>
                <string>StoreFront</string>
            </dict>
        </array>
        <key>storesToDelete</key>
        <array>
            <string>test.cldblr.com</string>
            <string>test.onprem.com</string>
        </array>
        <key>restrict_user_store_modification</key>
        <true/>
    </dict>
```

Verbessertes Webstore-Erlebnis

|Technische Vorschau ab Version 23.8.0|Aktivierungsformular|Feedback-Formular|

Endbenutzer können jetzt in einem Webinterface-Store angemeldet bleiben, bis sie sich abmelden oder die Sitzung abläuft. Endbenutzer können auch auf die Option „Einstellungen“ zugreifen, ohne sich vom aktuellen Store abzumelden. Klicken Sie auf das Ellipsensymbol, um auf die folgenden Optionen zuzugreifen:

- **Einstellungen**: Verwenden Sie diese Option, um Ihre Stores hinzuzufügen und zu verwalten.
- **Abmelden**: Verwenden Sie diese Option, um sich von Ihrem aktuellen Webinterface-Store abzumelden.

Unterstützung für ein verbessertes Single Sign-On (SSO)-Erlebnis für Web- und SaaS-Apps

|Technische Vorschau ab Version 22.3.5|Aktivierungsformular|Feedback-Formular|

Diese Funktion vereinfacht die Konfiguration von SSO für interne Web-Apps und SaaS-Apps bei der Verwendung von Identitätsanbietern (IdPs) von Drittanbietern. Das verbesserte SSO-Erlebnis reduziert den gesamten Prozess auf wenige Befehle. Es eliminiert die obligatorische Voraussetzung, Citrix Secure Private Access™ in der IdP-Kette zu konfigurieren, um SSO einzurichten. Es verbessert auch die Benutzererfahrung, vorausgesetzt, derselbe IdP wird für die Authentifizierung sowohl bei der Workspace-App als auch bei der gestarteten Web- oder SaaS-App verwendet.

Technische Vorschau zur allgemeinen Verfügbarkeit (GA)

DIENST ODER FUNKTION	VERSION DER ALLGEMEINEN VERFÜGBARKEIT
Unterstützung für die Erzwingung der biometrischen Authentifizierung für den Zugriff auf die Citrix Workspace-App	24.9.0
Unterstützung für schnelles Scannen	24.9.0
Unterstützung für App-Schutz	24.9.0
Unterstützung für die Authentifizierung mit FIDO2 beim Herstellen einer Verbindung zu einem lokalen Store	24.9.0
Unterstützung für mehrere Audiogeräte	24.9.0
Unterstützung für adaptives Audio	24.5.0
Unterstützung für Barrierefreiheit und VoiceOver	24.9.0
Unterstützung für externe Webcams	24.9.0

CITRIX WORKSPACE™-APP FÜR IOS

DIENST ODER FUNKTION	VERSION DER ALLGEMEINEN VERFÜGBARKEIT
Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen über UEM	24.7.0
Unterstützung für Dokumentenscanner	24.5.0
Unterstützung für FIDO2-basierte Authentifizierung	23.9.0
Unterstützung für Apples nativen Nicht-Spiegelmodus	23.3.0

Systemanforderungen und Kompatibilität

Die Citrix Workspace™-App für iOS muss auf die neueste Version aktualisiert werden, die im Apple Store verfügbar ist, um Kundensupport in Anspruch nehmen zu können.

Unterstützte Betriebssysteme

Die Citrix Workspace-App für iOS unterstützt die folgenden Betriebssysteme:

- iOS 26 und iPadOS 26.
- iOS 18 und iPadOS 18.
- iOS 17 und iPadOS 17.

Citrix® unterstützt zu jedem Zeitpunkt nur die neueste und die beiden vorherigen iOS-Betriebssystemversionen (N, N-1 und N-2).

Serveranforderungen

Überprüfen Sie, ob Sie alle aktuellen Hotfixes für Ihre Server installiert haben.

- Für Verbindungen zu virtuellen Desktops und Apps unterstützt die Citrix Workspace-App Citrix StoreFront und Web Interface.

  StoreFront:

  - StoreFront 3.6 oder höher (empfohlen). Die Citrix Workspace-App wurde mit der neuesten Version von StoreFront validiert; frühere unterstützte Versionen umfassen StoreFront 2.6 oder höher.

    Bietet direkten Zugriff auf StoreFront-Stores. Die Citrix Workspace-App unterstützt auch frühere Versionen von StoreFront.

    > **Hinweis:**

> Mit XenApp und XenDesktop 7.8 führte Citrix die Unterstützung für den virtuellen Framehawk-Kanal und 3D Pro ein. Diese Funktionalität wurde auf die Citrix Workspace-App erweitert.

- StoreFront konfiguriert mit einem Workspace für die Website.

  Bietet Zugriff auf StoreFront-Stores über einen Safari-Webbrowser. Benutzer müssen die ICA-Datei manuell über den Browser öffnen. Informationen zu den Einschränkungen dieser Bereitstellung finden Sie in der (/de-de/storefront.html)-Dokumentation zu StoreFront.

Web-Oberfläche:

- Web-Oberfläche 5.4 mit Web-Oberflächen-Sites
- Web-Oberfläche 5.4 mit XenApp- und XenDesktop-Sites
- Web-Oberfläche auf Citrix Gateway (nur Browser-basierter Zugriff mit Safari)

  Aktivieren Sie die von Citrix Gateway bereitgestellten Rewrite-Richtlinien.

- **Citrix Virtual Apps and Desktops™**, **XenApp** und **XenDesktop** (eines der folgenden Produkte):
  - Citrix Virtual Apps and Desktops 7 1808 oder höher
  - Citrix XenDesktop 7.x oder höher
  - Citrix XenApp 7.5 oder höher

Verbindungen, Zertifikate und Authentifizierung

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

	WORKSPACE FÜR WEB ÜBER BROWSER	STOREFRONT SERVICES-SITE (NATIV)	STOREFRONT XENAPP- UND XENDESKTOP-SITE (NATIV)	CITRIX GATEWAY ZU WORKSPACE FÜR WEB (BROWSER)	CITRIX GATEWAY ZU STOREFRONT SERVICES-SITE (NATIV)
Anonym	Ja	Ja			

CITRIX WORKSPACE™-APP FÜR IOS

	WORKSPACE FÜR WEB ÜBER BROWSER	STOREFRONT SERVICES-SITE (NATIV)	STOREFRONT XENAPP- UND XENDESKTOP-SITE (NATIV)	CITRIX GATEWAY ZU WORKSPACE FÜR WEB (BROWSER)	CITRIX GATEWAY ZU STOREFRONT SERVICES-SITE (NATIV)
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zwei-Faktor-Authentifizierung (Domäne mit Sicherheitstoken)				Ja*	Ja*
SMS				Ja*	Nein
Smartcard		Ja		Ja*	Ja*
Benutzerzertifikat				Ja (Citrix Gateway-Plug-in)	Ja (Citrix Gateway-Plug-in)

*Nur verfügbar für:

- Workspace für Websites.
- Bereitstellungen, die Citrix Gateway umfassen, mit oder ohne Installation des zugehörigen Plug-Ins auf dem Gerät.

Für Verbindungen zur Web Interface 5.4 unterstützt die Citrix Workspace-App die folgenden Authentifizierungsmethoden:

Hinweis:

Web Interface verwendet den Begriff „Explizit“, um die Domänen- und Sicherheitstoken-Authentifizierung darzustellen.

	WEB INTERFACE (BROWSER)	WEB INTERFACE XENAPP- UND XENDESKTOP ®-SITE	CITRIX GATEWAY ZU WEB INTERFACE (BROWSER)	CITRIX GATEWAY ZU WEB INTERFACE XENAPP- UND XENDESKTOP -SITE
Anonym	Ja			
Domäne	Ja	Ja	Ja*	
Domänen-Passthrough	Ja			
Sicherheitstoken			Ja*	
Zwei-Faktor-Authentifizierung (Domäne mit Sicherheitstoken)			Ja*	
SMS			Ja*	
Smartcard				
Benutzerzertifikat			Ja (Citrix Gateway-Plug-in erforderlich)	

Zertifikate

Private (selbstsignierte) Zertifikate

Sie können mit der Citrix Workspace-App erfolgreich auf Citrix-Ressourcen zugreifen:

- wenn ein privates Zertifikat auf dem Remote-Gateway installiert ist.
- wenn das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Gerät installiert ist.

> **Hinweis:**
>
> Wenn das Zertifikat des Remote-Gateways bei der Verbindung nicht überprüft werden kann, wird eine Warnung für nicht vertrauenswürdige Zertifikate angezeigt. Dieses Problem tritt auf, weil das Stammzertifikat nicht im lokalen Keystore enthalten ist. Wenn ein Benutzer die Warnung ignoriert und fortfährt, wird eine Liste von Anwendungen angezeigt; die Anwendungen können jedoch nicht gestartet werden.

Manuell installiertes Zertifikat

In iOS 10.3 und höher wird ein Zertifikat, das in einem manuell installierten Profil enthalten ist, nicht automatisch für SSL vertraut. Um manuell installierten Zertifikatsprofilen in iOS zu vertrauen:

1. Stellen Sie sicher, dass Sie das Zertifikatsprofil auf dem Gerät installiert haben.
2. Gehen Sie zu **Einstellungen** > **Allgemein** > **Info** > **Zertifikatsvertrauenseinstellungen**.

   Jedes Stammzertifikat, das über ein Profil installiert wurde, wird unter **Vollständiges Vertrauen für Stammzertifikate aktivieren** angezeigt.
3. Sie können das Vertrauen für jedes Stammzertifikat aktivieren oder deaktivieren.

Stammzertifikate auf iPad- und iPhone-Geräten importieren

Besorgen Sie sich das Stammzertifikat des Zertifikatausstellers und senden Sie es an ein auf Ihrem Gerät konfiguriertes E-Mail-Konto. Wenn Sie auf den Anhang klicken, werden Sie aufgefordert, das Stammzertifikat zu importieren.

Platzhalterzertifikate

Platzhalterzertifikate werden anstelle einzelner Serverzertifikate für jeden Server innerhalb derselben Domäne verwendet. Die Citrix Workspace-App unterstützt Platzhalterzertifikate.

Zwischenzertifikate und Citrix Gateway

Wenn Ihre Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat an das Citrix Gateway (oder Access Gateway)-Serverzertifikat angehängt werden. Für Access Gateway-Installationen lesen Sie außerdem Zertifikate installieren, verknüpfen und aktualisieren, die Ihren Anforderungen in der Citrix ADC-Dokumentation entsprechen.

Die RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen (nur über Web Interface) und alle unterstützten Access Gateway-Konfigurationen unterstützt.

Die Citrix Workspace-App unterstützt alle von Access Gateway unterstützten Authentifizierungsmethoden.

Gemeinsame Serverzertifikat-Validierungsrichtlinie

Versionen der Citrix Workspace-App haben eine strengere Validierungsrichtlinie für Serverzertifikate.

Wichtig

Vergewissern Sie sich vor der Installation der Citrix Workspace-App, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben korrekt konfiguriert sind. Verbindungen können fehlschlagen, wenn:

- die Server- oder Gateway-Konfiguration ein falsches Stammzertifikat enthält
- die Server- oder Gateway-Konfiguration nicht alle Zwischenzertifikate enthält
- die Server- oder Gateway-Konfiguration ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat enthält
- die Server- oder Gateway-Konfiguration ein querzertifiziertes Zwischenzertifikat enthält

Bei der Validierung eines Serverzertifikats verwendet die Citrix Workspace-App jetzt **alle** vom Server (oder Gateway) bereitgestellten Zertifikate. Wie in früheren Versionen prüft die Citrix Workspace-App dann auch, ob die Zertifikate vertrauenswürdig sind. Wenn die Zertifikate nicht vertrauenswürdig sind, schlägt die Verbindung fehl.

Diese Richtlinie ist strenger als die Zertifikatsrichtlinie in Webbrowsern. Viele Webbrowser enthalten eine große Anzahl von Stammzertifikaten, denen sie vertrauen.

Der Server (oder das Gateway) muss mit dem richtigen Satz von Zertifikaten konfiguriert werden. Ein falscher Satz von Zertifikaten kann dazu führen, dass Citrix Workspace-App-Verbindungen fehlschlagen.

Angenommen, ein Gateway ist mit diesen gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen, indem genau bestimmt wird, welches Stammzertifikat von der Citrix Workspace-App verwendet wird:

- Beispiel-Serverzertifikat
- Beispiel-Zwischenzertifikat
- Beispiel-Stammzertifikat

Anschließend prüft die Citrix Workspace-App, ob alle diese Zertifikate gültig sind. Die Citrix Workspace-App überprüft auch, ob das **Beispiel-Stammzertifikat** bereits vertrauenswürdig ist.

> **Hinweise:**

> - Wenn die Citrix Workspace-App dem **Beispiel-Stammzertifikat** nicht vertraut, schlägt die Verbindung fehl.
> - Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie eine strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet.

> Zum Beispiel gibt es derzeit zwei Zertifikate:

- DigiCert oder GTE CyberTrust Global Root
- DigiCert Baltimore Root oder Baltimore CyberTrust Root

Diese Zertifikate können dieselben Serverzertifikate validieren. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eines verfügbar (**DigiCert Baltimore Root** oder **Baltimore CyberTrust Root**).

Wenn Sie **GTE CyberTrust Global Root** am Gateway konfigurieren, schlagen die Citrix Workspace-App-Verbindungen auf diesen Benutzergeräten fehl. Konsultieren Sie die Dokumentation der Zertifizierungsstelle, um zu bestimmen, welches Stammzertifikat verwendet werden muss. Beachten Sie auch, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.

Anschließend verwendet die Citrix Workspace-App diese beiden Zertifikate. Die App sucht auf dem Benutzergerät nach einem Stammzertifikat. Wenn die App eines findet, das korrekt validiert wird und auch vertrauenswürdig ist (wie das **Beispiel-Stammzertifikat**), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl.

Diese Konfiguration stellt das Zwischenzertifikat bereit, das die Citrix Workspace-App benötigt, ermöglicht es der Citrix Workspace-App aber auch, jedes gültige, vertrauenswürdige Stammzertifikat zu wählen.

Nehmen wir nun an, dass ein Gateway mit diesen Zertifikaten konfiguriert ist:

- Beispiel-Serverzertifikat
- Beispiel-Zwischenzertifikat
- Falsches Stammzertifikat

Ein Webbrowser ignoriert möglicherweise das falsche Stammzertifikat. Die Citrix Workspace-App ignoriert das falsche Stammzertifikat jedoch nicht, und die Verbindung schlägt fehl.

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall wird das Gateway normalerweise mit allen Zwischenzertifikaten (aber nicht mit dem Stammzertifikat) konfiguriert, wie zum Beispiel:

- Beispiel-Serverzertifikat
- Beispiel-Zwischenzertifikat 1
- Beispiel-Zwischenzertifikat 2

> **Wichtig**

> Einige Zertifizierungsstellen verwenden ein querzertifiziertes Zwischenzertifikat. Solche Zertifikate sind für Situationen vorgesehen, in denen mehr als ein Stammzertifikat vorhanden ist und ein früheres Stammzertifikat gleichzeitig mit einem späteren Stammzertifikat verwendet wird. In solchen Fällen existieren mindestens zwei Zwischenzertifikate.

> Zum Beispiel hat das frühere Stammzertifikat **Class 3 Public Primary Certification Authority** das entsprechende querzertifizierte Zwischenzertifikat **Verisign Class 3 Public Primary Certification Authority - G5**. Es ist jedoch auch ein entsprechendes späteres Stammzertifikat **Verisign Class 3 Public Primary Certification Authority - G5** verfügbar,

> das **Class 3 Public Primary Certification Authority** ersetzt. Das spätere Stammzertifikat verwendet kein querzertifiziertes Zwischenzertifikat.

> **Hinweis:**

> Das querzertifizierte Zwischenzertifikat und das Stammzertifikat haben denselben Antragstellernamen (Ausgestellt für), aber das querzertifizierte Zwischenzertifikat hat einen anderen Ausstellernamen (Ausgestellt von). Der Ausstellername unterscheidet das querzertifizierte Zwischenzertifikat von einem gewöhnlichen Zwischenzertifikat (wie **Beispiel-Zwischenzertifikat 2**).

> Diese Konfiguration, bei der das Stammzertifikat und das querzertifizierte Zwischenzertifikat weggelassen werden, wird normalerweise empfohlen:

- Beispiel-Serverzertifikat
- Beispiel-Zwischenzertifikat

Vermeiden Sie es, das Gateway für die Verwendung des kreuzsignierten Zwischenzertifikats zu konfigurieren, da die Citrix Workspace-App das frühere Stammzertifikat auswählt:

- Beispiel-Serverzertifikat
- Beispiel-Zwischenzertifikat
- Beispiel für ein kreuzsigniertes Zwischenzertifikat \[nicht empfohlen\]

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

- Beispiel-Serverzertifikat

In solchen Fällen schlägt die Verbindung fehl, wenn die Citrix Workspace-App nicht alle Zwischenzertifikate finden kann.

Systemanforderungen für Microsoft Entra SSO

Die folgenden Systemanforderungen gelten für die Verwendung von Microsoft Entra SSO:

- Steuerungsebene: Citrix DaaS
  - Citrix Cloud Commercial (USA, EU und APS)

    - Citrix Cloud Japan
- Benutzerportal: Citrix Workspace
- Virtual Delivery Agent (VDA)
    - Windows: Version 2507 oder neuer
- Citrix Workspace-App
    - iOS: Version 2511 oder neuer
- Sitzungshost-Betriebssystem:
    - Windows 11, Version 24H2 mit 2025-09 Kumulativen Updates für Windows 11 (KB5065789) oder höher installiert (Build 26100.6725)

Überlegungen

- Microsoft Entra Single Sign-On wird nur unterstützt, wenn auf Citrix Workspace über die Citrix Workspace-App zugegriffen wird. Wenn Benutzer über einen Webbrowser auf Citrix Workspace zugreifen, funktioniert Single Sign-On nicht.
- Automatisches Client-Reconnect wird nicht unterstützt, wenn Microsoft Entra Single Sign-On für die Anmeldung an der Sitzung verwendet wird. Diese Funktion wird automatisch deaktiviert, wenn diese Anmeldemethode verwendet wird. Die Sitzungszuverlässigkeit ist weiterhin für die automatische Wiederverbindung bei Netzwerkunterbrechungen verfügbar.
- Wenn ein virtueller Desktop gesperrt ist, besteht das Standardverhalten darin, den Windows-Sperrbildschirm anzuzeigen. Je nach Ihren Authentifizierungsanforderungen müssen Sie möglicherweise das Verhalten der Sitzungssperre ändern. Weitere Informationen finden Sie unter Verhalten der Sitzungssperre.

Installation und Upgrade

Sie können die neueste Version der Citrix Workspace-App aus dem Apple Store herunterladen oder darauf aktualisieren.

- Erstbenutzer können die Citrix Workspace-App aus dem Apple Store herunterladen und auf ihrem Gerät installieren.
- Bestehende Benutzer können im Apple Store auf die neueste Version der Citrix Workspace-App aktualisieren.

Informationen zum Konfigurieren der Citrix Workspace-App finden Sie im Abschnitt Konfigurieren.

Informationen zu den in der Citrix Workspace-App für iOS verfügbaren Funktionen finden Sie unter Citrix Workspace-App-Funktionsmatrix.

Erste Schritte

Einrichtung

Die Citrix Workspace-App für iOS unterstützt die Konfiguration von Web Interface für Ihre Citrix Virtual Apps-Bereitstellung. Es gibt zwei Arten von Web Interface-Sites:

- XenApp- und XenDesktop®-Sites
- Citrix Virtual Apps and Desktops™- und Citrix DaaS-Sites (ehemals Citrix Virtual Apps and Desktops Service).

Web Interface-Sites ermöglichen Clientgeräten die Verbindung mit der Serverfarm. Die Authentifizierung zwischen der Citrix Workspace-App für iOS und einer Web Interface-Site kann über verschiedene Lösungen, einschließlich Citrix Secure Web Gateway, erfolgen.

Sie können StoreFront auch so konfigurieren, dass es Authentifizierungs- und Ressourcenbereitstellungsdienste für die Citrix Workspace-App bereitstellt. Die Konfiguration ermöglicht es Ihnen, zentralisierte Unternehmens-Stores zu erstellen, um Desktops, Anwendungen und andere Ressourcen für Benutzer bereitzustellen.

Weitere Informationen zur Konfiguration von Verbindungen, einschließlich Videos, Blogs und einem Supportforum, finden Sie unter `<http://community.citrix.com>`.

Bevor Ihre Benutzer auf Anwendungen zugreifen, die in Ihrer Citrix Virtual Apps and Desktops- und Citrix DaaS-Bereitstellung gehostet werden, konfigurieren Sie die folgenden Komponenten in Ihrer Bereitstellung wie hier beschrieben.

- Berücksichtigen Sie beim Veröffentlichen von Anwendungen auf Ihren Farmen oder Sites die folgenden Optionen, um die Benutzererfahrung beim Zugriff auf diese Anwendungen über StoreFront-Stores zu verbessern.
    - Stellen Sie sicher, dass Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen angeben, da diese Beschreibungen für Benutzer in der Citrix Workspace-App sichtbar sind.
    - Sie können veröffentlichte Anwendungen für Ihre mobilen Gerätebenutzer hervorheben. Sie können die Anwendungen unter der Liste „Featured“ (Empfohlen) auflisten. Um diese Liste

in der Citrix Workspace-App zu füllen, bearbeiten Sie die Eigenschaften der Anwendungen, die auf Ihren Servern veröffentlicht sind. Sie können nun die Zeichenfolge KEYWORDS: Featured an den Wert des Feldes **Anwendungsbeschreibung** anhängen.

- Der Bildschirm-Anpassungsmodus passt die Anwendung an die Bildschirmgröße mobiler Geräte an. Um diesen Modus zu aktivieren, bearbeiten Sie die Eigenschaften der Anwendungen, die auf Ihren Servern veröffentlicht sind, und hängen Sie die Zeichenfolge KEYWORDS: mobile an den Wert des Feldes Anwendungsbeschreibung an. Dieses Schlüsselwort aktiviert auch die automatische Bildlauffunktion für die Anwendung.
- Um alle Benutzer eines Stores automatisch für eine Anwendung zu abonnieren, hängen Sie die Zeichenfolge KEYWORDS: Auto an die Beschreibung an, wenn Sie die Anwendung in Citrix Virtual Apps veröffentlichen. Wenn sich Benutzer am Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer die Anwendung manuell abonnieren müssen.

- Wenn das Web Interface Ihrer Citrix Virtual Apps and Desktops- und Citrix DaaS™-Bereitstellung keine Site hat, erstellen Sie eine. Der Name der Site und wie Sie sie erstellen, hängt von der Version des Web Interface ab, das Sie installiert haben.

Manuelle Einrichtung

Im Allgemeinen versucht die Citrix Workspace-App, wenn sie eine Verbindung mit Citrix Gateway herstellt, nach der Authentifizierung eine XenApp- und XenDesktop-Site oder eine Citrix Virtual Apps-Website zu finden. Wird keine Site erkannt, zeigt die Citrix Workspace-App für iOS einen Fehler an. Um dies zu vermeiden, können Sie ein Konto manuell konfigurieren, damit die Citrix Workspace-App für iOS eine Verbindung mit Citrix Gateway herstellen kann.

1. Tippen Sie auf das Symbol **Konten** > **Kontenbildschirm** > **Pluszeichen (+)**. Der Bildschirm „Neues Konto“ wird angezeigt.
2. Tippen Sie in der oberen rechten Ecke des Bildschirms auf das Symbol links neben **Optionen** und tippen Sie auf **Manuelle Einrichtung**. Weitere Felder werden auf dem Bildschirm angezeigt.
3. Geben Sie im Feld **Adresse** die sichere URL der Site oder des Citrix Gateways ein (zum Beispiel `agee.mycompany.com`).
4. Wählen Sie eine der folgenden Verbindungsoptionen aus. Die anderen Felder auf dem Bildschirm ändern sich je nach Ihrer Auswahl.

- **Webinterface** – Wählen Sie diese Option, damit die Citrix Workspace-App eine Citrix Virtual Apps-Website anzeigt, die einem Webbrowser ähnelt. Diese Benutzeroberfläche wird auch als Webansicht bezeichnet.
- **XenApp-Dienste** – Wählen Sie diese Option, damit die Citrix Workspace-App für iOS eine bestimmte XenApp- und XenDesktop-Site findet, für die keine Authentifizierung über Citrix Gateway konfiguriert ist. Geben Sie in den zusätzlichen Optionen, die auf diesem Bildschirm angezeigt werden, die Anmeldeinformationen für die Site ein.
  - \<StoreFront FQDN\>: Wenn es viele Stores gibt, wird eine Liste angezeigt, und der Benutzer kann den hinzuzufügenden Store auswählen.
  - \<StoreFront FQDN\>/citrix/\<Store Name\>: Diese Option fügt den StoreFront-Store \<Store Name\> hinzu.
  - \<StoreFront FQDN\>/citrix/PnAgent/config.xml: Diese Option fügt den standardmäßigen Legacy-PNAgent-Store hinzu.
  - \<StoreFront FQDN\>/citrix/\<Store Name\>/PnAgent/config.xml: Diese Option fügt den Legacy-PNAgent-Store hinzu, der \<Store Name\> zugeordnet ist.
- Citrix Gateway – Wählen Sie diese Option, damit die Citrix Workspace-App für iOS über ein bestimmtes Citrix Gateway eine Verbindung zu einer XenApp- und XenDesktop-Site herstellt. Wählen Sie in den zusätzlichen Optionen auf diesem Bildschirm die Serveredition und die Anmeldeinformationen aus, einschließlich der Frage, ob ein Sicherheitstoken für die Authentifizierung erforderlich ist.

5. Für die Zertifikatssicherheit verwenden Sie die Einstellung im Feld „Zertifikatswarnungen ignorieren“, um festzulegen, ob Sie eine Verbindung zum Server herstellen möchten, selbst wenn dieser ein ungültiges, selbstsigniertes oder abgelaufenes Zertifikat besitzt. Die Standardeinstellung ist AUS. Wichtig: Wenn Sie diese Option aktivieren, stellen Sie sicher, dass Sie eine Verbindung zum richtigen Server herstellen. Citrix® empfiehlt dringend, dass alle Server über ein gültiges Zertifikat verfügen, um Benutzergeräte vor Online-Sicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt nicht, die Zertifikatssicherheit zu umgehen.
6. Speichern tippen.
7. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein (oder Token, wenn Sie die Zwei-Faktor-Authentifizierung ausgewählt haben), und tippen Sie dann auf „Anmelden“. Der Bildschirm der Citrix Workspace-App für iOS wird angezeigt, auf dem Sie auf Ihre Desktops zugreifen und Ihre Apps hinzufügen und öffnen können.

StoreFront

Wichtig:

- Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App für iOS Citrix Access Gateway Enterprise Edition ab Version 9.3 und Citrix Gateway bis Version 13.
- Die Citrix Workspace-App für iOS unterstützt nur XenApp- und XenDesktop-Sites auf Web Interface.
- Die Citrix Workspace-App für iOS unterstützt das Starten von Sitzungen über Workspace für Web, solange der Webbrowser mit Workspace für Web funktioniert. Wenn keine Starts erfolgen, konfigurieren Sie Ihr Konto direkt über die Citrix Workspace-App für iOS. Benutzer müssen die ICA-Datei manuell mit der Browserfunktion „In Workspace öffnen“ öffnen. Die Einschränkungen dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

Mit StoreFront bestehen die von Ihnen erstellten Stores aus Diensten, die eine Authentifizierungs- und Ressourcenbereitstellungsinfrastruktur für die Citrix Workspace-App für iOS bereitstellen. Erstellen Sie Stores, die Desktops und Anwendungen aus den folgenden Quellen zählen und zusammenfassen:

- Citrix Virtual Apps and Desktops- und Citrix DaaS-Sites
- Citrix Virtual Apps-Farmen

1. Installieren und konfigurieren Sie StoreFront. Einzelheiten finden Sie in der StoreFront-Produktdokumentation. Für Administratoren, die mehr Kontrolle benötigen, stellt Citrix eine Vorlage bereit, mit der Sie eine Download-Site für die Citrix Workspace-App für iOS erstellen können.
2. Konfigurieren Sie Stores für StoreFront wie für andere Citrix Virtual Apps and Desktops- und Citrix DaaS-Anwendungen. Für mobile Geräte ist keine spezielle Konfiguration erforderlich. Einzelheiten finden Sie unter „Benutzerzugriffsoptionen“ im Abschnitt „StoreFront“ der Produktdokumentation. Für mobile Geräte verwenden Sie eine der folgenden Methoden:
    - Bereitstellungsdateien. Sie können Benutzern Bereitstellungsdateien (.cr) zur Verfügung stellen, die Verbindungsdetails für ihre Stores enthalten. Nach der Installation öffnen Benutzer die Datei auf dem Gerät, um die Citrix Workspace-App für iOS automatisch zu konfigurieren. Standardmäßig bieten Workspace-Websites Benutzern eine

Bereitstellungsdatei für den einzelnen Store an, für den die Site konfiguriert ist. Alternativ können Sie die Citrix StoreFront-Verwaltungskonsole verwenden, um Bereitstellungsdateien für einzelne oder mehrere Stores zu generieren, die Sie manuell an Ihre Benutzer verteilen können.

- Manuelle Konfiguration. Sie können Benutzer direkt über die Citrix Gateway- oder Store-URLs informieren, um auf ihre Desktops und Anwendungen zuzugreifen. Für Verbindungen über Citrix Gateway müssen Benutzer auch die Produktedition und die erforderliche Authentifizierungsmethode kennen. Nach der Installation geben Benutzer diese Details in die Citrix Workspace-App ein, die versucht, die Verbindung zu überprüfen, und, falls erfolgreich, die Benutzer zur Anmeldung auffordert.
- Automatische Konfiguration. Tippen Sie auf dem Begrüßungsbildschirm auf **Konto hinzufügen** und geben Sie die URL des StoreFront-Servers in das Adressfeld ein. Die Konfiguration des Kontos erfolgt automatisch, während das Konto hinzugefügt wird.

Citrix Gateway konfigurieren

Wenn Sie Benutzer haben, die sich von außerhalb des internen Netzwerks verbinden, konfigurieren Sie die Authentifizierung über Citrix Gateway. Zum Beispiel Benutzer, die über das Internet von einem entfernten Standort aus eine Verbindung herstellen.

- Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App für iOS Citrix Access Gateway Enterprise Edition ab Version 9.3 und Citrix Gateway bis Version 13.

Web Interface

Um die Web Interface-Site zu konfigurieren, können Benutzer mit iPhone- und iPad-Geräten Anwendungen über Ihre Web Interface-Site und den integrierten Safari-Browser auf dem Mobilgerät starten. Konfigurieren Sie die Web Interface-Site genauso wie für andere Citrix Virtual Apps-Anwendungen. Wenn keine XenApp- und XenDesktop-Site für das Mobilgerät konfiguriert ist, verwendet die Citrix Workspace-App für iOS automatisch Ihre Web Interface-Site. Für Mobilgeräte ist keine spezielle Konfiguration erforderlich.

Der integrierte Safari-Browser unterstützt Web Interface 5.x.

So starten Sie Anwendungen auf dem iOS-Gerät

Auf dem Mobilgerät können sich Benutzer mit ihrem normalen Benutzernamen und Kennwort bei der Web Interface-Site anmelden.

Automatische Bereitstellung für Mobilgeräte

Verwenden Sie in StoreFront die Aufgaben **Export Multi-Store Provisioning File** und **Export Provisioning File**, um Dateien mit Verbindungsdetails für Stores zu generieren, einschließlich aller Citrix Gateway-Bereitstellungen und Beacons, die für die Stores konfiguriert sind. Stellen Sie diese Dateien den Benutzern zur Verfügung, damit sie die Citrix Workspace-App für iOS automatisch mit den Details der Stores konfigurieren können. Benutzer können Citrix Workspace-App für iOS-Bereitstellungsdateien auch von Workspace für Websites beziehen.

> **Wichtig:**
>
> In vielen Serverbereitstellungen verwenden Sie jeweils nur einen Server, um die Konfiguration der Servergruppe zu ändern. Überprüfen Sie, ob die Citrix StoreFront-Verwaltungskonsole auf keinem der anderen Server in der Bereitstellung ausgeführt wird. Sobald dies abgeschlossen ist, übertragen Sie Ihre Konfigurationsänderungen auf die Servergruppe, damit die anderen Server in der Bereitstellung aktualisiert werden.

1. Suchen und klicken Sie auf dem Windows-Startbildschirm oder dem Apps-Bildschirm auf die Kachel „Citrix StoreFront“. Wählen Sie den Knoten „Stores“ im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus.
2. Um eine Bereitstellungsdatei mit Details für mehrere Stores zu generieren, klicken Sie im Aktionsbereich auf „Export Multi-Store Provisioning File“ und wählen Sie die Stores aus, die in die Datei aufgenommen werden sollen.
3. Klicken Sie auf „Exportieren“ und speichern Sie die Bereitstellungsdatei mit der Erweiterung `.cr` an einem geeigneten Speicherort in Ihrem Netzwerk.

Benutzerzugriffsinformationen

Sie müssen Benutzern die Kontoinformationen der Citrix Workspace-App für iOS zur Verfügung stellen, die sie für den Zugriff auf ihre gehosteten Anwendungen, Desktops und Daten benötigen. Sie können diese Informationen bereitstellen, indem Sie:

- E-Mail-basierte Kontoerkennung konfigurieren
- Benutzern eine Bereitstellungsdatei zur Verfügung stellen
- Benutzern Kontoinformationen zur manuellen Eingabe bereitstellen

E-Mail-basierte Kontoerkennung konfigurieren

Sie können die Citrix Workspace-App für iOS so konfigurieren, dass sie die E-Mail-basierte Kontoerkennung verwendet. Nach der Konfiguration geben Benutzer bei der erstmaligen Installation und Konfiguration der Citrix Workspace-App für iOS ihre E-Mail-Adresse anstelle einer Server-URL ein. Die Citrix Workspace-App ermittelt den Access Gateway- oder StoreFront-Server oder die virtuelle Endpoint Management-Appliance, die der E-Mail-Adresse zugeordnet sind, basierend auf DNS-Dienst- (SRV-)Einträgen und fordert den Benutzer dann auf, sich anzumelden, um auf seine gehosteten Anwendungen, Desktops und Daten zuzugreifen.

> **Hinweis:**
>
> Die E-Mail-basierte Kontoerkennung wird nicht unterstützt, wenn die Citrix Workspace-App für iOS eine Verbindung zu einer Web Interface-Bereitstellung herstellt.

DNS-Dienststandort- (SRV-)Eintrag hinzufügen, um die E-Mail-basierte Erkennung zu ermöglichen

Während der Erstkonfiguration kann die Citrix Workspace-App Active Directory-DNS-Server kontaktieren, um Details zu den für Benutzer verfügbaren Stores abzurufen. Dies bedeutet, dass Benutzer die Zugangsdaten für ihre Stores nicht kennen müssen, wenn sie die Citrix Workspace-App für iOS installieren und konfigurieren. Stattdessen geben Benutzer ihre E-Mail-Adressen ein, und die Citrix Workspace-App kontaktiert den DNS-Server. Sie können die Domänendetails aus der E-Mail-Adresse abrufen.

Damit die Citrix Workspace-App verfügbare Stores basierend auf den E-Mail-Adressen der Benutzer finden kann:

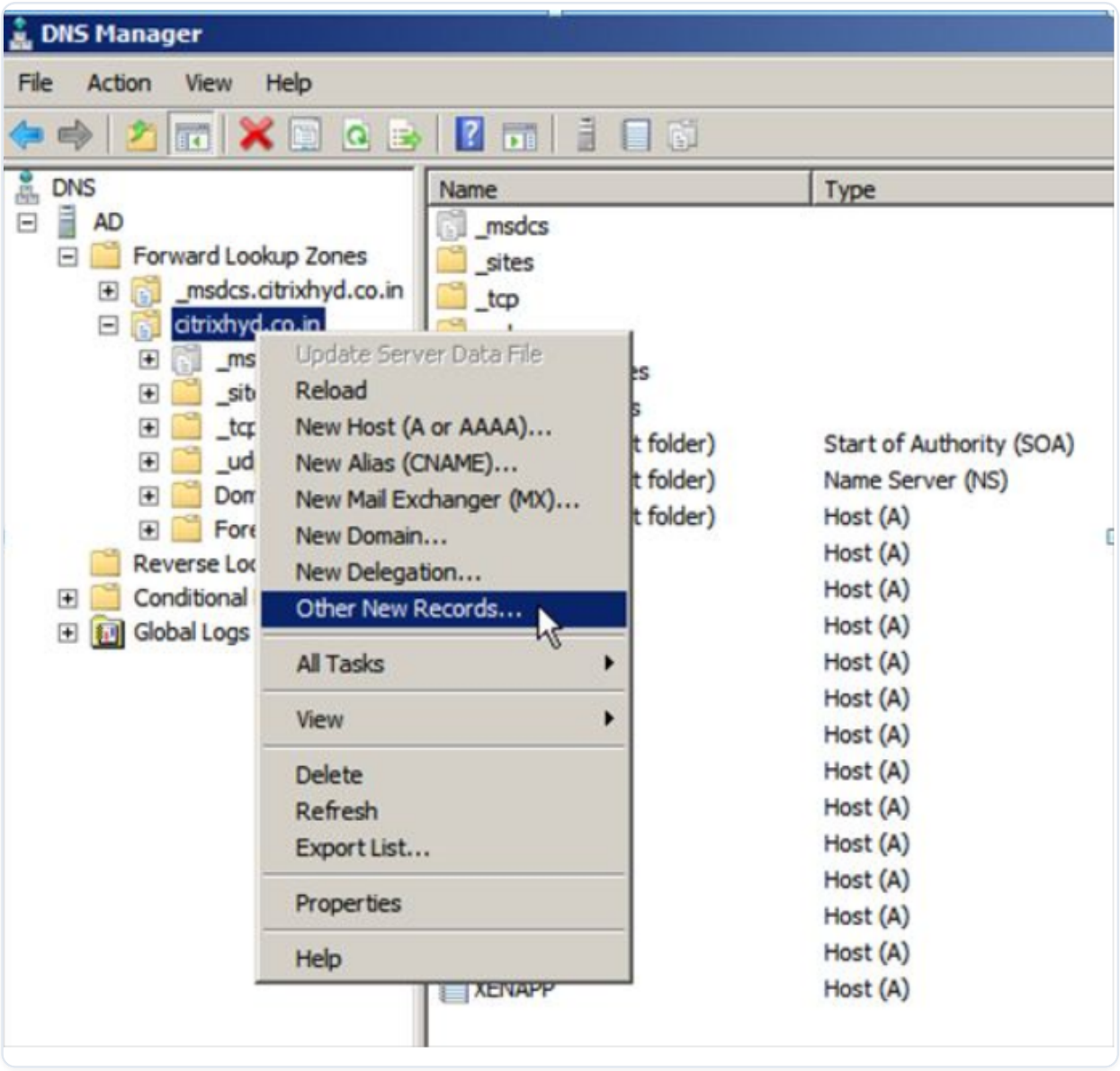
- konfigurieren Sie Service Location (SRV)-Locator-Ressourceneinträge für Access Gateway.
- konfigurieren Sie die StoreFront- oder AppController-Verbindungen auf Ihrem DNS-Server.

Sie müssen ein gültiges Serverzertifikat auf der Access Gateway-Appliance und dem StoreFront- oder AppController-Server installieren, um die E-Mail-basierte Kontoerkennung zu ermöglichen. Die vollständige Kette zum Stammzertifikat muss ebenfalls gültig sein. Für die beste Benutzererfahrung installieren Sie entweder ein Zertifikat mit:

- einem Subject
- einem Subject Alternative Name-Eintrag von *discoverReceiver.domain*.
- einem Wildcard-Zertifikat für die Domäne, die die E-Mail-Konten Ihrer Benutzer enthält.

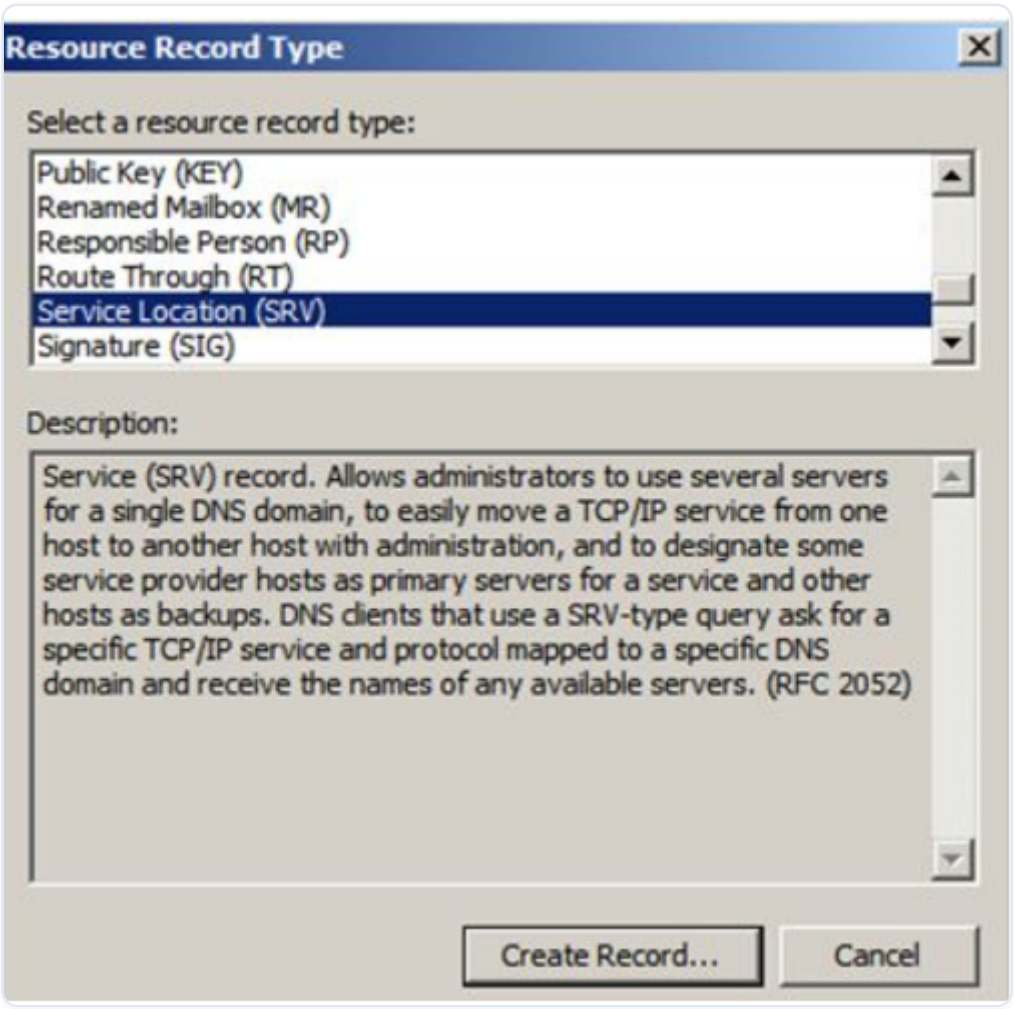
Damit Benutzer die Citrix Workspace-App für iOS mithilfe einer E-Mail-Adresse konfigurieren können, fügen Sie Ihrer DNS-Zone einen SRV-Eintrag wie folgt hinzu:

1. Melden Sie sich bei Ihrem DNS-Server an.
2. Klicken Sie in DNS mit der rechten Maustaste auf Ihre Forward-Lookupzone.
3. Klicken Sie auf **Weitere neue Datensätze.**



4. Das Dialogfeld **Ressourcendatensatztyp** wird angezeigt.
5. Wählen Sie unter **Ressourcendatensatztyp auswählen** die Option **Dienstspeicherort (SRV)** aus.

6. Wählen Sie **Datensatz erstellen.**



7. Das Dialogfeld „Eigenschaften“ wird angezeigt.
8. Wählen Sie die Registerkarte **Dienstspeicherort** aus.
9. Geben Sie unter **Dienst** den Hostwert _citrixreceiver ein.
10. Geben Sie unter **Protokoll** den Wert _tcp ein.
11. Geben Sie unter **Host, der diesen Dienst anbietet** den vollqualifizierten Domänennamen (FQDN) und den Port für Ihre Access Gateway Appliance (zur Unterstützung lokaler und externer Benutzer) oder den StoreFront- oder AppController-Server (zur Unterstützung von Benutzern nur im lokalen Netzwerk) an.
12. Klicken Sie auf OK.

> **Hinweis:**

> Ihr StoreFront-FQDN muss eindeutig und vom FQDN des Access Gateway Virtual Servers verschieden sein. Die Verwendung desselben FQDN für StoreFront und den Access Gateway Virtual Server wird nicht unterstützt. Die Citrix Workspace-App erfordert eine

> eindeutige StoreFront-FQDN-Adresse, die nur von Benutzergeräten aufgelöst werden kann, die mit dem internen Netzwerk verbunden sind. Andernfalls können Benutzer der Citrix Workspace-App die e-mail-basierte Kontoermittlung nicht verwenden.

Bereitstellen einer Bereitstellungsdatei für Benutzer

Sie können StoreFront verwenden, um Bereitstellungsdateien mit Verbindungsdetails für Konten zu erstellen. Sie stellen diese Dateien Ihren Benutzern zur Verfügung, damit diese die Citrix Workspace-App für iOS automatisch konfigurieren können. Nach der Installation der Citrix Workspace-App für iOS öffnen Benutzer einfach die `.cr`-Datei auf dem Gerät, um die Citrix Workspace-App für iOS zu konfigurieren. Wenn Sie Workspace für Websites konfigurieren, können Benutzer auch Bereitstellungsdateien für die Citrix Workspace-App für iOS von diesen Sites abrufen.

Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Bereitstellen von Kontoinformationen zur manuellen Eingabe für Benutzer

Wenn Sie Benutzern Kontodetails zur manuellen Eingabe bereitstellen, stellen Sie sicher, dass Sie die folgenden Informationen verteilen, damit sie sich erfolgreich mit ihren gehosteten Desktops verbinden können:

- Die StoreFront-URL oder die XenApp- und XenDesktop-Site, die Ressourcen hostet; zum Beispiel: `servername.company.com`.
- Für den Zugriff über Citrix Gateway geben Sie die Citrix Gateway-Adresse und die erforderliche Authentifizierungsmethode an.

Wenn ein Benutzer die Details für ein neues Konto eingibt, versucht die Citrix Workspace-App, die Verbindung zu überprüfen. Ist dies erfolgreich, fordert die Citrix Workspace-App für iOS den Benutzer auf, sich beim Konto anzumelden.

Citrix Workspace-App konfigurieren

Dieser Artikel listet Aufgaben auf, die Ihnen bei der Konfiguration der Citrix Workspace-App für iOS helfen.

Automatischer Start von Desktops und Apps

Ab Version 25.7.2 können Sie jetzt den automatischen Start von Desktops oder Anwendungen erleben.

> **Hinweis:**
>
> Die mobilen Plattformen unterstützen den Start nur einer Ressource gleichzeitig. Das Markieren mehrerer Ressourcen für den automatischen Start kann zu unerwartetem Verhalten führen.

Konfiguration

Um sicherzustellen, dass eine Kernanwendung in Citrix Workspace automatisch gestartet wird, müssen Administratoren die Zeichenfolge `KEYWORDS: AutoStartPrimaryApp` an die Anwendungsbeschreibung anhängen. Nach der Konfiguration wird die Anwendung für alle Benutzer automatisch gestartet.

Die folgenden Schritte sind für Administratoren:

1. **Verwaltungskonsole öffnen:**

   Starten Sie Citrix Studio oder das Citrix-Verwaltungsportal Ihres Unternehmens. Melden Sie sich mit einem Konto an, das über Berechtigungen zum Bearbeiten veröffentlichter Anwendungen verfügt.

2. **Anwendung suchen:**

   Gehen Sie zu **Anwendungen** und wählen Sie die Anwendung aus, die Sie für den automatischen Start konfigurieren möchten (z. B. Editor).

3. **Anwendungseigenschaften bearbeiten:**

Wählen Sie die Anwendung aus und wählen Sie dann **Bearbeiten** oder **Eigenschaften**. Suchen Sie das Feld **Beschreibung**.

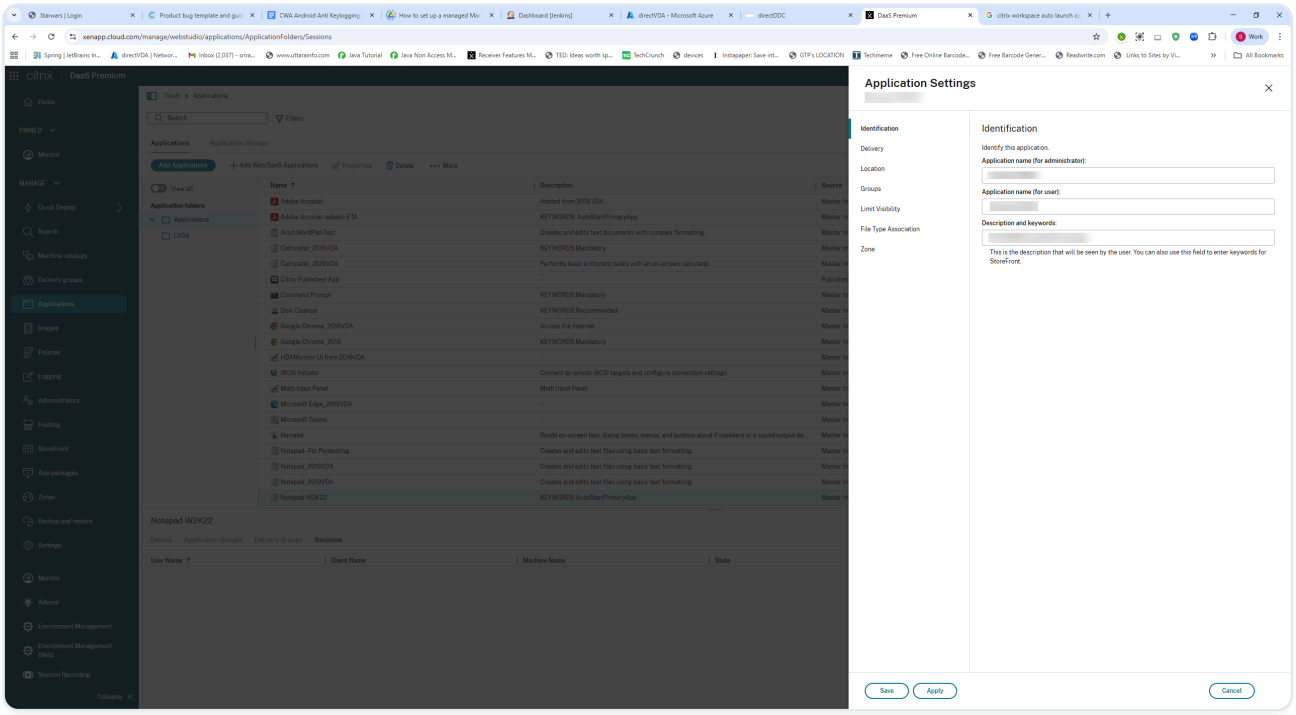
4. **Schlüsselwort für automatischen Start anhängen:**

   Fügen Sie am Ende der Beschreibung ein Leerzeichen hinzu und hängen Sie dann das folgende Schlüsselwort an:

   ```
   KEYWORDS:AutoStartPrimaryApp
   ```

5. **Änderungen speichern:**

   Klicken Sie auf **OK**, **Speichern** oder **Aktualisieren**, um die Änderungen zu übernehmen.



Verbesserte Audioqualität mit Echtzeit-Echounterdrückung

Ab Version 25.3.0 führt die Citrix Workspace-App für iOS die Echounterdrückungsfunktion ein, die kristallklaren Klang auf mobilen Geräten liefert. Diese Funktion eliminiert aktiv Echos in Echtzeit und gewährleistet eine reibungslose und unterbrechungsfreie Kommunikation während virtueller Meetings und Anrufe. Sie steigert die Produktivität, reduziert Störungen und bietet ein überragendes Benutzererlebnis, selbst unter schwierigen mobilen Netzwerkbedingungen.

Unterstützt GACS-authentifizierte Microservices (lokal)

Ab Version 25.1.0 unterstützt die Citrix Workspace-App für iOS Authenticated Microservices, wodurch GACS Benutzergruppen verwalten kann. Diese Funktion bietet Administratoren eine verbesserte Kontrolle für lokale Umgebungen. Weitere Informationen finden Sie unter Einstellungen für Benutzergruppen mithilfe eines Konfigurationsprofils verwalten.

Abrufen von GACS-Endpunkten per E-Mail, Store-URL oder domänenbasierter Discovery-API

Ab Version 24.9.0 können Administratoren einen Webstore basierend auf E-Mail-Adresse, Domäne und Store-URL konfigurieren, sodass der Global App Configuration Service (GACS) Benutzer identifizieren und zur entsprechenden benutzerdefinierten Web-URL leiten kann. Citrix Workspace-App für iOS-Geräte können jetzt GACS-Endpunkte über diese Discovery-API abrufen, wodurch die Notwendigkeit fest codierter Endpunkte entfällt und unnötige Aufrufe reduziert werden, wenn diese nicht konfiguriert sind. Dieses Update kommt sowohl Cloud- als auch lokalen Stores zugute, und Benutzer können Webstores direkt über die Store-URL konfigurieren, mit der Option, benutzerdefinierte Webstores über GACS hinzuzufügen. Weitere Informationen finden Sie unter Unterstützung für den Global App Configuration Service-Kanal.

Unterstützt GACS Authenticated Microservices (Cloud)

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS Authenticated Microservices, wodurch GACS Benutzergruppen für unsere Kunden verwalten kann. Dies bietet größere Flexibilität und Kontrolle und wird derzeit nur für Cloud-Stores unterstützt. Weitere Informationen finden Sie unter Einstellungen für Benutzergruppen mithilfe eines Konfigurationsprofils verwalten (Vorschau).

Feature-Flag-Verwaltung

Feature-Flags werden verwendet, um Funktionen dynamisch zu aktivieren oder zu deaktivieren. Wenn in der Produktion ein Problem mit der Citrix Workspace-App auftritt, kann die betroffene Funktion deaktiviert werden, selbst nachdem die Funktion ausgeliefert wurde.

Es ist keine Konfiguration erforderlich, um den Datenverkehr für die Feature-Verwaltung zu aktivieren, es sei denn, eine Firewall oder ein Proxy blockiert den ausgehenden Datenverkehr. In solchen Fällen müssen Sie den Datenverkehr zu bestimmten URLs oder IP-Adressen basierend auf Ihren Richtlinienanforderungen zulassen.

Datenverkehr für die Feature-Flag-Verwaltung aktivieren

Ab Citrix Workspace-App Version 24.10.0:

Um eine optimale Funktionalität und den Zugriff auf Vorschaufunktionen zu gewährleisten, müssen Sie den Datenverkehr zur folgenden URL zulassen:

- `features.netscalergateway.net`

> **Hinweis:**
>
> Ab Januar 2025 unterstützen Citrix Workspace-App-Versionen unter 24.10.0 keine vorherigen Funktionen mehr. Nach diesem Datum wird dieser Abschnitt irrelevant, da Versionen 24.10.0 oder höher diese Funktionen aktiviert haben. Um Probleme zu vermeiden, aktualisieren Sie auf Citrix Workspace-App Version 24.10.0 oder höher. Stellen Sie außerdem sicher, dass die Einstellung `features.netscalergateway.net` aktiviert ist. Andernfalls kann es zu Problemen mit Version 24.10.0 oder höher kommen.

Inaktivitätstimeout für die Citrix Workspace-App

Administratoren können die zulässige Leerlaufzeit festlegen. Nach Ablauf des Zeitüberschreitungswerts wird eine Authentifizierungsaufforderung angezeigt.

Der Wert für das Inaktivitätstimeout kann von 1 Minute bis 24 Stunden festgelegt werden. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert. Administratoren können die Eigenschaft inactivityTimeoutInMinutesMobile mithilfe eines PowerShell-Moduls konfigurieren. Klicken Sie auf PowerShell-Module für die Citrix Workspace-App-Konfiguration herunterladen, um die PowerShell-Module für die Citrix Workspace-App-Konfiguration herunterzuladen.

Wenn der angegebene Zeitüberschreitungswert erreicht ist, ist die Benutzererfahrung je nach konfiguriertem Authentifizierungstyp wie folgt:

- Nach dem Inaktivitätstimeout erhalten Sie eine Aufforderung zur biometrischen Authentifizierung, um erneut auf die Citrix Workspace-App zuzugreifen.
- Wenn Sie die Aufforderung zur biometrischen Authentifizierung abbrechen können, wird die folgende Meldung angezeigt:

  Citrix Workspace-App ist gesperrt.

  Sie müssen sich authentifizieren, um die Workspace-App weiterhin nutzen zu können.

Wenn der Passcode unter iOS nicht konfiguriert ist, müssen Sie sich nach dem Inaktivitätstimeout mit Ihren Anmeldeinformationen anmelden.

Hinweis:

Diese Funktion ist nur für Kunden mit Workspace (Cloud) verfügbar.

Programm zur Verbesserung der Kundenzufriedenheit (CEIP)

Was ist das Citrix Programm zur Verbesserung der Kundenzufriedenheit (CEIP) für die Citrix Workspace-App?

Das Citrix Programm zur Verbesserung der Kundenzufriedenheit (CEIP) erfasst Konfigurations- und Nutzungsdaten von der Citrix Workspace-App und sendet diese automatisch an Citrix Analytics. Diese Daten ermöglichen es Citrix, die Leistung zu analysieren und die Qualität, Funktionalität und Leistung der Citrix Workspace-App zu verbessern, die Ressourcenzuweisung für die Produktentwicklung zu optimieren und Service-Levels durch effektive Personalbesetzung und Infrastrukturinvestitionen zu unterstützen.

Alle Daten werden ausschließlich in aggregierter Form verwendet und analysiert, um sicherzustellen, dass kein einzelner Benutzer oder Gerät herausgegriffen oder spezifisch analysiert wird. Citrix erfasst über CEIP keine persönlich identifizierbaren Informationen (PII), und die gesamte Datenerfassung erfolgt in Übereinstimmung mit den relevanten Branchenstandards für Datenschutz und Datensicherheit.

Tools zur Erfassung von CEIP-Daten

Die Citrix Workspace-App für iOS verwendet Citrix Analytics und Google Firebase zur Erfassung der CEIP-Daten.

Erfasste Daten

Die spezifischen CEIP-Datenelemente, die von Citrix Analytics und Google Firebase erfasst werden, sind:

Sitzungsinformationen und Methode zum Starten der Sitzung	Citrix Stores und Store-Konfiguration	Authentifizierungstyp und	ICA®-Verbindungen

		Authentifizierungskonfiguration	
HDX™-Sitzungsstart	Store-App-Sitzung	WebView-Aktion öffnen	WebView-Aktion kopieren
WebView-Aktion teilen	Workspace-App-Bewertung	Verbindungsstatus, Verbindungsfehler, Nutzung des Verbindungscenters	Externes Display
Socket-Status	Sitzungsdauer	HDX über UDP	Sitzungsstartzeit
Geräteinformationen	Gerätemodellinformationen	Nutzungsstatistiken senden	App-Sprache, Workspace-App-Sprache
Tastatursprache	Citrix Store-Typ	Citrix Store-Kombination	Store-Protokolltyp
Anzahl der Stores	HDX UDP-Status	RSA-Token-Installationen	

Von welchen Benutzern werden CEIP-Daten erfasst?

Die Citrix Workspace-App erfasst die CEIP-Daten über Citrix Analytics, das so konfiguriert ist, dass es Benutzer aus allen Regionen einschließt. Die über Citrix Analytics erfassten CEIP-Daten umfassen jedoch Benutzerdaten aus der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK), während Google Firebase Benutzer in diesen Regionen ausschließt. Um sicherzustellen, dass diese Funktionalität vorhanden ist, aktualisieren Sie bitte auf die neueste Version.

Können Benutzer und Administratoren die CEIP-Datenerfassung deaktivieren?

Die CEIP-Datenerfassung kann in allen Gerichtsbarkeiten gemäß der nachstehenden Konfiguration vollständig deaktiviert werden.

Ab Version 2205 können Sie das Senden von CEIP-Daten (mit Ausnahme von zwei Datenelementen, wie in der nachstehenden Anmerkung angegeben) beenden, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Citrix Workspace-App für iOS.
2. Tippen Sie auf **Home** > **Einstellungen**.
3. Navigieren Sie zum Abschnitt **Allgemein** und deaktivieren Sie **Nutzungsstatistiken senden**.

Zusätzliche Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix. Die Daten werden wie im Citrix Services Security Exhibit beschrieben geschützt. Weitere Informationen finden Sie im Citrix Trust Center.

Citrix verwendet Google Firebase, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu erfassen. Überprüfen Sie, wie Google mit für Google Firebase erfassten Daten umgeht.

> **Hinweis:**
>
> Google Firebase schließt die Datenerfassung für Benutzer in der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK) aus.

Bekannte Einschränkungen

- Bei VDA 7.18 und früheren Versionen erfordert das Casting auf einen Workspace Hub, dass für den verwendeten Desktop oder andere Ressourcen die h.264-Vollbildrichtlinie aktiviert und die Legacy-Grafikrichtlinie deaktiviert ist.

Sitzungsfreigabe

Wenn Benutzer sich von einem Citrix Workspace-App-Konto abmelden, können sie sich weiterhin von Remotesitzungen trennen oder abmelden.

- **trennen**: Beendet die Verbindung auf diesem Gerät, aber Ihre Sitzung läuft auf dem Server weiter – Sie können später wieder eine Verbindung herstellen und dort fortfahren, wo Sie aufgehört haben. Der Benutzer kann dann ein anderes Gerät starten, die Citrix Workspace-App für iOS starten und sich wieder mit dem letzten Zustand verbinden, bevor er die Verbindung vom iOS-Gerät trennt. Diese Option ermöglicht es Benutzern, sich von einem Gerät mit einem anderen Gerät zu verbinden und die Arbeit in laufenden Anwendungen fortzusetzen.
- **Abmelden**: Meldet sich vom Konto ab und schließt die Windows-Anwendung. Es meldet sich auch vom Citrix Virtual Apps and Desktops- und Citrix DaaS-Server ab. Diese Option

ermöglicht es Benutzern, die Verbindung zum Server zu trennen und sich vom Konto abzumelden. Wenn sie die Citrix Workspace-App für iOS erneut starten, wird sie im Standardzustand geöffnet.

Cloud-Stores

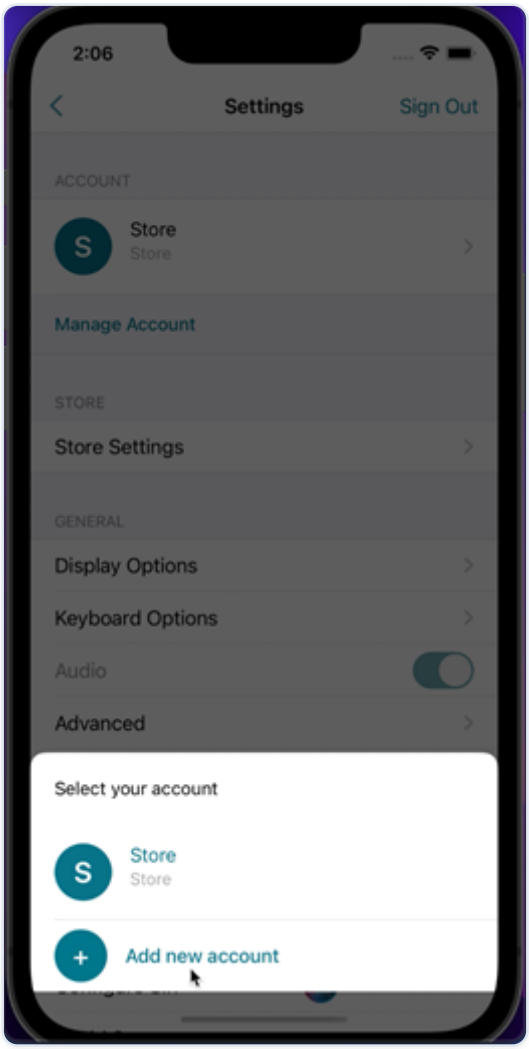
Sie können auf das Web, SaaS-Apps und von Ihrer Organisation gehostete Websites zugreifen, unabhängig von Ihrem Zugriffsstandort. Diese Funktion ist nur für Kunden mit Cloud-Stores verfügbar.

Unterstützung für mehrere Cloud-Stores

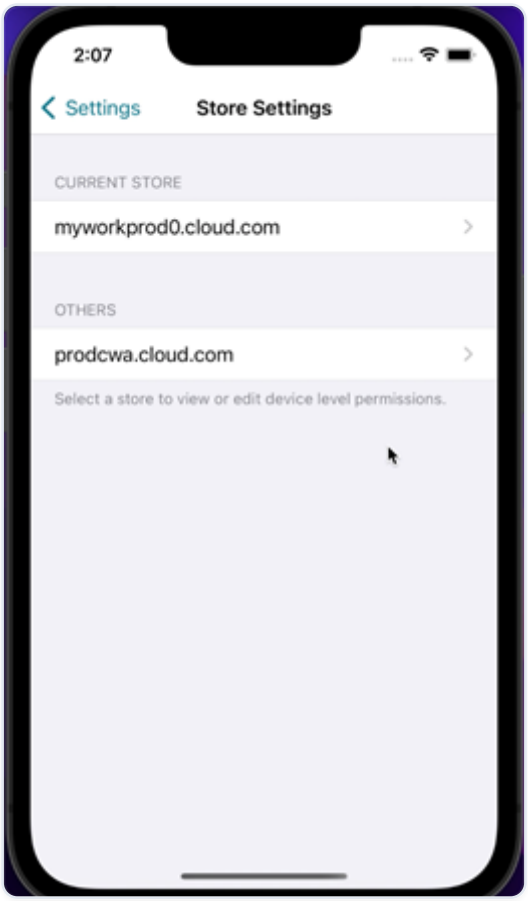
Ab der Version 24.1.0 können Sie der Citrix Workspace-App für iOS und iPadOS mehrere Cloud-Store-Konten hinzufügen. Endbenutzer können jetzt ganz einfach mehrere Stores hinzufügen und zwischen ihnen wechseln. Diese Funktion verbessert die Benutzererfahrung beim Zugriff auf mehrere Stores.

Führen Sie die folgenden Schritte aus, um ein weiteres Konto hinzuzufügen:

1. Navigieren Sie zu **Einstellungen > Konto verwalten**. Ein Dialogfeld mit einer Liste Ihrer Konten wird am unteren Bildschirmrand angezeigt.
2. Tippen Sie auf **Neues Konto hinzufügen**.



3. Geben Sie die von Ihrem IT-Administrator bereitgestellte URL oder E-Mail-Adresse ein. Um optional eine Smartcard für die Anmeldung zu verwenden, tippen Sie auf **Smartcard verwenden**.
4. Tippen Sie auf **Weiter**. Das Dialogfeld **Anmelden** wird mit Feldern für Ihren Benutzernamen, Ihr Kennwort, Ihre Domäne und Ihren Passcode angezeigt.
5. Geben Sie die Informationen ein. Weitere Informationen zu den Feldern erhalten Sie von Ihrem IT-Administrator.
6. Tippen Sie auf **Anmelden**. Ihr neues Konto ist jetzt eingerichtet.



Store-URL automatisch ausfüllen

Ab Version 23.2.0 können Sie beim Zugriff auf die umbenannte Citrix Workspace-App für iOS die Store-URL automatisch ausfüllen lassen. Diese Funktion reduziert den manuellen Aufwand und ermöglicht einen schnellen Zugriff auf die App. Weitere Informationen zur App-Personalisierung finden Sie unter App-Personalisierung.

Unterstützung für das gleichzeitige Löschen mehrerer Stores

Ab Version 24.2.0 unterstützt die Citrix Workspace-App für iOS die Auswahl und das Löschen mehrerer Stores. Diese Funktion verbessert die Benutzererfahrung bei der Arbeit mit mehreren Stores. Diese Funktion ist standardmäßig aktiviert.

Um mehrere Stores gleichzeitig vom Bildschirm **Stores** zu löschen, führen Sie die folgenden Schritte aus:

1. Tippen Sie auf dem Bildschirm **Stores** auf **Auswählen**.

2. Wählen Sie die zu löschenden Stores aus. Um alle Stores zu löschen, tippen Sie auf **Alle auswählen**.
3. Tippen Sie auf **Löschen**.

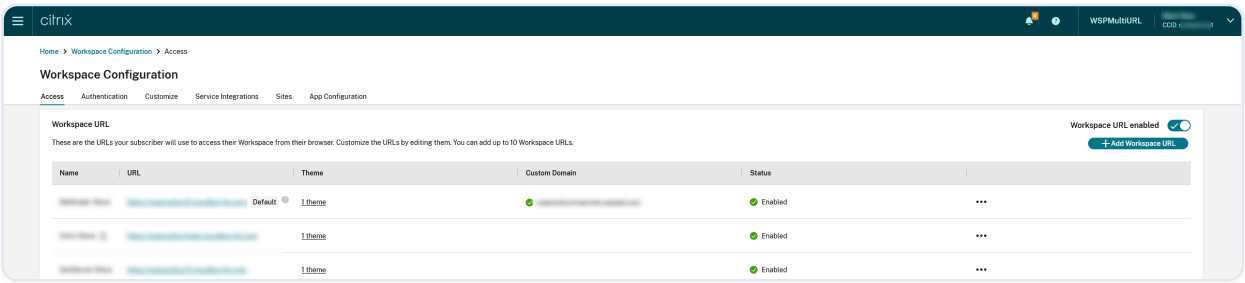
Unterstützung für Administratoren, um Benutzer daran zu hindern, den Store-Namen zu ändern

Bisher konnten Benutzer den Store-Namen über die Option **Konto bearbeiten** ändern.

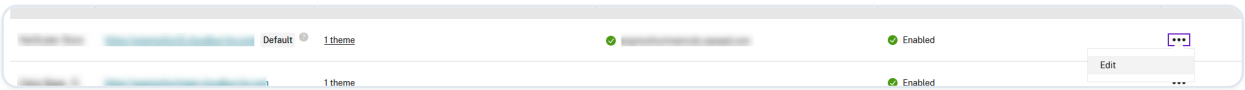
Ab Version 24.2.0 bietet die Citrix Workspace-App für iOS Administratoren die Möglichkeit, Benutzern das Ändern des Store-Namens zu untersagen. Mit dieser Funktion können Administratoren die Store-Namen leicht identifizieren und deren Konsistenz wahren.

Um Endbenutzern das Ändern des Store-Namens zu ermöglichen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich mit Ihren Anmeldeinformationen bei Citrix Cloud an.
2. Navigieren Sie zu **Workspace-Konfiguration > Zugriff**. Unter **Workspace-URL** finden Sie eine Liste der vorhandenen Store-URLs.



3. Klicken Sie auf das Ellipsenmenü des Stores, für den Sie Endbenutzern erlauben möchten, den Store-Namen zu ändern.
4. Wählen Sie **Bearbeiten**.



5. Wählen Sie im Dialogfeld **Workspace-URL bearbeiten** die Option **Endbenutzern erlauben, diesen Store-Namen in Workspace zu ändern (standardmäßig nicht erlaubt)**.

   Speichernamen deaktivieren(/en-us/citrix-workspace-app-for-ios/media/allow-admin-store.png)
6. Klicken Sie auf **Speichern**.

Speichernamen automatisch ausfüllen

Ab Version 24.2.0 unterstützt die Citrix Workspace-App für iOS die Aktualisierung von Speichernamen durch den Administrator und übermittelt die aktualisierten Speichernamen automatisch an den Benutzer. Diese Funktion verbessert die Benutzererfahrung, indem sie die Notwendigkeit manueller Eingriffe bei der Aktualisierung des Speichernamens eliminiert.

Hinweis:

Diese Funktion kann nur wirksam werden, wenn der Administrator dem Benutzer die Änderung des Speichernamens untersagt hat.

Verbesserung der Überwachung der Endbenutzererfahrung

Wir unterstützen jetzt die Client-Startmetriken von EUEM (Endbenutzererfahrungsüberwachung). EUEM hilft bei der Erfassung hochgranularer Daten zur Überwachung der Sitzungserfahrung in Echtzeit. Es sendet die Daten an das Director-Dashboard, damit der Administrator die Benutzererfahrung überwachen kann. Die Daten werden über den auf dem VDA vorhandenen Session Experience Monitoring Service (SEMS) erfasst. Die auf dem Dashboard zur Überwachung verfügbaren Client-Startmetrikdaten umfassen:

- Dauer des ICA-Dateidownloads.
- Client-Dauer der Sitzungserstellung. Die Client-Dauer der Sitzungserstellung stellt die Zeit dar, die zum Erstellen einer Sitzung benötigt wird. Sie wird ab dem Zeitpunkt des Starts einer ICA-Datei bis zum Aufbau der Verbindung berechnet.
- Client-Dauer der Sitzungssuche. Die Client-Dauer der Sitzungssuche stellt die Zeit dar, die benötigt wird, um jede Sitzung nach dem Hosten der angeforderten veröffentlichten Anwendung abzufragen. Die Überprüfung wird auf dem Client durchgeführt, um festzustellen, ob eine vorhandene Sitzung die Anwendungsstartanforderung verarbeiten kann.
- Citrix Echtzeitaufzeichnung der ICA-Roundtrip-Zeit, auch bekannt als ICA-RTT. ICA-RTT ist die Zeit, die vergeht, von dem Moment, in dem der Benutzer eine Taste drückt, bis die Antwort am Endpunkt angezeigt wird.

Verbesserte Benutzeroberfläche für den Offline-Modus der Dienstkontinuität

Ab Version 24.1.0 wurde die Benutzeroberfläche der Citrix Workspace-App für iOS verbessert, um informativer und moderner zu sein und eine benutzerfreundliche Erfahrung während Citrix Workspace-Ausfällen zu bieten. Die Fuzzy-Suchfunktion ist auch für den Offline-Modus enthalten. Mit dieser Funktion können Sie Ergebnisse für Apps oder Desktops mit eng übereinstimmendem Text und falsch geschriebenen Suchbegriffen finden. Weitere Informationen zur Dienstkontinuität finden Sie unter Dienstkontinuität.

Dienstkontinuität(/en-us/citrix-workspace-app-for-ios/media/service-continuity.png)

Unterstützung für den Global App Configuration Service-Kanal

Ab Version 23.4.5 können Administratoren jetzt den Global App Configuration Service verwenden, um Einstellungen zu definieren und diese zu testen, bevor die Konfiguration an alle Endbenutzer verteilt wird. Dieser Prozess stellt sicher, dass Funktionen und Merkmale vor der Produktion gründlich getestet werden.

> **Hinweis:**
>
> - Die Citrix Workspace-App für iOS unterstützt die Konfigurationen **Standard** und **Testkanal**. Standardmäßig befinden sich alle Benutzer im Kanal **Standard**.
>
> Weitere Informationen finden Sie in der Dokumentation zum Global App Configuration Service.

Weitere Informationen zur Konfiguration finden Sie unter Global App Configuration Service-Kanalunterstützung.

Auf Global App Configuration Service-fähige Webstores zugreifen

Ab Version 23.7.5 können Administratoren jetzt einen Webstore (Webinterface) für die e-mail-basierte Store-Erkennung konfigurieren. Basierend auf der E-Mail-Adresse, die Endbenutzer beim Hinzufügen eines Stores (auf dem Willkommensbildschirm) eingeben, hilft der Global App Configuration Service, die vom Administrator definierte benutzerdefinierte Web-URL (Webinterface) zu identifizieren. Der Endbenutzer wird dann automatisch zum vom Administrator konfigurierten Webstore weitergeleitet. Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter Zulässiges benutzerdefiniertes Webportal.

Workspace-App mit Unified Endpoint Management-Lösungen konfigurieren

Ab Version 23.3.0 unterstützt die Citrix Workspace-App für iOS die Administratorkonfiguration der Workspace-App mithilfe von AppConfig-basierten Schlüssel-Wert-Paaren unter Verwendung von Unified Endpoint Management (UEM)-Lösungen.

Konfiguration

Führen Sie die folgenden Schritte aus, um Ihre Workspace Store-URL mithilfe von Unified Endpoint Management-Lösungen zu konfigurieren:

> **Hinweis:**
>
> Zu Demonstrationszwecken wird in diesem Beispiel Microsoft Intune als UEM-Lösung verwendet. Die unten aufgeführten Schritte und die angezeigte Benutzeroberfläche unterscheiden sich je nach UEM-Anbieter.

1. Melden Sie sich bei Ihrem Unified Endpoint Management (UEM)-Anbieter an.
2. Fügen Sie die Citrix Workspace-App hinzu, die Sie von Ihrem UEM-Anbieter verwalten lassen möchten. Sie können die App über das Portal Ihres UEM-Anbieters hochladen, um die Verwaltung durch Ihren UEM-Anbieter zu ermöglichen. Alternativ können Sie die App im App Store verknüpfen.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.
4. Fügen Sie der XML-Eigenschaftsliste ein Schlüssel-Wert-Paar hinzu und geben Sie die folgenden Werte ein:
   - **Schlüssel**: `url`
   - **Werttyp**: `String`
   - **Wert**: Ihre Store-URL (zum Beispiel `prodcwa.cloud.com`)


Settings Edit

Configuration key	Value type	Configuration value
url	String	prodcwa.cloud.com

Einschränkungen

- Wenn ein Cloud-Store bereits eingerichtet ist und der Administrator einen neuen Cloud-Store konfiguriert, wird Ihr vorhandener Cloud-Store gelöscht. Dabei werden auch alle zugehörigen Daten oder Einstellungen des vorhandenen Cloud-Stores gelöscht. Sie erhalten eine Benachrichtigung in Citrix Workspace. Sie müssen sich dann erneut anmelden, damit der neue Cloud-Store zu Citrix Workspace hinzugefügt wird.
    - Die obige Aussage gilt nur für bestehende Cloud-Stores. Wenn ein lokaler Store bereits konfiguriert ist und der Administrator einen neuen Cloud- oder lokalen Store konfiguriert, wird der neue Store hinzugefügt und es erfolgt keine Löschung.
- Um neue Konfigurationen anzuwenden, müssen Sie die Citrix Workspace-App zwangsweise beenden und neu starten.

Verbesserungen an Unified Endpoint Management-Lösungen

Ab Version 23.4.5 unterstützt die Citrix Workspace-App für iOS einige weitere Konfigurationen mithilfe von AppConfig-basierten Schlüssel-Wert-Paaren zur Konfiguration der Citrix Workspace-App. Zuvor konnten Administratoren Store-URLs konfigurieren. Jetzt können Administratoren Endbenutzer daran hindern, Store-URLs zu ändern, und steuern, wie die App angezeigt wird.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

Die Details sind wie folgt:

KONFIGURATIONSSCHLÜSSEL	WERTTYP	KONFIGURATIONSWERT
`url`	`String`	Die Store-URL. Zum Beispiel, `prodcwa.cloud.com`
`storeType`	`Integer`	• (Standard) Wenn auf 1 gesetzt, können Benutzer das Laden des nativen oder Standard-Stores sehen. - Wenn auf 2 gesetzt, können Benutzer den Store in

KONFIGURATIONSSCHLÜSSEL	WERTTYP	KONFIGURATIONSWERT
		einer Weboberfläche anzeigen.
`restrict_user_store_modification`	`Boolean`	• Wenn auf **true** gesetzt, können Benutzer den Store nicht ändern (hinzufügen/löschen/bearbeiten). - Wenn auf **false** gesetzt, können Benutzer den Store ändern. **Hinweis:** Wenn das Flag auf true gesetzt ist, werden alle vorhandenen Stores gelöscht, bevor ein UEM-konfigurierter Store hinzugefügt wird.

Unterstützung für die Konfiguration des Gerätenamens über UEM

Ab Version 24.3.5 ermöglicht die Citrix Workspace-App für iOS Administratoren, Gerätenamen basierend auf Benutzergruppen über Unified Endpoint Management (UEM) zuzuweisen und zu identifizieren.

Um den Gerätenamen mit UEM zu konfigurieren, führen Sie die folgenden Schritte aus:

> **Hinweis:**
>
> Zu Demonstrationszwecken wird in diesem Beispiel Microsoft Intune als UEM-Lösung verwendet. Die folgenden Schritte und die angezeigte Benutzeroberfläche können je nach UEM-Anbieter variieren.

1. Melden Sie sich bei Ihrem UEM-Anbieter an.

2. Fügen Sie die Citrix Workspace-App hinzu, die Sie von Ihrem UEM-Anbieter verwalten lassen möchten. Sie können die App über das Portal Ihres UEM-Anbieters hochladen, um die Verwaltung durch Ihren UEM-Anbieter zu ermöglichen. Alternativ können Sie die App im App Store verknüpfen.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.
4. Fügen Sie ein Schlüssel-Wert-Paar zur XML-Eigenschaftsliste hinzu und geben Sie die folgenden Werte ein:
    - Schlüssel: deviceName
    - Werttyp: String
    - Wert: Name des Geräts (zum Beispiel, MY_IPHONE_Device)

Gerätename(/en-us/citrix-workspace-app-for-ios/media/device-name.png)

Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen über UEM

Zuvor konnten Sie die Store-URL in der Citrix Workspace-App nur über das Unified Endpoint Management (UEM) konfigurieren.

Ab Version 24.7.0 können Sie die Einstellungen der Citrix Workspace-App auf den verwalteten Geräten auch mit jeder UEM-Lösung konfigurieren, die in Ihrer Infrastruktur bereitgestellt wird.

> **Hinweis:**

> Als Administrator gilt: Wenn Sie die Möglichkeit haben, die Einstellungen der Citrix Workspace-App über UEM und den Global App Configuration Service (GACS) zu konfigurieren, haben die UEM-Einstellungen Vorrang vor GACS.

> Im Folgenden finden Sie eine JSON-Beispieldatei zur Konfiguration der Citrix Workspace-App-Einstellungen:

```
<dict>

    <key>stores</key>

    <array>
```

```
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store 1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
                            <key>value</key>
                            <true/>
                        </dict>
```

```
                </array>
            </dict>
            <dict>
                <key>category</key>
                <string>authentication</string>
                <key>userOverride</key>
                <false/>
                <key>settings</key>
                <array>
                    <dict>
                        <key>name</key>
                        <string>settings_auth_web_browser</string>
                        <key>value</key>
                        <string>embedded</string>
                    </dict>
                </array>
            </dict>
        </array>
    </dict>
    <dict>
        <key>url</key>
        <string>https://teststore.cloud.com</string>
```

```
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>StoreFront1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
                            <key>value</key>
                            <false/>
                        </dict>
                    </array>
                </dict>
                <dict>
```

```
                <key>category</key>
                <string>authentication</string>
                <key>userOverride</key>
                <false/>
                <key>settings</key>
                <array>
                    <dict>
                        <key>name</key>
                        <string>settings_auth_web_browser</string>
                        <key>value</key>
                        <string>system</string>
                    </dict>
                </array>
            </dict>
        </array>
    </dict>
</array>
<key>storesToDelete</key>
<array>
    <string>test.cldblr.com</string>
    <string>test.cloud.com</string>
</array>
```

```
    <key>restrict_user_store_modification</key>
    <false/>
</dict>
```

Hinweis:

Das `userOverride`-Flag ermöglicht es dem Benutzer, die Einstellungen der Citrix Workspace-App zu ändern. Wenn das `userOverride`-Flag auf „true“ gesetzt ist, kann der Benutzer die Einstellungen ändern. Wenn das `userOverride`-Flag für bestimmte Einstellungen auf „false“ gesetzt ist, kann der Benutzer diese in den Einstellungen der Citrix Workspace-App nicht ändern.

Schlüssel-Wert-Paar-Tabelle für Workspace-App-Einstellungen

Die folgende Tabelle enthält die Informationen zu den Schlüssel-Wert-Paaren:

Hinweis:

Sie müssen Einstellungen, die für eine Kategorie spezifisch sind, in einem Block unter dieser Kategorie hinzufügen.

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Authentifizierung	Aufforderung zur Verwendung von Biometrie überspringen	Aktiviert oder deaktiviert die biometrische Authentifizierung.	settings_skip_consent_for_biometric_protected_password_saving Wert	true/false	Boolesch	FALSCH

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Audio	Audio	Ermöglicht Benutzern, den Ton in der virtuellen App oder auf dem Desktop ein- oder auszuschalten.	settings_audio_stream	true/false	Boolesch	WAHR
Tastatur	Unicode-Tastatur verwenden	Ermöglicht Benutzern die Verwendung einer Standard-Unicode-Tastatur.	settings_use_unicode_keyboard	true/false	Boolean	WAHR
Tastatur	Automatische Tastatur	Aktiviert oder deaktiviert die In-Session-Tastatur.	settings_automatic_keyboard	true/false	Boolean	WAHR
Tastatur	Tastaturlayout-Synchronisierung	Ermöglicht Benutzern, zu einem	settings_keyboard_layout_sync	true/false	Boolean	FALSCH

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		bevorzugten Tastaturlayout auf dem Gerät zu wechseln.				
Tastatur	Benutzerdefinierte Tastaturen verwenden	Ermöglicht Benutzern die Verwendung von Tastaturen von Drittanbietern, die in der virtuellen Sitzung heruntergeladen werden.	settings_allow_keyboard_extensions	true/false	Boolesch	FALSCH
Anzeige	Sitzungsauflösung	Ermöglicht Benutzern die Auswahl der Bildschirmauflösung.	settings_resolution	0–9	Integer	5 (iPad) 3 (iPhone)

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Anzeige	Präsentationsmodus	Ermöglicht Ihnen, Ihr iOS-Gerät als Trackpad zur Steuerung Ihrer Sitzung zu verwenden, während Sie ein externes Display nutzen.	settings_presentation_mode	true/false	Boolean	FALSCH
Display	Externes Display	Verbindet ein externes Display mit dem Gerät.	settings_external_display	true/false	Boolean	WAHR
Erweitert	Strenge Zertifikatvalidierung	Erzwingt eine strengere Kontrolle bei der Serverzertifikatvalidierung.	settings_strictCertValidation	true/false	Boolean	FALSCH
Erweitert	TLS-Versionen	Ermöglicht Benutzer	settings_tlsVersion	0–3	Integer	0

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		n, ihre TLS-Einstellungen zu Fehlerbehebungszwecken zu ändern.				
Erweitert	Natives Kombinationsfeld verwenden	Ermöglicht die Verwendung der nativen iOS-Auswahlfunktion.	settings_native_combobox	true/false	Boolesch	TRUE
Erweitert	Touch-Aktivierung (nur iPad)	Aktiviert Touch für alle Apps und Desktops, einschließlich derer, die die Touch-Option nicht nativ aktiviert haben.	settings_multitouch_on	true/false	Boolesch	wahr (iPad) falsch (iPhone)

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Erweitert	Vollbildansicht	Ermöglicht die Anzeige Ihrer Apps und Desktops im Vollbildmodus.	settings_mobile_window_fullscreen	true/false	Boolesch	wahr (iPad) falsch (iPhone)
Erweitert	Wiederverbindung bei Anmeldung	Ermöglicht die automatische Wiederverbindung einer Sitzung, wenn ein neues Konto hinzugefügt wird oder während der Anmeldung.	settings_reconnect_logon	true/false	Boolesch	FALSE
Erweitert	Wiederverbindung bei Aktualisierung	Stellt automatisch eine Verbindung zu einer Sitzung her, die	settings_reconnect_refresh	true/false	Boolesch	FALSCH

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		von einem anderen Gerät gestartet wurde, wenn die Apps oder Desktops auf dem zweiten Gerät aktualisiert werden.				
Erweitert	HTTP-Proxy aktivieren	Ermöglicht die Verwendung des HTTP-Proxys für eine Sitzung.	settings_use_local_proxy	true/false	Boolesch	WAHR
Erweitert	Abgeleitete Anmeldeinformationen verwenden	Ermöglicht die Verwendung abgeleiteter Anmeldeinformationen.	setting_useDerivedCredentials	true/false	Boolesch	FALSCH

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
erweitert	Smartcard in Sitzung	Ermöglicht die Verwendung eines Smartcard-Geräts innerhalb einer Sitzung. Diese Einstellung erlaubt Benutzern nicht, sich bei der Sitzung zu authentifizieren.	settings_usesSmartCardInsideSession	true/false	Boolesch	FALSCH
erweitert	EDT zulassen	Aktiviert die Unterstützung für adaptiven Transport.	settings_allowUdp	true/false	Boolesch	WAHR
erweitert	Automatischer Tablet-Modus	Ermöglicht das Starten der virtuellen Sitzung	settings_enableTabModeSwitch	true/false	Boolesch	WAHR

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		im Tablet-Modus, wenn keine externe Tastatur oder Maus erkannt wird.				
Erweitert	Bildschirm eingeschaltet lassen	Den Bildschirm eingeschaltet lassen.	settings_stay_awake	true/false	Boolesch	FALSCH
Erweitert	iPad-Speicher verwenden	Ermöglicht den Zugriff auf lokale Laufwerke auf Ihrem Gerät.	settings_client_drive	true/false	Boolesch	falsch
X1-Maus	X1-Maus zulassen	Ermöglicht Ihnen, den Zugriff auf Ihre Citrix X1-Maus umzuschalten.	settings_allow_X1_mouse	true/false	Boolesch	FALSCH

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
X1-Maus	Citrix® X1-Mausgeschwindigkeit	Ermöglicht Benutzern, die Geschwindigkeit des Mauszeigers innerhalb der virtuellen Sitzung zu steuern.	settings_x1MouseSpeed	1,2	Integer	200 (iPadPro) 100 (Alle anderen Geräte)
X1-Maus	Remote-Cursorbild fürCitrix X1-Maus verwenden	Der Cursor wird an die App oder den Desktop innerhalb einer Sitzung angepasst. Wenn sich der Cursor beispielsweise über einem Textfeld befindet, ändert er sich entsprec	settings_X1_mouse_server_side_cursor	true/false	Boolesch	WAHR

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		hend dem Textfeld.				
Authentifizierung	Webbrowser für die Authentifizierung	Ermöglicht es Ihnen, die Verwendung von SafariViewController anstelle von WKWeb auf dem Gerät zu identifizieren.	settings_auth_web_browser	System/eingebettet	String	Eingebettet
thirdPartyServices	LaunchDarkly	Aktiviert das LaunchDarkly-Flag für die Funktionen der Citrix Workspace-App.	enableLaunchDarkly	true/false	Boolesch	wahr (Nicht-EU-Regionen)

Schlüssel-Wert-Paar-Tabelle für neue Symbolleisten-Menüoptionen

Die folgende Tabelle enthält die Schlüssel-Wert-Paar-Informationen für die neue Symbolleiste:

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Symbolleiste	Neue Symbolleiste	Der Schlüssel, der die neue Symbolleiste aktiviert.	enableNewToolbar	true/false	Boolesch	WAHR
Symbolleiste	trennen	Bietet Optionen zum Abmelden von der Sitzung, zum trennen der Sitzung oder zum Abbrechen der Aktion.	enableCloseToolbarOption	true/false	Boolesch	WAHR
Symbolleiste	Tastatur	Aktiviert oder deaktiviert die Tastatur innerhalb der Sitzung.	enableKeyboardToolbarOption	true/false	Boolesch	WAHR
Symbolleiste	Zeiger	Aktiviert oder deaktiviert den Zeiger in einer Sitzung.	enablePointerToolbarOption	true/false	Boolesch	WAHR

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Symbolleiste	Bildschirmlupe	Vergrößert den ausgewählten Bereich der Sitzung.	enableMagnifierToolbarOption	true/false	Boolesch	WAHR
Symbolleiste	Apps wechseln	Ermöglicht das Wechseln zwischen geöffneten Apps.	enableSwitchAppsToolbarOption	true/false	Boolesch	WAHR
Symbolleiste	Verbindungsstärke	Zeigt die Netzwerkverbindungsstärke der Sitzung an.	enableConnectionStrengthToolbarOption	true/false	Boolesch	WAHR
Symbolleiste	Strg+Alt+Entf	Bietet Optionen zum Schließen, Sperren oder Abmelden der Sitzung.	enableCtrlAltDelToolbarOption	true/false	Boolean	TRUE
Symbolleiste	Geräte	Ermöglicht die Verbindung zu externen Geräten	enableDevicesToolbarOption.	true/false	Boolean	TRUE

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Symbolleiste	Devices-Pair	Ermöglicht die Kopplungsoption mit externen Peripheriegeräten.	enablePairToolbarOption	true/false	Boolean	TRUE
Symbolleiste	Virtuelle Maus	Aktiviert die virtuelle Maus in der Sitzung.	enableSoftMouseToolbarOption	true/false	Boolesch	TRUE
Symbolleiste	Pfeiltasten	Aktiviert die vier Pfeiltasten, mit denen der Benutzer innerhalb der Sitzung navigieren kann.	enableArrowKeysToolbarOption	true/false	Boolesch	TRUE
Symbolleiste	Anzeige	Führt den Benutzer zu den Anzeigeeinstellungen der CWA-App.	enableDisplaySettingsToolbarOption.	true/false	Boolesch	TRUE
Symbolleiste	Casting	Aktiviert oder deaktivier	enableCastingToolbarOption.	true/false	Boolean	TRUE

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		t die Casting-Funktionalität				
Symbolleiste	Kamera	Ermöglicht Benutzern, die vordere, hintere oder externe Kamera zu aktivieren.	enableCameraToolbarOption	true/false	Boolean	TRUE
Symbolleiste	Dokument scannen	Ermöglicht Benutzern, ein Dokument innerhalb der Desktopsitzung zu scannen.	enableScanDocumentToolbarOption	true/false	Boolean	TRUE
Symbolleiste	Hilfe	Aktiviert das Hilfemenü, das für Erstanwender nützlich ist, um im Symbolleistenmenü	enableHelpToolbarOption	true/false	Boolean	TRUE

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
		zu navigieren.				

Schlüssel-Wert-Paar-Tabelle für Sitzungswiederverbindungseinstellungen

Die folgende Tabelle enthält die Schlüssel-Wert-Paar-Informationen für die neue Symbolleiste:

KATEGORIE	EINSTELLUNG	BESCHREIBUNG	SCHLÜSSEL	WERT	WERTTYP	STANDARDWERT
Erweitert	Sitzungswiederverbindung	Aktiviert die Sitzungswiederverbindung	settings_manual_reconnect	true/false	Boolean	TRUE

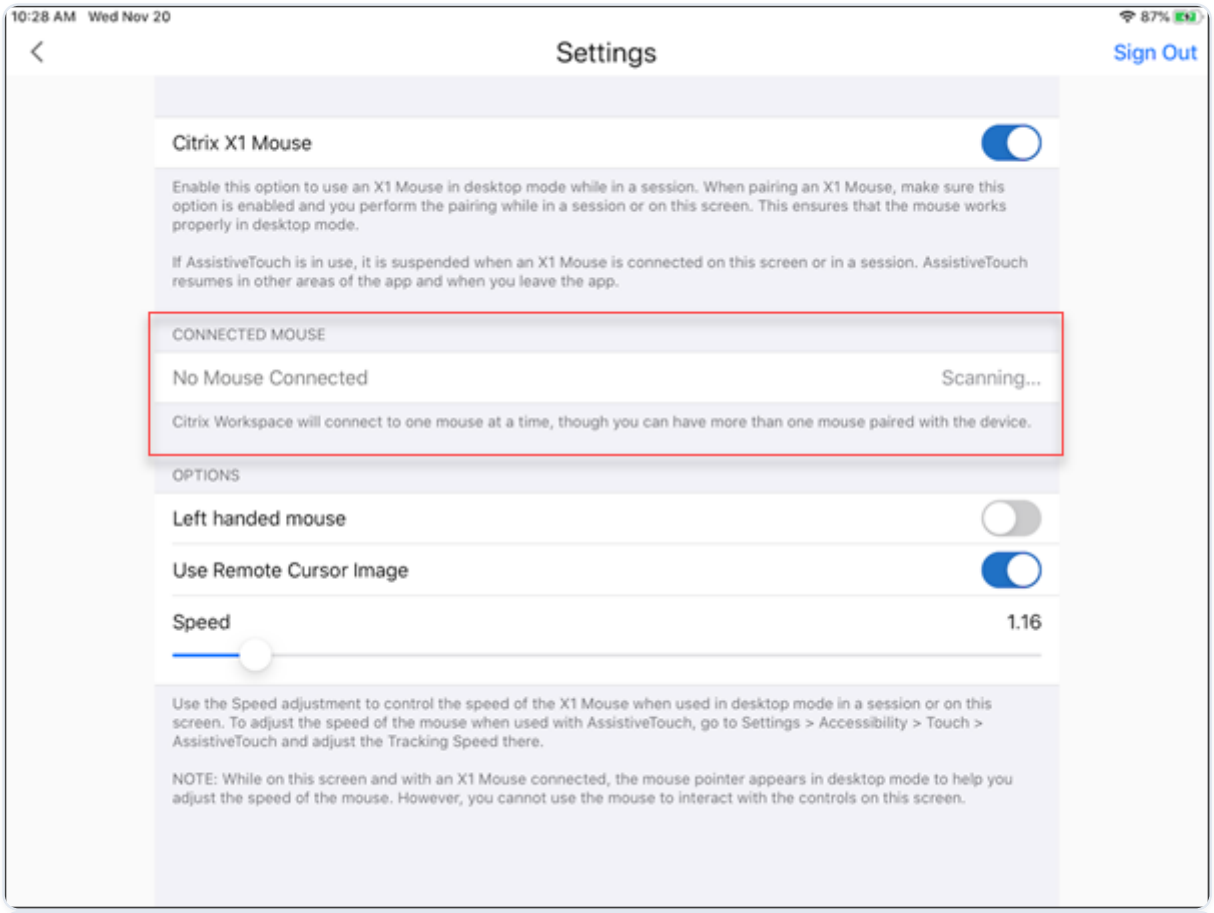
Peripheriegeräte

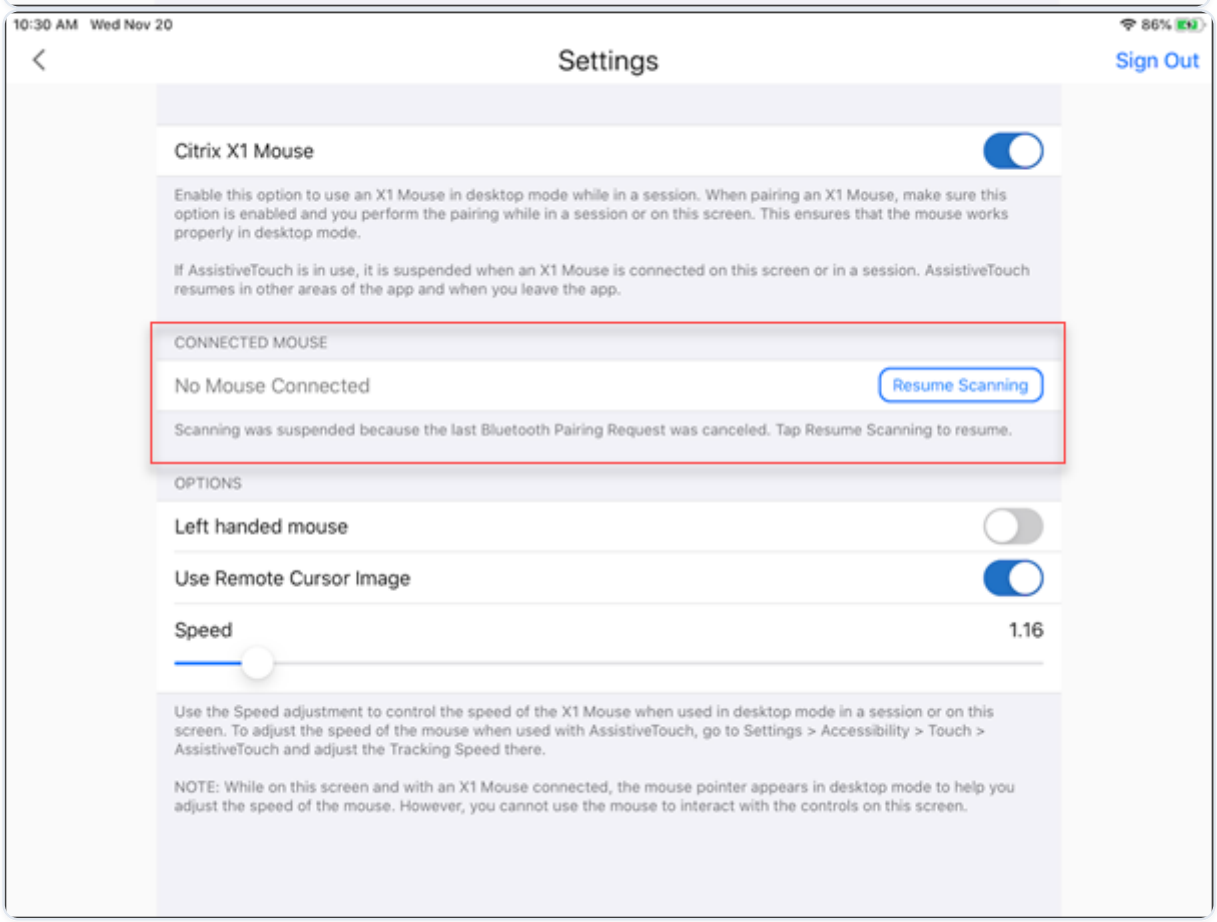
Citrix® X1 Maus

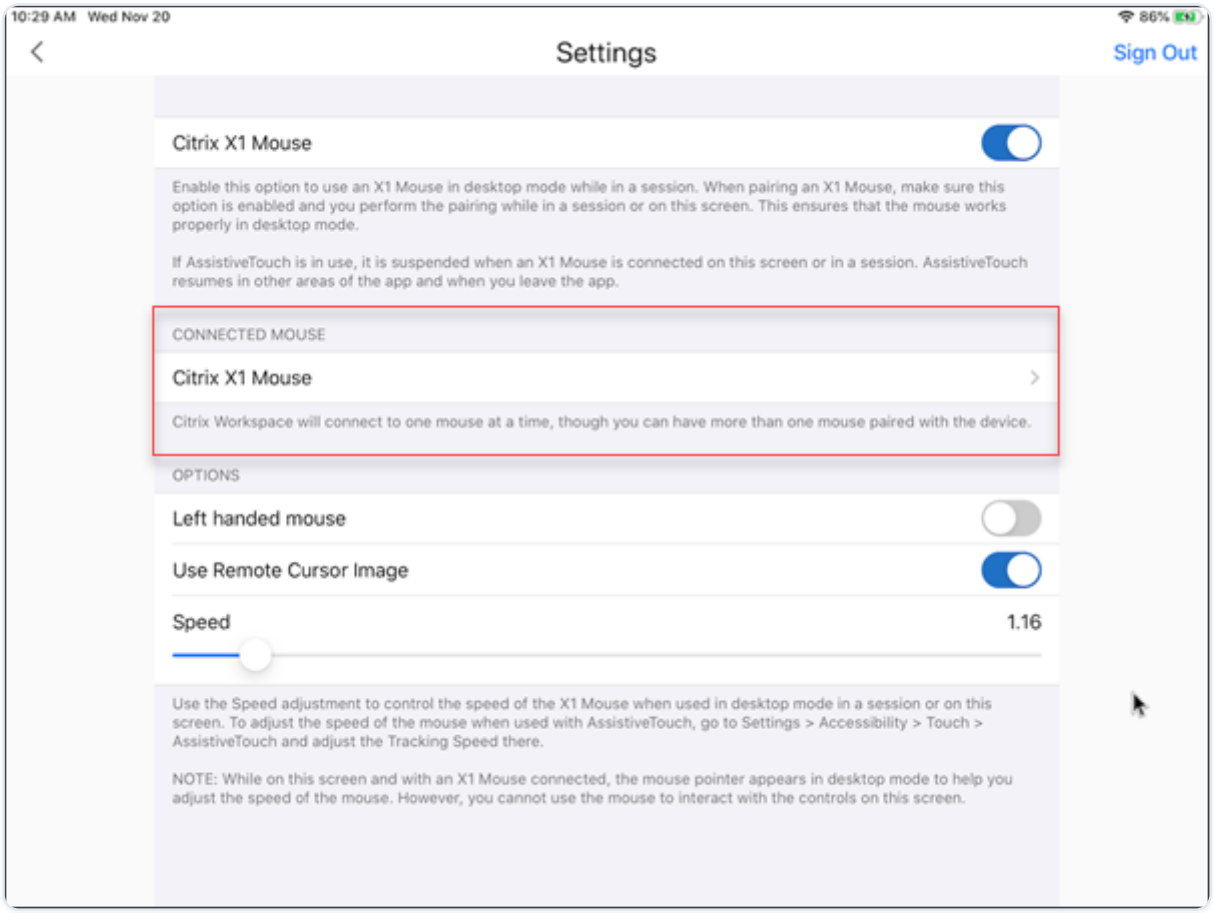
Citrix X1 Maus: Kopplungs- und Verbindungsstatus

Mit dieser Funktion haben Sie mehr Kontrolle über den Kopplungsvorgang der Citrix X1 Maus. Auf dem Bildschirm **Einstellungen** können Sie:

- Koppeln Sie die Citrix X1 Maus. Sie können eine X1 Maus auch während einer Sitzung koppeln.
- Den Verbindungsstatus anzeigen.


10:28 AM Wed Nov 20
87%
Settings
Sign Out
Citrix X1 Mouse
Enable this option to use an X1 Mouse in desktop mode while in a session. When pairing an X1 Mouse, make sure this option is enabled and you perform the pairing while in a session or on this screen. This ensures that the mouse works properly in desktop mode.
If AssistiveTouch is in use, it is suspended when an X1 Mouse is connected on this screen or in a session. AssistiveTouch resumes in other areas of the app and when you leave the app.
CONNECTED MOUSE
No Mouse Connected
Scanning...
Citrix Workspace will connect to one mouse at a time, though you can have more than one mouse paired with the device.
OPTIONS
Left handed mouse
Use Remote Cursor Image
Speed
1.16
Use the Speed adjustment to control the speed of the X1 Mouse when used in desktop mode in a session or on this screen. To adjust the speed of the mouse when used with AssistiveTouch, go to Settings > Accessibility > Touch > AssistiveTouch and adjust the Tracking Speed there.
NOTE: While on this screen and with an X1 Mouse connected, the mouse pointer appears in desktop mode to help you adjust the speed of the mouse. However, you cannot use the mouse to interact with the controls on this screen.

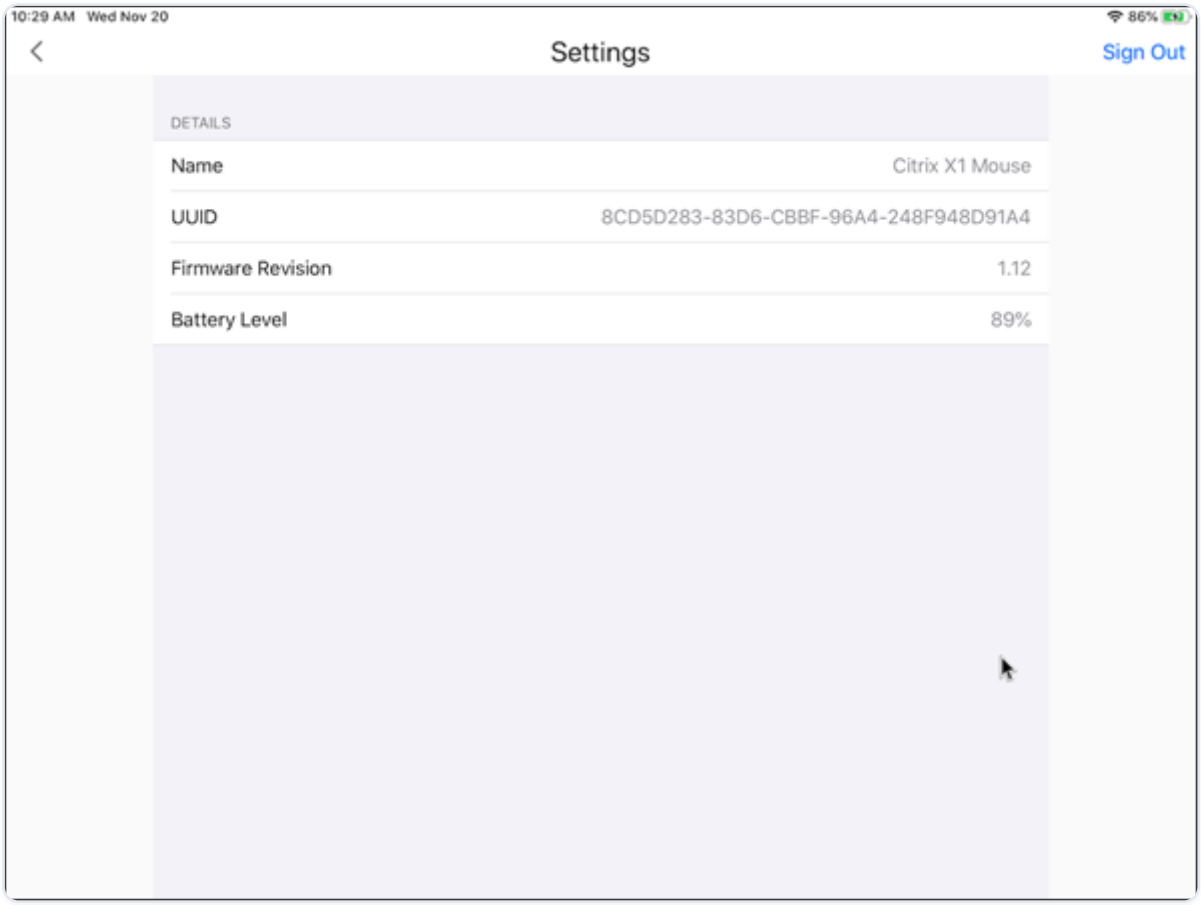

10:30 AM Wed Nov 20
86%
Settings
Sign Out
Citrix X1 Mouse
Enable this option to use an X1 Mouse in desktop mode while in a session. When pairing an X1 Mouse, make sure this option is enabled and you perform the pairing while in a session or on this screen. This ensures that the mouse works properly in desktop mode.
If AssistiveTouch is in use, it is suspended when an X1 Mouse is connected on this screen or in a session. AssistiveTouch resumes in other areas of the app and when you leave the app.
CONNECTED MOUSE
No Mouse Connected
Resume Scanning
Scanning was suspended because the last Bluetooth Pairing Request was canceled. Tap Resume Scanning to resume.
OPTIONS
Left handed mouse
Use Remote Cursor Image
Speed
1.16
Use the Speed adjustment to control the speed of the X1 Mouse when used in desktop mode in a session or on this screen. To adjust the speed of the mouse when used with AssistiveTouch, go to Settings > Accessibility > Touch > AssistiveTouch and adjust the Tracking Speed there.
NOTE: While on this screen and with an X1 Mouse connected, the mouse pointer appears in desktop mode to help you adjust the speed of the mouse. However, you cannot use the mouse to interact with the controls on this screen.



- Zeigen Sie die Eigenschaften der Citrix X1 Maus an, z. B. **Name**, **UUID**, **Firmware-Revision** und **Akkustand**. Tippen Sie dazu auf den Eintrag der Citrix X1 Maus unter **VERBUNDENE MAUS**.



Eigenschaften der verbundenen Maus:



AssistiveTouch

Wenn die AssistiveTouch-Funktion unter iOS 13 oder höher aktiviert ist, wird der AssistiveTouch-Cursor angezeigt, wenn Sie zwischen dem Desktop-Mausmodus und dem AssistiveTouch-Modus wechseln.

> **Hinweis:**

> Im Desktop-Mausmodus wird der Zeigercursor angezeigt. Im AssistiveTouch-Modus wird der runde Cursor angezeigt.

> Der AssistiveTouch-Cursor wird in den folgenden Fällen angezeigt:

- Eine Sitzung verlassen
- Zum iOS App-Umschalter-Bildschirm wechseln
- Zum iOS-Startbildschirm oder einer anderen App wechseln

Der Desktopmodus wird fortgesetzt, wenn Sie zur Citrix Workspace-App zurückkehren und sich in einer Sitzung befinden.

Unterstützung für externen Monitor und Symbolleiste

Sie können die Citrix X1-Maus verwenden, um die Symbolleiste auf einem externen Monitor zu bedienen. Sie können die Kerbe der Symbolleiste horizontal verschieben, während die Symbolleiste geschlossen ist. Wenn Sie Ihr iOS-Gerät an den externen Monitor anschließen, erkennt die Citrix Workspace-App automatisch die Bildschirmauflösung des externen Monitors. Sie können die Schaltfläche **Anzeige** in der Symbolleiste verwenden, um eine bestimmte Bildschirmauflösung auszuwählen. Sie können auf die Option **Anzeige** zugreifen, ohne zuerst ein Konto hinzufügen oder sich anmelden zu müssen.

Generische Maus

Unterstützung für generische Maus und Trackpad

Sie können eine generische Maus oder ein Trackpad verwenden, um in HDX™-Sitzungen mit der rechten Maustaste zu klicken, zu scrollen und zu schweben. Die Aktionen ähneln denen der Citrix X1-Maus. Der Stil des lokalen Mauszeigers ändert sich, um dem des Remote-Cursors zu entsprechen.

> **Hinweise:**

- Diese Funktion ist unter iPadOS 13.4 und höher verfügbar.
- Diese Funktion wird auf iPhones nicht unterstützt.

Einschränkung

Wenn Sie während einer Sitzung einen externen Monitor angeschlossen haben, verbleibt der generische Mauszeiger aufgrund einer iOS-Einschränkung auf dem nativen Gerät.

Unterstützung für generische Maus auf externen Monitoren

Sie können eine generische Maus auf externen Monitoren verwenden, die an ein iPad angeschlossen sind. Eine generische Maus wird auf Geräten mit iOS 13.4 oder höher unterstützt.

> **Wichtig:**

Um eine generische Maus mit externen Monitoren zu verwenden, stellen Sie sicher, dass der **Präsentationsmodus** in Ihrer Citrix Workspace-App deaktiviert ist, indem Sie zu **Einstellungen** > **Anzeigeoptionen** navigieren.

Die Symbolleiste auf dem externen Monitor ist ausgeblendet, wenn Sie eine generische Maus verwenden. Außerdem wird der Mauszeiger auf dem externen Monitor gespiegelt und erscheint gleichzeitig auf Ihrem iPad-Bildschirm und auf dem externen Monitor.

Erweiterte Unterstützung für mehrere Monitore mit generischer Maus für iPad

Sie können die Desktopsitzung auf einen externen Monitor erweitern, wenn Sie Ihr iPad mit einer generischen Maus verbinden. Diese Funktion unterstützt iPadOS Version 14.0 und höher.

Hinweis:

- Diese Funktion kann in früheren Versionen teilweise verfügbar sein. Um die vollständige Funktion zu nutzen, aktualisieren Sie auf Version 22.1.0.
- Deaktivieren Sie AssistiveTouch in den iOS-**Einstellungen** > **Bedienungshilfen** > **Tippen** > **AssistiveTouch**, damit die Citrix Workspace-App primäre Mausklicks empfangen kann.

Erweiterten Modus konfigurieren

So aktivieren Sie den **Erweiterten** Modus:

1. Verbinden Sie den externen Monitor mit dem iPad mithilfe des HDMI-Kabels und der erforderlichen Adapter.

   Hinweis:

   Die Einrichtung funktioniert am besten mit einem USB-C Digital AV Multiport Adapter oder Lightning Digital AV Adapter von Apple.

2. Navigieren Sie zu den Anwendungs-**Einstellungen** > **Anzeigeoptionen** und schalten Sie die **Externe Anzeige EIN**. Es erscheinen verschiedene Anzeigemodi. Spiegel- und Präsentationsmodi verwenden ebenfalls eine generische Maus, wenn die iPadOS-Version 14.0 oder höher ist.

3. Wählen Sie die Option **Erweitern**.



Sie können einen der folgenden Anzeigemodi auswählen:

- Spiegeln: Ermöglicht es Ihnen, die Anzeige auf dem externen Monitor, der mit dem iPad verbunden ist, zu spiegeln.
- Präsentation: Ermöglicht es Ihnen, Ihren externen Monitor in ein Trackpad umzuwandeln.
- Erweitern: Ermöglicht es Ihnen, verschiedene Ansichten oder Bildschirme auf jeder Anzeige darzustellen.

Hinweis:

- Stellen Sie den Modus **Erweitern** ein, bevor Sie die Desktopsitzung starten und erweitern.
- Der Modus **Erweitern** wird auf dem iPhone bis auf Weiteres nicht unterstützt.

Anzeigearrangement konfigurieren

So konfigurieren Sie das Anzeigearrangement:

1. Wählen Sie den Modus **Erweitern** aus, die Option **Anzeigearrangement** wird angezeigt.
2. Positionieren Sie die Kachel **Externes Display** links, oben, rechts oder unten zur iPad-Anzeige neu.

Hinweis:

Sie können das Anzeigearrangement während einer Sitzung über die In-Session-Symbolleiste > Symbol für die Einstellung **Anzeige** anpassen.



Hinweis:

Die Auflösung des externen Displays hängt ab von:

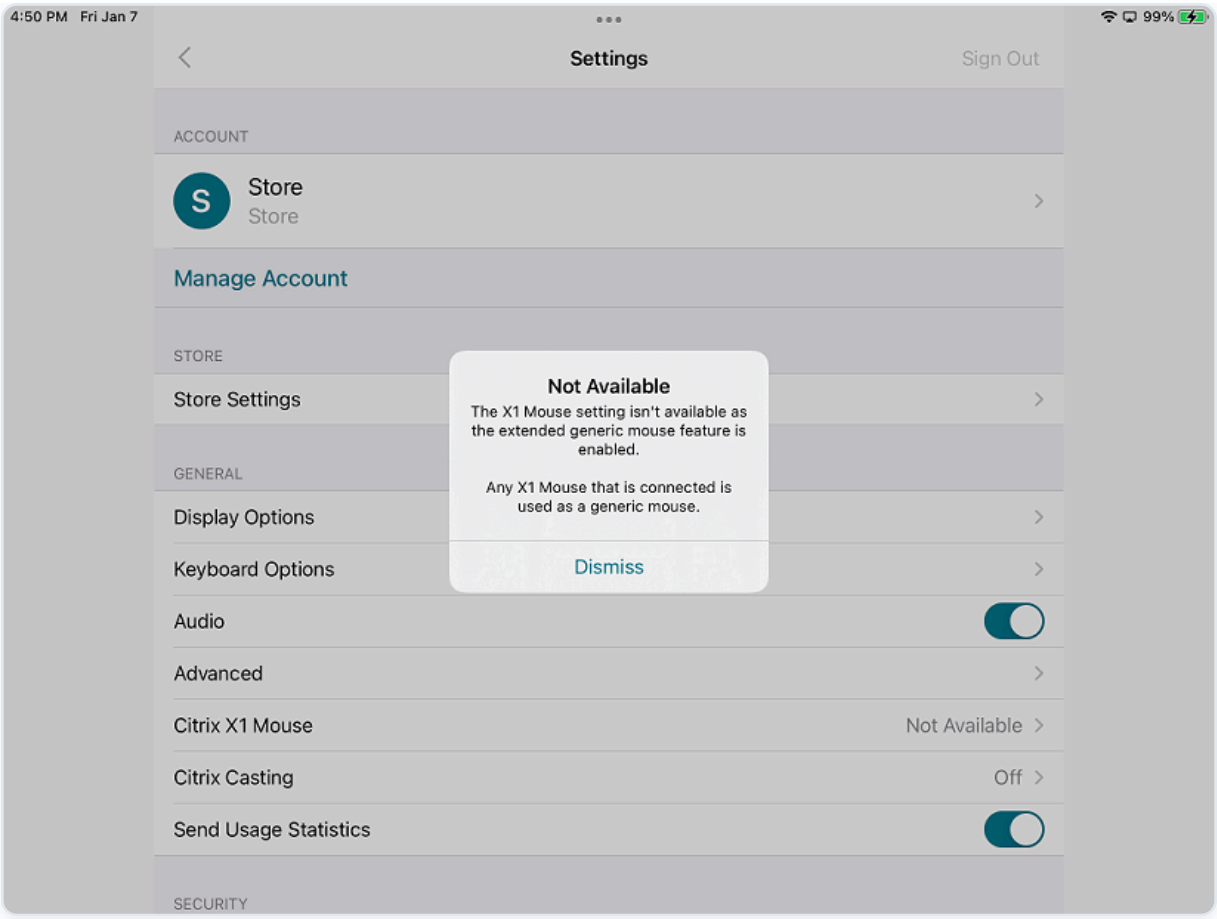
- Adaptern
- iPad
- verwendeter anderer Hardware

Generischer Mausmodus versus Citrix X1 Mausmodus

Der generische Mausmodus hat automatisch Vorrang vor dem Citrix X1 Mausmodus. Wenn eine X1 Maus angeschlossen ist, wird sie stattdessen als generische Maus verwendet. Daher ist die Einstellungsseite der X1 Maus nicht zugänglich, wenn das Feature-Flag für die generische Maus aktiviert ist.

Hinweis:

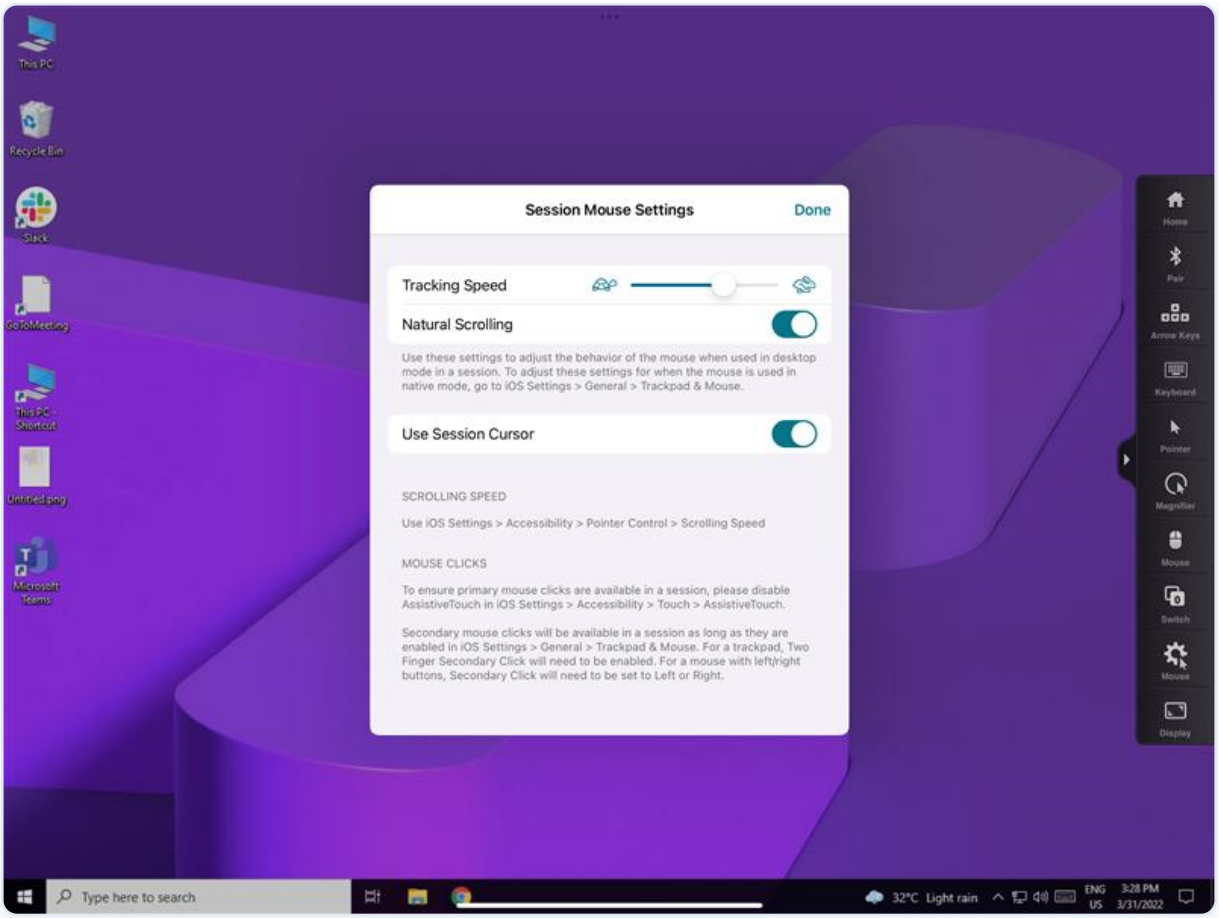
Für iPadOS Version 14.0 und höher verhält sich jede X1 Maus, die mit dem iPad verbunden ist, wie eine Bluetooth-Maus.



Symbol für generische Maus

Das Symbol für die **Mauseinstellungen** wird in der In-Session-Symbolleiste neben dem Symbol für die **Anzeigeeinstellungen** hinzugefügt. Verwenden Sie die **Mauseinstellungen**, um die Tracking-Geschwindigkeit der generischen Maus während einer Sitzung anzupassen. Sie können auch die Verwendung des Remote-Cursorbilds umschalten.

> **Hinweis:**
>
> Sie können die Tracking-Geschwindigkeit der nativen Maus in den iOS-Einstellungen anpassen.



Funktionseinschränkungen

- Um sicherzustellen, dass die Citrix Workspace-App primäre Mausklicks empfängt, deaktivieren Sie AssistiveTouch in den iOS-**Einstellungen** > **Bedienungshilfen** > **Tippen** > **AssistiveTouch**.
- Die Optionen für Tracking-Geschwindigkeit und natürliches Scrollen in den iOS-Einstellungen wirken sich nicht auf die generische Maus innerhalb der Sitzung aus. Die Scrollgeschwindigkeit

kann jedoch über die iOS-**Einstellungen** gesteuert werden. Sie können die Optionen für Tracking-Geschwindigkeit und natürliches Scrollen über den Bildschirm **Mauseinstellungen** in der Sitzungssymbolleiste aufrufen.

- Wenn ein iPad im Split-Modus verwendet wird und der Monitor angeschlossen ist, funktioniert die generische Maus nur im Spiegelmodus innerhalb einer Desktopsitzung.
- Befindet sich der native Cursor über dem Multitasking-Menü, bevor die App die Zeigersperre erhält, d. h. vor dem Start der Sitzung, werden die Mausereignisse nicht empfangen. Als Problemumgehung ziehen Sie das Benachrichtigungszentrum herunter, bewegen den nativen Zeiger an eine andere Position und schließen das Benachrichtigungszentrum.
- Die Audioumleitung schlägt fehl, wenn Sie ein iPad an einen externen Monitor anschließen. Der Ton wird über die iPad-Lautsprecher wiedergegeben.

Bekannte Probleme in der Funktion

- Während die Sitzung aktiv ist, wird das Desktop-Bild, das auf einem iPad oder einem externen Monitor angezeigt wird, gestört, wenn Sie Folgendes ändern:
  - Bildschirmanordnung
  - Auflösung
  - Ausrichtung oder
  - Anzeigemodi

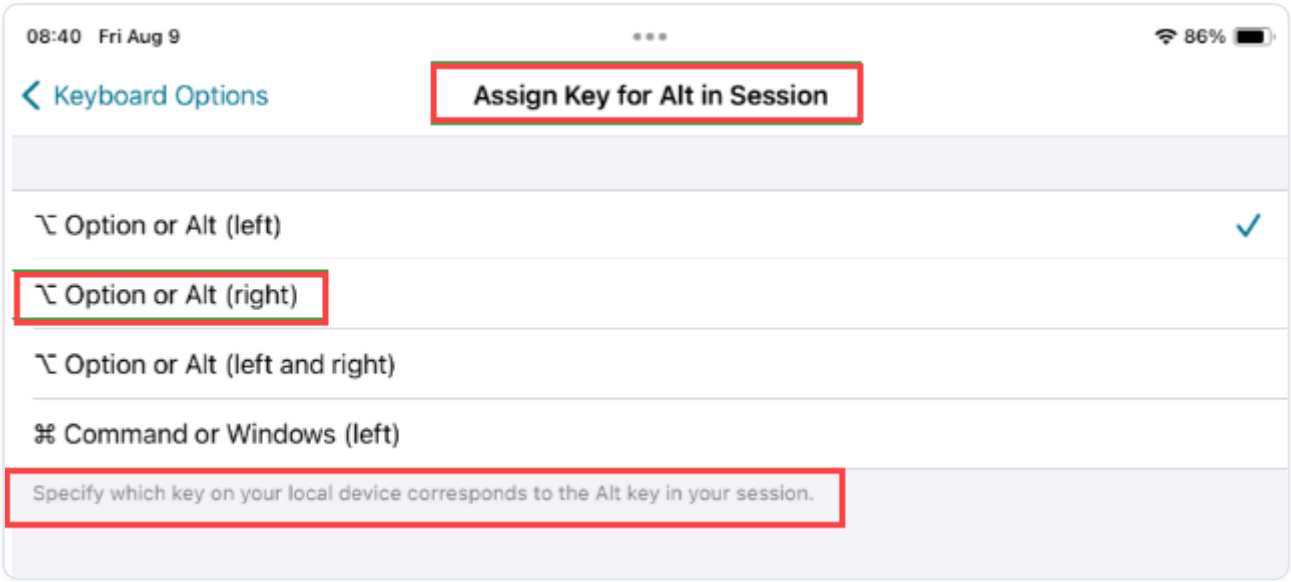
  Als Problemumgehung trennen Sie den Monitor und verbinden Sie ihn erneut. Wenn das Problem weiterhin besteht, trennen Sie die Verbindung und starten Sie die Sitzung neu. .
- In seltenen Fällen kann es zu einer Verzögerung von einigen Sekunden im Audio kommen, wenn das Video auf dem externen Monitor wiedergegeben wird.
- In seltenen Fällen wird die VDA-Anzeige auf einem iPad und auf dem externen Monitor abgeschnitten. Als Problemumgehung trennen Sie den Monitor und verbinden Sie ihn erneut. Wenn das Problem weiterhin besteht, trennen Sie die Verbindung und starten Sie die Sitzung neu.
- Wenn Sie das Video auf dem externen Monitor im Vollbildmodus maximieren, können Probleme mit der Videoqualität auftreten.
- In seltenen Fällen schlägt innerhalb einer Desktopsitzung der Versuch fehl, Apps von einem iPad auf den externen Monitor zu verschieben. Als Problemumgehung trennen Sie den Monitor und verbinden Sie ihn erneut. Wenn das Problem weiterhin besteht, trennen Sie die Verbindung und starten Sie die Sitzung neu.

- In seltenen Fällen sind die Anzeigemodi unter den Anzeigeoptionen nicht sichtbar, wenn Sie ein iPad über Adapter von Drittanbietern mit einem externen Monitor verbinden.
- Manchmal wird innerhalb der VDA-Sitzung eine Linie unter dem Mauszeiger beobachtet.

Tastaturunterstützung

Zuordnung der rechten Optionstaste zur Alt-Taste

Ab Version 24.12.0 führt die Citrix Workspace-App für iOS eine Verbesserung ein, die es Benutzern ermöglicht, die rechte Optionstaste der **Alt**-Taste in der Sitzung zuzuordnen. Diese neue Option ergänzt die vorhandenen Zuordnungen – linke Optionstaste, **Befehls- oder Windows**-Taste und beide Optionstasten – und bietet Benutzern mehr Flexibilität bei der Tastaturkonfiguration.



Tastaturlayout-Synchronisierung

Die Tastaturlayout-Synchronisierung ermöglicht Benutzern, bevorzugte Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist standardmäßig deaktiviert.

Um die Tastaturlayout-Synchronisierung zu aktivieren, gehen Sie zu **Einstellungen** > **Tastaturoptionen** und aktivieren Sie die Option **Tastaturlayout-Synchronisierung**.

> **Hinweis:**

> Die Verwendung der Option für das lokale Tastaturlayout aktiviert den Client-IME (Eingabemethoden-Editor). Wenn Sie in japanischer, chinesischer oder koreanischer

> Sprache arbeiten und den Server-IME bevorzugen, deaktivieren Sie die Option für das lokale Tastaturlayout, indem Sie die Option unter **Einstellungen** > **Tastatur** deaktivieren.

Voraussetzungen

- Für Linux VDA aktivieren Sie die Richtlinie zur Client-Tastaturlayout-Synchronisierung und IME-Verbesserung.
- Für Windows VDA aktivieren Sie die Richtlinien für Unicode-Tastaturlayout-Zuordnung, Client-Tastaturlayout-Synchronisierung und IME-Verbesserung.
- Der VDA muss Version 7.16 oder höher sein.

Unterstützung für Tastaturlayout für Windows VDA und Linux VDA

TASTATURLAYOUT UNTER IOS	TASTATURSPRACHE	TASTATURLAYOUT UNTER WINDOWS	TASTATURLAYOUT UNTER LINUX
Belarusian(Belarus)	Belarusian(Belarus)	Belarussische (Belarus) Tastatur	by
Bulgarisch	Bulgarisch	Bulgarische (Schreibmaschine) Tastatur	bg
Chinesisch (vereinfacht)	Chinesisch (vereinfacht, China)	Citrix IME – Chinesisch (vereinfacht, China)	zh
Chinesisch (traditionell)	Chinesisch (traditionell, Taiwan)	Citrix IME – Chinesisch (traditionell, Taiwan)	tw
Kroatisch	Kroatisch (Kroatien)	Kroatische Tastatur	hr
Tschechisch	Tschechisch	Tschechische Tastatur	cz
Dänisch	Dänisch	Dänische Tastatur	df
Niederländisch	Niederländisch (Niederlande)	Internationale Tastatur (USA)	us

TASTATURLAYOUT UNTER IOS	TASTATURSPRACHE	TASTATURLAYOUT UNTER WINDOWS	TASTATURLAYOUT UNTER LINUX
Niederländisch (Belgien)	Niederländisch	Belgische Tastatur (Punkt)	be
Englisch (Australien)	Englisch (Australien)	US-Tastatur	us
Englisch (Kanada)	Englisch (Kanada)	US-Tastatur	us
Englisch (UK)	Englisch (Vereinigtes Königreich)	Tastatur des Vereinigten Königreichs	gb
Englisch (US)	Englisch (Vereinigte Staaten)	US-Tastatur	us
Estnisch	Estnisch	Estnische Tastatur	ee
Finnisch	Finnisch	Finnische Tastatur	fi
Französisch (Kanada)	Französisch (Kanada)	Französische Tastatur	fr
Französisch (Schweiz)	Französisch (Frankreich)	Schweizer französische Tastatur	ch
Französisch (Frankreich)	Französisch (Frankreich)	Französische Tastatur	fr
Deutsch (Österreich)	Deutsch (Österreich)	Deutsche Tastatur	at
Deutsch (Schweiz)	Deutsch (Schweiz)	Schweizer deutsche Tastatur	ch
Deutsch (Deutschland)	Deutsch (Deutschland)	Deutsche Tastatur	at
Griechisch	Griechisch	Griechische Tastatur	gr
Ungarisch	Ungarisch	Ungarische Tastatur	hu
Isländisch	Isländisch	Isländische Tastatur	is

TASTATURLAYOUT UNTER IOS	TASTATURSPRACHE	TASTATURLAYOUT UNTER WINDOWS	TASTATURLAYOUT UNTER LINUX
Irisch	Irisch		ie
Italienisch	Italienisch (Italien)	Italienische Tastatur	it
Japanisch	Japanisch	Citrix IME – Japanisch	jp
Koreanisch	Koreanisch	Citrix IME – Koreanisch	kr
Lettisch	Lettisch	Lettische Tastatur	lv
Norwegisch	Norwegisch (Bokmål)	Norwegische Tastatur	Nein
Polnisch	Polnisch	Polnische (Programmierer) Tastatur	pl
Portugiesisch (Brasilien)	Portugiesisch (Brasilien)	Portugiesische (Brasilien ABNT) Tastatur	br
Portugiesisch (Portugal)	Portugiesisch (Portugal)	Portugiesische Tastatur	pt
Rumänisch	Rumänisch (Rumänien)	Rumänische (Legacy) Tastatur	ro
Russisch (Russland)	Russisch	Russische Tastatur	ru
Slowakisch	Slowakisch	Slowakische Tastatur	sk
Slowenisch	Slowenisch	Slowenische Tastatur	si
Spanisch (Mexiko)	Spanisch (Mexiko)	Lateinamerikanische Tastatur	Lateinamerika
Spanisch (Spanien)	Spanisch (Spanien)	Spanische Tastatur	es

TASTATURLAYOUT UNTER IOS	TASTATURSPRACHE	TASTATURLAYOUT UNTER WINDOWS	TASTATURLAYOUT UNTER LINUX
Schwedisch (Schweden)	Schwedisch (Schweden)	Schwedische Tastatur	se
Türkisch	Türkisch	Türkische F-Tastatur	tr
Ukrainisch	Ukrainisch	Ukrainische Tastatur	ua

Unterstützung für Sondertasten

Unterstützung für die folgenden einzelnen Tasten auf einer externen Tastatur unter iOS 13.4 und höher:

- PageUp
- PageDown
- Startseite
- End
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Unterstützung spezieller Tastenkombinationen

Diese Version bietet Unterstützung für die folgenden Tastenkombinationen auf externen iOS-Tastaturen:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + STRG + S
- Windows + T
- Windows + U
- Windows + Zahl
- Windows + NACH-OBEN
- Windows + Down
- Windows + Left
- Windows + Right
- Windows + X
- Windows + K
- STRG + ESC

Verbesserungen der erweiterten Tastatur

Ab Version 23.5.0 wurde die Funktionalität der erweiterten Tastatur verbessert, um eine bessere Benutzererfahrung zu bieten. Die folgenden Verbesserungen wurden vorgenommen:

- Die Benutzeroberfläche der erweiterten Symbolleiste anheften oder lösen.
- Die erweiterte Symbolleiste synchron mit der Bildschirmdrehung drehen.
- Unterstützung der Windows-Symboltaste und von Tastenkombinationen mit 3 Tasten.
- Verbesserung der Benutzererfahrung in Szenarien mit mehreren Monitoren.
- Die Benutzeroberfläche der erweiterten Symbolleiste automatisch öffnen oder zuklappen.
- Verbesserung der Benutzererfahrung für den Stage Manager-Modus (auf dem iPad mit M1-Chip).

IME-Benutzeroberfläche

Im Allgemeinen bietet IME UI-Komponenten wie das Kandidatenfenster und das Kompositionsfenster. Das Kompositionsfenster enthält die Kompositionszeichen und Kompositions-UI-Elemente, zum Beispiel Unterstreichung und Hintergrundfarbe. Das Kandidatenfenster zeigt die Kandidatenliste an.

IME-Benutzeroberfläche(/en-us/citrix-workspace-app-for-ios/media/ime-ui.png)

Das Kompositionsfenster ermöglicht es Ihnen, zwischen den bestätigten Zeichen und den zu komponierenden Zeichen zu unterscheiden. Das Kompositionsfenster und das Kandidatenfenster bewegen sich mit dem Eingabecursor.

Dadurch bietet die Funktion:

- Eine verbesserte Eingabe von Zeichen an der Cursorposition im Kompositionsfenster.
- Eine verbesserte Anzeige im Kompositions- und Kandidatenfenster.

Derzeit können Sie diese Funktion in den auf Windows-VDAs gehosteten Sitzungen verwenden, und sie unterstützt sowohl Bildschirmtastaturen als auch externe physische Tastaturen.

Generischer Client-IME für ostasiatische Sprachen

Die Funktion „Generischer Client-Eingabemethoden-Editor (IME)“ verbessert die Eingabe- und Anzeigeerfahrung mit chinesischen, japanischen und koreanischen (CJK) Sprachzeichen auf iOS-Geräten. Diese Funktion ermöglicht es Ihnen, CJK-Zeichen an der Cursorposition zu komponieren, wenn Sie sich in einer Sitzung mit Ihren Client-IMEs befinden. Die Funktion ist für Windows-VDA-Umgebungen verfügbar. Es wird empfohlen, den Client-IME anstelle des VDA-seitigen IME für eine bessere Benutzererfahrung zu verwenden.

Voraussetzungen

- Aktivieren Sie die Client-Tastaturlayoutsynchronisierung und IME-Verbesserung und aktivieren Sie die Unicode-Tastaturlayoutzuordnung auf Ihrem Windows-VDA über die Gruppenrichtlinie.

  Tastatur-IME(/en-us/citrix-workspace-app-for-ios/media/keyboard-ime.png)

Weitere Informationen finden Sie im Knowledge Center-Artikel CTX312404.

Sie können die Optionen auch über die folgenden Registrierungen auf Ihrem Windows-VDA aktivieren:

```
-  HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0

-  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value = DWORD 1

-  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value =
DWORD 1
```

- Aktivieren Sie die Option **Settings** > **Keyboard Options** > **Keyboard Layout Sync** in der Citrix Workspace-App.

  Tastaturoptionen(/en-us/citrix-workspace-app-for-ios/media/keyboard-options.png)

Unterstützung für den Scancode-Eingabemodus

Ab Version 24.1.0 können Sie **Scancode** als Tastatureingabemodus auswählen, wenn Sie eine externe physische Tastatur verwenden. Diese Funktion ist hilfreich, wenn Sie iOS-Geräte mit einer Standardtastatur eines externen Windows-PCs verwenden. Mit **Scancode** können Sie das Tastaturlayout des VDA anstelle der iOS-Tastatur verwenden. Auf diese Weise können Sie den Eingabestil der externen Windows-Tastatur vollständig übernehmen, anstatt den von iOS. Dies ist vorteilhaft beim Tippen in ostasiatischen Sprachen, da es die gesamte Benutzererfahrung erheblich verbessert. Der Endbenutzer könnte feststellen, dass er das Tastaturlayout des Servers anstelle des Clients verwendet. Weitere Informationen finden Sie im Abschnitt Anwendungsfall in diesem Artikel.

Um die Funktion **Scancode** zu verwenden, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Citrix Workspace-App für iOS und navigieren Sie zu **Einstellungen > Tastaturoptionen**.
2. Tippen Sie auf **Eingabemodus für externe Tastaturen**.
3. Wählen Sie eine der folgenden Optionen:

   - **Scancode:** Sendet die Tastenposition von der clientseitigen Tastatur an den VDA, und der VDA generiert das entsprechende Zeichen. Wendet das serverseitige Tastaturlayout an.
   - **Unicode:** Sendet die Taste von der clientseitigen Tastatur an den VDA, und der VDA generiert dasselbe Zeichen im VDA. Wendet das clientseitige Tastaturlayout an.

   Standardmäßig ist **Unicode** als Eingabemodus sowohl für die Software- oder Bildschirmtastatur als auch für die externe Tastatur ausgewählt.
4. Tippen Sie auf **Scancode**.

Wenn Sie sich in einer Sitzung befinden, können Sie das Tastaturlayout des Remote-Servers oder VDA wechseln und mit dem Tastaturlayout des Remote-Servers oder VDA eingeben.

Anwendungsfall

Betrachten Sie zum Beispiel ein Szenario, in dem Sie ein US-amerikanisches internationales Tastaturlayout verwenden, das mit Ihrem iOS-Gerät verbunden ist. Wenn Sie **Scancode** wählen und die Taste neben der Feststelltaste auf Ihrer externen Tastatur eingeben, wird der **Scancode 1E** an den VDA gesendet. Der VDA verwendet dann **1E**, um das Zeichen **a** anzuzeigen. Wenn Sie **Unicode** wählen und die Taste neben der Feststelltaste auf Ihrer externen Tastatur eingeben, wird das Zeichen **a** an den VDA gesendet. Selbst wenn der VDA ein anderes Tastaturlayout verwendet, das an derselben Position ein anderes Zeichen hat, erscheint das Zeichen **a** auf dem Bildschirm.

> **Hinweis:**
>
> **Unicode** ist der bevorzugte Modus für die Eingabe, wenn Sie eine Bildschirmtastatur auf Ihren Mobilgeräten verwenden. Dies liegt daran, dass die Tasten einer Bildschirmtastatur im Allgemeinen keinen Scancode generieren.

Verbesserungen bei der Unterstützung externer Tastaturkürzel

Ab Version 24.1.0 ermöglicht die Citrix Workspace-App für iOS die Verwendung weiterer Tastaturkürzel von externen Tastaturen in einer Remotedesktop- oder App-Sitzung. Im Folgenden sind wichtige Verbesserungen an externen Tastaturkürzeln aufgeführt:

- Unterstützung für Windows-Tastatur-spezifische Tasten wie **Einfügen**, **Entf** und Ziffernblock.
- Wenn Sie eine Taste gedrückt halten und nicht loslassen, reagiert der Remotedesktop/die App korrekt.
- Unterstützung von Tastenkombinationen mit mehr als drei Tasten.

Zusätzlich können Sie jetzt die spezifische Taste für **Alt** über die folgenden Optionen unter **Einstellungen > Tastaturoptionen > Spezifische Taste für Alt zuweisen** konfigurieren:

- **Option oder Alt (links)**: Sendet **Alt** mit **Option (links) oder Alt (links)**.
- **Befehl oder Windows (links)**: Sendet **Alt** mit den Tasten **Befehl (links) oder Windows (links)**.
- **Option oder Alt (links und rechts)**: Sendet **Alt** mit der Taste **Option oder Alt (links und rechts)**.

Die Option **Spezifische Taste für Alt zuweisen** hilft, Konflikte zwischen der macOS-Taste **Option** und der Windows-Taste **Alt** zu vermeiden.

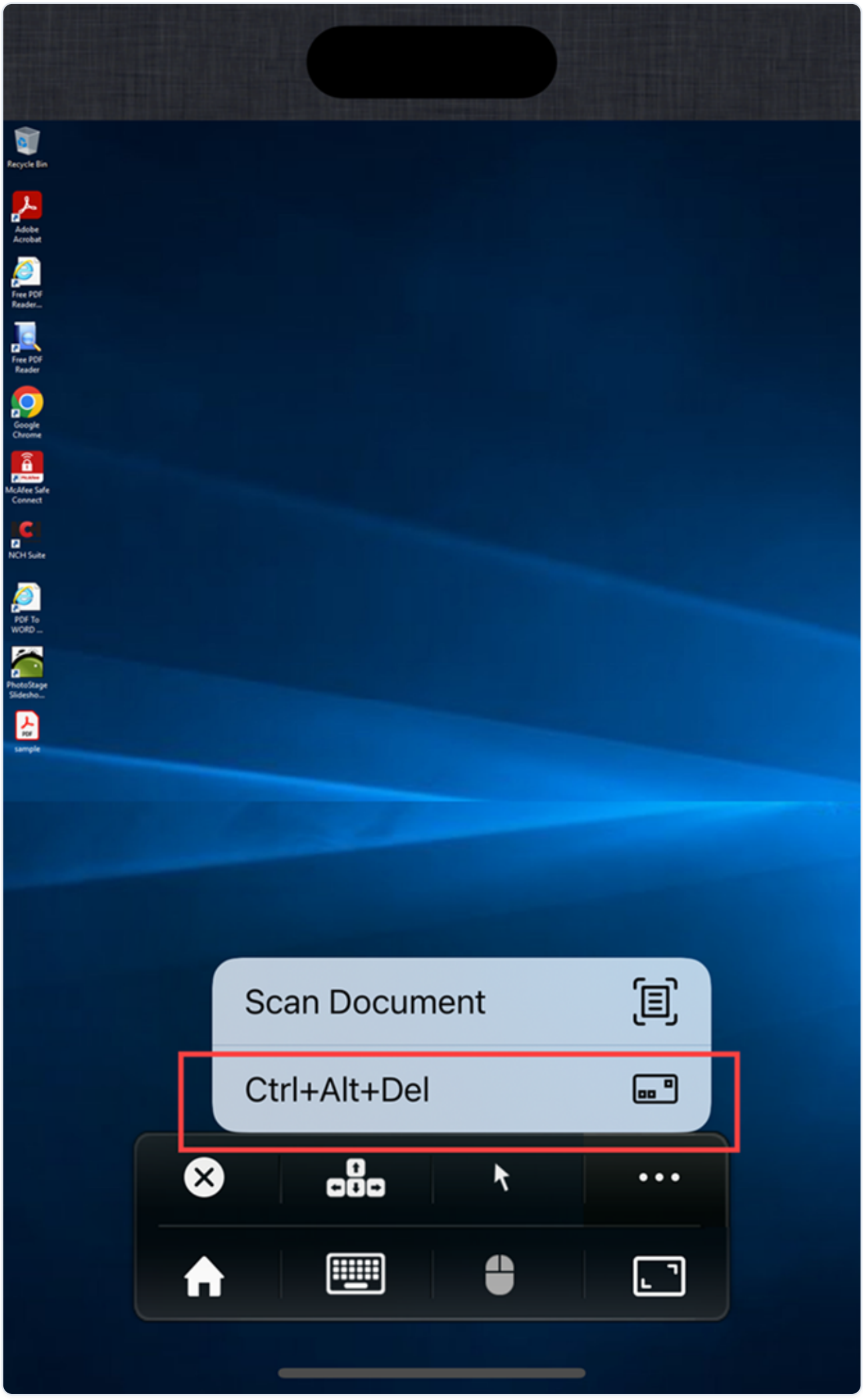
Einschränkungen

Die folgenden iOS-Systemtastenkombinationen werden derzeit nicht unterstützt:

- **Befehl (Windows)-H**: Zum Startbildschirm wechseln.
- **Befehl (Windows)-Leertaste**: Suchfeld ein- oder ausblenden.
- **Befehl (Windows)-Tab**: Zur nächsten zuletzt verwendeten App unter den geöffneten Apps wechseln.
- **Befehl (Windows)-Umschalt-3**: Einen Screenshot erstellen.
- **Befehl (Windows)-Umschalt-4**: Einen Screenshot erstellen und sofort Markup öffnen, um ihn anzuzeigen oder zu bearbeiten.
- **Befehl (Windows)-Option (Alt)-D**: Das Dock ein- oder ausblenden.
- **Befehl (Windows)-Strg-Q**: Gerät sperren.
- **AltGr** auf der europäischen Tastatur wird nicht unterstützt. Wenn Sie Sonderzeichen mit **AltGr** eingeben möchten, verwenden Sie stattdessen die folgenden Tastenkombinationen:
  - macOS **Option+*** Tastenkombination oder
  - Windows OS **Alt + Ziffernblock-Tastenkombination**.

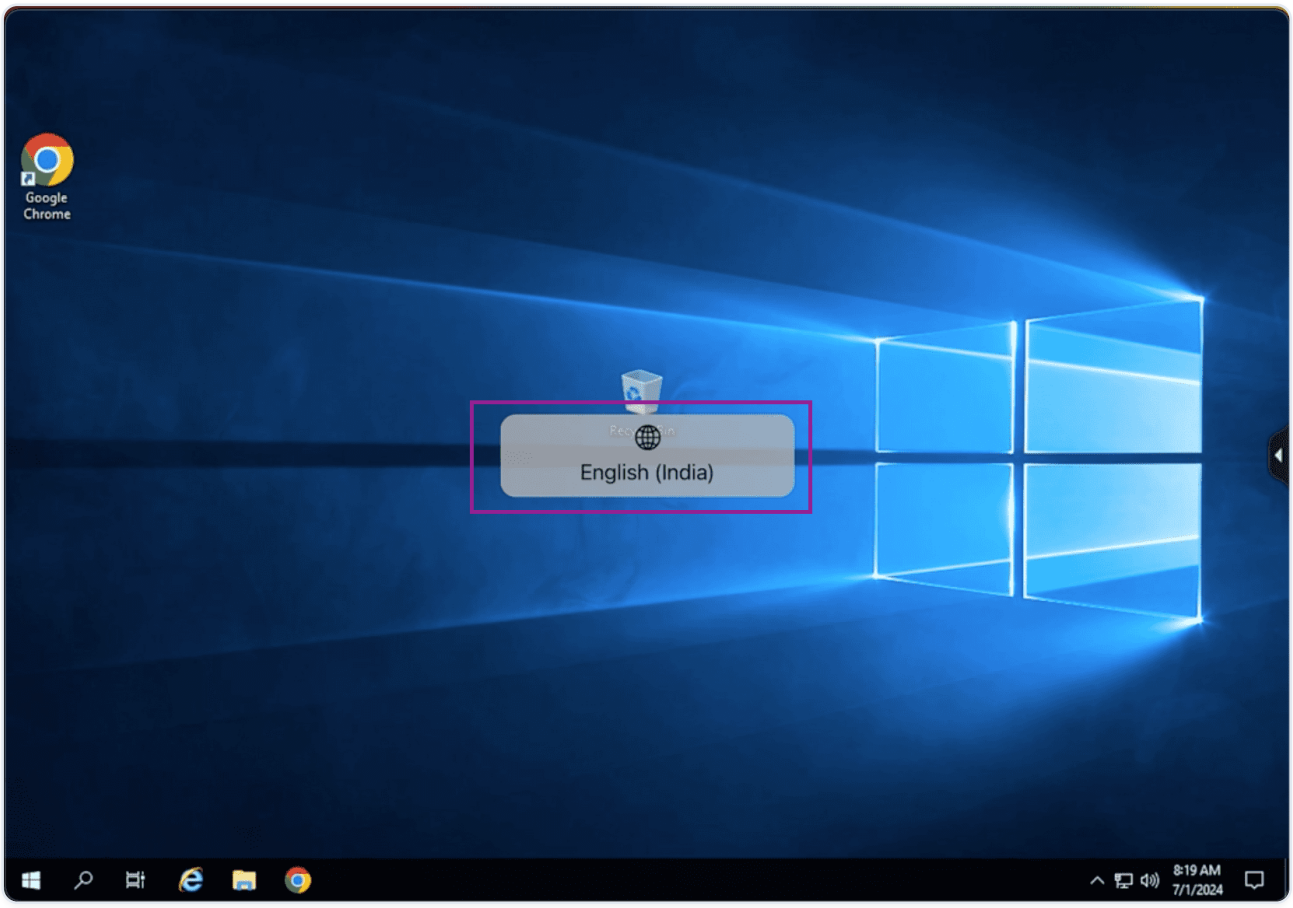
Hinzufügen der Tastenkombination Strg+Alt+Entf zur Sitzungssymbolleiste

Ab dieser Version bietet die Sitzungssymbolleiste jetzt die Möglichkeit, die Funktion **Strg+Alt+Entf** per Knopfdruck auszuführen. Diese Option ermöglicht es Benutzern, sich abzumelden, Benutzer zu wechseln, das System zu sperren oder den Task-Manager aufzurufen.


Recycle Bin
Adobe Acrobat
Free PDF Reader...
Free PDF Reader
Google Chrome
McAfee Safe Connect
NCH Suite
PDF To WORD ...
PhotoStage Slidesho...
sample
Scan Document
Ctrl+Alt+Del

Erkennung und Anzeige von Tastatursprachwechseln in der virtuellen Sitzung

Ab Version 24.7.0 erkennt die Citrix Workspace-App für iOS jetzt automatisch einen Wechsel der Tastatursprache und zeigt eine entsprechende Meldung in der virtuellen Sitzung an. Wenn Sie die Tastatursprache über die Globus-Taste auf der Gerätetastatur oder einer externen Tastatur wechseln, wird eine Meldung auf dem Bildschirm angezeigt, die über die aktuelle Tastatursprache informiert. Diese Funktion stellt sicher, dass Sie die aktuelle Tastatursprache innerhalb der virtuellen Sitzung kennen.



Mikrofon- und Kamerazugriff

Sie können jetzt über eine VDA-Sitzung auf Ihr Mikrofon und Ihre Kamera für Audio-Video-Konferenzen zugreifen. Die Citrix Workspace-App benötigt Ihre Berechtigung für den Zugriff auf Mikrofon oder Kamera, die Sie erteilen können, indem Sie auf Ihrem Gerät zu den **Einstellungen** navigieren und die Kamera oder das Mikrofon aktivieren.

Außerdem wurde der Mikrofon- und Kamerazugriff pro Store als Teil der Sicherheitsfunktion für clientselektives Vertrauen hinzugefügt, um der Citrix Workspace-App den Zugriff von einer VDA-Sitzung zu ermöglichen.

Die Citrix Workspace-App benötigt die Berechtigung des Benutzers für den Zugriff auf das Mikrofon oder die Kamera.

Sie können die Zugriffsebenen konfigurieren, indem Sie zu **Einstellungen > Store-Einstellungen** navigieren. Klicken Sie im Menü **Store-Einstellungen** auf einen Store, um den erforderlichen Mikrofon- oder Kamerazugriff zu aktivieren. Die ausgewählte Einstellung für den Mikrofon- oder Kamerazugriff wird pro Store angewendet.

Unterstützung für externe Webcams

Die Citrix Workspace-App für iOS unterstützt jetzt extern angeschlossene Webcams in Ihren DaaS-Sitzungen. Schließen Sie eine Webcam über USB an und verwenden Sie sie für Videokonferenzen, indem Sie auf das Kamerasymbol klicken und dann die Option **Externe Webcam** auswählen. Dies verbessert das Sitzungserlebnis durch die Nutzung der den Endbenutzern zur Verfügung stehenden Ressourcen.

> **Hinweis:**
>
> - Die externe Webcam wird nur auf iPads mit iOS 17 oder höher und einem USB-C-Anschluss unterstützt.
> - Die Option „Externe Webcam“ wird nur angezeigt, nachdem eine externe Kamera erkannt wurde.
> - Die Einstellungen der Client-App haben keine Auswirkung auf die Kamera innerhalb einer HDX-Sitzung. Sie müssen die von Citrix aktivierte schwebende Kamerataste verwenden, um die Kameraposition zu wechseln.

> Externe Webcam(/en-us/citrix-workspace-app-for-ios/media/external-webcam.png)

Wenn Sie das nächste Mal eine Videokonferenz-App verwenden, merkt sich das System Ihre Präferenz und verwendet die Kameraeinstellung entsprechend. Wenn Sie beispielsweise den letzten Videoanruf mit der Präferenz **Externe Webcam** beendet haben, wird beim nächsten Mal die externe Webcam standardmäßig ausgewählt.

Sie können Ihre Kameraeinstellung ändern, indem Sie auf das Kamerasymbol auf Ihrem Bildschirm tippen. Sie können die Kameraeinstellung auch während Ihrer Anrufe ändern.

Diese Funktion ist für Kunden sowohl in Cloud- als auch in On-Premises-Stores verfügbar.

Unterstützung für Barrierefreiheit und VoiceOver

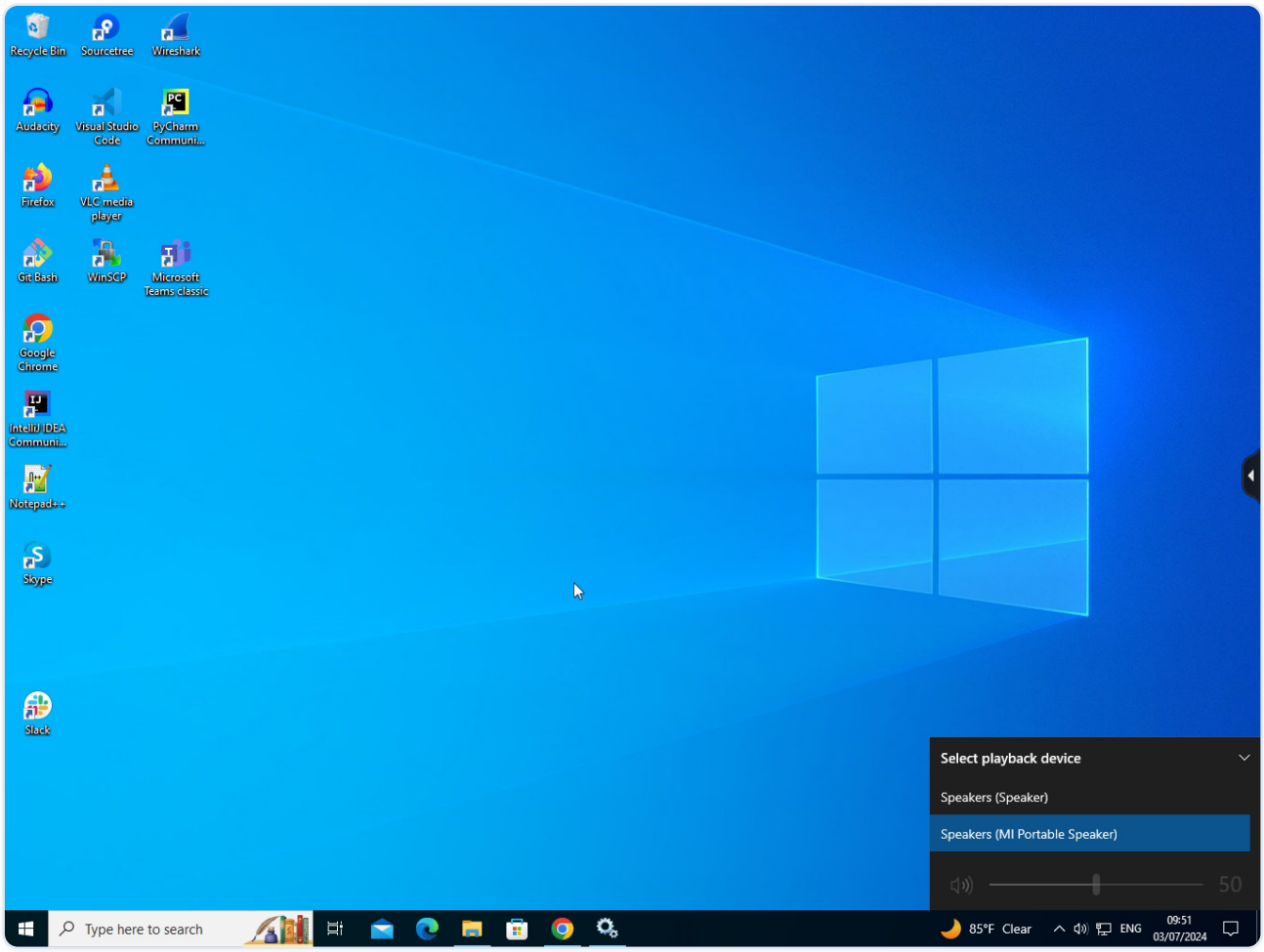
Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS die Funktion für Barrierefreiheit und VoiceOver. Diese Funktion hilft Endbenutzern, die Schwierigkeiten haben, den Bildschirm zu sehen. Der Erzähler liest die Bildschirmelemente laut vor, wenn die Citrix Workspace-App und die Benutzeroberfläche der virtuellen Sitzungen verwendet werden.

Um die VoiceOver-Funktion zu aktivieren, navigieren Sie zu den iOS-**Einstellungen > Bedienungshilfen > VoiceOver** und schalten Sie sie ein.

Sie müssen die von iOS bereitgestellten Standardgesten für die Barrierefreiheit verwenden, um mit der Citrix Workspace-App zu interagieren. Sie können beispielsweise auf dem Bildschirm nach links und rechts wischen, um zwischen den Menüs zu navigieren, während die VoiceOver-Funktion für jedes Element abgespielt wird. Weitere Informationen finden Sie unter Erste Schritte mit den Bedienungshilfen auf dem iPhone und Erste Schritte mit den Bedienungshilfen auf dem iPad in der Apple Support-Dokumentation.

Unterstützung für mehrere Audiogeräte

Ab Version 24.7.0 unterstützt die Citrix Workspace-App für iOS die Anzeige aller verfügbaren Audiogeräte, die lokal in der virtuellen Desktopsitzung verbunden sind. Mit dieser Funktion können Sie Audiogeräte innerhalb der virtuellen Desktopsitzung wechseln. Wenn Sie Audiogeräte in den lokalen Geräteeinstellungen wechseln, werden die Änderungen automatisch auf die virtuelle Desktopsitzung angewendet. Diese Funktion wird auch für Plug-and-Play-Geräte unterstützt.



Einschränkung

- Geräte, die nur Lautsprecher oder nur Mikrofon sind, werden nicht unterstützt.
- Apple AirPlay-Geräte werden nicht unterstützt.
- Diese Funktion unterstützt in der virtuellen Sitzung jeweils entweder ein Bluetooth-Gerät oder ein kabelgebundenes Headset-Gerät.

Unterstützung für adaptives Audio

Ab Version 24.5.0 unterstützt die Citrix Workspace-App für iOS adaptives HDX-Audio. Diese Funktion verbessert die Benutzererfahrung durch verbesserte Audioqualität und geringe Latenz.

Weitere Informationen finden Sie im Artikel Audiopolitik-Einstellung in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung für Rückkamera

Ab Version 23.2.0 unterstützt die Citrix Workspace-App für iOS jetzt das Umschalten der Kameraposition von vorne nach hinten und umgekehrt innerhalb einer HDX-Sitzung.

Wenn Sie die Kamera in der virtuellen Sitzung aufrufen, erscheint ein schwebender Kamerabutton auf dem Bildschirm, um das Umschalten der Kameraposition zu ermöglichen. Sie können den schwebenden Button auch frei auf dem Bildschirm bewegen und überall platzieren.



Um die Kameraposition zwischen der vorderen und hinteren Position in den virtuellen Sitzungen zu wechseln, führen Sie die folgenden Schritte aus:

1. Öffnen Sie eine Client-App, die Videos aufnimmt.
2. Starten Sie die Videoaufnahme.
3. Tippen Sie auf den schwebenden Kamerabutton, der auf dem Bildschirm erscheint, um zwischen Front- und Rückkamera zu wechseln.

> **Hinweis:**
>
> Die Einstellungen der Client-App haben keine Auswirkung auf die Kamera innerhalb einer HDX-Sitzung. Sie müssen die schwebende Kamerataste verwenden, die von Citrix aktiviert wird, um die Kameraposition zu wechseln.

Bekannte Probleme

Die schwebende Taste ist teilweise oder vollständig verdeckt, wenn die Casting-Funktion oder die Dokumentenscan-Funktion aktiviert ist.

Grafik und Anzeige

Verbesserte Grafikleistung

Ab Version 24.1.0 unterstützt die Citrix Workspace-App für iOS hardwarebeschleunigte H.264-Videokodierung oder -dekodierung. Die Multimedia-Engine von Citrix HDX verwendet jetzt Apples Video Toolbox-Framework für die Kodierung und Dekodierung. Dieses Framework komprimiert und dekomprimiert Videos schneller und in Echtzeit. Diese Verbesserung reduziert die CPU-Auslastung bei der Multimedia-Nutzung.

Automatische Synchronisierung der Grafikeinstellungen mit nativen iOS-Einstellungen

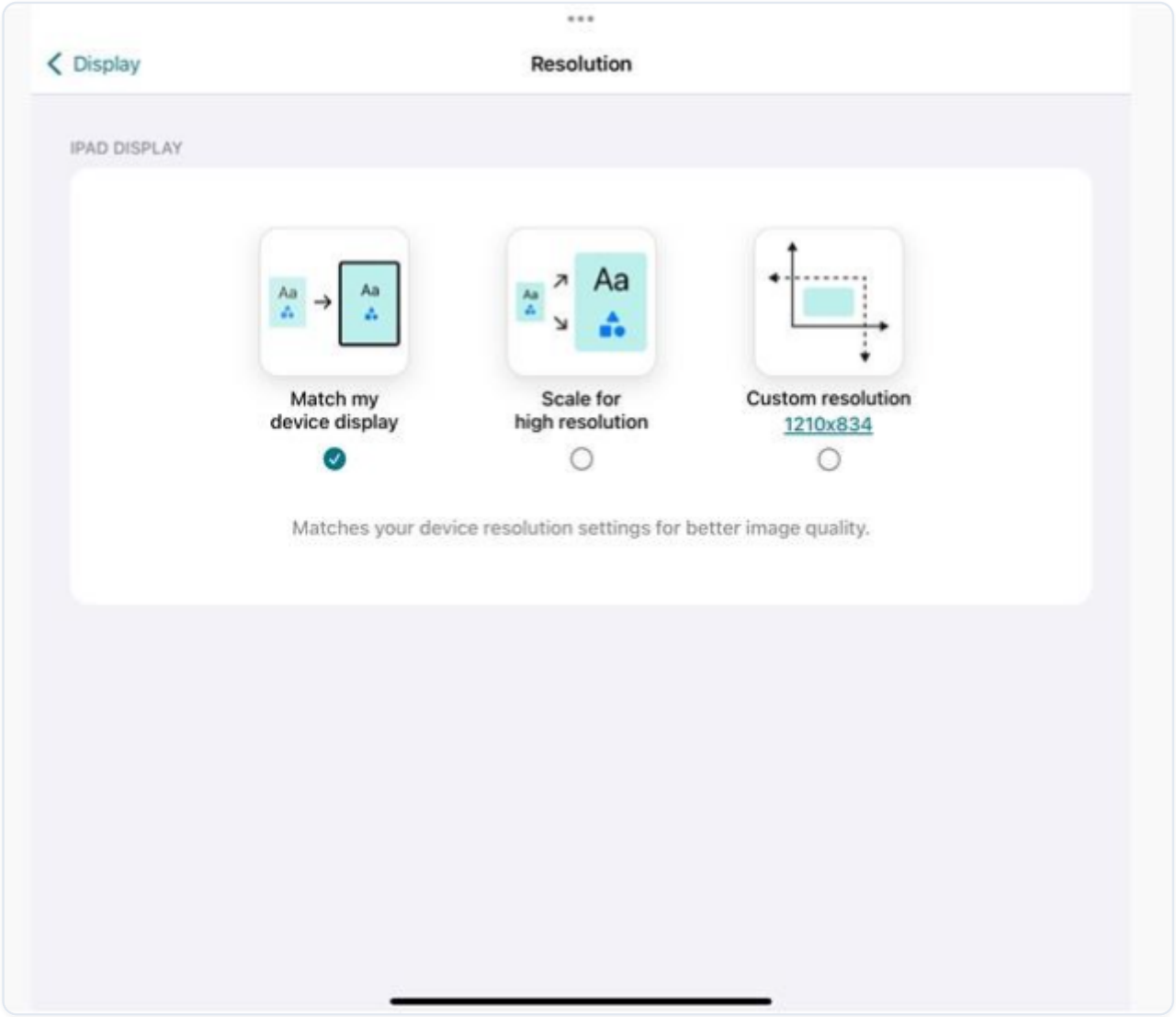
Die neu hinzugefügte Option **Anzeige meines Geräts anpassen** liest die DPI-Skalierung automatisch aus den iOS-Einstellungen, sodass Sie die Auflösung nicht manuell konfigurieren müssen. Für externe Displays ersetzt die App die Auflösungsliste durch fünf konsolidierte

Optionen. Dieses Update reduziert die Konfigurationskomplexität und bietet ein nativeres Anzeigeerlebnis.

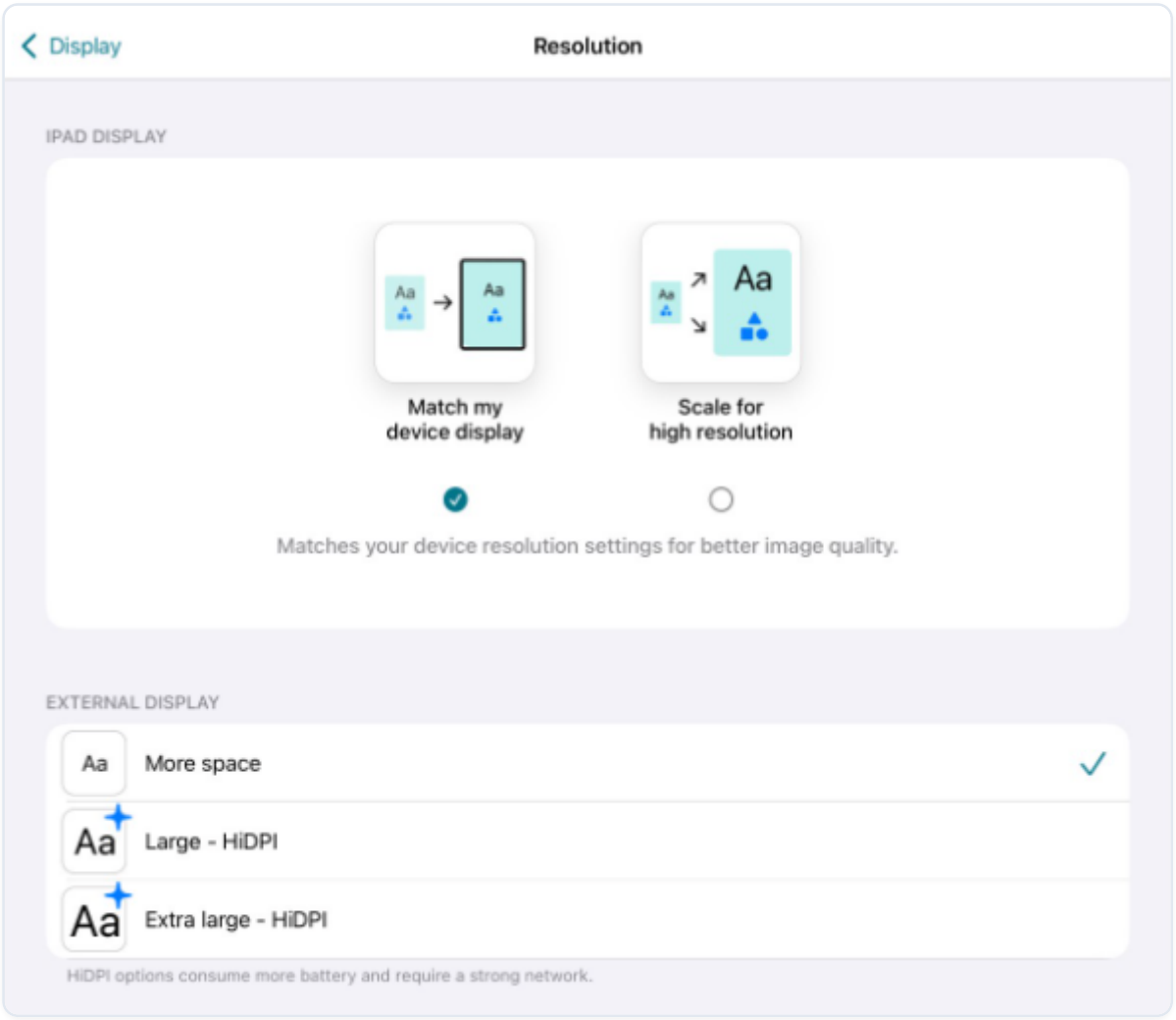
Um diese Funktion zu verwenden, gehen Sie zu **Einstellungen** > **Anzeigeoptionen** > **Auflösung**.

Die folgenden Screenshots zeigen die Anzeigeoptionen auf iPhone und iPad:

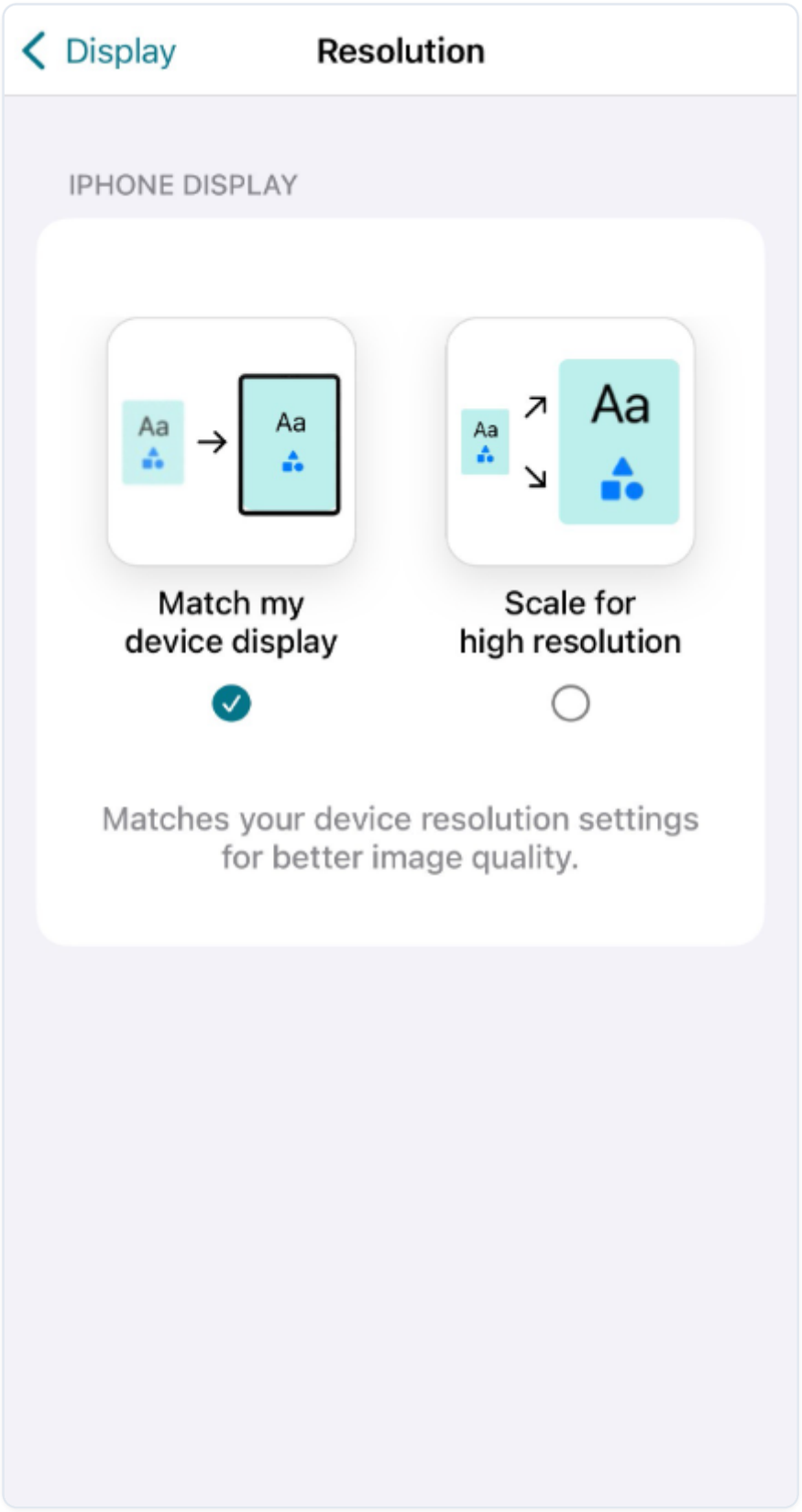
- Auflösungsoptionen für das Hauptdisplay.



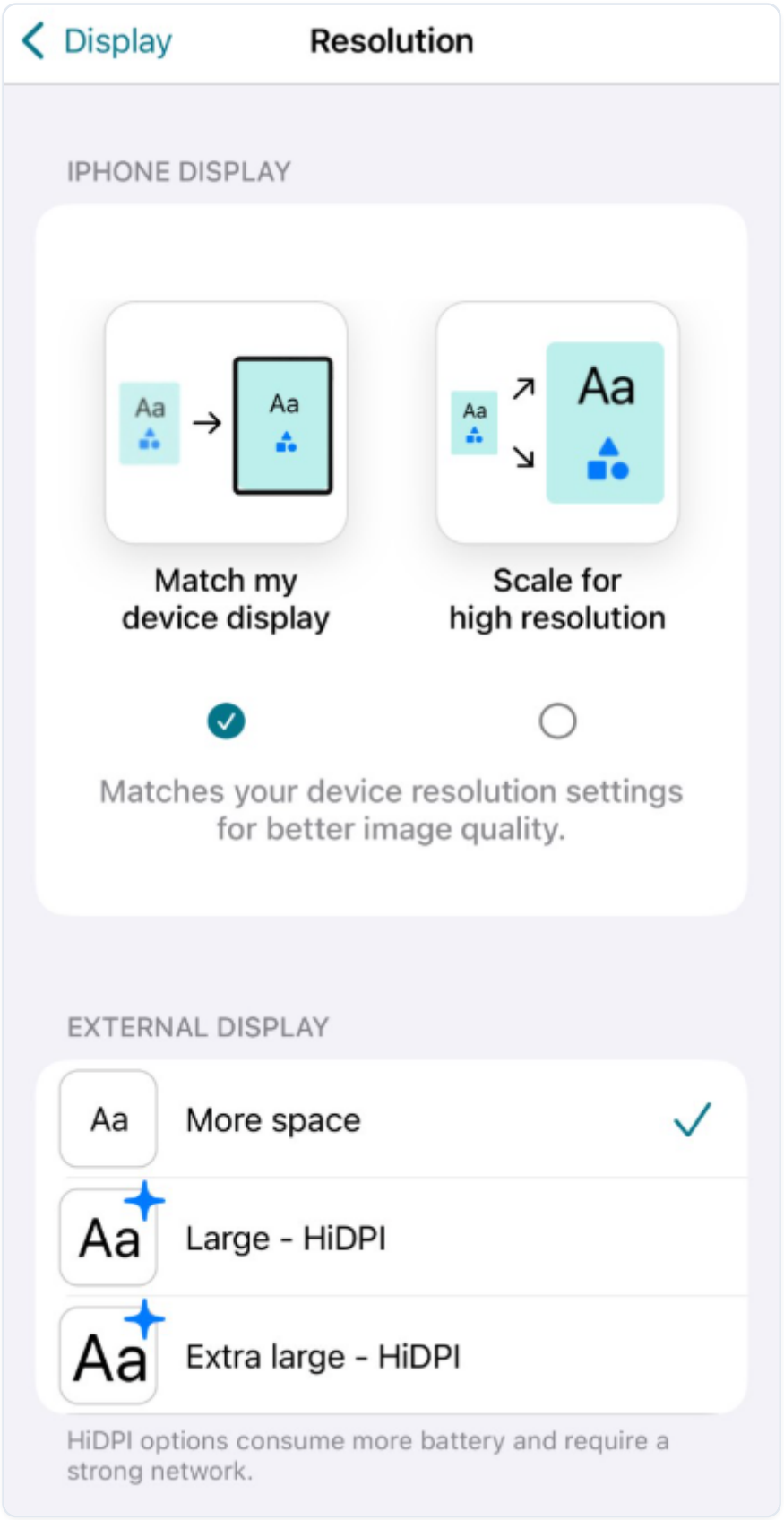
- Auflösungsoptionen für externe Displays.



- Auflösungsoptionen für das Hauptdisplay.



- Optionen für die Auflösung externer Bildschirme.



Clientlaufwerkzuordnung (CDM)

Sie können für jeden konfigurierten Store einen spezifischen Gerätespeicherzugriff auswählen. Der Gerätespeicherzugriff bietet die folgenden Optionen.

- Kein Zugriff
- Schreibgeschützter Zugriff
- Lese- und Schreibzugriff
- Jedes Mal nachfragen

Wenn Sie **Jedes Mal nachfragen** auswählen, wird eine Aufforderung angezeigt, in der Sie bei jedem Start den Typ des Gerätespeicherzugriffs auswählen müssen. Standardmäßig ist die Option **Kein Zugriff** ausgewählt.

> **Hinweis:**

> Diese Funktion gilt nur für direkte ICA®-Starts und für Citrix Gateway konfigurierte Stores. Stores ohne End-to-End-SSL-Einrichtung werden nicht unterstützt.

> Die Einstellungen für den **Gerätespeicher** sind unter einem neuen Abschnitt in den Einstellungen namens **Store-Einstellungen** verfügbar. Um den **Gerätespeicher** anzuzeigen, navigieren Sie zu **Einstellungen** > **Store-Einstellungen**.

Citrix Ready® Workspace Hub

Der Citrix Ready Workspace Hub kombiniert digitale und physische Umgebungen, um Apps und Daten in einem sicheren Smart Space bereitzustellen. Das komplette System verbindet Geräte (oder Dinge) wie mobile Apps und Sensoren, um eine intelligente und reaktionsschnelle Umgebung zu schaffen.

Der Citrix Ready Workspace Hub basiert auf der Raspberry Pi 3-Plattform. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, verbindet sich mit dem Citrix Ready Workspace Hub und überträgt die Apps oder Desktops auf einem größeren Bildschirm.

Weitere Informationen zum Citrix Ready Workspace Hub finden Sie in der Dokumentation zum Citrix Ready Workspace Hub.

Der Citrix Ready Workspace Hub unterstützt aus Sicherheitsgründen eine Secure Sockets Layer (SSL)-Verbindung zwischen mobilen Geräten und dem Hub. Legen Sie einen Fully Qualified Domain Name (FQDN) entweder manuell oder automatisch fest, um jedes Gerät eindeutig zu identifizieren. Weitere Informationen finden Sie unter Sicherheitsverbindung in der Dokumentation zum Citrix Ready Workspace Hub.

Der Citrix Ready Workspace Hub wird in der Citrix Workspace-App aktiviert, wenn alle folgenden Systemanforderungen erfüllt sind:

- Citrix Workspace-App 1810.1 für iOS oder höher
- Bluetooth aktiviert
- Mobilgerät und Workspace Hub verwenden dasselbe WLAN-Netzwerk

Citrix Ready Workspace Hub konfigurieren

Um die Funktionen des Citrix Ready Workspace Hub zu aktivieren, gehen Sie zu **Einstellungen** und tippen Sie auf **Citrix Casting**, um die Funktion auf Ihrem Gerät zu aktivieren. Weitere Informationen finden Sie in der Hilfedokumentation für iOS-Geräte.

Die Citrix Workspace-App integriert ein neues Verfahren, um einen Workspace Hub zur vertrauenswürdigen Liste auf iOS-Geräten hinzuzufügen oder daraus zu entfernen. Weitere Informationen finden Sie unter Sicherheitsverbindung.

Unterstützung für Dokumentenscanner

Ab Version 24.5.0 unterstützt die Citrix Workspace-App für iOS die Dokumentenscanner-Funktion. Mit dieser Funktion können Sie jetzt mehrere Dokumente scannen und speichern, alles innerhalb der Desktopsitzung. Diese Funktion ist standardmäßig aktiviert.

Voraussetzungen

- Die Clientlaufwerkzuordnung (CDM) muss für den Store aktiviert sein.
- Die Dokumentenscanner-Funktion erfordert Lese- und Schreibzugriff auf Ihrem Gerät. Um den Zugriff zu aktivieren, führen Sie die folgenden Schritte aus:

  a. Tippen Sie in Ihrem Profil auf **Anwendungseinstellungen > Store-Einstellungen**.

  b. Tippen Sie auf Ihren aktuellen Store.

  c. Tippen Sie auf **Gerätespeicher** und wählen Sie dann **Vollzugriff**.

Um Dokumente mit dem Dokumentenscanner zu scannen, führen Sie die folgenden Schritte aus:

1. Wählen Sie in der In-Session-Symbolleiste das Ellipsenmenü und dann **Dokument scannen**. Die Kamera-App wird geöffnet.

   Dokument scannen(/en-us/citrix-workspace-app-for-ios/media/scan-document.png)

2. Tippen Sie auf die Auslösetaste, um das Foto aufzunehmen. Wenn Sie erneut aufnehmen möchten, tippen Sie auf **Wiederholen**.

Bild aufnehmen(/en-us/citrix-workspace-app-for-ios/media/capture-image.png)

3. Optional: Schneiden Sie das gescannte Dokument zu. Nachdem Sie die gewünschte Größe zugeschnitten haben, tippen Sie auf **Scan behalten**. Die Kamera-App wird erneut geöffnet, damit Sie weitere Bilder aufnehmen können.

   Scan behalten(/en-us/citrix-workspace-app-for-ios/media/keep-scan.png)

4. Nachdem Sie die erforderlichen Bilder aufgenommen haben, tippen Sie auf **Speichern**.

   Bild speichern(/en-us/citrix-workspace-app-for-ios/media/save-image.png)

5. Wählen Sie die Dateiformatoption, um das gescannte Dokument im gewünschten Format zu speichern.

   Dateiformat auswählen(/en-us/citrix-workspace-app-for-ios/media/select-file-format.png)

6. Tippen Sie auf **OK**.

   Gescannte Dokumente(/en-us/citrix-workspace-app-for-ios/media/scanned-document.png)

Alle gescannten Dokumente sind im Ordner **CitrixScannedDocuments** im lokalen Speicher des Geräts zugänglich. Sie können die **CitrixScannedDocuments** auch im Sitzungsdateimanager aufrufen.

Sitzungsdateimanager(/en-us/citrix-workspace-app-for-ios/media/session-file-manager.png)

Unterstützung für AirPrint-fähige Drucker

Ab Version 23.9.0 können Endbenutzer jetzt Dokumente aus ihren aktiven Sitzungen auf iOS-Geräten mit AirPrint-fähigen Druckern drucken. Dadurch entfällt die Notwendigkeit, Drucker über Kabel oder Netzwerk anzuschließen. Die AirPrint-fähigen Drucker werden zusammen mit den anderen verfügbaren Druckern aufgelistet, sobald Benutzer einen Druckbefehl initiieren.

Um mit einem AirPrint-fähigen Drucker zu drucken, müssen Benutzer Folgendes sicherstellen.

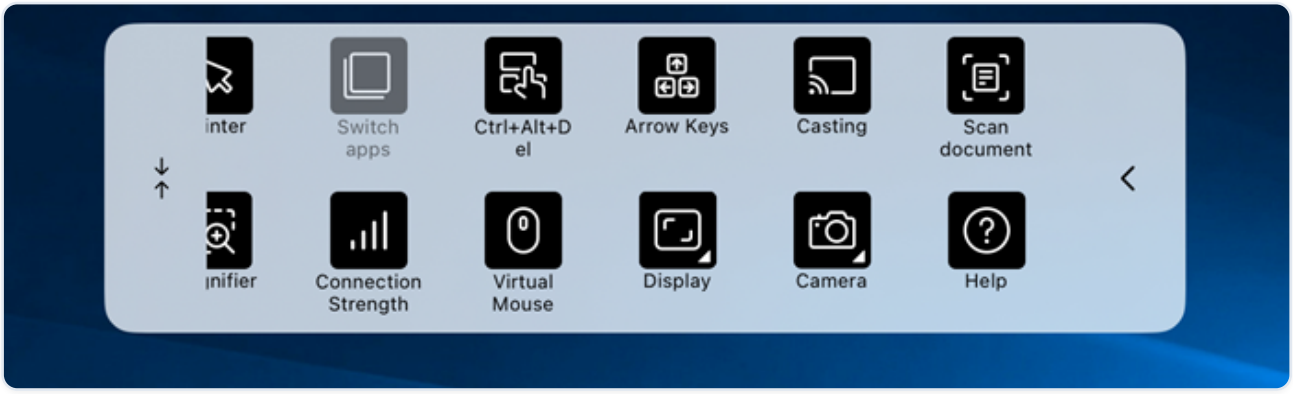
- Der erforderliche Drucker muss AirPrint-kompatibel und AirPrint-fähig sein.
- Das Gerät des Benutzers muss mit demselben WLAN-Netzwerk verbunden sein wie der AirPrint-fähige Drucker.

Diese Funktionalität ist für iOS-Plattformen sowohl in Cloud- als auch in lokalen Umgebungen verfügbar.

Benutzererfahrung

Neue In-Session-Symbolleiste

Ab Version 25.3.0 ist die neue Symbolleiste standardmäßig aktiviert, wenn keine Administratoreinstellung über den Global App Configuration Service (GACS) und Mobile Device Management (MDM) konfiguriert ist.



Verbesserung der geräteübergreifenden Multi-Screen-Erfahrung

Ab Version 25.1.0 verbessert die Citrix Workspace-App für iOS die Benutzererfahrung für iPads, die an externe Monitore oder Docks angeschlossen sind. Diese Updates umfassen die Möglichkeit, Anwendungen auf mehrere Bildschirme zu verteilen, um das Multitasking zu verbessern. Diese Funktion ist standardmäßig aktiviert.

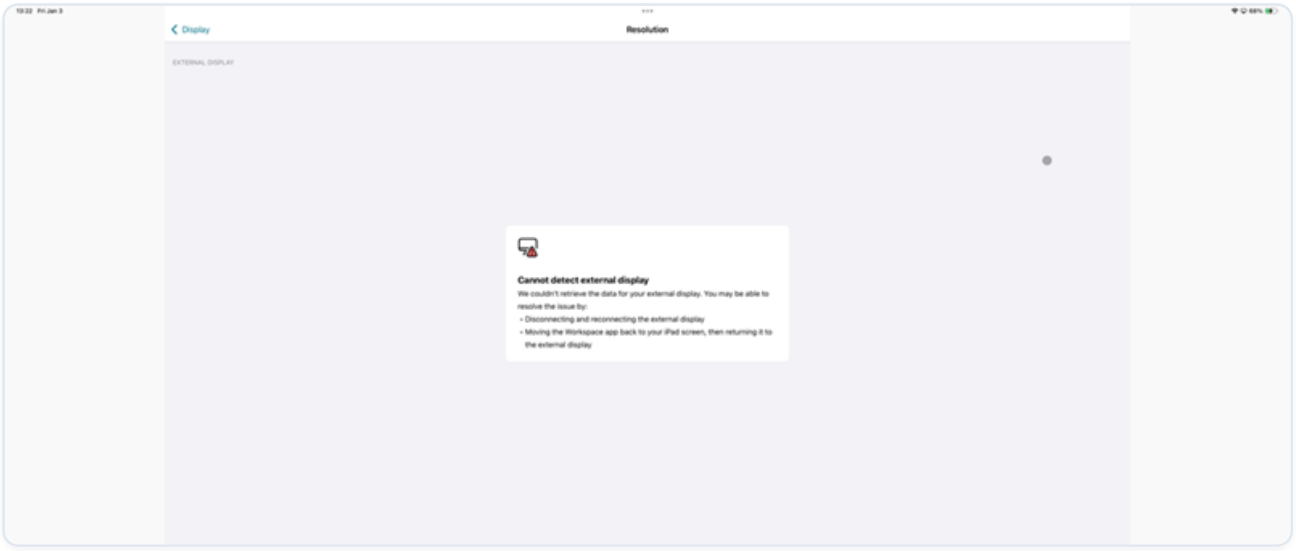
Benutzer können aus einer Reihe verfügbarer Auflösungen sowohl für externe Monitore als auch für den nativen Bildschirm des iPads wählen, um unterschiedlichen Präferenzen gerecht zu werden. Mehrere Bildschirmkonfigurationen bleiben auch beim Wechsel zwischen lokalen Apps und Sitzungen erhalten, was Kontinuität und Produktivität gewährleistet. Diese Funktion behebt auch Maus-Sperrprobleme, die durch Stage Manager verursacht werden.

Voraussetzungen:

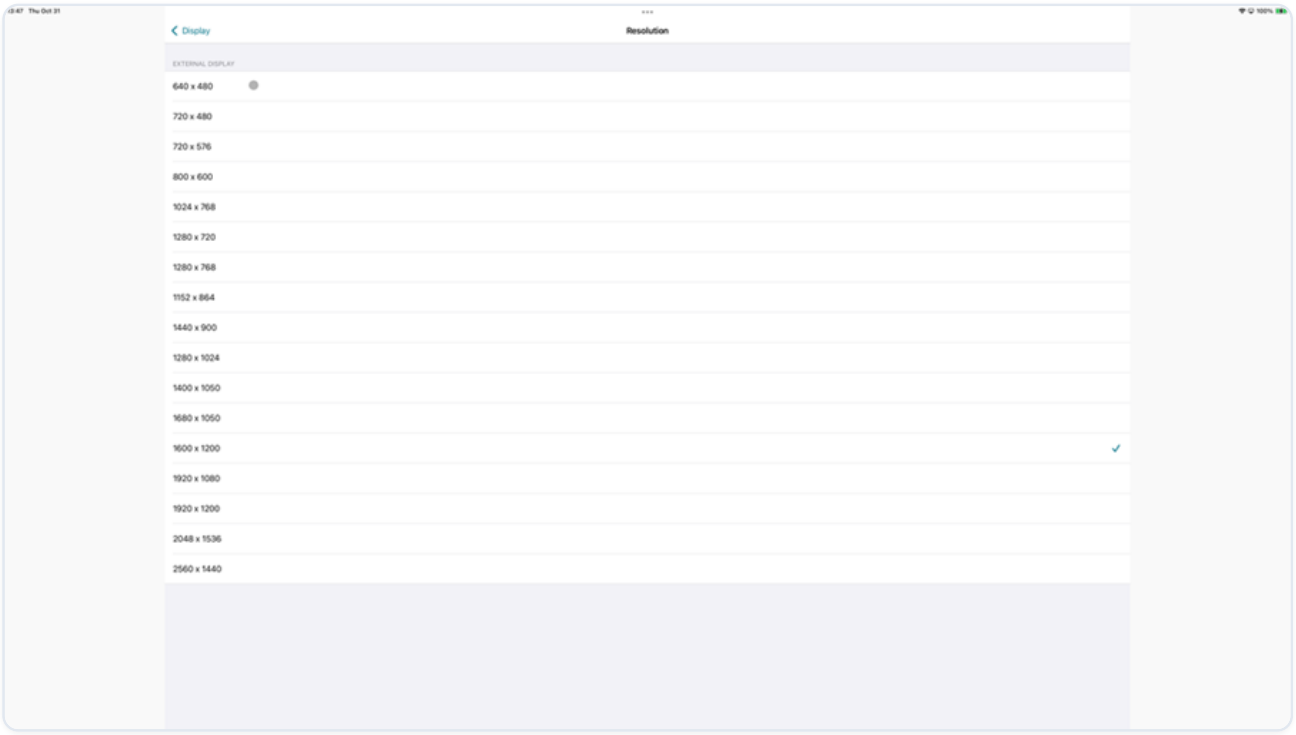
Stage Manager muss auf dem iPad aktiviert sein.

Einschränkungen:

Wenn der Benutzer die Citrix Workspace™-App direkt auf einem externen Display startet, wird die Auflösungsliste leer angezeigt, wenn in den Vollbildmodus gewechselt wird. Dies tritt aufgrund eines iOS-Systemfehlers auf, und die Citrix Workspace-App zeigt eine Warnung **Externes Display kann nicht erkannt werden** an, wie im Screenshot gezeigt.



Eine Liste der unterstützten externen Displayauflösungen für den Vollbildmodus:

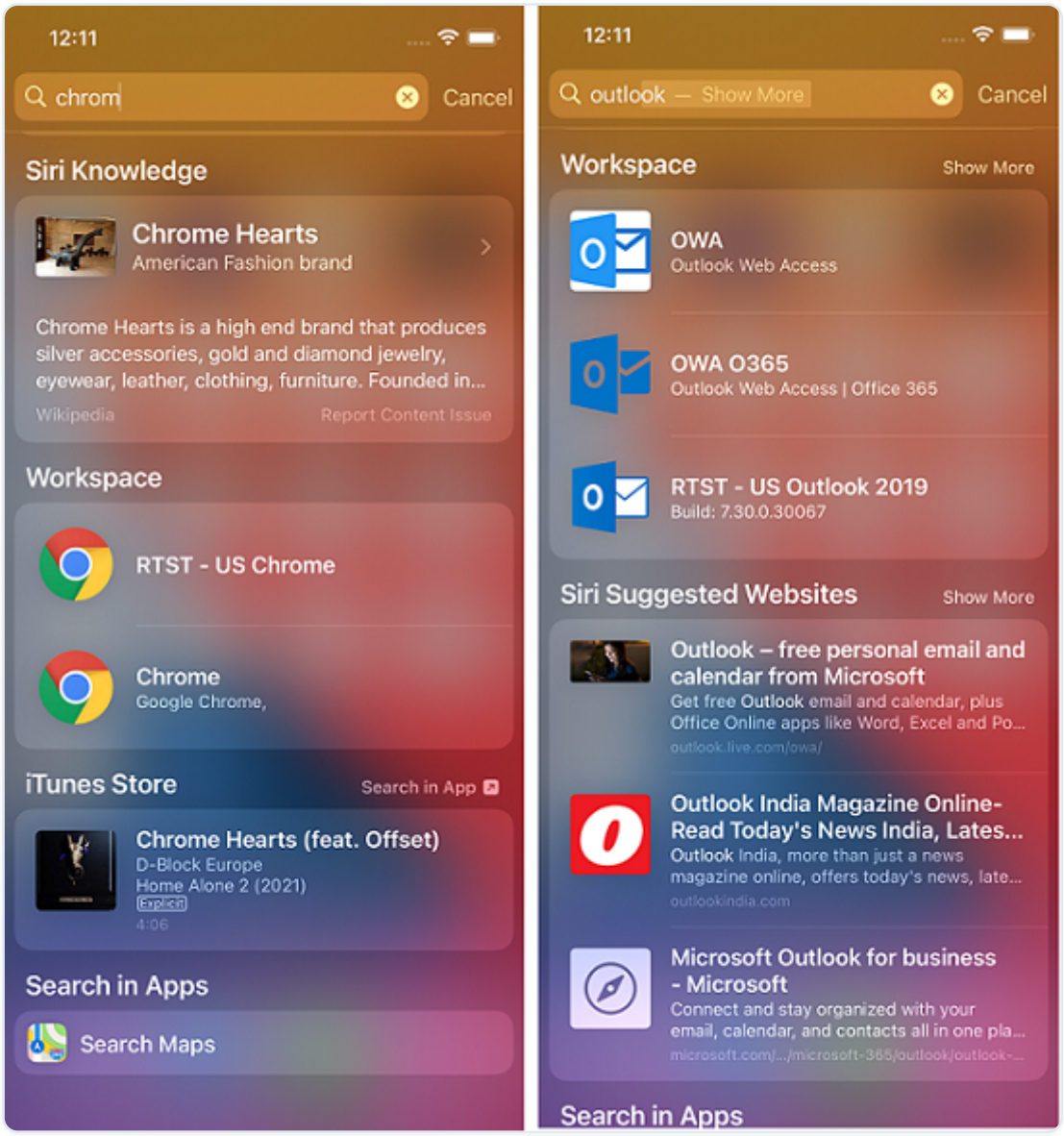


Wenn die Sitzung auf einem externen Display in den Vollbildmodus wechselt, wird eine Toast-Nachricht angezeigt, die Benutzer auffordert, das Citrix Workspace-App-Fenster zurück auf den iPad-Bildschirm zu verschieben, wenn sie Multi-Monitor-Funktionen verwenden möchten, wie in der folgenden Abbildung gezeigt.



Verbesserung der Spotlight-Suche

Das App-Symbol stimmt mit der entsprechenden App-Suche überein. Zuvor wurde das Symbol der Citrix Workspace-App für alle Suchvorgänge angezeigt.



Zugriff auf zuletzt verwendete Apps mittels 3D-Touch-Geste

Sie können eine Liste der zuletzt gestarteten Apps für den schnellen Zugriff aufrufen, wenn Sie die 3D-Touch-Geste (langes Drücken) auf dem Symbol der **Citrix Workspace-App** verwenden.

Akkustatusanzeige

Der Akkustatus des Geräts wird jetzt im Benachrichtigungsbereich innerhalb der virtuellen Desktopsitzung angezeigt.

Diese Funktion wird nur auf VDA-Versionen 7.18 und höher unterstützt.

> **Hinweis:**

> In Sitzungen, die auf Microsoft Windows 10 VDAs ausgeführt werden, kann die Akkustatusanzeige etwa 1 bis 2 Minuten dauern, bis sie angezeigt wird.

Funktion für langes Drücken zum Zugriff auf Ressourcen

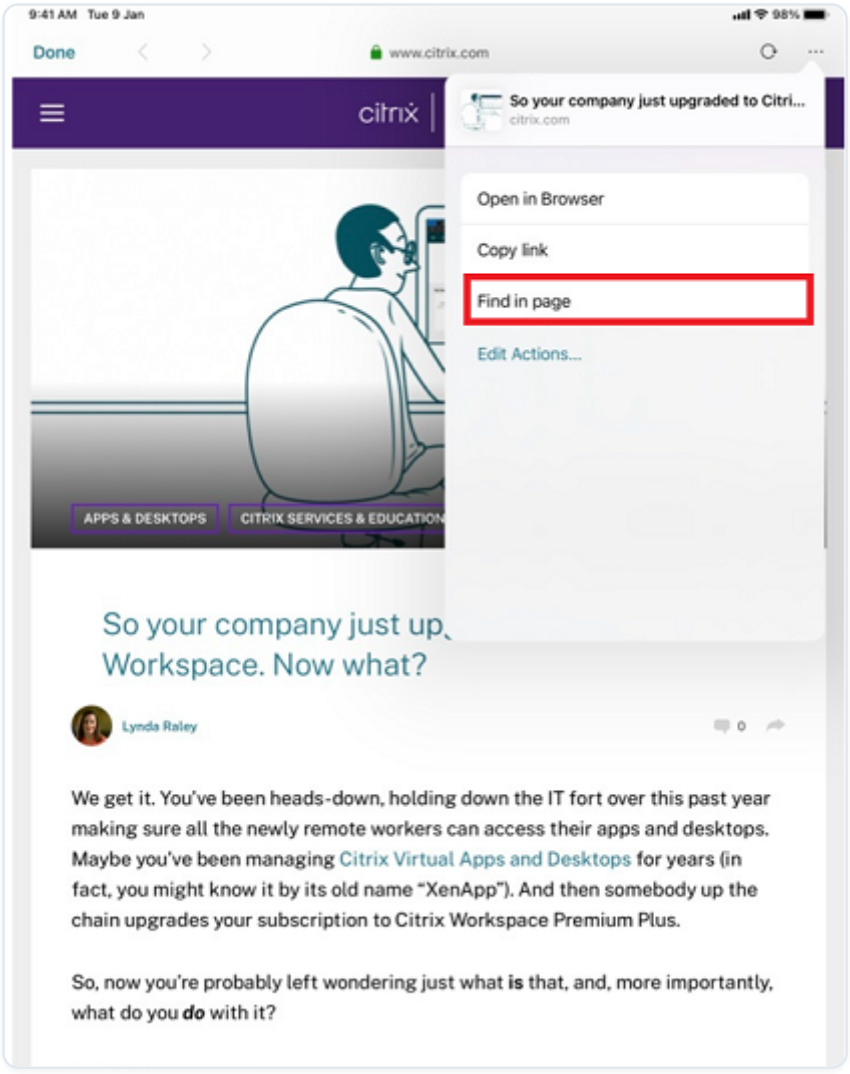
Sie können jetzt das Symbol der Citrix Workspace-App lange drücken und auf Ihre zuletzt gestartete Ressource zugreifen. Sie können jetzt die Citrix Workspace-App beenden und auf Ihre zuletzt gestartete Ressource zugreifen.

Verbesserung der Funktion „Auf Seite suchen“

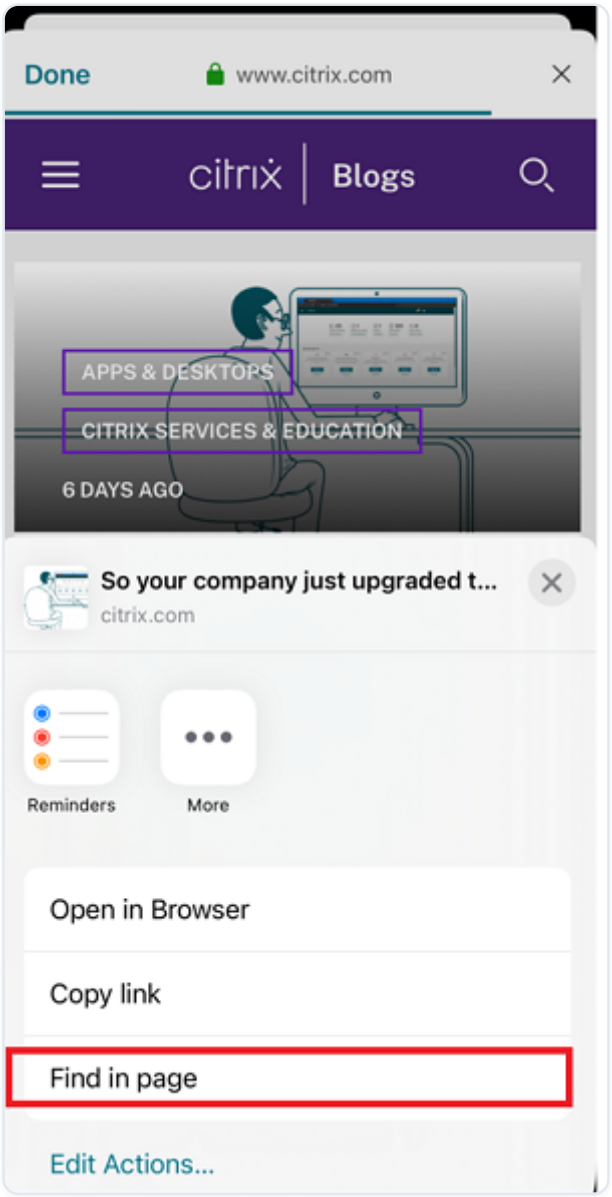
Die Verbesserung der Funktion „Auf Seite suchen“ ermöglicht Ihnen die Suche nach Wörtern oder Phrasen. Diese Usability-Verbesserung ist in Ihren Web- und Software-as-a-Service (SaaS)-Apps anwendbar.

So suchen Sie:

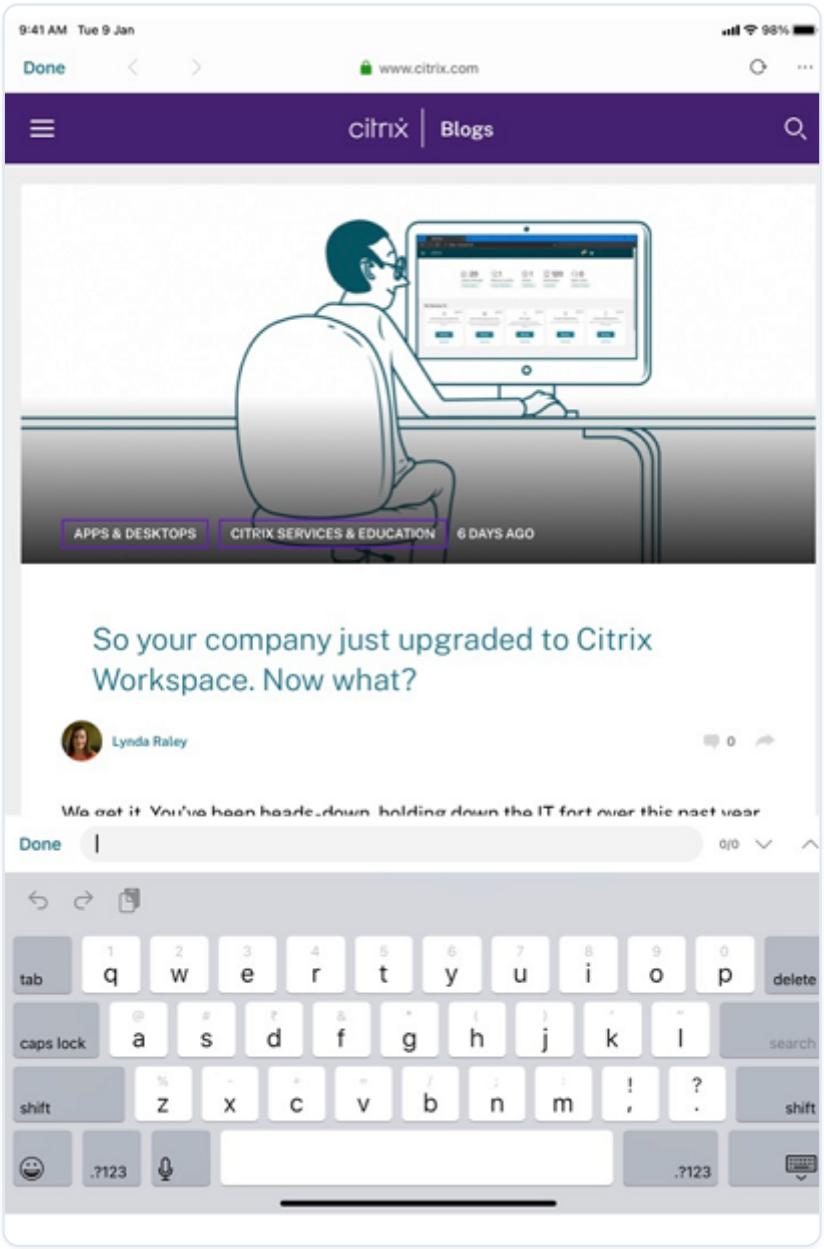
1. Tippen Sie auf Ihrem iPad auf die Schaltfläche mit den Auslassungspunkten (...) in der oberen rechten Ecke und wählen Sie dann **Auf Seite suchen**.



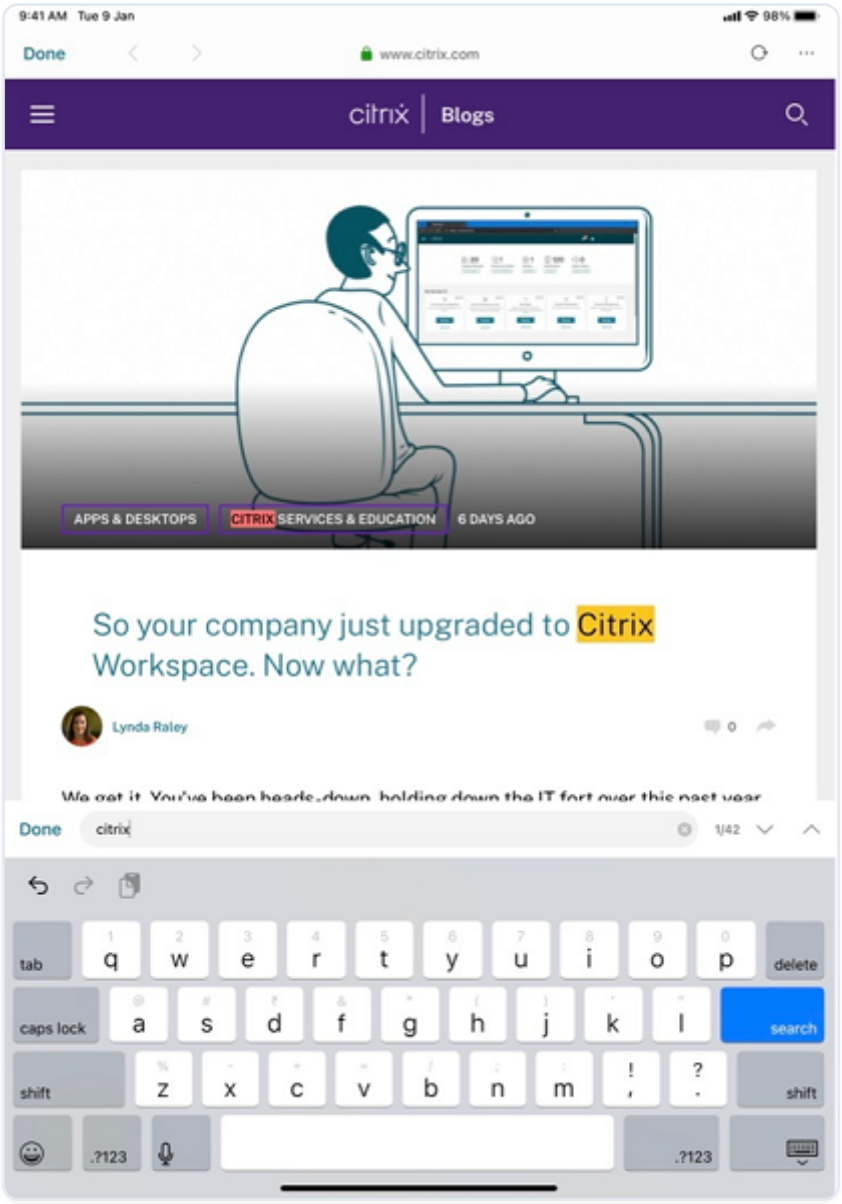
Tippen Sie auf Ihrem iPhone auf die Schaltfläche mit den Auslassungspunkten (...) in der unteren rechten Ecke und wählen Sie dann **Auf Seite suchen**.



Die Bildschirmtastatur wird angezeigt.



1. Geben Sie den Text, nach dem Sie suchen möchten, in das Textfeld ein (geben Sie beispielsweise das Wort „Citrix®“ ein). Die Suchergebnisse werden angezeigt.



Symbolleiste in der Sitzung neu positionieren

Sie können die Symbolleiste in der Sitzung entweder oben oder rechts auf dem Bildschirm neu positionieren. Wenn Sie die Symbolleistenkerbe vom Symbolleistenrand wegziehen, werden die rechteckige Ziehanzeige und das Ablageziel angezeigt. Ziehen Sie die Ziehanzeige über das Ablageziel, um die Symbolleiste neu zu positionieren.

Hinweise:

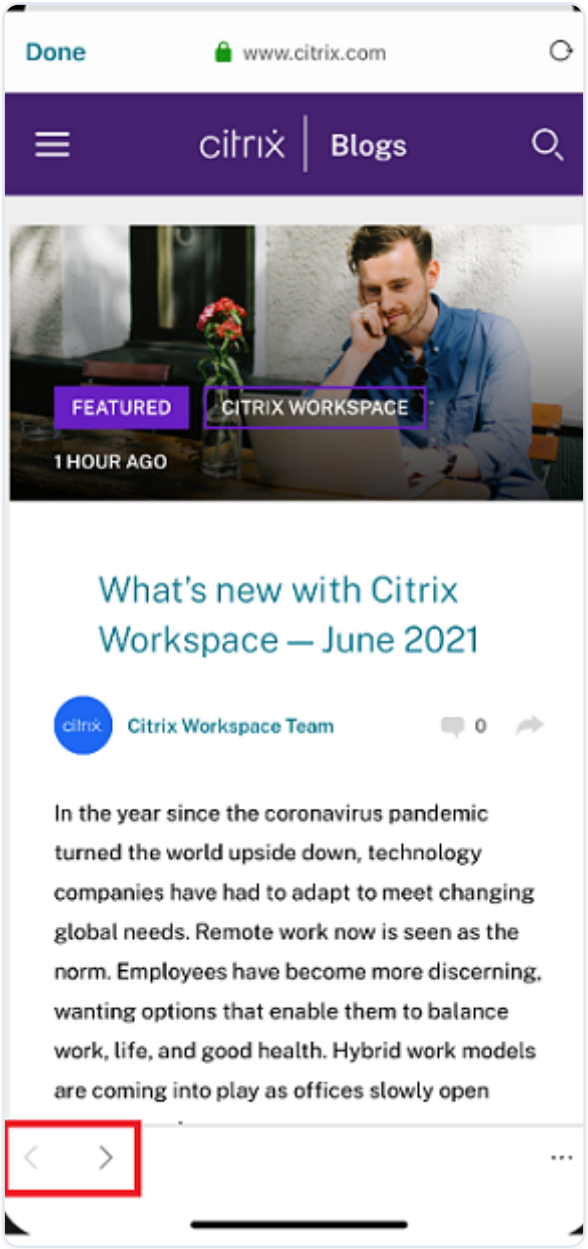
- Die Funktion ist nur für iPad-Benutzer anwendbar.
- Die Funktion arbeitet mit Berührung oder Maus.
- Die Funktion arbeitet mit einem iPad oder auf einem externen Display.

- Die letzte Position der Symbolleiste bleibt für die nächste Sitzung oder den Anwendungsstart erhalten.

Zwischen SaaS- und Web-Apps wechseln

Die Usability-Verbesserung ermöglicht Ihnen, innerhalb von Web- und Software-as-a-Service (SaaS)-Apps vor- und zurückzunavigieren.

Die Navigationsschaltflächen werden unten links in Ihren Workspace-Web- und SaaS-App-Sitzungen Ihres iPhones angezeigt.



Die Navigationsschaltflächen erscheinen oben links in Ihren Workspace Web- und SaaS-App-Sitzungen auf Ihrem iPad.

Navigation(/en-us/citrix-workspace-app-for-ios/media/navigationa.png)

Migration von lokalen zu Cloud-Konten

Administratoren können Endbenutzer nahtlos von einer lokalen StoreFront-Store-URL zu einer Workspace-URL migrieren. Administratoren können die Migration mit minimaler Endbenutzerinteraktion mithilfe des Global App Configuration Service durchführen.

So konfigurieren Sie:

1. Navigieren Sie zur Global App Configuration Store Settings API URL und geben Sie die Cloud-Store-URL ein. Zum Beispiel, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigieren Sie zu **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > klicken Sie auf **POST**.
3. Klicken Sie auf **INVOKE API**.
4. Geben Sie die Payload-Details ein und laden Sie sie hoch. Geben Sie das Ablaufdatum des StoreFront-Stores im Epoch-Zeitstempel im Millisekundenformat ein.

   Zum Beispiel:

   ```
   "migrationUrl": [

   {



   "url": "<cloud store url>"

   "StoreFrontValidUntil": "<epoch timestamp in milliseconds>",

   }

   ]   ,
   ```

5. Klicken Sie auf **EXECUTE**, um den Dienst zu übertragen.

Endbenutzererfahrung

Wenn Sie als Endbenutzer die Citrix Workspace-App zum ersten Mal verwenden, wird nach erfolgreicher Authentifizierung der Migrationsbildschirm **Introducing the new Citrix Workspace**

angezeigt (falls zutreffend). Nachdem Sie auf die Option **Try new Citrix Workspace now** tippen, beginnt die Migration. Nach erfolgreicher Migration können Sie auf den Workspace Store (Cloud Store) zugreifen.

> **Hinweis:**
>
> Sie können die Migration dreimal überspringen. Später wird die Migration erzwungen, ohne die Möglichkeit, sie zu überspringen.

Neuer Workspace(/en-us/citrix-workspace-app-for-ios/media/new-workspace.png)

Nachdem Sie zum Workspace (Cloud) Store migriert haben, können Sie sowohl den StoreFront- als auch den Workspace Store unter **Einstellungen** anzeigen. Wenn Sie von einem Cloud Store zum lokalen StoreFront Store wechseln, wird ein Feedback-Bildschirm angezeigt, um Ihre Antwort zu erfassen.

> **Hinweis:**
>
> Der StoreFront-Store hat ein Ablaufdatum. Nach dem Ablaufdatum wird der Store gelöscht.

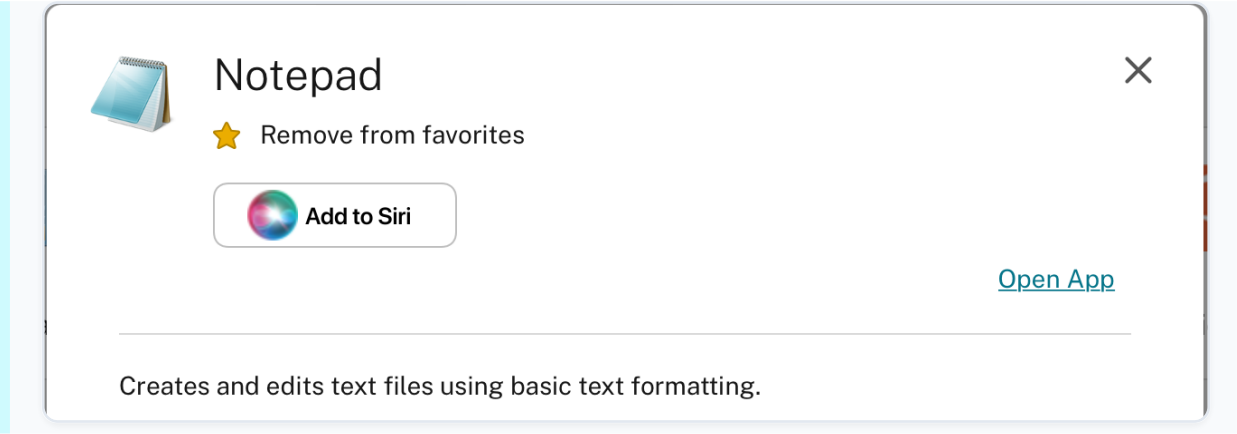
Siri-Integration

Sie können mit Siri interagieren, um Ressourcen wie Apps und Desktops zu starten, ohne jedes Mal die Citrix Workspace-App zu starten.

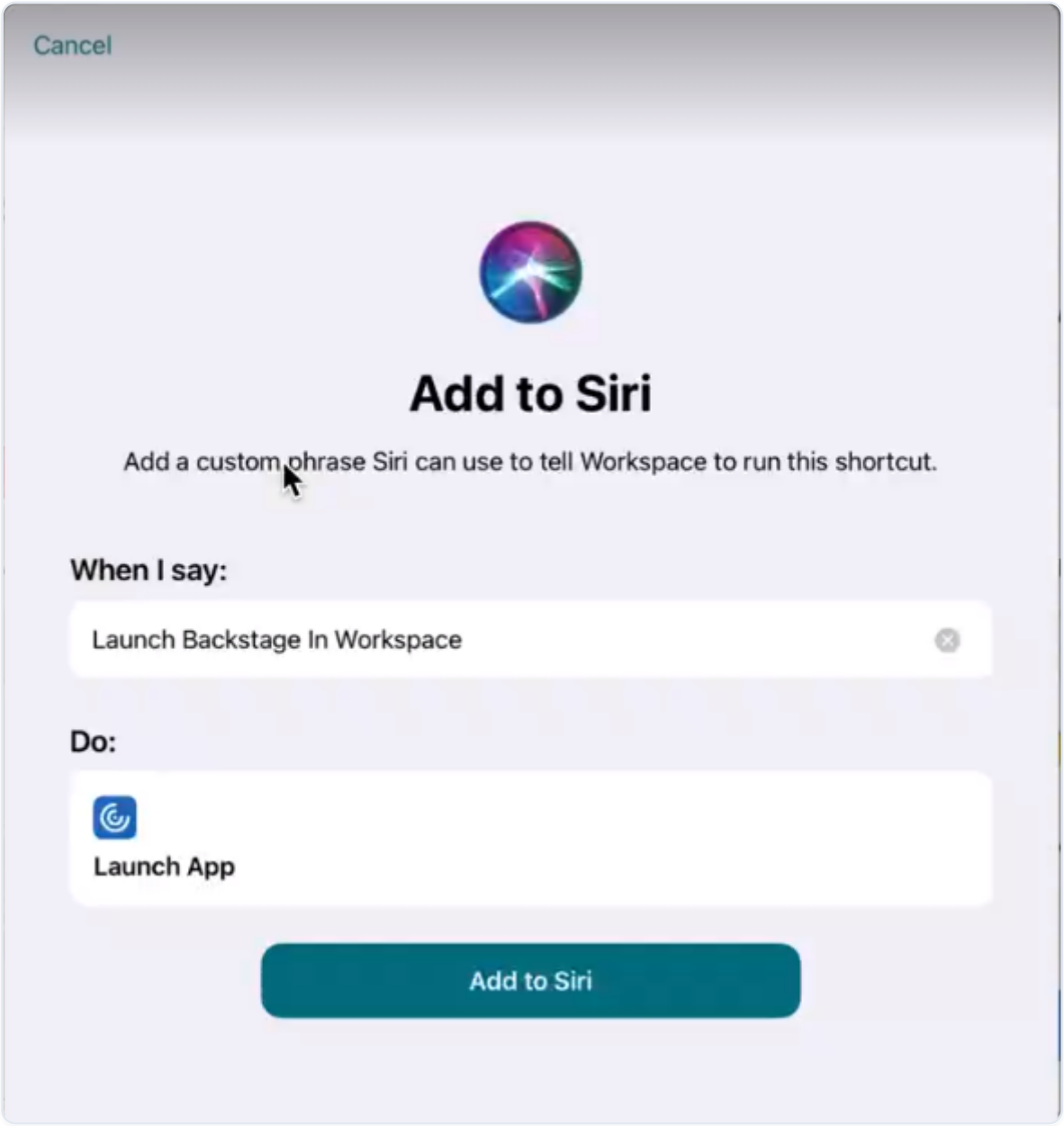
Konfigurieren

1. Starten Sie die Citrix Workspace-App und tippen Sie auf **Apps** oder **Desktops**. Wählen Sie die Ressource aus, die Sie der Siri-Verknüpfung hinzufügen möchten.
2. Tippen Sie auf die Auslassungspunkte (…). Ein Dialogfeld wird angezeigt.

> **Hinweis:**
>
> Wenn Sie ein iPhone- oder iPad-Desktop-Benutzer sind, tippen Sie auf **Auslassungspunkte** (…) > Bildschirm **App-Details** > **Details anzeigen**. Ein Dialogfeld wird angezeigt. Fahren Sie mit Schritt 3 fort.



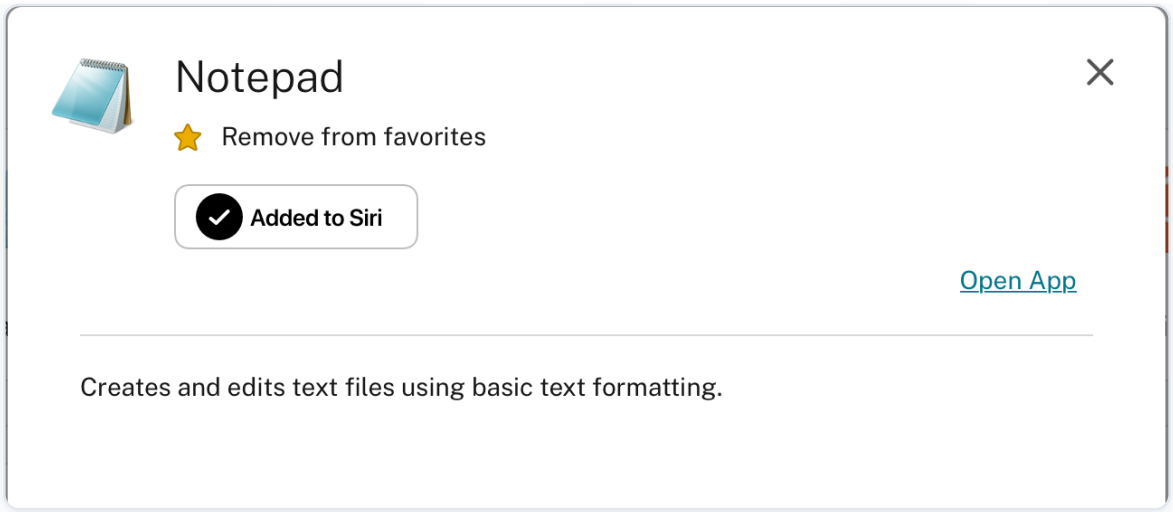
3. Tippen Sie auf **Zu Siri hinzufügen**. Das Dialogfeld **Zu Siri hinzufügen** wird angezeigt.



4. (Optional) Bearbeiten Sie den benutzerdefinierten Satz zum Aufrufen von Siri. Tippen Sie auf **Zu Siri hinzufügen**. Die Ressource ist jetzt der Siri-Verknüpfung hinzugefügt. Schließen Sie das Dialogfeld.

Hinweis:

Einige Geräte unterstützen die Aufzeichnung des benutzerdefinierten Satzes zum Aufrufen von Siri.



Anwendungseinstellungen

Starten Sie die Citrix Workspace-App und tippen Sie auf Ihr Profilsymbol > **Anwendungseinstellungen** > **Siri-Konfiguration**. Um die Funktion zu aktivieren, tippen Sie auf **Zu Siri hinzufügen**.

Sie können die Ressource jetzt mit Ihrer Stimme starten.

So bearbeiten oder löschen Sie die Verknüpfung

1. Wählen Sie die Ressource aus.
2. Tippen Sie auf die Auslassungspunkte (…). Ein Dialogfeld wird angezeigt.
3. Tippen Sie auf **Zu Siri hinzugefügt**. Das Dialogfeld **Verknüpfung bearbeiten** wird angezeigt.

Unterstützung für separates Sitzungsfenster in der Citrix Workspace-App

Ab Version 24.1.0 führt die Citrix Workspace-App für iOS ein separates Sitzungsfenster ein, das Multitasking effizienter und benutzerfreundlicher macht. Mit dieser Funktion können Sie ein Desktop-ähnliches Erlebnis haben. Wenn die Funktion für separate Sitzungsfenster aktiviert ist, können Sie Sitzungen einfach per Drag & Drop auf die angeschlossenen externen Monitore

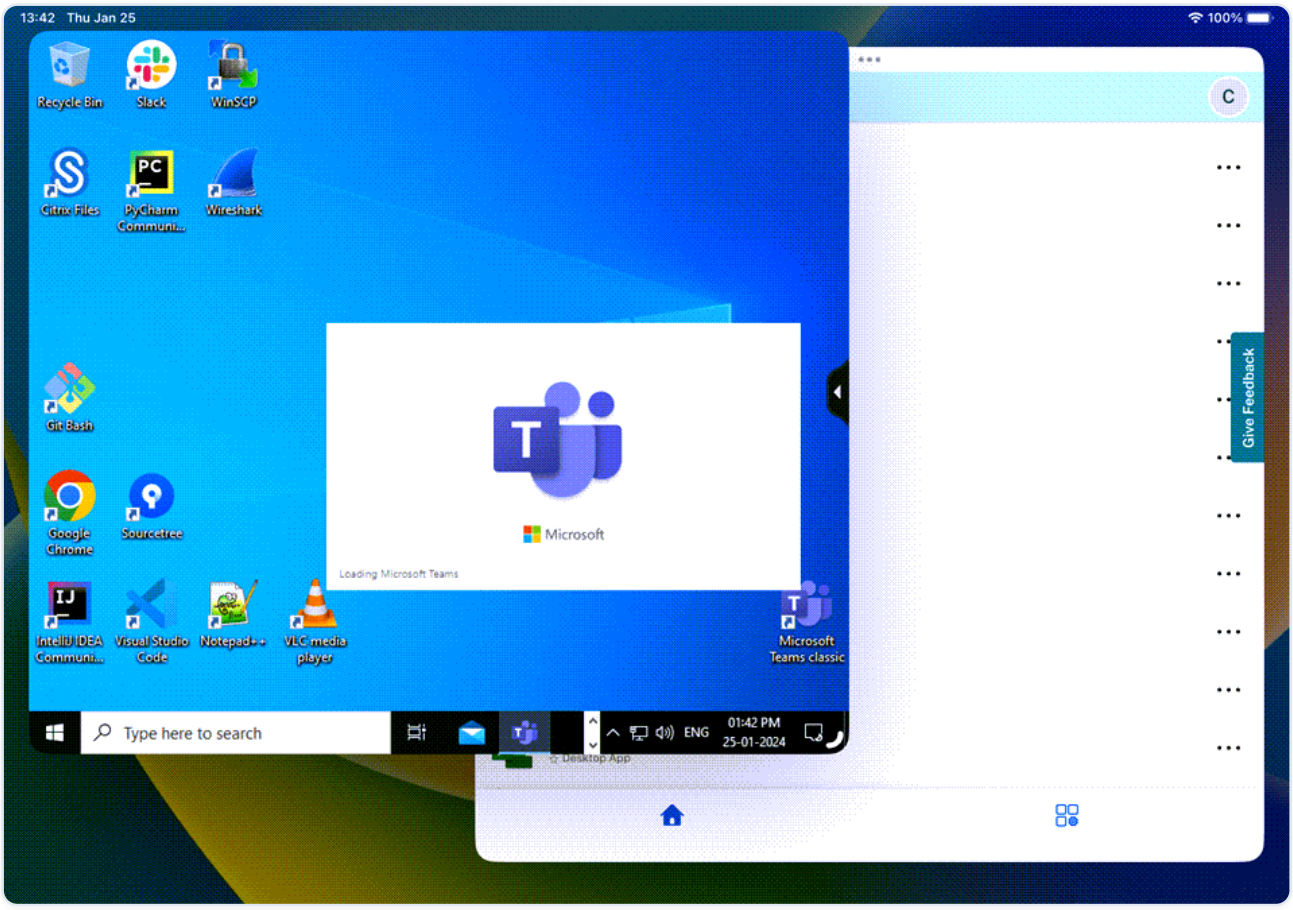
ziehen. Dadurch kann der Hauptmonitor des iPads für Multitasking mit anderen Apps verwendet werden.

Die folgenden Verbesserungen sind in dieser Funktion enthalten:

- Wenn Sie auf die Schaltfläche **Home** in der Sitzungsmenüleiste klicken, wird das Citrix Workspace-UI-Fenster geöffnet, anstatt das HDX™-Sitzungsfenster zu schließen. Diese Verbesserung ermöglicht es Ihnen, die Citrix Workspace-UI und die HDX-Sitzung gleichzeitig zu verwenden. Wenn Sie eine neue Sitzung über die Citrix Workspace-UI starten, wird die vorhandene automatisch getrennt.
- Wenn Sie auf die Schaltfläche **Anzeigeoptionen** in der Sitzungsmenüleiste klicken, wird ein Einstellungsfenster über der HDX-Sitzung angezeigt. Dieses Fenster ermöglicht es Ihnen, die Sitzungsauflösung anstelle der Citrix Workspace-UI-Einstellungen anzupassen.

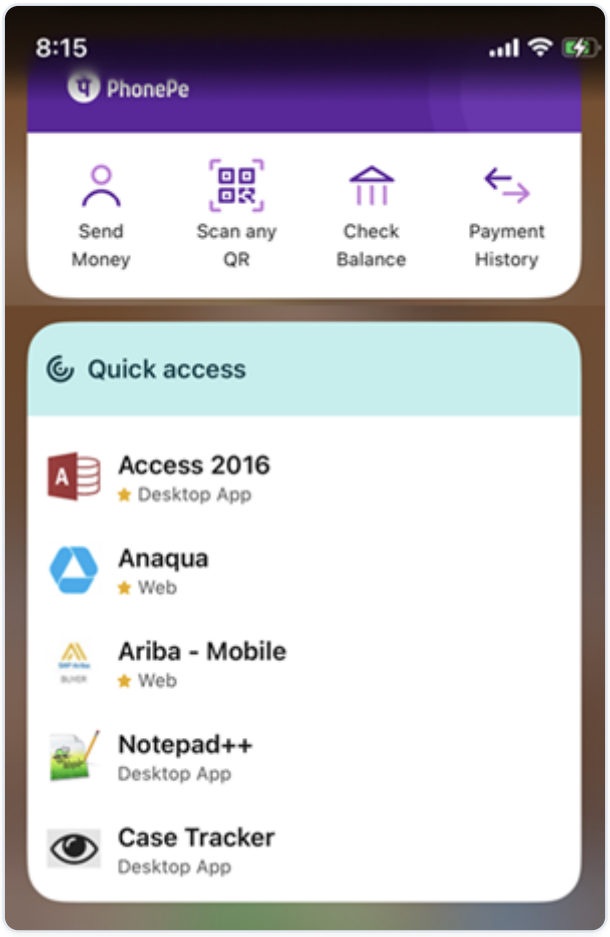
> **Hinweis:**
>
> Diese Funktion wird nur auf Geräten unterstützt, die die Stage Manager-Funktion unterstützen. Alle iPhone-Geräte und einige iPad-Geräte unterstützen diese Funktion nicht. Weitere Informationen zur Stage Manager-Funktion finden Sie unter Stage Manager auf dem iPad ein- oder ausschalten in der Apple-Supportdokumentation.

> Um die Funktion für separate Sitzungsfenster zu konfigurieren, navigieren Sie zu **Einstellungen -> Erweitert -> Multitasking** und wählen Sie **Separates Sitzungsfenster**.



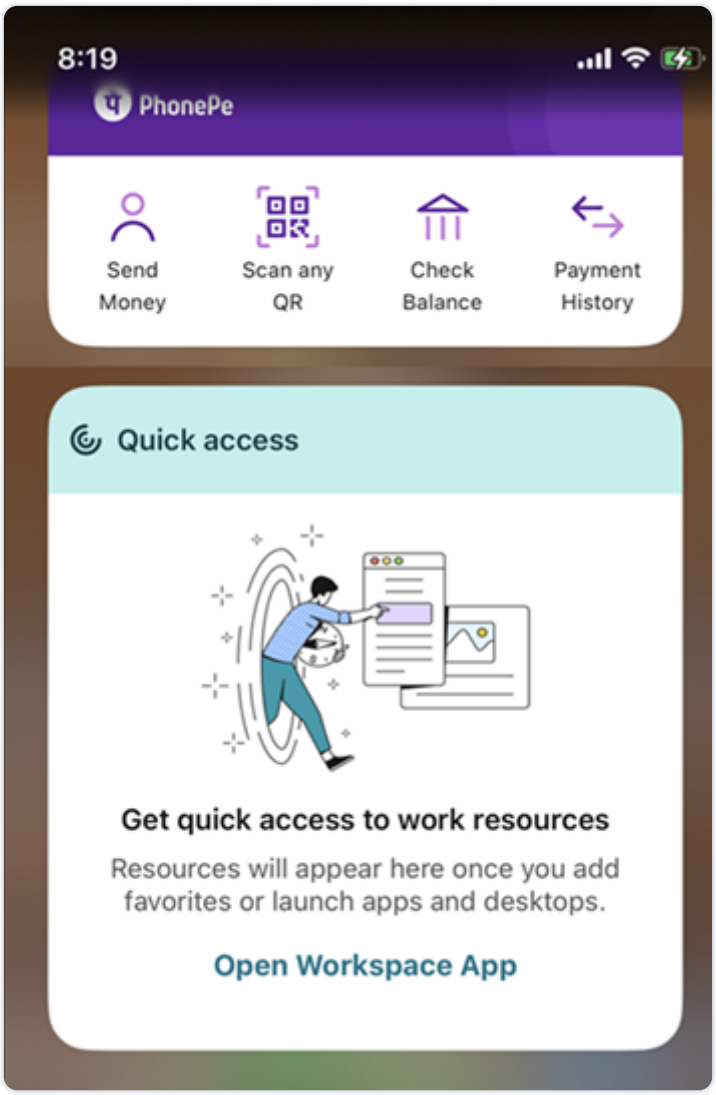
Apps und Desktops als Widgets anzeigen

Ab Version 23.11.0 können Endbenutzer ihre virtuellen Apps und Desktops direkt von ihren iPhones und iPads aus starten. Sie müssen die Citrix Workspace-App nicht öffnen, um eine App- oder Desktopsitzung zu starten. Ein Benutzer kann maximal fünf virtuelle Apps und Desktops als Widgets haben.



Die Widgets werden automatisch gemäß den folgenden Kriterien erstellt:

- Drei bevorzugte und zwei zuletzt geöffnete Apps oder Desktops werden als Widgets angezeigt
- Wenn keine bevorzugten Apps oder Desktops vorhanden sind, werden bis zu fünf zuletzt geöffnete Apps und Desktops als Widgets angezeigt
- Wenn keine kürzlich geöffneten Apps oder Desktops vorhanden sind, werden bis zu fünf bevorzugte Apps oder Desktops als Widgets angezeigt
- Wenn noch keine Apps oder Desktops als Favoriten hinzugefügt wurden und keine Apps oder Desktops kürzlich geöffnet wurden, werden Benutzer aufgefordert, die Citrix Workspace-App für iOS zu öffnen. Sie können dann bestimmte Apps oder Desktops als Favoriten markieren.



Webansicht für Web- und SaaS-Apps

Webseite

Externes Teilen von Webseiten

Sie können die Webseiten, die Sie aus der Citrix Workspace-App öffnen, mit anderen teilen. Sie können:

- einen Link aus einer Webansicht kopieren
- eine Webseite direkt in Safari öffnen
- Links direkt an Personen oder Apps senden

Zum Teilen tippen Sie auf das **...**-Symbol oben rechts in der Webansicht oder tippen Sie lange auf einen beliebigen Link innerhalb der Webansicht und tippen Sie auf die gewünschte Option.

Webansicht

Erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps

Sie können eine erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps haben. Diese Verbesserung ermöglicht Ihnen Folgendes:

- Die URL Ihrer Apps anzeigen.
- Die Sicherheitsinformationen Ihrer Apps anzeigen.
- Ihre Apps teilen.

Außerdem können Sie Ihre Apps jetzt nach links und rechts wischen, um vorwärts bzw. rückwärts zu navigieren.

Web-Viewer der Citrix Workspace Mobile App

Der Web-Viewer ist eine In-App-Browsing-Lösung, die innerhalb der Citrix Workspace-App ausgeführt wird. Er ermöglicht Benutzern, Web- oder SaaS-Apps sicher aus der Citrix Workspace-App zu öffnen. Der Web-Viewer gewährleistet eine konsistente Benutzeroberfläche beim Zugriff auf verschiedene Web- oder SaaS-Apps. Er verbessert die Produktivität und bietet eine bessere Leistung beim Rendern der Apps.

Mit dem anhaltenden Fokus auf die Bereicherung der Benutzererfahrung bietet Ihnen der neue Web-Viewer eine verbesserte und naturnähere Browser-ähnliche Erfahrung, komplett mit den folgenden Funktionen:

- VPN-loser Zugriff auf interne Webseiten
- SSO für Web und SaaS mit adaptiven Zugriffsrichtlinien
- Dateidownload mit Vorschau
- Nahtlose Navigation zwischen Seiten und Websites
- Möglichkeit zum Teilen von URLs
- Auf Seite suchen
- konsistente Ansicht beim Zugriff auf Links über den Aktivitätsfeed

Administratoren können Secure Private Access (SPA) aktivieren, einschließlich Download-, Zwischenablage-, Navigationsbeschränkungen, Dateiupload und Wasserzeichen in verschiedenen Kombinationen pro URL.

Passwortverwaltung

Passwörter speichern

Mithilfe der Citrix Web Interface Management Konsole können Sie die Authentifizierungsmethode so konfigurieren, dass Benutzer ihre Passwörter speichern können. Wenn Sie das Benutzerkonto konfigurieren, wird das verschlüsselte Passwort gespeichert, bis sich der Benutzer zum ersten Mal verbindet. Beachten Sie Folgendes:

- Wenn Sie das Speichern von Passwörtern aktivieren, speichert die Citrix Workspace-App für iOS das Passwort auf dem Gerät für zukünftige Anmeldungen und fordert keine Passwörter an, wenn Benutzer eine Verbindung zu Anwendungen herstellen.

  > **Hinweis:**
  >
  > Das Passwort wird nur gespeichert, wenn Benutzer bei der Erstellung eines Kontos ein Passwort eingeben. Wenn für das Konto kein Passwort eingegeben wird, wird kein Passwort gespeichert, unabhängig von der Servereinstellung.

- Wenn Sie das Speichern von Passwörtern deaktivieren (Standardeinstellung), fordert die Citrix Workspace-App für iOS Benutzer jedes Mal zur Eingabe von Passwörtern auf, wenn sie sich verbinden.

> **Hinweis:**
>
> Bei direkten StoreFront-Verbindungen ist das Speichern von Passwörtern nicht verfügbar.

Passwortspeicherung überschreiben

Wenn Sie den Server so konfigurieren, dass Passwörter gespeichert werden, können Benutzer, die lieber bei der Anmeldung Passwörter eingeben möchten, die Passwortspeicherung überschreiben:

- Beim Erstellen des Kontos lassen Sie das Passwortfeld leer.
- Beim Bearbeiten eines Kontos löschen Sie das Passwort und speichern Sie das Konto.

Verwendung

Die Citrix Workspace-App verfügt über eine Funktion, die den Verbindungsprozess optimiert, indem Sie Ihr Passwort speichern können, wodurch der zusätzliche Schritt entfällt, eine Sitzung jedes Mal authentifizieren zu müssen, wenn Sie die Citrix Workspace-App öffnen.

> **Hinweis:**
>
> Die Funktionalität **Passwort speichern** unterstützt derzeit das PNA-Protokoll. Sie unterstützt den StoreFront-*nativen* Modus nicht. Diese Funktionalität funktioniert jedoch, wenn StoreFront den PNA-*Legacy*-Modus aktiviert.

StoreFront zum Speichern von Passwörtern konfigurieren

So konfigurieren Sie StoreFront, um die Funktion **Passwort speichern** zu aktivieren:

1. Wenn Sie einen vorhandenen Store konfigurieren, fahren Sie mit Schritt 3 fort.
2. Um eine neue StoreFront-Bereitstellung zu konfigurieren, befolgen Sie die Best Practices, die unter Installieren, Einrichten, Aktualisieren und Deinstallieren beschrieben sind.
3. Öffnen Sie die Citrix StoreFront-Verwaltungskonsole. Stellen Sie sicher, dass die Basis-URL HTTPS verwendet und mit dem allgemeinen Namen übereinstimmt, der bei der Generierung Ihres SSL-Zertifikats angegeben wurde.
4. Wählen Sie den Store aus, den Sie konfigurieren möchten.
5. Klicken Sie auf **XenApp® Service Support konfigurieren**.
6. Aktivieren Sie **XenApp Service support**, wählen Sie den **Standard-Store** (optional) aus und klicken Sie auf **OK**.
7. Navigieren Sie zur Vorlagenkonfigurationsdatei unter c:\\inetpub\\wwwroot\\Citrix\\\<store name\>\\Views\\PnaConfig\\.
8. Erstellen Sie eine Sicherungskopie von Config.aspx.
9. Öffnen Sie die ursprüngliche Datei Config.aspx.
10. Bearbeiten Sie die Zeile \<EnableSavePassword\>**false**\</EnableSavePassword\>, um den Wert **false** in **true** zu ändern.
11. Speichern Sie die bearbeitete Datei Config.aspx.
12. Führen Sie auf dem StoreFront-Server PowerShell mit Administratorrechten aus.
13. In der PowerShell-Konsole:

a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`

b. Geben Sie „Set-ExecutionPolicy RemoteSigned“ ein.

c. Geben Sie „.\\ImportModules.ps1“ ein.

d. Geben Sie „Set-DSServiceMonitorFeature –ServiceUrl“ `https://localhost:443/StoreFrontMonitor` ein.

14. Wenn Sie eine StoreFront-Gruppe haben, führen Sie dieselben Befehle auf allen Mitgliedern der Gruppe aus.

Citrix Gateway zum Speichern von Kennwörtern konfigurieren

> **Hinweis:**
>
> Diese Konfiguration verwendet Citrix Gateway-Lastenausgleichsserver.

So konfigurieren Sie Citrix Gateway zur Unterstützung der gespeicherten Kennwortfunktionalität:

1. Melden Sie sich bei der Citrix Gateway-Verwaltungskonsole an.
2. Befolgen Sie die Best Practices von Citrix, um ein Zertifikat für Ihre virtuellen Lastenausgleichsserver zu erstellen.
3. Navigieren Sie auf der Registerkarte „Konfiguration“ zu **Traffic Management** > **Lastenausgleich** > **Server** und klicken Sie auf **Hinzufügen**.
4. Geben Sie den Servernamen und die IP-Adresse des StoreFront-Servers ein.
5. Klicken Sie auf **Erstellen**. Wenn Sie eine StoreFront-Gruppe haben, wiederholen Sie Schritt 5 für alle Server in der Gruppe.
6. Navigieren Sie auf der Registerkarte „Konfiguration“ zu **Traffic Management** > **Lastenausgleich** > **Monitor** und klicken Sie auf **Hinzufügen**.
7. Geben Sie einen Namen für den Monitor ein. Wählen Sie **StoreFront** als Typ aus. Wählen Sie unten auf der Seite **Sicher** aus (erforderlich, da der StoreFront-Server HTTPS verwendet).
8. Klicken Sie auf die Registerkarte **Spezielle Parameter**. Geben Sie den zuvor konfigurierten StoreFront-Namen ein, wählen Sie **Backed Services prüfen** aus und klicken Sie auf **Erstellen**.

9. Navigieren Sie auf der Registerkarte **Configuration** zu **Traffic Management** > **Load Balancing** > **Service Group**s und klicken Sie auf **Add**.
10. Geben Sie einen Namen für Ihre Service Group ein, stellen Sie das Protokoll auf **SSL** ein und klicken Sie auf **Ok**.
11. Wählen Sie auf der rechten Seite des Bildschirms unter Erweiterte Einstellungen die Option **Settings** aus.
12. Aktivieren Sie Client-IP und geben Sie Folgendes für den Header-Wert ein: **X-Forwarded-For**, und klicken Sie auf **OK**.
13. Wählen Sie auf der rechten Seite des Bildschirms unter Erweiterte Einstellungen die Option **Monitors** aus. Klicken Sie auf den Pfeil, um neue Monitore hinzuzufügen.
14. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann das Dropdown-Menü **Select Monitor** aus. Eine Liste der Monitore (konfiguriert auf Citrix Gateway) wird angezeigt.
15. Klicken Sie auf das Optionsfeld neben dem Monitor, den Sie zuvor erstellt haben, und klicken Sie auf **Select**, dann auf **Bind**.
16. Wählen Sie auf der rechten Seite des Bildschirms (unter Erweiterte Einstellungen) die Option **Members** aus. Klicken Sie auf den Pfeil, um neue Dienstgruppenmitglieder hinzuzufügen.
17. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann das Dropdown-Menü **Select Member** aus.
18. Wählen Sie das Optionsfeld **Server Based** aus. Eine Liste der Servermitglieder (konfiguriert auf Citrix Gateway) wird angezeigt. Klicken Sie auf das Optionsfeld neben dem StoreFront-Server, den Sie zuvor erstellt haben.
19. Geben Sie 443 für die Portnummer ein und geben Sie eine eindeutige Nummer für die Hash-ID an, klicken Sie dann auf **Create**, dann auf **Done**. Wenn alles ordnungsgemäß konfiguriert wurde, sollte **Effective State** ein grünes Licht anzeigen, was darauf hinweist, dass die Überwachung ordnungsgemäß funktioniert.
20. Navigieren Sie zu **Traffic Management -\> Load Balancing -\ > Virtual Servers** und klicken Sie auf **Add**. Geben Sie einen Namen für den Server ein und wählen Sie **SSL** als Protokoll aus.
21. Geben Sie die IP-Adresse für den StoreFront-Lastenausgleichsserver ein und klicken Sie auf **OK**.
22. Wählen Sie die Bindung **Load Balancing Virtual Server Service Group** aus, klicken Sie auf den Pfeil und fügen Sie die zuvor erstellte Service Group hinzu. Klicken Sie zweimal auf **OK**.
23. Weisen Sie das für den virtuellen Load Balance-Server erstellte SSL-Zertifikat zu. Wählen Sie **No Server Certificate** aus.

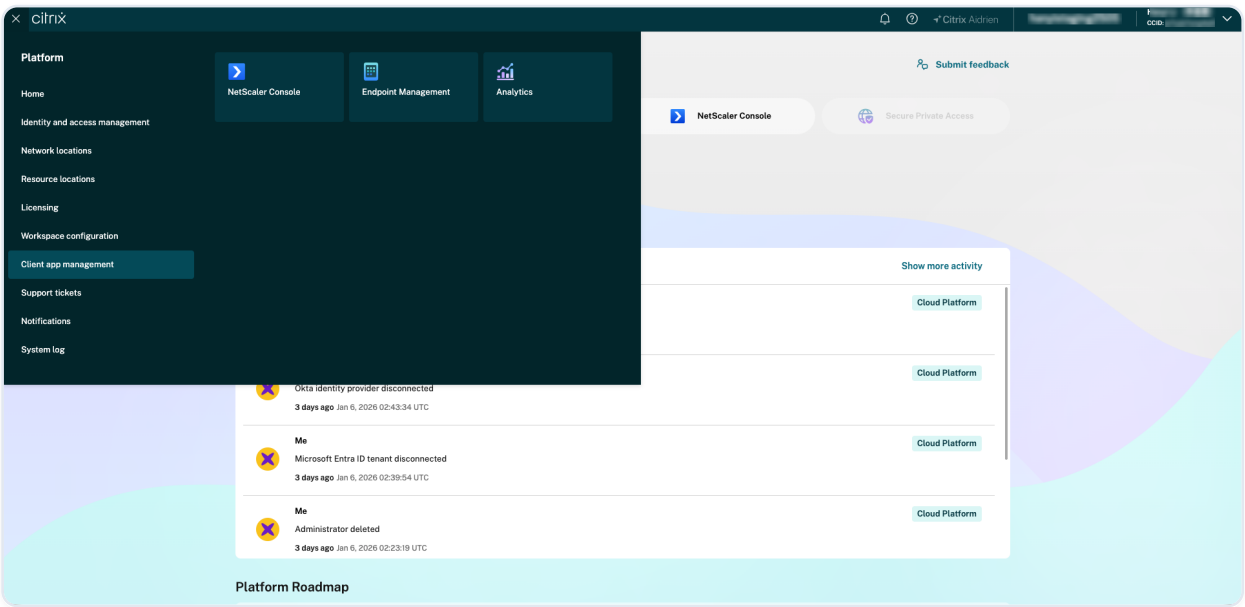
24. Wählen Sie das Load-Balance-Serverzertifikat aus der Liste und klicken Sie auf **Binden**.
25. Fügen Sie das Domänenzertifikat zum Load-Balance-Server hinzu. Klicken Sie auf **Kein CA-Zertifikat**.
26. Wählen Sie das Domänenzertifikat und klicken Sie auf **Binden**.
27. Wählen Sie auf der rechten Seite des Bildschirms **Persistenz** aus.
28. Ändern Sie die Persistenz in **SOURCEIP** und stellen Sie das Zeitlimit auf **20** ein. Klicken Sie auf **Speichern** und dann auf **Fertig**.
29. Fügen Sie auf Ihrem Domänen-DNS-Server den Load-Balance-Server hinzu (falls noch nicht erstellt).
30. Starten Sie die Citrix Workspace-App für iOS auf Ihrem iOS-Gerät und geben Sie die vollständige XenApp-URL ein.

GACS- und MDM-Unterstützung für die Konfiguration der Sitzungssymbolleiste

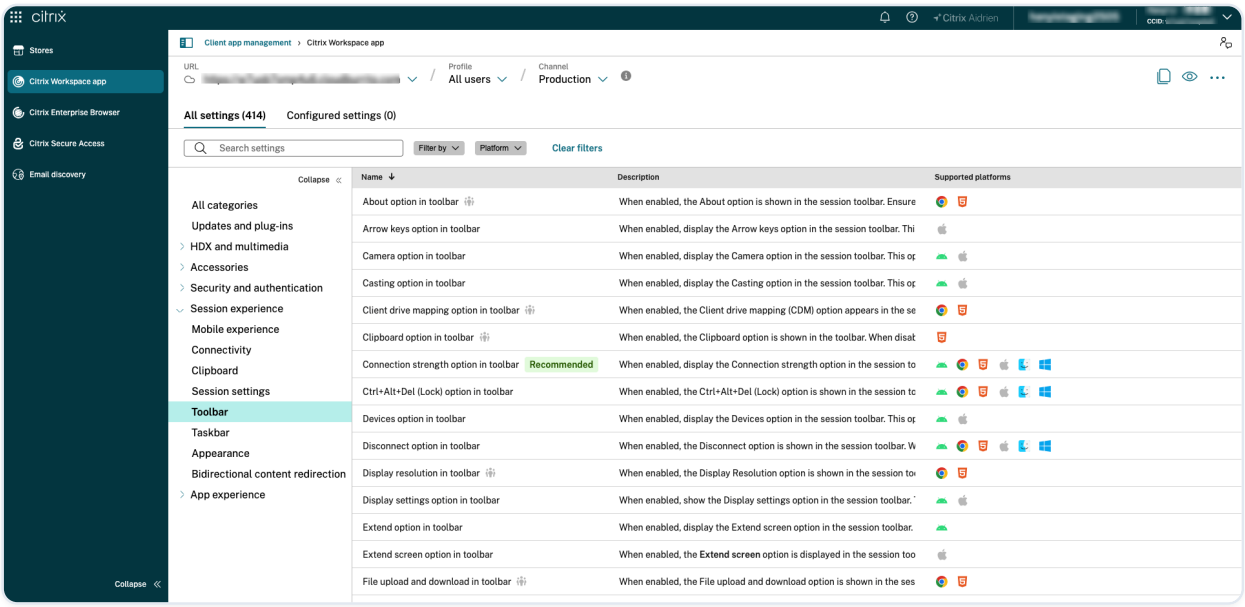
Sie können diese Funktion mithilfe des Global App Configuration Service (GACS) und des Mobile Device Management (MDM) konfigurieren.

Verwenden von GACS

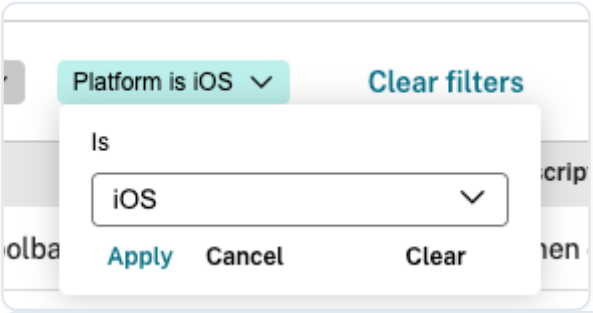
1. Melden Sie sich bei Ihrem **Citrix Cloud™**-Konto an und navigieren Sie zu **Client App Management**.

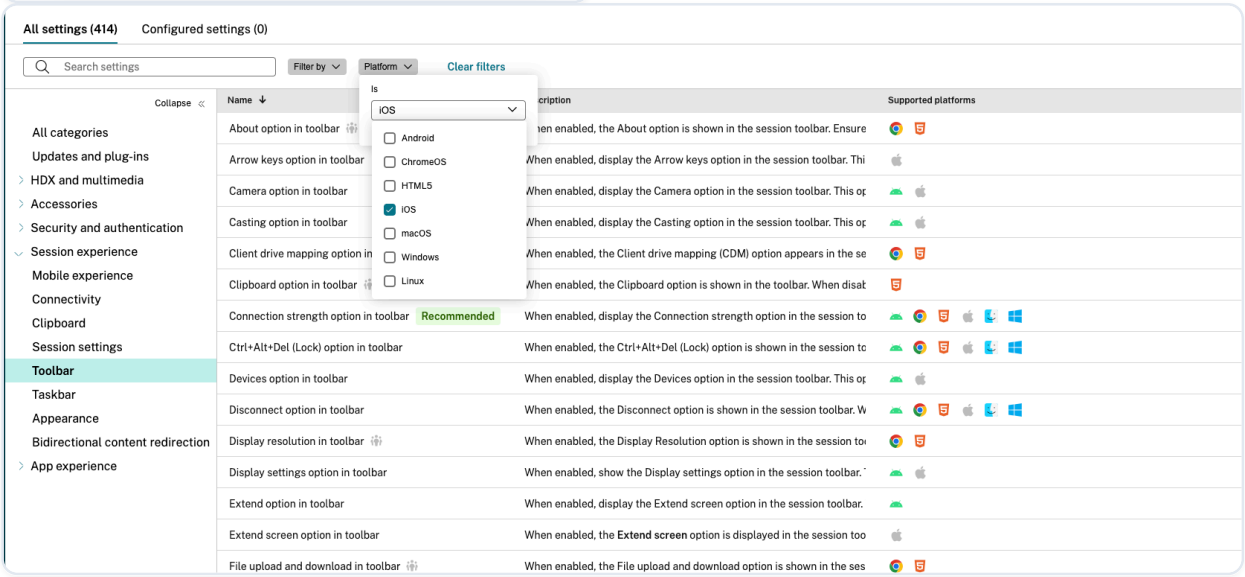


2. Klicken Sie auf **Citrix Workspace app > Session Experience > Session Toolbar**.

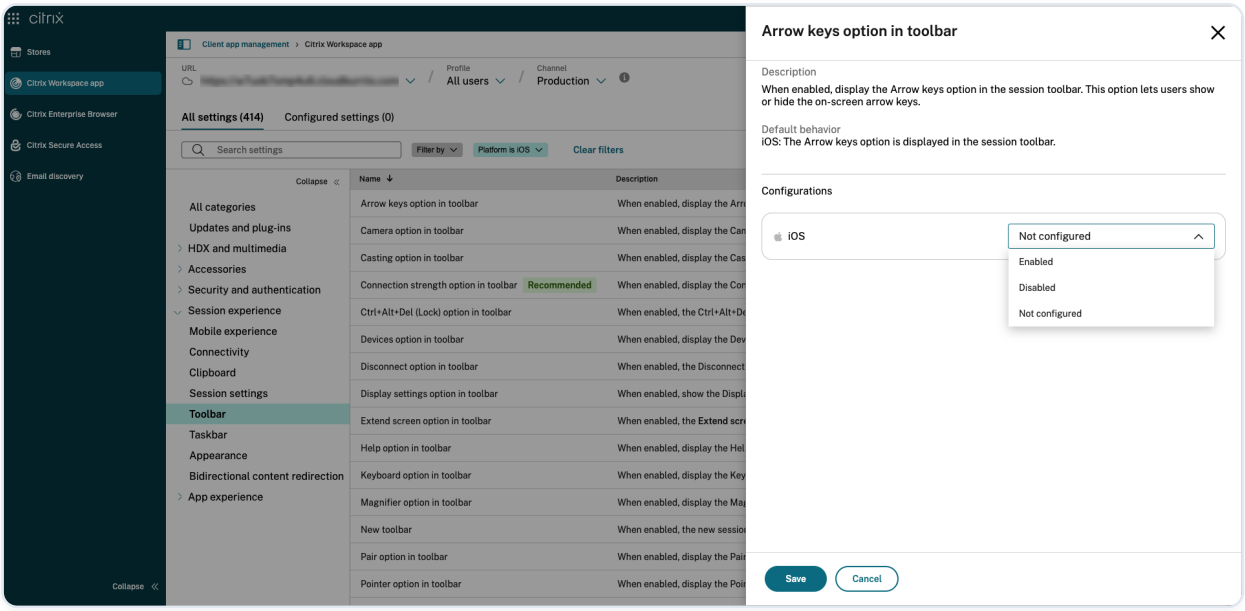


3. Unter dem Abschnitt **Symbolleiste**. Navigieren Sie zur gewünschten Option in der Symbolleiste und klicken Sie auf die Spalte, die Sie bearbeiten möchten. Sie können auch nach Plattform filtern (z. B. iOS oder eine andere Plattform) und dann auf **Anwenden** klicken.



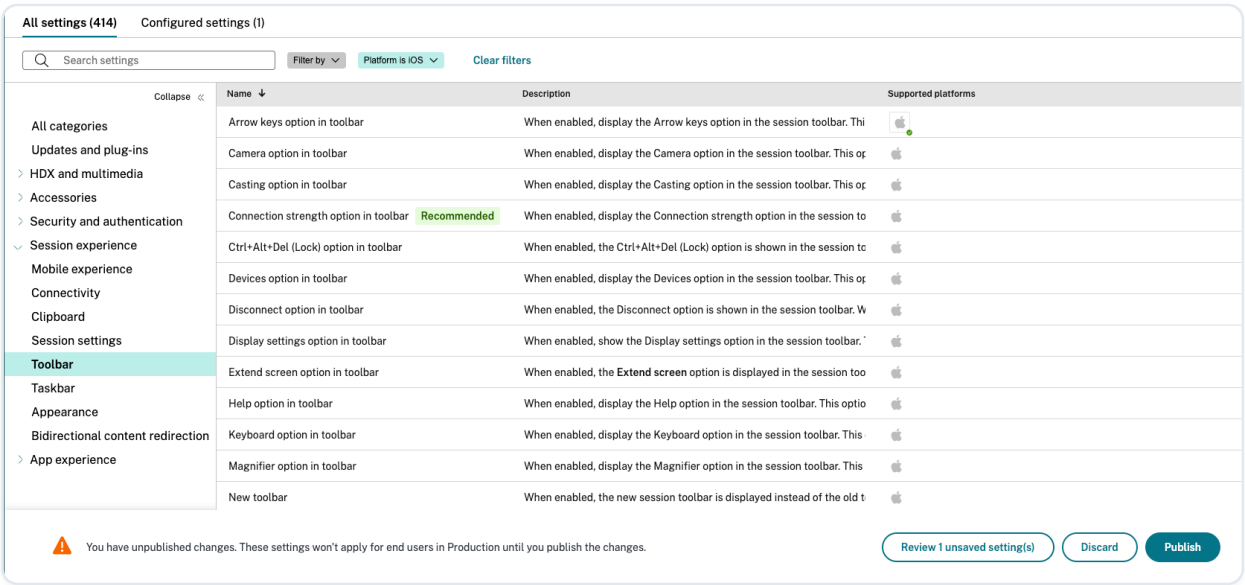


4. Aktivieren Sie das Konfigurationskontrollkästchen und klicken Sie dann. Sie können die Symbolleistenoption nun anpassen, um sie *auszublenden* oder *anzuzeigen*.



5. Klicken Sie nach dem Ändern der Konfiguration auf **Speichern**.

6. Klicken Sie auf **Veröffentlichen**, um die Einstellungen zu speichern.



Hinweis:

Aufgrund des Citrix Cloud-Cachings kann es bis zu 6 Stunden dauern, bis Änderungen wirksam werden.

Verwenden von MDM

Diese Konfiguration wird über Ihre MDM-Lösung als **Managed App Configuration** für die Bundle-ID der Citrix Workspace-App bereitgestellt. MDM-Konfigurationen haben Vorrang vor GACS-Einstellungen. Die Einstellungen werden im `XML/plist`-Format als Teil der Managed App Configuration von Apple gespeichert.

Beispiel-MDM-Konfiguration für die Symbolleiste

```
<dict>

    <key>category</key>

    <string>toolbar</string>

    <key>userOverride</key>

    <false/>

    <key>settings</key>

    <array>

        <dict>

            <key>name</key>

            <string>enableKeyboardToolbarOption</string>

            <key>value</key>

            <true/>

        </dict>

        <dict>

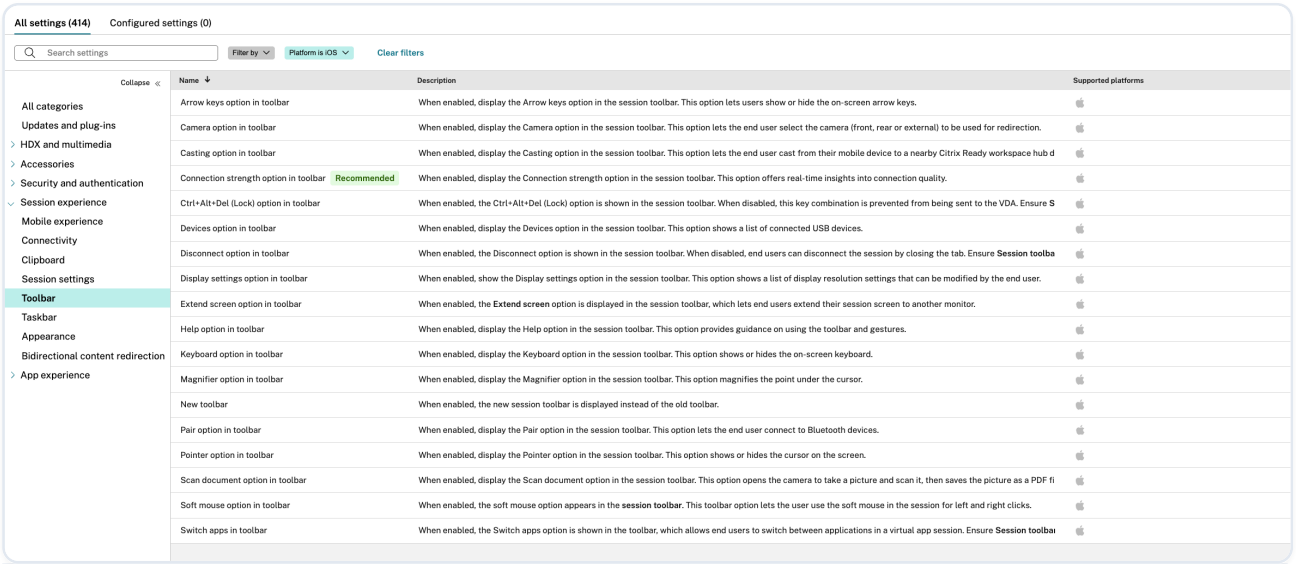
            <key>name</key>

            <string>enableCloseToolbarOption</string>

            <key>value</key>
```

```
            <false/>
        </dict>
        <dict>
            <key>name</key>
            <string>enableCameraToolbarOption</string>
            <key>value</key>
            <true/>
        </dict>
    </array>
</dict>
```

iOS-Symbolleistensymbole-Konfiguration



NAME	BESCHREIBUNG	MDM-EINSTELLUNGSSCHLÜSSEL
Pfeiltastenoption in der Symbolleiste	Wenn aktiviert, wird die Pfeiltastenoption in der Sitzungssymbolleiste angezeigt. Mit dieser Option	`enableArrowKeysToolbarOption`

NAME	BESCHREIBUNG	MDM-EINSTELLUNGSSCHLÜSSEL
	können Benutzer die Bildschirm-Pfeiltasten ein- oder ausblenden.	
Kameraoption in der Symbolleiste	Wenn aktiviert, wird die Kameraoption in der Sitzungssymbolleiste angezeigt. Mit dieser Option kann der Endbenutzer die Kamera (Vorder-, Rück- oder externe Kamera) auswählen, die für die Umleitung verwendet werden soll.	`enableCameraToolbarOption`
Casting-Option in der Symbolleiste	Wenn aktiviert, wird die Casting-Option in der Sitzungssymbolleiste angezeigt. Mit dieser Option kann der Endbenutzer Inhalte von seinem Mobilgerät auf ein nahegelegenes Citrix Ready Workspace Hub-Gerät übertragen.	`enableCastingToolbarOption`
Option Verbindungsstärke in der Symbolleiste	Wenn aktiviert, wird die Option Verbindungsstärke in der Sitzungssymbolleiste angezeigt. Diese Option bietet Echtzeit-Einblicke in die Verbindungsqualität.	`enableConnectionStrengthToolbarOption`
Option Strg+Alt+Entf (Sperren) in der Symbolleiste	Wenn aktiviert, wird die Option Strg+Alt+Entf (Sperren) in der Sitzungssymbolleiste angezeigt. Wenn deaktiviert, wird verhindert, dass diese Tastenkombination an den VDA gesendet wird. Stellen Sie sicher, dass die Sitzungssymbolleiste aktiviert	`enableCtrlAltDelToolbarOption`

NAME	BESCHREIBUNG	MDM-EINSTELLUNGSSCHLÜSSEL
	ist, damit diese Einstellung wirksam wird.	
Option Geräte in der Symbolleiste	Wenn aktiviert, wird die Option Geräte in der Sitzungssymbolleiste angezeigt. Diese Option zeigt eine Liste der verbundenen USB-Geräte an.	`enableDevicesToolbarOption`
Option trennen in der Symbolleiste	Wenn aktiviert, wird die Option trennen in der Sitzungssymbolleiste angezeigt. Wenn deaktiviert, können Endbenutzer die Sitzung durch Schließen des Tabs trennen. Stellen Sie sicher, dass die Sitzungssymbolleiste aktiviert ist, damit diese Einstellung wirksam wird.	`enableCloseToolbarOption`
Option Anzeigeeinstellungen in der Symbolleiste	Wenn aktiviert, wird die Option Anzeigeeinstellungen in der Sitzungssymbolleiste angezeigt. Diese Option zeigt eine Liste der Anzeigeeinstellungen an, die vom Endbenutzer geändert werden können.	`enableDisplaySettingsToolbarOption`
Hilfe-Option in der Symbolleiste	Wenn aktiviert, wird die Hilfe-Option in der Sitzungssymbolleiste angezeigt. Diese Option bietet Anleitungen zur Verwendung der Symbolleiste und von Gesten.	`enableHelpToolbarOption`

NAME	BESCHREIBUNG	MDM-EINSTELLUNGSSCHLÜSSEL
Tastatur-Option in der Symbolleiste	Wenn aktiviert, wird die Tastatur-Option in der Sitzungssymbolleiste angezeigt. Diese Option blendet die Bildschirmtastatur ein oder aus.	`enableKeyboardToolbarOption`
Lupen-Option in der Symbolleiste	Wenn aktiviert, wird die Lupen-Option in der Sitzungssymbolleiste angezeigt. Diese Option vergrößert den Punkt unter dem Cursor.	`enableMagnifierToolbarOption`
Neue Symbolleiste	Wenn aktiviert, wird die neue Sitzungssymbolleiste anstelle der alten Symbolleiste angezeigt.	`enableNewToolbar`
Kopplungs-Option in der Symbolleiste	Wenn aktiviert, wird die Kopplungs-Option in der Sitzungssymbolleiste angezeigt. Diese Option ermöglicht es dem Endbenutzer, sich mit Bluetooth-Geräten zu verbinden.	`enablePairToolbarOption`
Zeigeroption in der Symbolleiste	Wenn aktiviert, wird die Zeigeroption in der Sitzungssymbolleiste angezeigt. Diese Option zeigt oder verbirgt den Cursor auf dem Bildschirm.	`enablePointerToolbarOption`
Option „Dokument scannen“ in der Symbolleiste	Wenn aktiviert, wird die Option „Dokument scannen“ in der Sitzungssymbolleiste angezeigt. Diese Option öffnet die Kamera, um ein	`enableScanDocumentToolbarOption`

NAME	BESCHREIBUNG	MDM-EINSTELLUNGSSCHLÜSSEL
	Bild aufzunehmen und zu scannen, und speichert das Bild dann als PDF-Datei.	
Option „Soft-Maus“ in der Symbolleiste	Wenn aktiviert, wird die Soft-Maus-Option in der Sitzungssymbolleiste angezeigt. Diese Symbolleistenoption ermöglicht es dem Benutzer, die Soft-Maus in der Sitzung für Links- und Rechtsklicks zu verwenden.	`enableSoftMouseToolbarOption`
Apps in der Symbolleiste wechseln	Wenn aktiviert, wird die Option „Apps wechseln“ in der Symbolleiste angezeigt, die es Endbenutzern ermöglicht, in einer virtuellen App-Sitzung zwischen Anwendungen zu wechseln. Stellen Sie sicher, dass die Sitzungssymbolleiste aktiviert ist, damit diese Einstellung wirksam wird.	`enableSwitchAppsToolbarOption`

Store-Konfiguration

Verbesserte, neue anpassbare Symbolleiste

Ab Version 24.12.0 führt die Citrix Workspace-App für iOS eine neue anpassbare Symbolleiste ein. Die überarbeitete Desktop Viewer-Symbolleiste verbessert die Benutzererfahrung und den Support durch größere Flexibilität. Administratoren können die Symbolleiste während der Sitzung jetzt an die Anforderungen ihrer Organisation anpassen.

FUNKTION	BESCHREIBUNG
Administratorkontrolle	Administratoren können die Symbolleiste anpassen und auswählen, welche Optionen dem Endbenutzer angezeigt werden.
Benutzeroberfläche und Skinning	Die Symbolleiste des **Desktop Viewers** wurde mit einer neuen Benutzeroberfläche und Skinning-Optionen überarbeitet.
Umschaltbares Layout	Die Symbolleiste kann zwischen einem ein- und zweispaltigen Layout wechseln.
Anpassbare Symbolleiste	Administratoren können wählen, ob sie Benutzern die alte oder die neue Symbolleiste bereitstellen möchten.
Ziehfunktion	Im Querformat kann die Symbolleistenkerbe nur entlang des oberen Bildschirmrands verschoben werden. Im Hochformat kann die Kerbe horizontal von links nach rechts oder von rechts nach links sowie vertikal entlang des Bildschirmrands gezogen werden.
Schnellzugriffssymbole	Neue Symbole für den schnellen Zugriff auf häufig verwendete Funktionen wurden eingeführt.

FUNKTION	BESCHREIBUNG
Gestenführung	Bietet Anleitungen für Einzelklick, Rechtsklick, Ziehen, Zoomen, Zeiger umschalten und Tastaturnutzung.
Symbolleistenführung	Enthält Optionen für Geräte, Tastatur, Zeiger, Lupe, Soft-Maus, Anzeige, Kamera, Schalter, Scrollen und mehr.

Standardmenüoptionen:

MENÜOPTION	BESCHREIBUNG
Pfeiltasten	Zeigt ein Navigations-Pfeiltastenfeld für die Sitzungsnavigation an.
Tastatur	Zeigt die iOS-System-Soft-Tastatur zusammen mit einem erweiterten Tastaturzubehör mit Steuertasten an.
Zeiger	Zeigt einen Windows-ähnlichen Mauszeiger im Sitzungsfenster an.
Lupe	Zeigt einen fensterähnlichen Mauszeiger zusammen mit einer Lupe an.
Virtuelle Maus	Diese Option zeigt eine Soft-Maus auf dem Bildschirm an.
Wechseln	Switch-Apps wird verwendet, um zwischen mehreren virtuellen Apps zu wechseln, die gleichzeitig in einem einzigen Virtual Desktop Agent geöffnet sind.
Anzeige	Zeigt die modale Ansicht der Vollbild-Anzeigeeinstellungen an.
Strg+Alt+Entf	Sendet die Tastenkombination Strg+Alt+Entf an den Virtual Desktop Agent.

MENÜOPTION	BESCHREIBUNG
Koppeln	Ermöglicht das Koppeln mit einem sekundären iPhone- oder iPad-Gerät, das als Trackpad fungiert.
trennen	Wenn die Nachhaltigkeitsfunktion aktiviert ist, bietet sie die Möglichkeit, zwischen Abmelden und trennen zu wählen, andernfalls wird die Sitzung getrennt.
Einstellungen für externe Maus	Zeigt die modale Ansicht der Sitzungsmaus-Einstellungen an.
Kamera	Sie können den zu verwendenden Kameratyp auswählen: Vorderseite, Rückseite oder extern. Öffnet die Kamera, um Dokumente in ein PDF zu scannen und in den Virtual Desktop Agent hochzuladen.
Hilfehandbuch	Bietet Anleitungen zur Verwendung von Symbolleistenfunktionen, Gesten und Menüoptionen zum Navigieren und Interagieren mit der Sitzung.

Option für anpassbare Symbolleiste(/en-us/citrix-workspace-app-for-ios/media/customizable-toolbar-1.png)

Variable Menüoptionen:

MENÜOPTION	BESCHREIBUNG
Scannen	Zeigt eine Vollbildkamera zum Scannen von Dokumenten an.
Übertragen	Zeigt Optionen zum Übertragen des Bildschirms an.

Option für variable anpassbare Symbolleiste(/en-us/citrix-workspace-app-for-ios/media/customizable-toolbar-2.png)

Sie können die Funktion über den Global App Configuration Service (GACS) aktivieren und sicherstellen, dass das Feature-Flag eingeschaltet ist.

Um diese Funktion über GACS zu aktivieren, sollten Administratoren die folgenden Schritte ausführen:

1. Navigieren Sie in Citrix Cloud zu **Workspace Configuration** > **App Configuration** > **Configure**.
2. Wählen Sie unter **Citrix Workspace™ app** die Option **Session Experience**.
3. Klicken Sie auf **Toolbar** und aktivieren Sie die gewünschte Option.

Anpassbare Symbolleiste – GACS(/en-us/citrix-workspace-app-for-ios/media/toolbar-gacs.png)

Authentifizierung

Verbesserte Citrix®-Sicherheit mit vorausgefülltem Benutzernamen

Ab Version 25.1.0 können Sie Unified Endpoint Management (UEM) verwenden, um den Benutzernamen in einem bestimmten Format an verwaltete Geräte zu übertragen. Unter iOS liest die Citrix Workspace-App diese Konfiguration, ruft den Benutzernamen ab und füllt ihn im Authentifizierungsdialogfeld voraus, wodurch er schreibgeschützt wird. Dies stellt sicher, dass nur der registrierte Gerätebesitzer die App auf diesem spezifischen Gerät authentifizieren und darauf zugreifen kann.

Administratoren erhalten die Möglichkeit, die Benutzerauthentifizierung auf mehreren iOS-Geräten von einem zentralen Standort aus effizient zu verwalten und gleichzeitig sicherzustellen, dass sich nur autorisierte Benutzer anmelden können.

Diese Funktion vereinfacht auch den Anmeldevorgang, indem sie die Notwendigkeit für Benutzer eliminiert, ihre Anmeldeinformationen manuell einzugeben, wodurch das Fehlerrisiko reduziert und die gesamte Benutzererfahrung verbessert wird. Durch die Kombination von robuster Zugriffssteuerung mit einem nahtlosen Anmeldeablauf unterstützt die Citrix Workspace™-App für iOS sowohl verbesserte Sicherheit als auch verbesserte Benutzerfreundlichkeit.

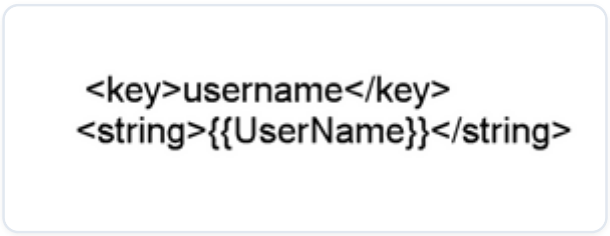
Sie können diese Funktion über UEM mit den folgenden Einstellungen konfigurieren:

> **Hinweis:**
>
> Dieses Beispiel verwendet Microsoft Intune als UEM-Lösung zur Demonstration. Die Schritte und die Benutzeroberfläche können je nach UEM-Anbieter variieren.

1. Melden Sie sich bei Ihrem UEM-Anbieter an.
2. Fügen Sie die Citrix Workspace-App Ihrem UEM-Anbieter zur Verwaltung hinzu. Laden Sie sie über das UEM-Portal hoch oder verknüpfen Sie sie mit dem App Store.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.

4. Fügen Sie ein Schlüssel-Wert-Paar zur XML-Eigenschaftsliste hinzu und füllen Sie die folgenden Werte aus:
    - **Schlüssel:** `username`
    - **Werttyp:** `String`
    - **Wert:** Payload-Variable, die im Microsoft Intune-Portal dokumentiert ist.

Microsoft Intune:



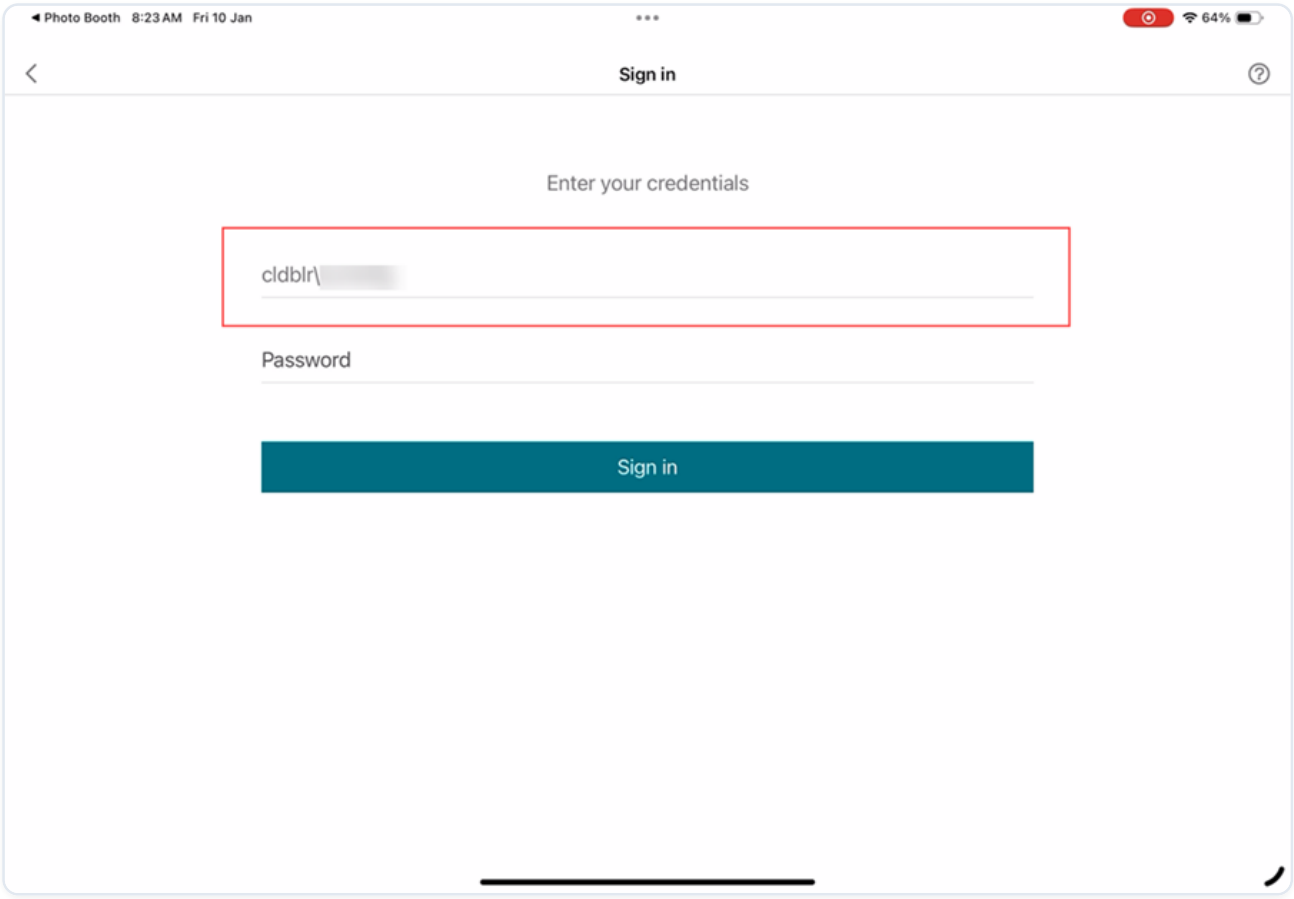
Weitere Informationen finden Sie unter – iOS- und iPadOS-Geräteeinstellungen zur Verwendung gängiger iOS/iPadOS-Funktionen in Intune.

Jamf:

```
<key>username</key>

    <string>$USERNAME</string>
```

Weitere Informationen finden Sie unter – Nutzlastvariablen für Konfigurationsprofile.



Einschränkung:

Das System unterstützt nur die native Anmeldeseite. Für die webbasierte Anmeldung wird das Vorausfüllen des Benutzernamens nicht unterstützt.

Schnelle Smartcard

Ab Version 24.12.0 bietet die Citrix Workspace-App für iOS Smartcard-Verbesserungen für eine verbesserte Authentifizierungsleistung und Benutzerfreundlichkeit. Dieses Update bringt erhebliche Verbesserungen bei der Smartcard-Unterstützung, wodurch die Benutzererfahrung reibungsloser und effizienter wird. Mit der Integration der Unterstützung für gleichzeitige Protokolle und des schnellen Smartcard-Protokolls können Benutzer eine schnellere Authentifizierung und eine nahtlose Nutzung von Smartcard-Lesegeräten erwarten. Die schnelle Smartcard ist mit der CNG-API (Crypto Next Generation) auf dem Windows-Desktop kompatibel.

> **Hinweis:**

> Wenden Sie sich an den Citrix Helpdesk, um diese Funktion zu aktivieren.

> **Einschränkungen:**

- Gleichzeitigkeit wird in der Citrix Workspace-App für iOS nicht vollständig unterstützt.
- Plug & Play wird nicht unterstützt.

Erzwingen des Citrix-Zugriffs über die Citrix Workspace-App

Ab Version 24.12.0 können Administratoren Benutzer auf iOS-Geräten dazu verpflichten, ausschließlich über die native App auf Citrix Workspace zuzugreifen. Wenn diese Funktion aktiviert ist, werden Benutzer, die versuchen, auf die Store-URL und Browser von Drittanbietern zuzugreifen, automatisch zur Citrix Workspace-App umgeleitet. Dadurch wird sichergestellt, dass sie alle Funktionen der nativen App nutzen und eine nahtlose Benutzererfahrung genießen können. Darüber hinaus bietet diese Funktion Administratoren eine bessere Kontrolle über die Benutzerumgebung und erhöht die Sicherheit, indem der Authentifizierungsprozess innerhalb der nativen App verbleibt und das Herunterladen von ICA-Dateien entfällt.

Administratoren können diese Funktion über ihr Citrix Cloud-Konto aktivieren. Diese Funktion wird derzeit nur für Cloud-Stores unterstützt. Weitere Informationen finden Sie unter Endbenutzer zur Authentifizierung und zum Zugriff auf Apps und Desktops über die native App verpflichten.

Aufforderung zur Aktivierung der Biometrie überspringen

Bisher wurden Endbenutzer aufgefordert, zu wählen, ob sie biometrische Daten wie Touch ID oder Face ID zur Authentifizierung in der Citrix Workspace-App verwenden möchten. Ab Version 24.9.0 können Administratoren diese Aufforderung nun überspringen, wodurch der Anmeldevorgang für Benutzer optimiert wird.

Wenn Biometrie aktiviert ist, werden Benutzerkennwörter sicher im Schlüsselbund gespeichert und durch biometrische Authentifizierung geschützt. Nach Ablauf des Authentifizierungstokens werden Benutzer automatisch zur biometrischen Verifizierung aufgefordert. Wenn Biometrie auf dem Gerät nicht konfiguriert ist, müssen Benutzer ihre Anmeldeinformationen manuell eingeben, wenn das Token abläuft.

Diese Funktion wird derzeit nur für lokale Stores unterstützt, die die Lightweight Directory Access Protocol (LDAP)-Authentifizierung verwenden.

Konfiguration

Die folgenden Methoden können verwendet werden, um die biometrische Authentifizierung zu aktivieren:

- Mobile Device Management (MDM)

- Global App Configuration Service (GACS)

Um die biometrische Authentifizierung über MDM zu aktivieren, müssen Administratoren die folgende Einstellung verwenden:

- Schlüssel: `settings_skip_consent_for_biometric_protected_password_saving`
- Wert: `true/false`
- Standardwert: `false`

  – Wenn auf `true` festgelegt, wird die biometrische Wiederanmeldefunktion automatisch für Endbenutzer angewendet, ohne ihnen die Möglichkeit zu geben, sie auszuwählen oder abzulehnen.

  – Wenn auf `false` festgelegt, ist die biometrische Wiederanmeldefunktion optional, und Benutzer können wählen, ob sie diese akzeptieren oder ablehnen möchten.

Um die biometrische Authentifizierung über GACS zu aktivieren, müssen Administratoren die folgenden Schritte ausführen:

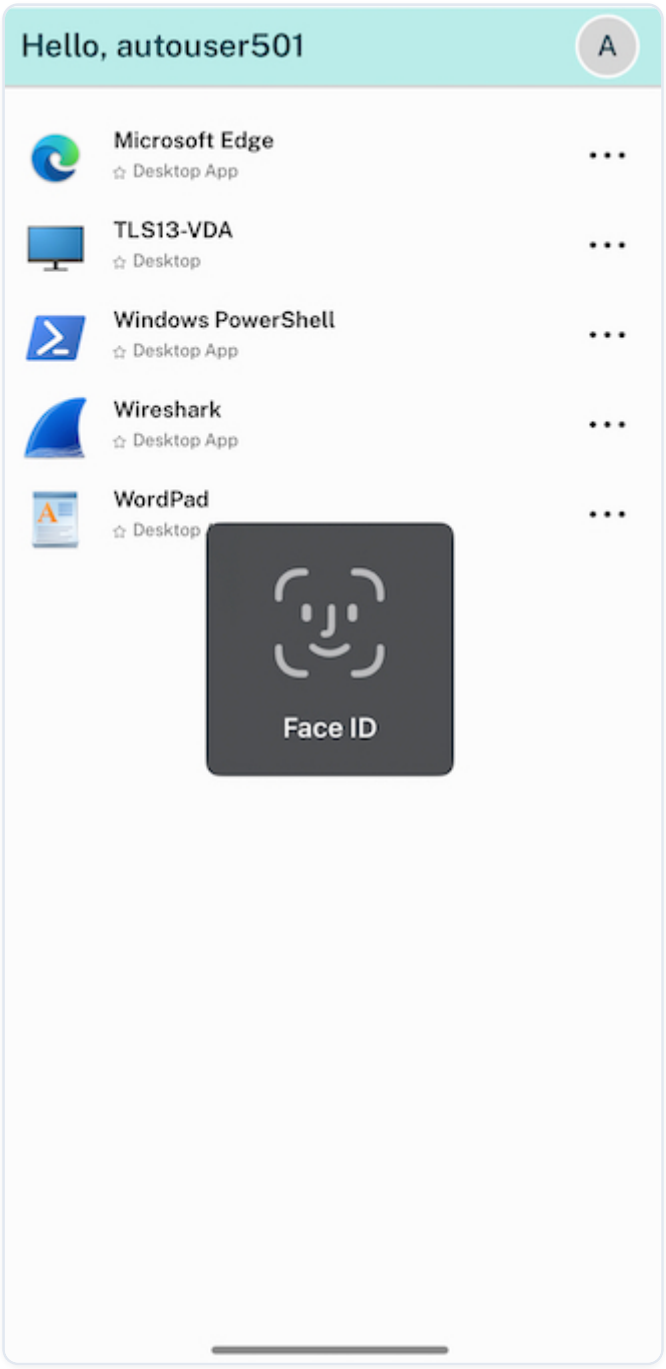
1. Navigieren Sie in Citrix Cloud zu **Workspace-Konfiguration** > **App-Konfiguration** > **Konfigurieren**.
2. Wählen Sie unter **Citrix Workspace-App** die Option **Sicherheit und Authentifizierung**.
3. Aktivieren Sie unter **Authentifizierung** die Option **Aufforderung zur Verwendung von Biometrie überspringen**.

Weitere Informationen finden Sie unter Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen über UEM.

Unterstützung für die Erzwingung der biometrischen Authentifizierung für den Zugriff auf die Citrix Workspace-App

Administratoren können jetzt die biometrische Authentifizierung eines Geräts erzwingen, um für ihre Benutzer auf die Citrix Workspace-App zuzugreifen. Mit dieser Funktion wird beim Öffnen der Citrix Workspace-App nach dem Schließen oder beim Wiederherstellen aus dem minimierten Zustand eine Aufforderung zur Face ID- oder Touch ID-Verifizierung angezeigt, um das Gerät zu entsperren und sich anzumelden. Wenn das Gerät keine biometrische Authentifizierung unterstützt, wird die Kennwort- oder Passcode-Authentifizierungsmethode verwendet, um auf die App zuzugreifen. Wenn der Passcode auf dem Gerät nicht aktiviert ist, wird das Konto abgemeldet,

und der Benutzer muss sich erneut anmelden, um auf die Citrix Workspace-Anwendung zuzugreifen.



Administratoren können diese Funktion mithilfe der Unified Endpoint Management-Lösung mit den folgenden Schlüssel-Wert-Paaren konfigurieren:

- **Schlüssel**: verify_biometric_on_app_foreground_transition
- **Werttyp**: Boolean
- **Wert**: true oder false
    - Wenn auf **true** gesetzt, ist die biometrische Authentifizierung für Endbenutzer erforderlich, um auf die Citrix Workspace-App zuzugreifen.

- Wenn auf **false** gesetzt, wird die biometrische Authentifizierung für den Zugriff auf die Citrix Workspace-App nicht erzwungen. Benutzer haben die Möglichkeit, die biometrische Authentifizierung zu deaktivieren.



Unterstützung der Authentifizierung mit FIDO2 beim Herstellen einer Verbindung zu einem lokalen Store

Ab Version 24.7.0 können Benutzer sich bei der Citrix Workspace-App für iOS mit FIDO2-basierter passwortloser Authentifizierung anmelden, wenn sie eine Verbindung zu einem lokalen Store herstellen. FIDO2 bietet eine nahtlose Authentifizierungsmethode, die es Unternehmensmitarbeitern ermöglicht, auf die Citrix Workspace-App für iOS zuzugreifen, ohne Benutzername oder Passwort eingeben zu müssen. Diese Funktion unterstützt sowohl Roaming- (nur USB) als auch Plattform-Authentifikatoren (nur PIN-Code, Touch ID und Face ID).

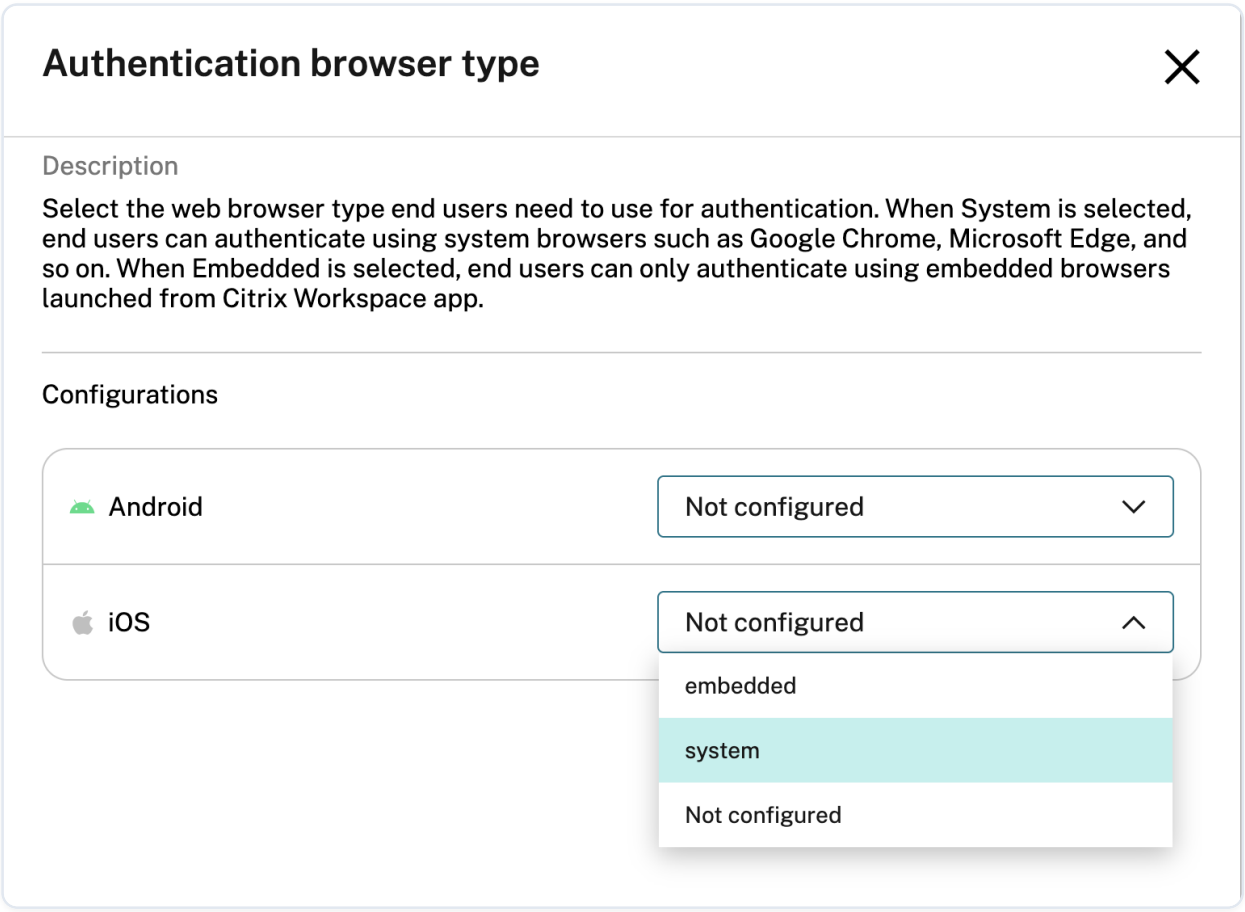
Sie können diese Funktion über den Global App Configuration Service und Unified Endpoint Management konfigurieren.

> **Hinweis:**
>
> Diese Funktion wird nur im Systembrowser unterstützt.

Verwenden des Global App Configuration Service

Führen Sie die folgenden Schritte aus, um die Konfiguration mit dem Global App Configuration Service vorzunehmen:

1. Melden Sie sich mit Ihren Anmeldeinformationen bei Citrix Cloud an.
2. Navigieren Sie zu **Workspace Configuration** > **App configuration**.
3. Wählen Sie auf der Seite **App configuration** den Store aus und tippen Sie dann auf **Configure**.
4. Navigieren Sie auf der Seite **Workspace URL** zu **Security and Authentication** > **Authentication**.
5. Wählen Sie unter **Authentication browser type** die Option **iOS** und dann **system** aus dem Dropdown-Menü aus.



6. Tippen Sie auf **Publish Drafts**, um die Einstellungen für den ausgewählten Store zu veröffentlichen.

Weitere Informationen zum Global App Configuration Service finden Sie unter Configure settings for on-premises stores in der Dokumentation zum Global App Configuration Service.

Verwenden der Lösungen für das Unified Endpoint Management

Führen Sie die folgenden Schritte aus, um die Konfiguration mit Unified Endpoint Management vorzunehmen:

1. Melden Sie sich bei Ihrem Unified Endpoint Management (UEM)-Anbieter an.
2. Fügen Sie die Citrix Workspace-App hinzu, die Sie von Ihrem UEM-Anbieter verwalten lassen möchten. Sie können die App über das Portal Ihres UEM-Anbieters hochladen, um die Verwaltung durch Ihren UEM-Anbieter zu ermöglichen. Alternativ können Sie die App im App Store verknüpfen.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.
4. Fügen Sie das Schlüssel-Wert-Paar zur XML-Eigenschaftsliste hinzu und geben Sie die folgenden Werte ein:

```
<dict>

                    <key>category</key>

                    <string>authentication</string>

                    <key>userOverride</key>

                    <false/>

                    <key>settings</key>

                    <array>

                        <dict>

                            <key>name</key>

                            <string>settings_auth_web_browser</string>

                            <key>value</key>

                            <string>system</string>

                        </dict>

                    </array>

  </dict>
```

Weitere Informationen finden Sie unter Configure Workspace app using Unified Endpoint Management solutions.

Clientzertifikat-Authentifizierung

Wichtig:

- Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App:

    - Citrix Access Gateway Enterprise Edition Version 9.3
    - NetScaler Gateway Version 10.x bis Version 11.0
    - Citrix Gateway Version 11.1 und höher

- Die Citrix Workspace-App für iOS unterstützt die Clientzertifikatsauthentifizierung.
- Nur Access Gateway Enterprise Edition 9.x und 10.x (und spätere Versionen) unterstützen die Clientzertifikatsauthentifizierung.
- Authentifizierungstypen mit doppelter Quelle müssen CERT und LDAP sein.
- Die Citrix Workspace-App unterstützt auch die optionale Clientzertifikatsauthentifizierung.
- Es werden nur P12-formatierte Zertifikate unterstützt.

Benutzer, die sich bei einem virtuellen Citrix Gateway-Server anmelden, können auch basierend auf den Attributen des Clientzertifikats authentifiziert werden, das dem virtuellen Server präsentiert wird. Die Clientzertifikatsauthentifizierung kann auch mit einem anderen Authentifizierungstyp, LDAP, verwendet werden, um eine Double-Source-Authentifizierung bereitzustellen.

Administratoren können Endbenutzer basierend auf den Clientzertifikatattributen wie folgt authentifizieren:

- Die Clientauthentifizierung ist auf dem virtuellen Server aktiviert.
- Der virtuelle Server fordert ein Clientzertifikat an.
- Ein Stammzertifikat an den virtuellen Server auf Citrix Gateway binden.

Wenn sich Benutzer beim virtuellen Citrix Gateway-Server anmelden, können sie nach der Authentifizierung den Benutzernamen und die Domäneninformationen aus dem Feld **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** im Zertifikat extrahieren. Dies hat das Format `username@domain`.

Die Authentifizierung ist abgeschlossen, wenn der Benutzer den Benutzernamen und die Domäne extrahiert und die erforderlichen Informationen (z. B. das Kennwort) bereitstellt. Wenn der Benutzer kein gültiges Zertifikat und keine gültigen Anmeldeinformationen bereitstellt oder wenn die Extraktion von Benutzername/Domäne fehlschlägt, schlägt die Authentifizierung fehl.

Sie können Benutzer basierend auf dem Clientzertifikat authentifizieren, indem Sie den Standardauthentifizierungstyp auf die Verwendung des Clientzertifikats festlegen. Sie können auch

eine Zertifikataktion erstellen, die definiert, was während der Authentifizierung basierend auf einem Client-SSL-Zertifikat zu tun ist.

So konfigurieren Sie die XenApp®-Farm

Erstellen Sie eine XenApp-Farm für mobile Geräte in der Citrix Virtual Apps™-Konsole oder der Web Interface-Konsole. Die Konsole hängt von der Version von Citrix Virtual Apps ab, die Sie installiert haben.

Die Citrix Workspace-App verwendet eine XenApp-Farm, um Informationen über die Anwendungen abzurufen, auf die ein Benutzer Zugriffsrechte hat. Dieselben Informationen werden an die auf dem Gerät ausgeführten Apps weitergegeben. Diese Methode ähnelt der Art und Weise, wie Sie das Webinterface für herkömmliche SSL-basierte Citrix Virtual Apps-Verbindungen verwenden, bei denen Sie das Citrix Gateway konfigurieren können.

Konfigurieren Sie die XenApp-Farm für die Citrix Workspace-App für mobile Geräte, um Verbindungen vom Citrix Gateway wie folgt zu unterstützen:

1. Wählen Sie in der XenApp-Farm **Sicheren Clientzugriff verwalten** > **Einstellungen für sicheren Clientzugriff bearbeiten**.
2. Ändern Sie die Zugriffsmethode in Gateway Direct.
3. Geben Sie den FQDN des Citrix Gateway-Geräts ein.
4. Geben Sie die Informationen zur Secure Ticket Authority (STA) ein.

So konfigurieren Sie das Citrix Gateway-Gerät

Für die Clientzertifikatsauthentifizierung konfigurieren Sie Citrix Gateway mit Zwei-Faktor-Authentifizierung mithilfe der Authentifizierungsrichtlinien Cert und LDAP. So konfigurieren Sie das Citrix Gateway-Gerät:

1. Erstellen Sie eine Sitzungsrichtlinie auf Citrix Gateway, um eingehende Citrix Virtual Apps-Verbindungen von der Citrix Workspace-App zuzulassen. Geben Sie den Speicherort Ihrer neu erstellten XenApp-Farm an.

    - Erstellen Sie eine Sitzungsrichtlinie, um zu identifizieren, dass die Verbindung von der Citrix Workspace-App stammt. Wenn Sie die Sitzungsrichtlinie erstellen, konfigurieren Sie den folgenden Ausdruck und wählen Sie „Alle Ausdrücke abgleichen“ als Operator für den Ausdruck aus:

      ```
      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
      ```

- Legen Sie in der zugehörigen Profilkonfiguration für die Sitzungsrichtlinie auf der Registerkarte **Sicherheit** die **Standardautorisierung** auf **Zulassen** fest.

  Überprüfen Sie auf der Registerkarte **Veröffentlichte Anwendungen**, ob die Einstellung kein globales Setting ist (Sie haben das Kontrollkästchen „Global überschreiben“ aktiviert), ob das Feld **ICA® Proxy** auf **EIN** gesetzt ist.

  Geben Sie im Feld **Adresse** des Webinterfaces die URL einschließlich der config.xml für die XenApp-Farm ein, die die Gerätebenutzer verwenden, zum Beispiel:

  - /XenAppServerName/Citrix/PNAgent/config.xml oder
  - /XenAppServerName/CustomPath/config.xml.

- Binden Sie die Sitzungsrichtlinie an einen virtuellen Server.
- Erstellen Sie Authentifizierungsrichtlinien für Zertifikat und LDAP.
- Binden Sie die Authentifizierungsrichtlinien an den virtuellen Server.
- Konfigurieren Sie den virtuellen Server so, dass er Clientzertifikate im TLS-Handshake anfordert. Navigieren Sie dazu zu **Zertifikat** > **SSL-Parameter öffnen** > **Clientauthentifizierung** > setzen Sie **Clientzertifikat** auf **Obligatorisch**.

> **Wichtig:**
>
> - Wenn das auf dem Citrix Gateway verwendete Serverzertifikat Teil einer Zertifikatskette ist. Wenn es sich beispielsweise um ein Zwischenzertifikat handelt, installieren Sie die Zertifikate auf dem Citrix Gateway. Informationen zur Installation von Zertifikaten finden Sie in der Citrix Gateway-Dokumentation.
> - Der Benutzer muss das Zertifikat manuell importieren, wenn das Clientzertifikat vor der Authentifizierung als obligatorisch festgelegt ist.

So konfigurieren Sie das Mobilgerät

Wenn die Clientzertifikatsauthentifizierung auf Citrix Gateway aktiviert ist, werden Benutzer basierend auf bestimmten Attributen des Clientzertifikats authentifiziert. Nach der Authentifizierung können Sie den Benutzernamen und die Domäne aus dem Zertifikat extrahieren. Sie können für jeden Benutzer spezifische Richtlinien anwenden.

1. Öffnen Sie in der Citrix Workspace-App das **Konto**, und geben Sie im Feld „Server“ den passenden FQDN Ihres Citrix Gateway-Servers ein. Zum Beispiel GatewayClientCertificateServer.organization.com. Die Citrix Workspace-App erkennt automatisch, dass das Clientzertifikat erforderlich ist.
2. Benutzer können entweder ein neues Zertifikat installieren oder eines aus der Liste der bereits installierten Zertifikate auswählen. Laden Sie für die iOS-Clientzertifikatsauthentifizierung das Zertifikat ausschließlich über die Citrix Workspace-App herunter und installieren Sie es.
3. Nachdem Sie ein gültiges Zertifikat ausgewählt haben, werden die Felder für Benutzername und Domäne auf dem Anmeldebildschirm mit dem Benutzernamen aus dem Zertifikat vorausgefüllt. Ein Endbenutzer kann weitere Details, einschließlich des Kennworts, eingeben.
4. Wenn die Clientzertifikatsauthentifizierung auf optional gesetzt ist, können Benutzer die Zertifikatsauswahl überspringen, indem sie auf der Zertifikatsseite auf „Zurück“ drücken. In diesem Fall fährt die Citrix Workspace-App mit der Verbindung fort und zeigt dem Benutzer den Anmeldebildschirm an.
5. Nachdem Benutzer die erste Anmeldung abgeschlossen haben, können sie Anwendungen starten, ohne das Zertifikat erneut bereitzustellen. Die Citrix Workspace-App speichert das Zertifikat für das Konto und verwendet es automatisch für zukünftige Anmeldeanfragen.

Unterstützung zum Wechseln des Webbrowsers für die Authentifizierung

Ab Version 23.2.0 können Administratoren den für den Authentifizierungsprozess verwendeten Browser von einem eingebetteten Browser auf einen Systembrowser auf iOS- oder iPad-Geräten umstellen, wenn eine erweiterte Authentifizierungsrichtlinie auf der lokalen Citrix Gateway- und StoreFront-Bereitstellung konfiguriert ist.

Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren

Administratoren können den für den Authentifizierungsprozess verwendeten Browser vom eingebetteten Browser zum Systembrowser wechseln. Dies ist nur möglich, wenn eine erweiterte Authentifizierungsrichtlinie auf der lokalen Citrix Gateway- und StoreFront-Bereitstellung konfiguriert ist. Um eine erweiterte Authentifizierungsrichtlinie zu konfigurieren, konfigurieren Sie die NetScaler Rewrite-Richtlinie über die NetScaler-Befehlszeile:

1. `enable ns feature REWRITE`
2. `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
3. `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ(\"/cgi/authenticate\")" insert_auth_browser_type_hdr_act`

4. `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_pol -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Der Wechsel zum Systembrowser bietet weitere Funktionen, wie zum Beispiel:

- Bessere Erfahrung mit zertifikatbasierter Authentifizierung.
- Möglichkeit, ein vorhandenes Benutzerzertifikat aus dem Geräteschlüsselspeicher während des Authentifizierungsprozesses zu verwenden.
- Unterstützung für einige Authentifikatoren von Drittanbietern wie SITHS eID.

Der eingebettete Browser wird als Standardbrowser für die Authentifizierung verwendet, wenn der Administrator die oben genannte Rewrite-Richtlinie nicht konfiguriert hat.

Diese Tabelle listet die Browser auf, die für die Authentifizierung basierend auf der Konfiguration auf dem NetScaler® Gateway und dem Global App Config Service verwendet werden:

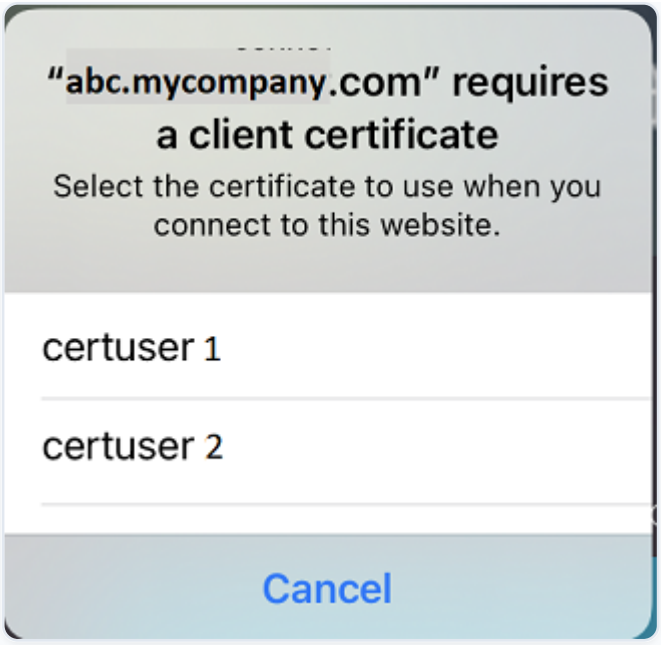
NETSCALER GATEWAY	GLOBAL APP CONFIGURATION SERVICE	FÜR DIE AUTHENTIFIZIERUNG VERWENDETER BROWSER
System	System	System
System	Eingebettet	System
Eingebettet	System	System
Eingebettet	Eingebettet	Eingebettet
Keine Konfiguration	System	System
Keine Konfiguration	Eingebettet	Eingebettet

Unterstützung der zertifikatbasierten Authentifizierung für lokale Stores

Endbenutzer können jetzt die zertifikatbasierte Authentifizierung verwenden, bei der die Zertifikate im Geräteschlüsselbund gespeichert werden. Beim Anmelden erkennt die Citrix Workspace-App die Liste der Zertifikate auf Ihrem Gerät, und Sie können ein Zertifikat zur Authentifizierung auswählen.

> **Wichtig:**

Nachdem Sie das Zertifikat ausgewählt haben, bleibt die Auswahl für den nächsten Start der Citrix Workspace-App bestehen. Um ein anderes Zertifikat auszuwählen, können Sie „Safari zurücksetzen“ in den iOS-Geräteeinstellungen wählen oder die Citrix Workspace-App neu installieren.



Hinweis:

Diese Funktion unterstützt lokale Bereitstellungen.

So konfigurieren Sie:

1. Navigieren Sie zur URL Global App Configuration Store Settings API und geben Sie die Cloud Store-URL ein. Zum Beispiel, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigieren Sie zu **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > klicken Sie auf **POST**.
3. Klicken Sie auf **INVOKE API**.
4. Geben Sie die Payload-Details ein und laden Sie sie hoch. Wählen Sie einen der folgenden Werte aus:
    - "Embedded": Sie können WKWebView verwenden. Diese Option ist standardmäßig festgelegt.

- "system": Sie können den Safari View Controller verwenden.

Zum Beispiel:

```
"category": "Authentication",

"userOverride": false,

"settings": [

{ "name": "Web Browser to use for Authentication", "value":
"*Embedded*/*System*" },
```

Auf iOS- oder iPad-Geräten können Administratoren den Browser wechseln, der für den Authentifizierungsprozess verwendet wird. Sie können vom eingebetteten Browser zum Systembrowser wechseln, wenn eine erweiterte Authentifizierungsrichtlinie auf dem lokalen Citrix Gateway und der StoreFront-Bereitstellung konfiguriert ist. Weitere Informationen finden Sie unter Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren.

5. Klicken Sie auf **EXECUTE**, um den Dienst zu übertragen.

Smartcards

Die Citrix Workspace-App unterstützt SITHS-Smartcards nur für In-Session-Verbindungen.

Wenn Sie FIPS Citrix Gateway-Geräte verwenden, konfigurieren Sie Ihre Systeme so, dass SSL-Neuverhandlungen abgelehnt werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123680.

Die folgenden Produkte und Konfigurationen werden unterstützt:

- Unterstützte Lesegeräte:
  - Precise Biometrics Tactivo für iPad Mini Firmware-Version 3.8.0
  - Precise Biometrics Tactivo für iPad (vierte Generation) und Tactivo für iPad (dritte Generation) und iPad 2 Firmware-Version 3.8.0
  - BaiMobile® 301MP und 301MP-L Smartcard-Lesegeräte
  - Thursby PKard USB-Lesegerät
  - Feitian iR301 USB-Lesegerät
  - Type-C CCID-kompatible Lesegeräte

    - Twocanoes Smartcard-Dienstprogramm-Lesegerät
- Unterstützte VDA Smartcard-Middleware
    - ActiveIdentity
- Unterstützte Smartcards:
    - PIV-Karten
    - Common Access Card (CAC)
- Unterstützte Konfigurationen:
    - Smartcard-Authentifizierung bei Citrix Gateway mit StoreFront 2.x und XenDesktop 7.x oder höher oder XenApp 6.5 oder höher

So konfigurieren Sie die Citrix Workspace-App für den Zugriff auf Apps

1. Wenn Sie die Citrix Workspace-App automatisch für den Zugriff auf Apps konfigurieren möchten, wenn Sie ein Konto erstellen, geben Sie im Feld „Adresse“ die entsprechende URL Ihres Stores ein. Beispiel:
    - StoreFront.organization.com
    - netscalervserver.organization.com
2. Wählen Sie die Option **Smartcard verwenden**, wenn Sie eine Smartcard zur Authentifizierung verwenden.

> **Hinweis:**

> Anmeldungen beim Store sind etwa eine Stunde lang gültig. Danach müssen sich Benutzer erneut anmelden, um andere Anwendungen zu aktualisieren oder zu starten.

Unterstützung für generische Lesegeräte auf Typ-C-Basis

Ab Version 23.12.0 unterstützt die Citrix Workspace-App für iOS nun Typ-C-CCID-kompatible Lesegeräte für die Smartcard-Authentifizierung. Zuvor wurden nur Lesegeräte mit Lightning-Anschluss unterstützt. Die Integration von Typ-C-Smartcard-Lesegeräten in die Citrix Workspace-App bietet zwei Vorteile: Benutzer können sich über die Citrix Workspace-App authentifizieren und die Smartcard nahtlos in ihren virtuellen Desktopsitzungen verwenden.

Unterstützung für das Twocanoes Smartcard-Dienstprogramm-Lesegerät

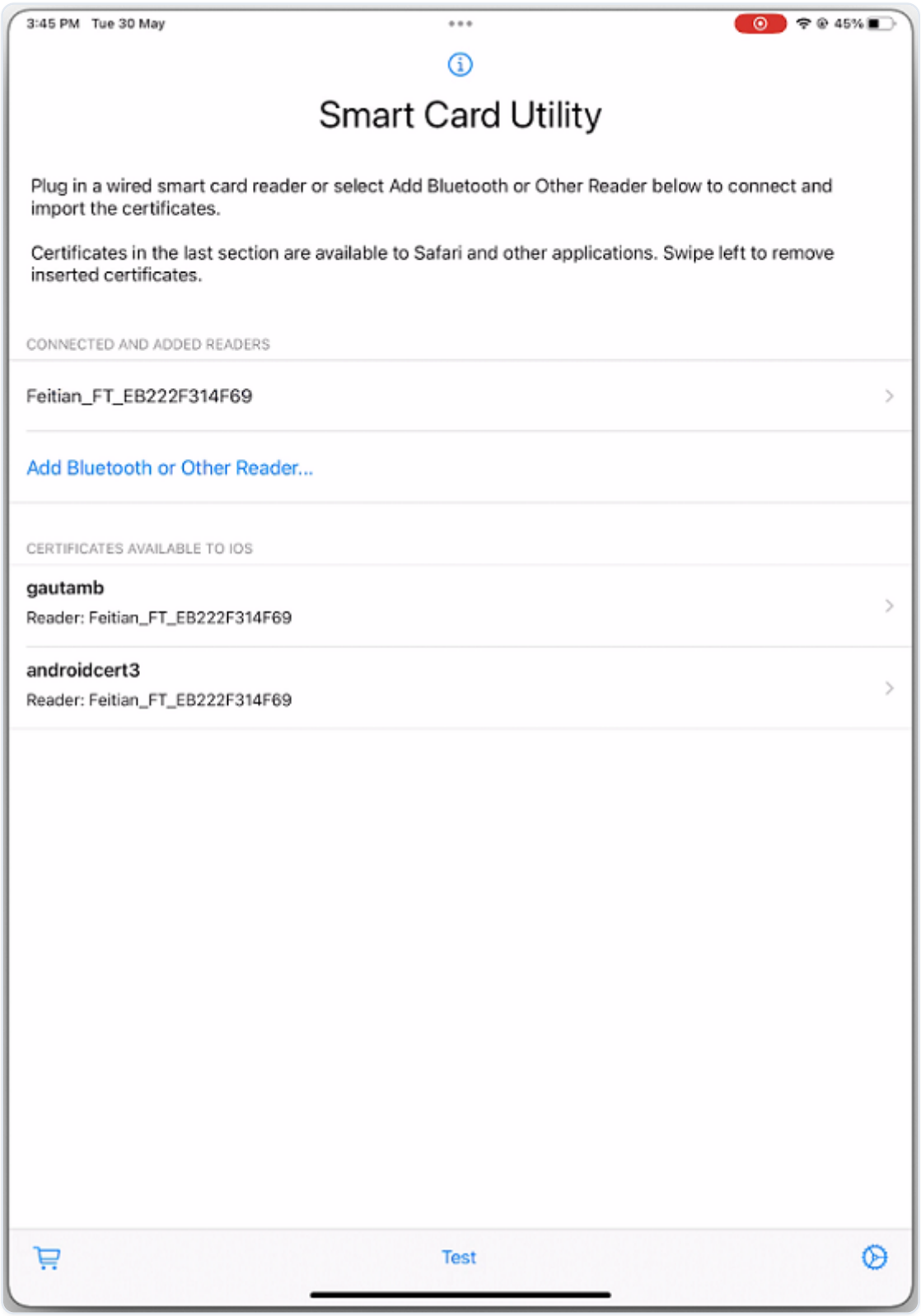
Ab Version 24.3.5 unterstützt die Citrix Workspace-App für iOS die Twocanoes Smartcard-Dienstprogramm-Lesegeräte. Weitere Informationen zu unterstützten Smartcard-Lesegeräten finden Sie unter Smartcards.

Hinweis:

Der Twocanoes Smartcard-Dienstprogramm USB-C-Leser wird sowohl für die Anmeldung bei der Citrix Workspace-App als auch für die Anmeldung bei virtuellen Sitzungen unterstützt. Der Twocanoes Smartcard-Dienstprogramm Bluetooth-Leser wird jedoch nur für die Anmeldung bei der Citrix Workspace-App und nicht für die Anmeldung bei virtuellen Sitzungen unterstützt.

Um den Twocanoes Smartcard-Dienstprogramm Bluetooth-Leser zu konfigurieren, führen Sie die folgenden Schritte aus:

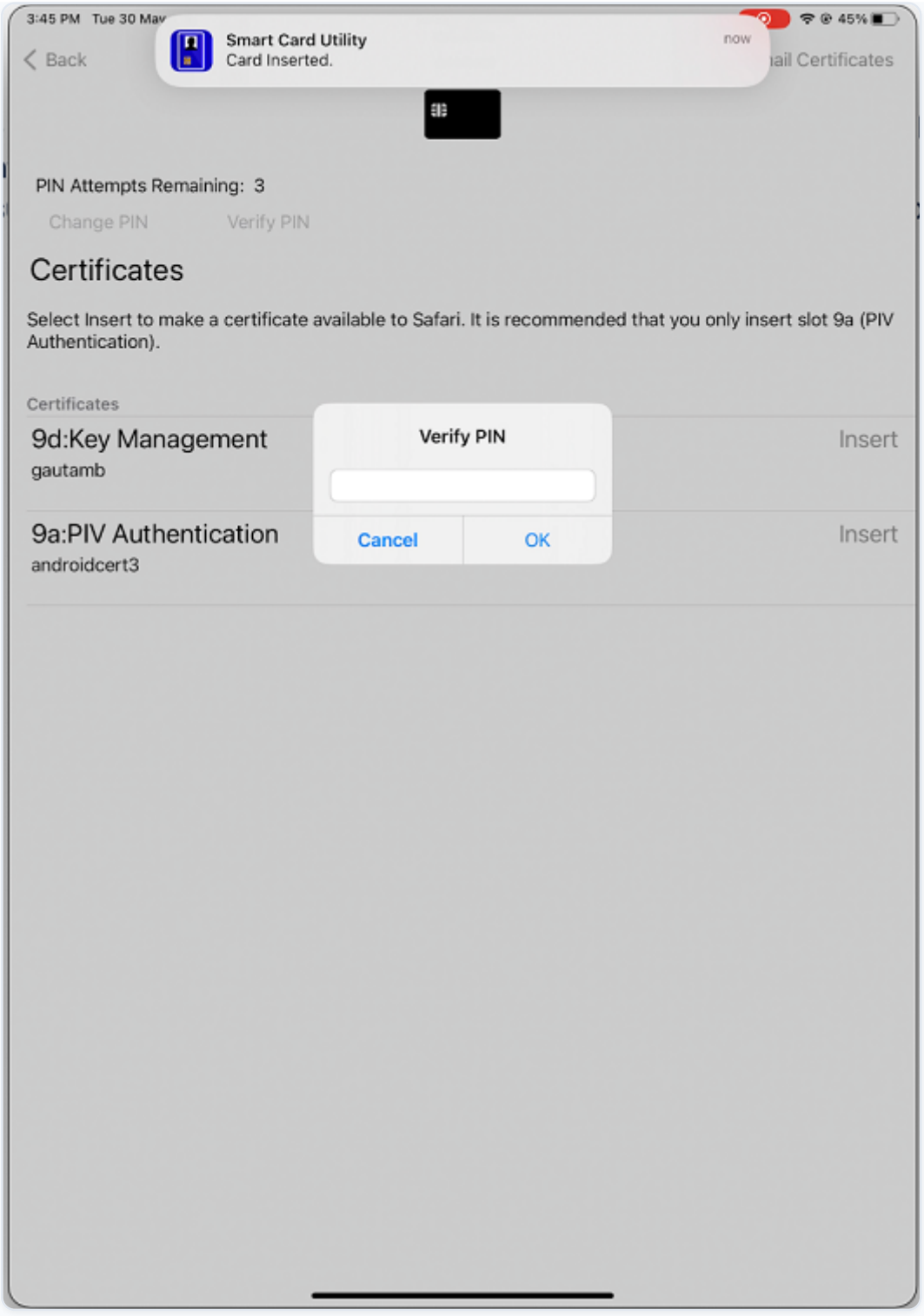
1. Laden Sie die Smart Card Utility-App aus dem App Store herunter und installieren Sie sie. Weitere Informationen finden Sie unter Smart Card Utility Bluetooth Reader Quick Start in der Twocanoes-Wissensdatenbank.
2. Stellen Sie sicher, dass Bluetooth auf Ihrem Gerät aktiviert ist und die Smartcard in den Leser eingelegt ist.
3. Öffnen Sie die Smart Card Utility-App.



4. Wenn Sie den Bluetooth-Leser verwenden, tippen Sie auf **Bluetooth oder anderen Leser hinzufügen…** und wählen Sie Ihren Leser zum Verbinden aus.

> **Hinweis:**

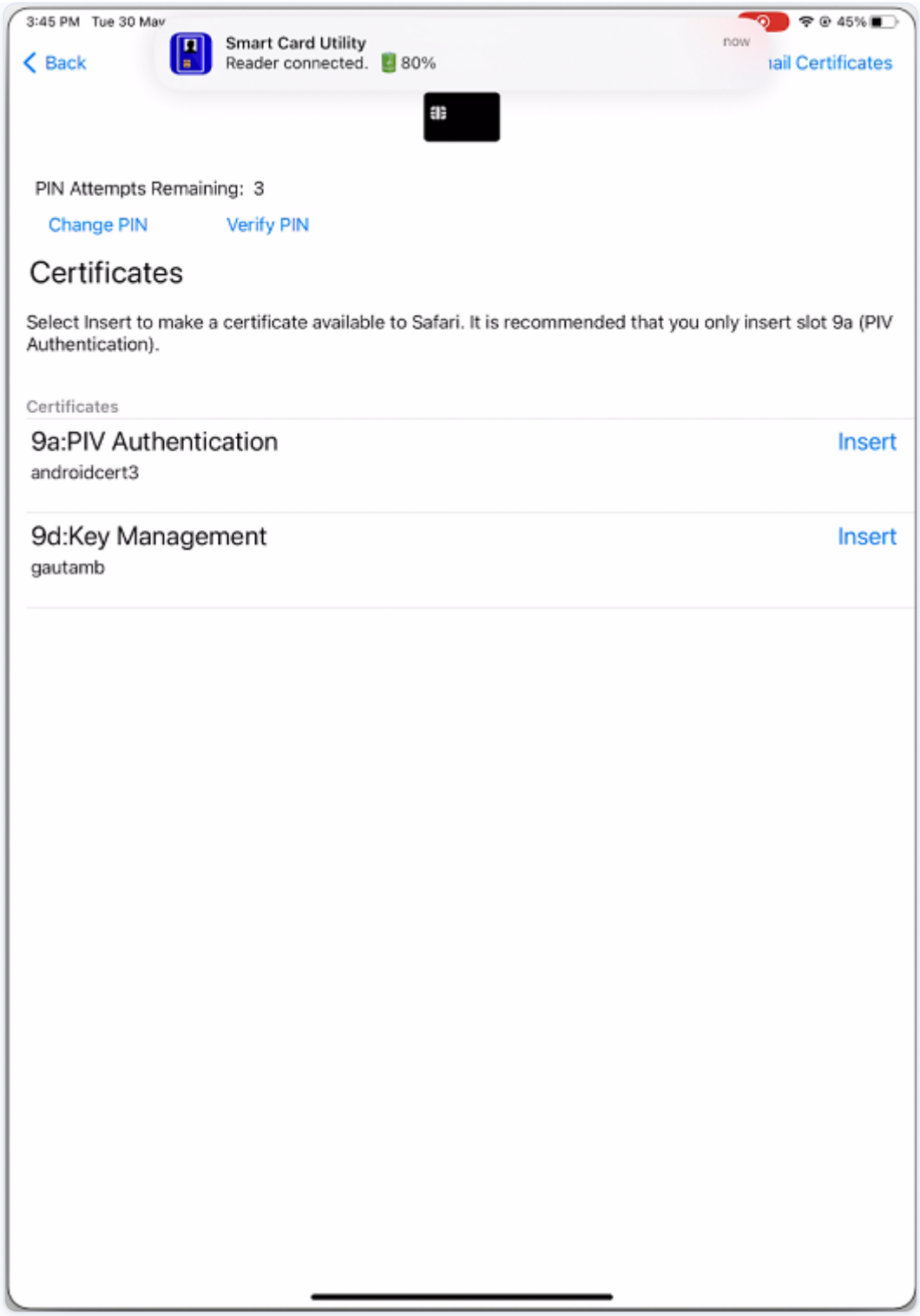
Wenn der Leser mit PIN-Kopplung aktiviert ist, müssen Sie die **PIN** eingeben, wenn Sie dazu aufgefordert werden. Die **PIN** befindet sich auf der Rückseite des Lesers.



5. Tippen Sie auf **Einfügen** bei dem erforderlichen Zertifikat, um es in die Schlüsselbundschnittstelle zu kopieren.

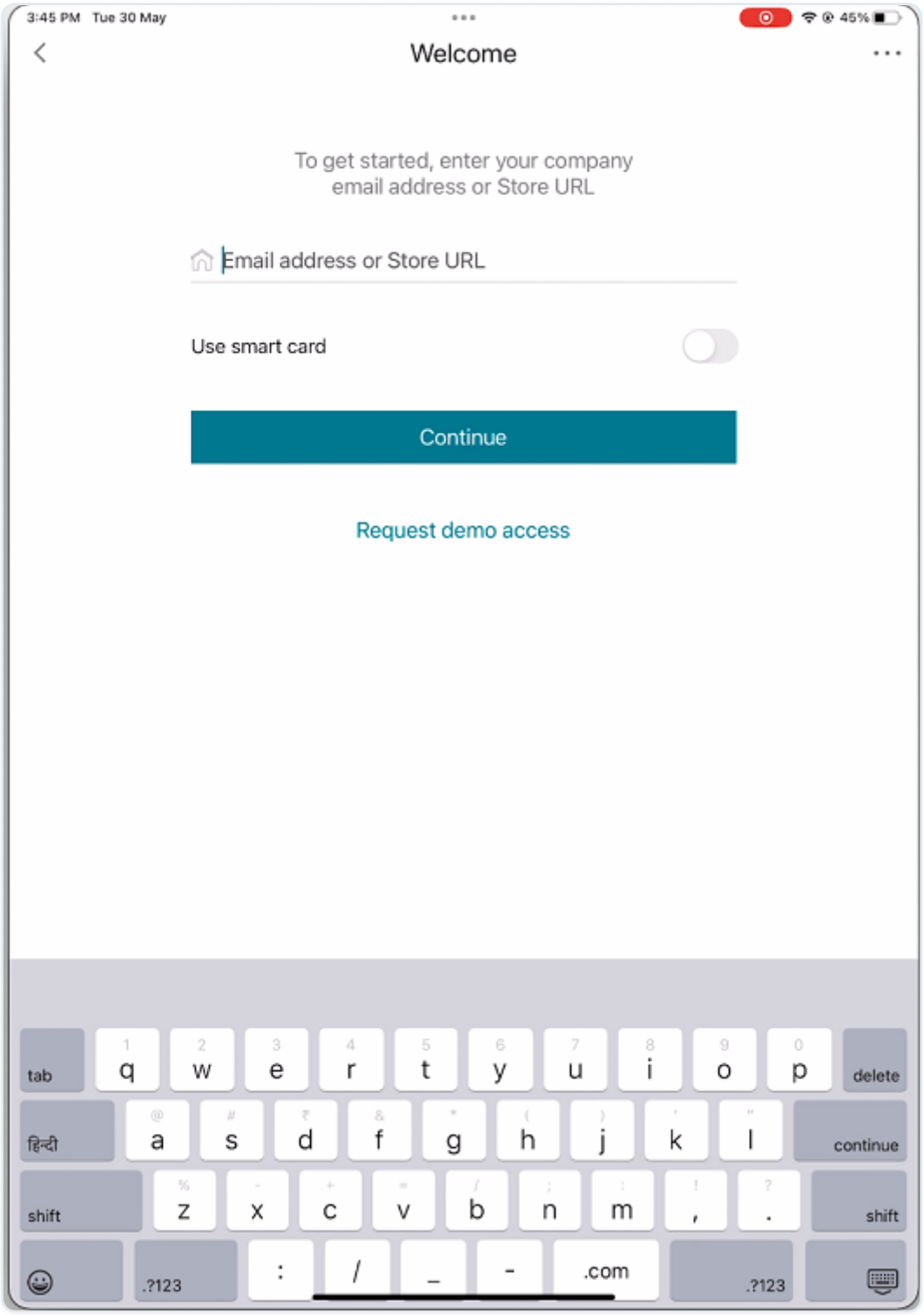
Hinweis:

Die Smart Card Utility-App hat eine von Apple bereitgestellte Cryptokit-Erweiterung implementiert, um Zertifikate in Form von Token in die Schlüsselbundschnittstelle zu schreiben. Weitere Informationen finden Sie unter Smartcard-Authentifizierung konfigurieren in der Apple-Entwicklerdokumentation.

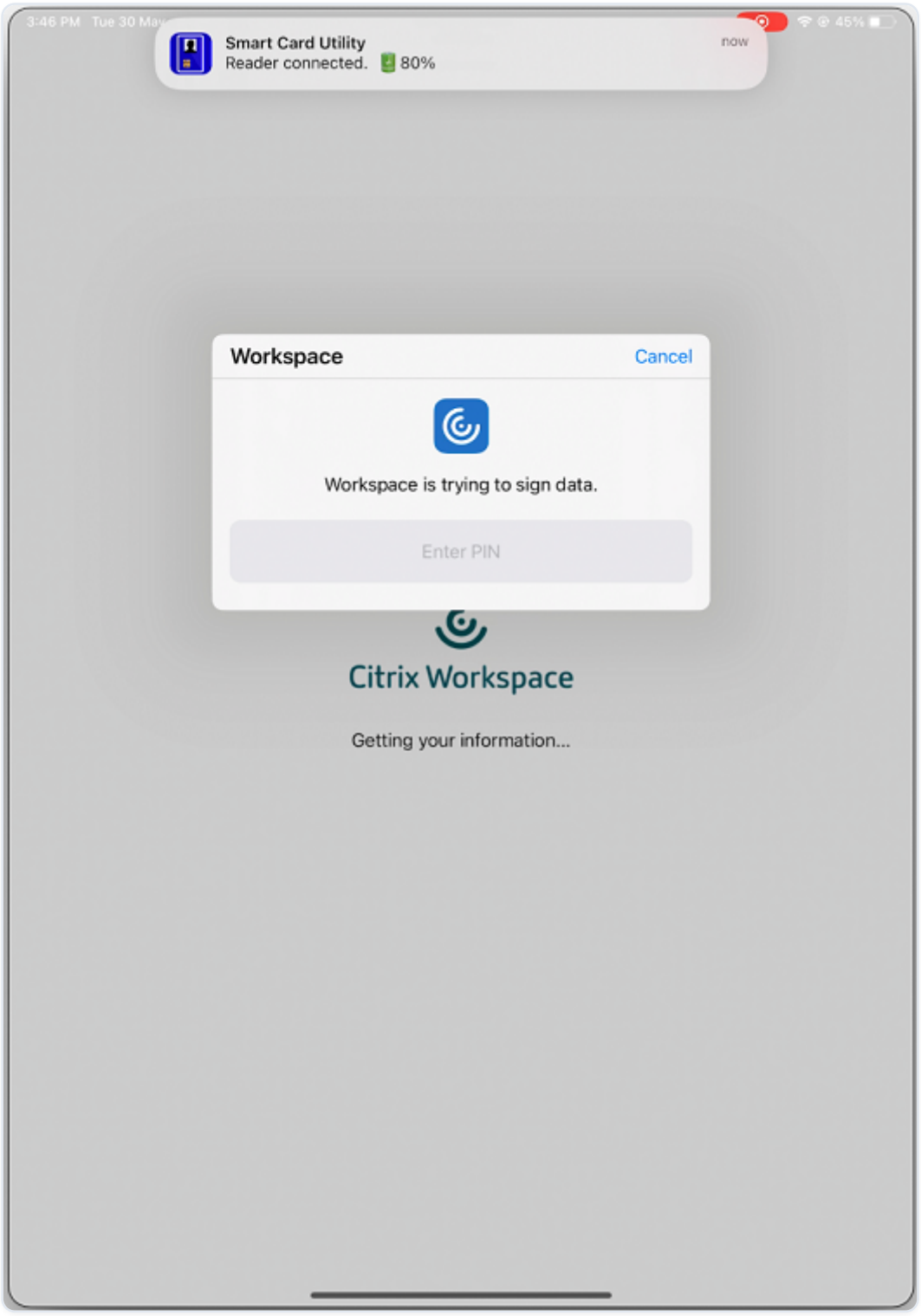


6. Stellen Sie sicher, dass der Leser mit dem Gerät verbunden bleibt.

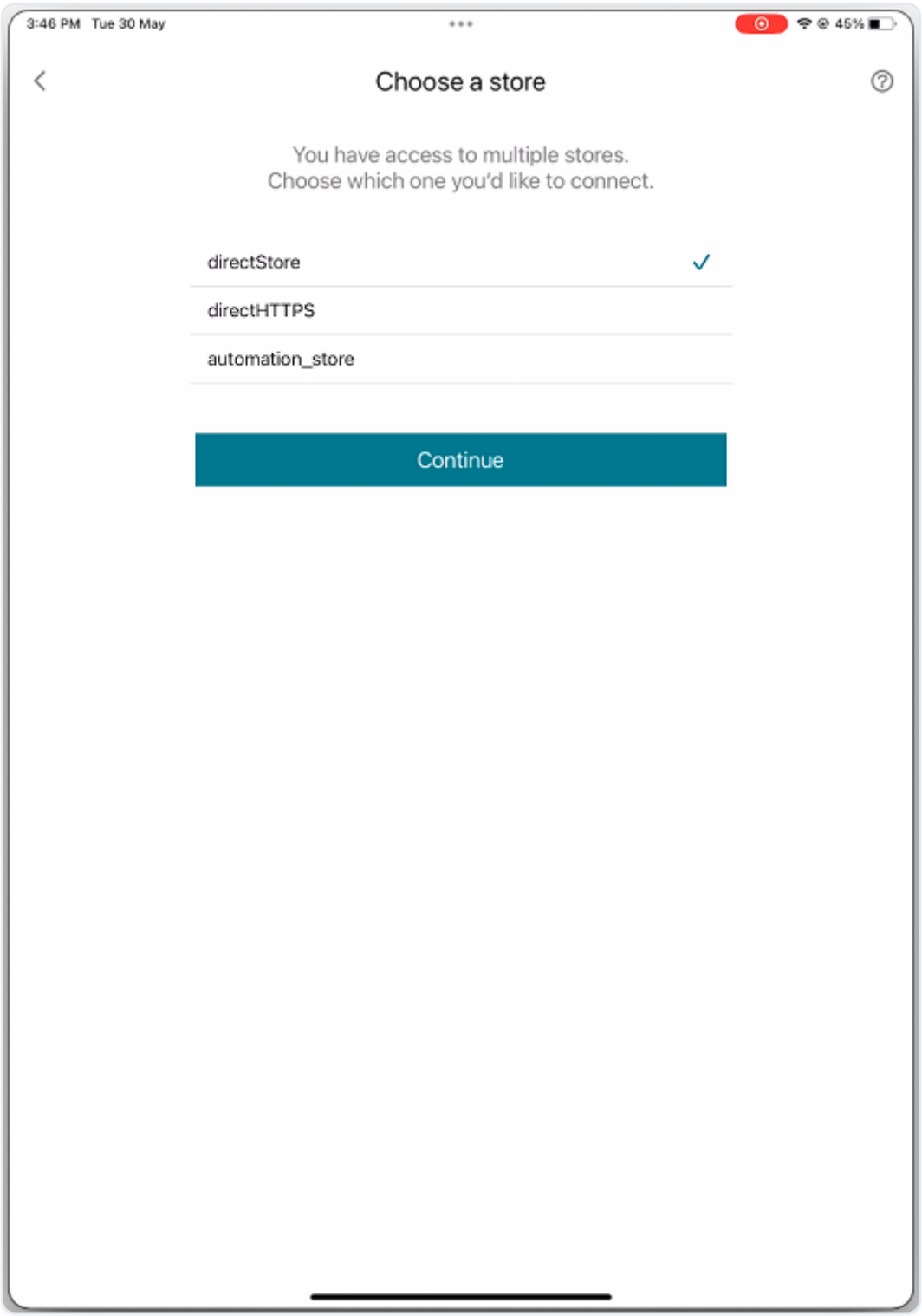
7. Öffnen Sie die Citrix Workspace-App und geben Sie die Store-URL ein, die mit Smartcard-Authentifizierung konfiguriert ist.



8. Wählen Sie auf dem Zertifikatsbildschirm das erforderliche Zertifikat aus und geben Sie die von Ihrem IT-Administrator bereitgestellte Smartcard-PIN ein, um sich anzumelden.



9. Wenn Sie Zugriff auf mehrere Stores haben, wählen Sie den gewünschten Store aus und tippen Sie auf **Weiter**.



10. Nach erfolgreicher Authentifizierung sind Sie bei der Citrix Workspace-App angemeldet.

YubiKey-Unterstützung für Smartcard-Authentifizierung

Ab Version 23.12.0 können Sie die Smartcard-Authentifizierung jetzt mit YubiKey durchführen. Diese Funktion bietet ein Authentifizierungserlebnis mit einem einzigen Gerät für die Citrix Workspace-App sowie für die virtuellen Sitzungen und veröffentlichten Apps in der VDA-Sitzung. Sie macht das Anschließen von Smartcard-Lesegeräten oder anderen externen Authentifikatoren

überflüssig. Sie vereinfacht die Endbenutzererfahrung, da YubiKey eine Vielzahl von Protokollen wie OTP, FIDO und so weiter unterstützt.

Um sich bei der Citrix Workspace-App anzumelden, müssen Endbenutzer den YubiKey in ihr iPhone oder iPad einstecken, den Smartcard-Schalter aktivieren und ihre Store-URL angeben.

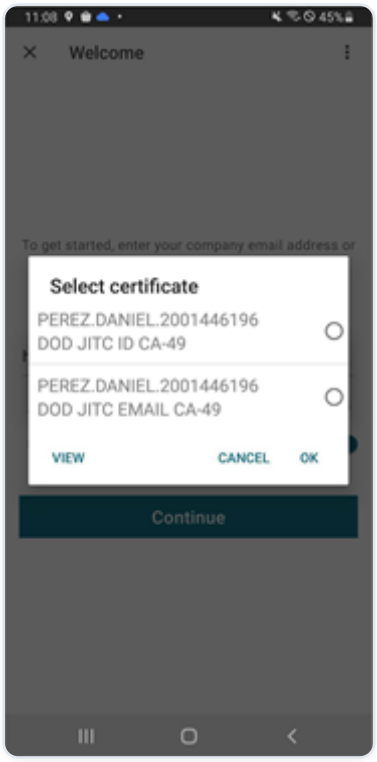
Hinweis:

Diese Funktion unterstützt nur die direkte Verbindung zur Citrix Workspace-App bei StoreFront-Bereitstellungen und nicht über Citrix Gateway. Die YubiKey-Unterstützung für die Smartcard-Authentifizierung über Citrix Gateway wird in einer zukünftigen Version verfügbar sein. Die Citrix Workspace-App für iOS unterstützt nur die YubiKey 5-Serie. Weitere Informationen zu YubiKey finden Sie unter YubiKey 5-Serie.

Unterstützung für mehrere Zertifikate bei der Smartcard-Authentifizierung

Bisher zeigte die Citrix Workspace-App für iOS das Zertifikat an, das im ersten Steckplatz der verbundenen Smartcard verfügbar war.

Ab Version 24.1.0 zeigt die Citrix Workspace-App für iOS alle auf der Smartcard verfügbaren Zertifikate an. Diese Funktion ermöglicht es Ihnen, das erforderliche Zertifikat während der Authentifizierung über die Smartcard-Authentifizierung auszuwählen.



Alle auf der Smartcard verfügbaren Zertifikate anzeigen

Ab Version 23.7.5 zeigt die Citrix Workspace-App für iOS nun mehrere auf der Smartcard verfügbare Zertifikate an und ermöglicht Ihnen die Auswahl des Zertifikats für die Smartcard-basierte Authentifizierung. Das erforderliche Zertifikat kann auf der Seite **Zertifikat auswählen** ausgewählt werden, sobald der Smartcard-Schalter aktiviert wurde.



RSA SecurID-Authentifizierung

Die Citrix Workspace-App unterstützt die RSA SecurID-Authentifizierung für Secure Web Gateway-Konfigurationen. Die Konfigurationen erfolgen über die Webinterface und für alle Citrix Gateway-Konfigurationen.

URL-Schema für den Softwaretoken in der Citrix Workspace-App für iOS erforderlich: Der von der Citrix Workspace-App verwendete RSA SecurID-Softwaretoken registriert nur das URL-Schema com.citrix.securid.

Wenn Endbenutzer sowohl die Citrix Workspace-App als auch die RSA SecurID-App auf ihrem iOS-Gerät installiert haben, müssen Benutzer das URL-Schema **com.citrix.securid** auswählen, um den RSA SecurID Software Authenticator (Softwaretoken) in die Citrix Workspace-App auf ihren Geräten zu importieren.

So importieren Sie einen RSA SecurID-Softtoken

Um einen RSA-Softtoken mit der Citrix Workspace-App zu verwenden, stellen Sie als Administrator sicher, dass die Endbenutzer Folgendes beachten:

- die Richtlinie für die PIN-Länge
- den PIN-Typ (nur numerisch und alphanumerisch)
- die Beschränkungen für die Wiederverwendung von PINs

Nachdem sich der Endbenutzer erfolgreich am RSA-Server authentifiziert hat, muss er die PIN nur einmal einrichten. Nach der PIN-Verifizierung sind sie auch beim StoreFront-Server authentifiziert. Nach allen Überprüfungen zeigt die Workspace-App die verfügbaren veröffentlichten Anwendungen und Desktops an.

So verwenden Sie einen RSA-Softtoken

1. Importieren Sie den RSA-Softtoken, den Sie von Ihrer Organisation erhalten haben.
2. Wählen Sie in der E-Mail mit Ihrer angehängten SecurID-Datei **In Workspace öffnen** als Importziel aus. Nach dem Import des Softtokens wird die Citrix Workspace-App automatisch geöffnet.
3. Wenn Ihre Organisation ein Kennwort zur Vervollständigung des Imports bereitgestellt hat, geben Sie das von Ihrer Organisation bereitgestellte Kennwort ein und klicken Sie auf **OK**. Nach dem Klicken auf **OK** wird eine Meldung angezeigt, dass der Token erfolgreich importiert wurde.

4. Schließen Sie die Importmeldung, und tippen Sie in der Citrix Workspace-App auf **Konto hinzufügen**.
5. Geben Sie die von Ihrer Organisation bereitgestellte URL für den Store ein und klicken Sie auf **Weiter**.
6. Geben Sie auf dem Anmeldebildschirm Ihre Anmeldeinformationen ein: Benutzername, Kennwort und Domäne. Geben Sie für das Feld PIN **0000** ein, es sei denn, Ihre Organisation hat Ihnen eine andere Standard-PIN mitgeteilt. Die PIN 0000 ist eine RSA-Standard-PIN, aber Ihre Organisation hat sie möglicherweise geändert, um ihren Sicherheitsrichtlinien zu entsprechen.
7. Klicken Sie oben links auf **Anmelden**. Eine Meldung zum Erstellen einer PIN wird angezeigt.
8. Geben Sie eine PIN mit 4 bis 8 Ziffern ein und klicken Sie auf **OK**. Eine Meldung zur Bestätigung Ihrer neuen PIN wird angezeigt.
9. Geben Sie Ihre PIN erneut ein und klicken Sie auf **OK**. Sie können jetzt auf Ihre Apps und Desktops zugreifen.

Nächster Token-Code

Die Citrix Workspace-App unterstützt die Funktion für den nächsten Token-Code, wenn Sie Citrix Gateway mit RSA SecurID-Authentifizierung konfigurieren. Wenn Sie drei falsche Kennwörter eingeben, wird eine Fehlermeldung im Citrix Gateway-Plug-In angezeigt. Um sich anzumelden, warten Sie auf den nächsten Token. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers deaktiviert wird, wenn sich ein Benutzer zu oft mit einem falschen Kennwort anmeldet.

Abgeleitete Anmeldeinformationen

Die Citrix Workspace-App unterstützt abgeleitete Purebred-Anmeldeinformationen. Beim Herstellen einer Verbindung zu einem Store, der abgeleitete Anmeldeinformationen zulässt, können Benutzer sich mit einer virtuellen Smartcard bei der Citrix Workspace-App anmelden. Diese Funktion wird nur bei lokalen Bereitstellungen unterstützt.

> **Hinweis:**
>
> Citrix Virtual Apps and Desktops™ 7 1808 oder höher sind erforderlich, um diese Funktion zu verwenden.

So aktivieren Sie abgeleitete Anmeldeinformationen in der Citrix Workspace-App:

1. Gehen Sie zu **Einstellungen** > **Erweitert** > **Abgeleitete Anmeldeinformationen**.
2. Tippen Sie auf **Abgeleitete Anmeldeinformationen verwenden**.

So erstellen Sie eine virtuelle Smartcard zur Verwendung mit abgeleiteten Anmeldeinformationen:

1. Tippen Sie unter **Einstellungen** > **Erweitert** > **Abgeleitete Anmeldeinformationen** auf **Neue virtuelle Smartcard hinzufügen**.
2. Bearbeiten Sie den Namen der virtuellen Smartcard.
3. Geben Sie eine 8-stellige, nur aus Ziffern bestehende PIN ein und bestätigen Sie diese.
4. Tippen Sie auf **Weiter**.
5. Tippen Sie unter Authentifizierungszertifikat auf **Zertifikat importieren…**
6. Der Dokumentenwähler wird angezeigt. Tippen Sie auf **Durchsuchen**.
7. Wählen Sie unter Speicherorte **Purebred-Schlüsselbund**.
8. Wählen Sie das passende Authentifizierungszertifikat aus der Liste.
9. Tippen Sie auf **Schlüssel importieren**.
10. Wiederholen Sie die Schritte 5–9 für das Zertifikat für digitale Signaturen und das Verschlüsselungszertifikat, falls gewünscht.
11. Tippen Sie auf **Speichern**.

Sie können drei oder weniger Zertifikate für Ihre virtuelle Smartcard importieren. Das Authentifizierungszertifikat ist erforderlich, damit die virtuelle Smartcard ordnungsgemäß funktioniert. Das Verschlüsselungszertifikat und das Zertifikat für digitale Signaturen können zur Verwendung in einer VDA-Sitzung hinzugefügt werden.

> **Hinweis:**
>
> Beim Herstellen einer Verbindung zu einer HDX™-Sitzung wird die erstellte virtuelle Smartcard in die Sitzung umgeleitet.

Bekannte Einschränkungen

- Benutzer können nur eine aktive Karte gleichzeitig haben.

- Sobald eine virtuelle Smartcard erstellt wurde, kann sie nicht bearbeitet werden. Löschen Sie die Karte und erstellen Sie sie neu.
- Eine PIN kann bis zu zehnmal ungültig sein. Wenn sie nach zehn Versuchen ungültig ist, wird die virtuelle Smartcard gelöscht.
- Wenn Sie abgeleitete Anmeldeinformationen auswählen, überschreibt die virtuelle Smartcard eine physische Smartcard.

User-Agent

Die Citrix Workspace-App sendet einen User-Agent-String in Netzwerkanfragen, der zur Konfiguration von Authentifizierungsrichtlinien verwendet werden kann, einschließlich der Umleitung der Authentifizierung an andere Identitätsanbieter (IdPs).

Hinweis

Die Versionsnummern, die als Teil des User-Agent in der folgenden Tabelle aufgeführt sind, sind Beispiele und werden automatisch basierend auf den von Ihnen verwendeten Versionen aktualisiert.

SZENARIO	IOS (WKWEBVIEW)	IOS (SAFARI VIEW CONTROLLER)	IPADOS (WKWEBVIEW)	IPADOS (SAFARI VIEW CONTROLLER)
Cloud-Store	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 605.1.15 (KHTML, wie Gecko) Mobil/ 15E148 CWA/	Standard-Safari-User-Agent-String.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 605.1.15 (KHTML, wie Gecko) Mobil/ 15E148 CWA/	Standard-Safari-User-Agent-String.

SZENARIO	IOS (WKWEBVIEW)	IOS (SAFARI VIEW CONTROLLER)	IPADOS (WKWEBVIEW)	IPADOS (SAFARI VIEW CONTROLLER)
	24.7.0 iOS/18.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone AuthManager/24.7.0.1		24.7.0 iOS/18.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1.	
Cloud store - SaaS und Web-App	Standard-WKWebview-User-Agent-String.	Standard-Safari-User-Agent-String.	Wenn `isFeatureUseSafariUserAgentForSaasWebviewEnabled` aktiviert ist, wird folgender User-Agent gesendet Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15) AppleWebKit/605.1.15	Standard-Safari-User-Agent-String.

SZENARIO	IOS (WKWEBVIEW)	IOS (SAFARI VIEW CONTROLLER)	IPADOS (WKWEBVIEW)	IPADOS (SAFARI VIEW CONTROLLER)	
			(KHTML, wie Gecko) / Version/ 13.4 Wenn `Safari/ 605.1.15 shouldTun nelWebVie wTraffic` auf True gesetzt ist, wird folgender User-Agent gesendet Mozilla/5.0 (Macintosh ; Intel Mac OS X 10_15) AppleWeb Kit/ 605.1.15 (KHTML, wie Gecko) / Version/ 13.4		

SZENARIO	IOS (WKWEBVIEW)	IOS (SAFARI VIEW CONTROLLER)	IPADOS (WKWEBVIEW)	IPADOS (SAFARI VIEW CONTROLLER)	
			Safari/ 605.1.15/ CitrixReceiver/24.5.0/ X1Class CWACapable		
On-Premises Store	Standard-WKWebview-User-Agent-String.	Standard-Safari-User-Agent-String.	---	Standard-Safari-User-Agent-String.	
On-Premises Store mit NetScaler Gateway	Standard-WKWebview-User-Agent-String.	Standard-Safari-User-Agent-String.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 605.1.15 (KHTML, wie Gecko) Mobile/ 15E148 CWA/ 24.7.0 iOS/ 18.0 X1Class CWACapable 302RedirectionCapable CFNetwork	Standard-Safari-User-Agent-String.	

SZENARIO	IOS (WKWEBVIEW)	IOS (SAFARI VIEW CONTROLLER)	IPADOS (WKWEBVIEW)	IPADOS (SAFARI VIEW CONTROLLER)
			Darwin CWA-iPad AuthManager/24.7.0.1	
On-Premises Store mit NetScaler Gateway und nFactor-Authentifizierung	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 605.1.15 (KHTML, wie Gecko) Mobil/ 15E148 CWA/ 24.7.0 iOS/ 18.0 X1Class CWAFähig 302Umleitungsfähig CFNetwork Darwin CWA-iPhone AuthManager/24.7.0.1	Standard-Safari-User-Agent-String.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/ 605.1.15 (KHTML, wie Gecko) Mobil/ 15E148 CWA/ 24.7.0 iOS/ 18.0 X1Class CWAFähig 302Umleitungsfähig CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1	Standard-Safari-User-Agent-String.

User-Agent-String für WKWebView

Ab Version 23.3.5 enthält der User-Agent-String, der bei einigen der über WKWebView initiierten Netzwerkanfragen verwendet wird, standardmäßig den Citrix Workspace-App-Bezeichner.

Daher wurde er geändert von: `Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0`

Zu einem der folgenden:

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone` (iPhone-Beispiel)

Oder

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad` (iPad-Beispiel)

nFactor-Authentifizierung

Unterstützung für Multi-Faktor-(nFactor)-Authentifizierung

Die Multi-Faktor-Authentifizierung erhöht die Sicherheit einer Anwendung, indem sie von Benutzern verlangt, mehrere Identitätsnachweise für den Zugriff zu erbringen. Die Multi-Faktor-Authentifizierung ermöglicht es dem Administrator, Authentifizierungsschritte und die zugehörigen Formulare zur Erfassung von Anmeldeinformationen zu konfigurieren.

Die native Citrix Workspace-App kann dieses Protokoll unterstützen, indem sie auf der bereits für StoreFront implementierten Forms-Anmeldeunterstützung aufbaut. Die Web-Anmeldeseite für virtuelle Citrix Gateway- und Traffic Manager-Server nutzt dieses Protokoll ebenfalls.

Weitere Informationen finden Sie unter SAML-Authentifizierung und Multi-Faktor-(nFactor)-Authentifizierung.

Einschränkungen:

- Wenn die nFactor-Unterstützung aktiviert ist, können Sie keine biometrische Authentifizierung wie Touch ID und Face ID verwenden.

Unterstützung für erweiterte nFactor-Authentifizierungsrichtlinien

Wir unterstützen jetzt die zertifikatbasierte Authentifizierung in der Citrix Workspace-App, wenn diese über erweiterte nFactor-Authentifizierungsrichtlinien auf Citrix Gateway konfiguriert wird. Die nFactor-Authentifizierung hilft bei der Konfiguration flexibler und agiler Multi-Faktor-Schemata.

User-Agent-String:

Bei der erweiterten (nFactor-)Authentifizierung für die Citrix Workspace-App auf einem iPhone oder iPad wird der Authentifizierungsprozess an eine eingebettete WebView umgeleitet. Der resultierende User-Agent-String kann je nach Betriebssystemversion, CWA-Build-Version, Gerätemodell und AuthManager-Version leicht variieren. Betrachten Sie beispielsweise die folgenden User-Agent-Strings für iPhone und iPad.

Für iPhone:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/16.2 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone AuthManager/3.3.0.0
```

Für iPad:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0
```

Hinweis:

- Die Versions- oder Gerätemodellinformationen können je nach Umgebung variieren.
- Um Citrix Workspace-App für iOS-spezifische, auf User-Agents basierende Richtlinien während der Authentifizierung anzuwenden, verwenden Sie die folgenden Schlüsselwörter:
  - iOS
  - CWA
  - CWACapable

Unterstützung für FIDO2-basierte Authentifizierung beim Verbinden mit einer HDX-Sitzung

Ab Version 23.9.0 unterstützt die Citrix Workspace-App für iOS jetzt die passwortlose Authentifizierung innerhalb einer Citrix Virtual Apps and Desktops-Sitzung mithilfe von FIDO2-basierten Authentifizierungsmethoden. Diese Funktion ermöglicht es Benutzern, sich auf einer

WebAuthn-unterstützten Website in Browsern wie Google Chrome oder Microsoft Edge mit FIDO2-unterstützten Yubico-Sicherheitsschlüsseln anzumelden. Das einfache Öffnen einer WebAuthn-unterstützten Website löst die passwortlose Authentifizierung aus. Es werden nur Geräte mit Lightning-Anschluss unterstützt (Geräte mit USB-C- oder USB-4-Anschlüssen werden nicht unterstützt). Die Anmeldung bei der Citrix Workspace-App oder Desktopsitzung mithilfe der passwortlosen Authentifizierung wird nicht unterstützt.

Weitere Informationen zu den Voraussetzungen finden Sie unter Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2 in der Citrix Virtual Apps and Desktops-Dokumentation.

Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit einem Cloud Store

Ab Version 24.5.0 können Benutzer sich bei der Citrix Workspace-App mit FIDO2-basierter passwortloser Authentifizierung authentifizieren, wenn sie sich mit einem Cloud Store verbinden. FIDO2 bietet eine nahtlose Authentifizierungsmethode, die es Unternehmensmitarbeitern ermöglicht, auf Apps und Desktops innerhalb virtueller Sitzungen zuzugreifen, ohne Benutzernamen oder Kennwort eingeben zu müssen. Diese Funktion unterstützt sowohl Roaming- (nur USB) als auch Plattform-Authentifikatoren (nur PIN-Code, Touch ID und Face ID). Diese Funktion ist standardmäßig aktiviert.

> **Hinweis:**
>
> Die FIDO2-Authentifizierung wird standardmäßig mit den benutzerdefinierten Chrome-Tabs unterstützt. Wenn Sie die FIDO2-Authentifizierung mit WebView verwenden möchten, registrieren Sie Ihr Interesse über dieses Podio-Formular.

Unterstützung für die Konfiguration der Speicherung von Authentifizierungstoken in der lokalen Bereitstellung

Die Citrix Workspace-App für iOS bietet jetzt eine Option zum Konfigurieren der Speicherung von Authentifizierungstoken auf der lokalen Festplatte für lokale Stores. Mit dieser Funktion können Sie die Speicherung des Authentifizierungstokens für eine verbesserte Sicherheit deaktivieren. Nach der Deaktivierung müssen Sie sich nach einem System- oder Sitzungsneustart erneut authentifizieren, um auf die Sitzung zugreifen zu können.

Gehen Sie wie folgt vor, um die Speicherung von Authentifizierungstoken in der lokalen Bereitstellung mithilfe der Konfigurationsdatei der Verwaltung zu deaktivieren:

1. Öffnen Sie die Datei web.config mit einem Texteditor. Diese befindet sich normalerweise unter `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkontoelement in der Datei (store ist der Kontoname Ihrer Bereitstellung). Beispiel: `<account id=... name="Store">`
3. Navigieren Sie vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

```
<properties>

    <property name="TokenPersistence" value="false" />

</properties>
```

Das Folgende ist ein Beispiel für die Datei web.config:

```
<account id="########################################" name="Store
Service"

    description="" published="true" updaterType="None"
remoteAccessType="StoresOnly">

    <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_Store">

            <metadata>

                <plugins>

                    <clear />

                </plugins>

                <trustSettings>

                    <clear />
```

```
                </trustSettings>
                <properties>
                    <clear />
                    <property name="TokenPersistence" value="false" />
                 </properties>
            </metadata>
        </annotatedServiceRecord>
    </annotatedServices>
    <metadata>
    <plugins>
      <clear />
    </plugins>
    <trustSettings>
      <clear />
    </trustSettings>
    <properties>
    </properties>
 </metadata>
</account>
```

Neuauthentifizierung nach Sitzungs-Timeout

Ab Version 23.3.0 werden Sie aufgefordert, sich bei der Citrix Workspace-App erneut zu authentifizieren, wenn Ihre Sitzung seit Ihrer letzten Anmeldung abgelaufen ist. Sie werden zur Zwei-Faktor-Authentifizierung oder zur Eingabe von Benutzername und Kennwort aufgefordert, wenn Sie sich über das Web oder einen nativen Client mit der Citrix Workspace-App verbinden.

Sicher

Um die Kommunikation zwischen Ihrer Serverfarm und der Citrix Workspace-App zu sichern, integrieren Sie Ihre Verbindungen zur Serverfarm mit einer Reihe von Sicherheitstechnologien, einschließlich Citrix Gateway.

Hinweis:

Citrix empfiehlt die Verwendung von Citrix Gateway, um die Kommunikation zwischen StoreFront-Servern und den Geräten der Benutzer zu sichern.

- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch als Sicherheitsproxyserver, HTTPS-Proxyserver bekannt).

  Sie können Proxyserver verwenden, um den Zugriff auf und von Ihrem Netzwerk zu beschränken und Verbindungen zwischen der Citrix Workspace-App und Servern zu verwalten. Die Citrix Workspace-App unterstützt SOCKS- und sichere Proxy-Protokolle.
- Secure Web Gateway.

  Sie können Secure Web Gateway mit Web Interface verwenden, um einen einzigen, sicheren und verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereitzustellen.

  Sie können Secure Web Gateway mit Web Interface verwenden, um einzelne, sichere und verschlüsselte Daten bereitzustellen. Die Server in internen Unternehmensnetzwerken können über das Internet auf die gesicherten Daten zugreifen.
- SSL Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen.
- Eine Firewall.

  Netzwerk-Firewalls können Pakete basierend auf der Zieladresse und dem Port zulassen oder blockieren.

Wenn Sie die Citrix Workspace-App über eine Netzwerk-Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuordnet (d. h. Network Address Translation oder NAT), konfigurieren Sie die externe Adresse.

Unterstützung für Multi-Site-Store-Failover basierend auf dem geografischen Standort

Ab Version 24.12.0 verbessert die Funktion zur Multi-Store-Failover-Behandlung das Multi-Store-Failover, indem Store-Adressprüfungen asynchron ausgeführt und veraltete Store-Einträge entfernt werden, wenn eine neue Failover-Store-Adresse erkannt wird. Wenn ein Failover aufgrund eines Ausfalls auftritt, leitet der Global Server Load Balancer (GSLB) den Client zu einem neuen Standort um. Diese Funktion stellt sicher, dass beim Starten eines zuvor hinzugefügten Stores der Gateway-Detektor prüft, ob sich die Store-Adresse basierend auf dem geografischen Standort des Benutzers geändert hat. Wenn eine neue Adresse gefunden wird, entfernt der Client automatisch den alten Store-Eintrag und fügt den neuen hinzu. Dieser Prozess läuft im Hintergrund ab und ermöglicht einen nahtlosen Übergang zum neuen Store ohne manuelles Eingreifen. Beachten Sie, dass diese Funktion nur für lokale Stores gilt.

Voraussetzung:

Der Benutzer muss sich beim Store anmelden.

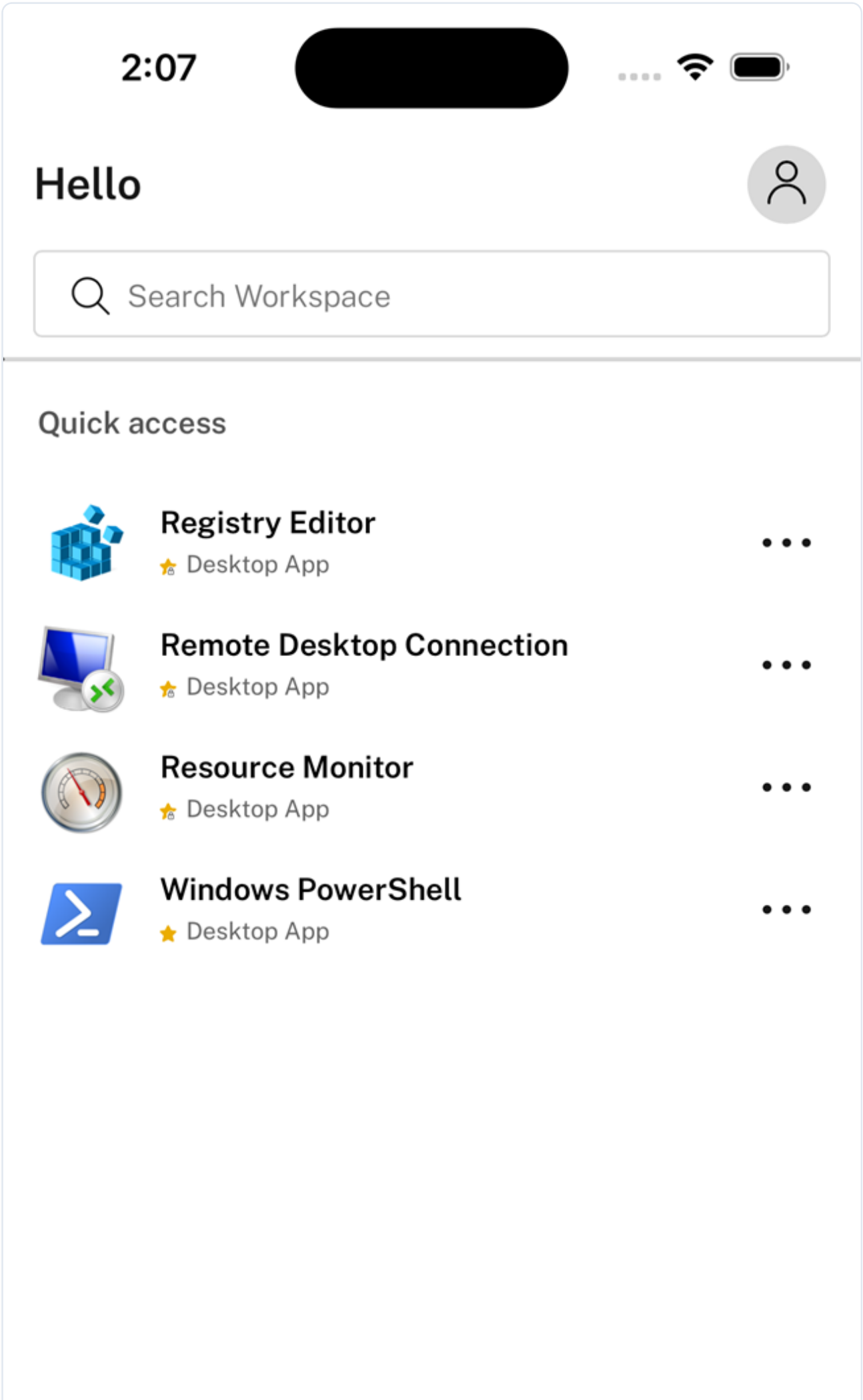
Einschränkung:

Wenn das Anmeldesitzungs-Cookie abläuft, erfolgt das Multi-Store-Failover nicht automatisch, da die API zum Abrufen der URL fehlschlägt. In diesem Fall wird die Anmeldeseite angezeigt.

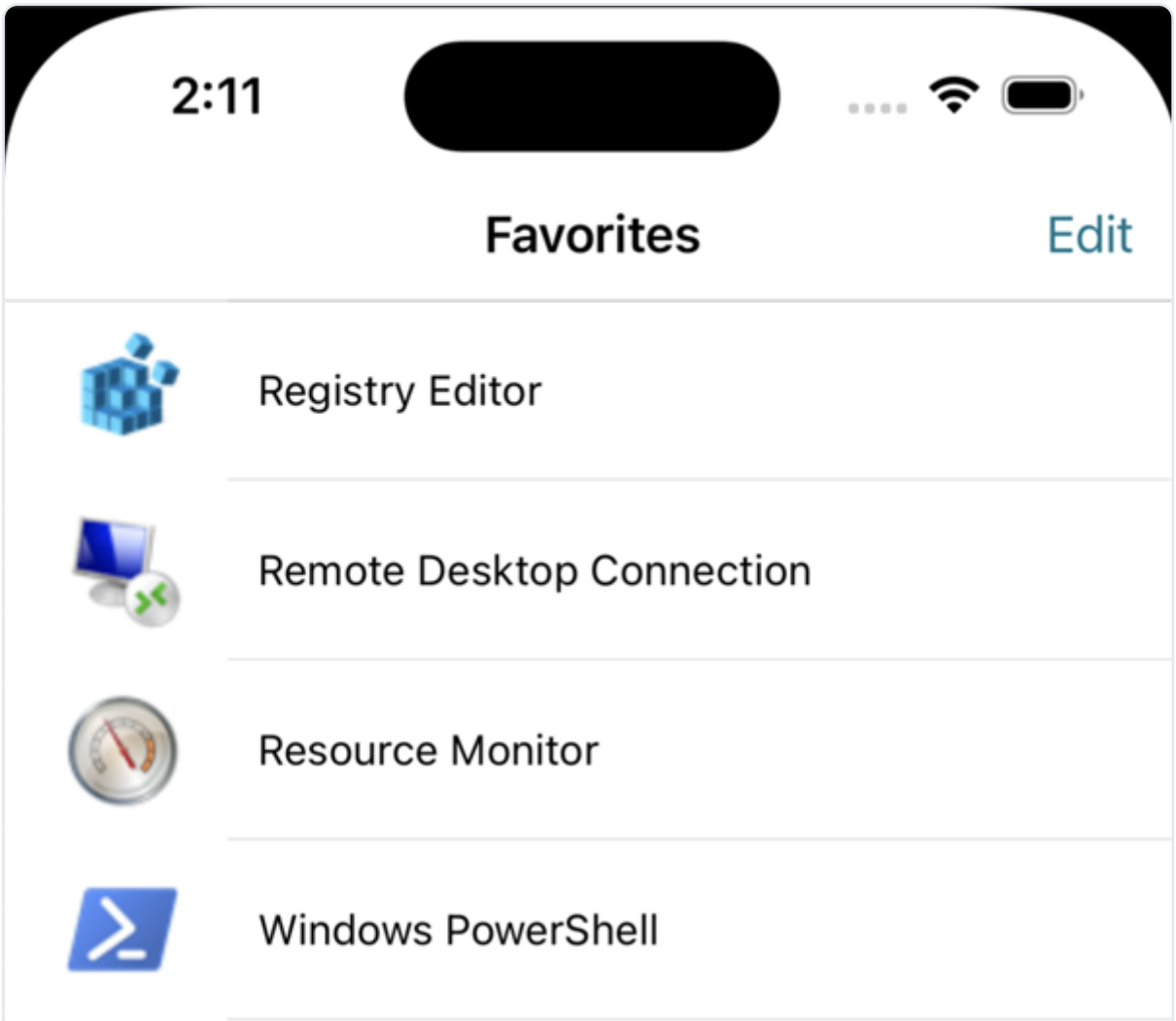
Unterstützung für WSUI lokal über Gateway

Ab Version 24.12.0 unterstützt die Citrix Workspace-App für iOS die Web-Benutzeroberfläche für den lokalen Store, der sich ebenfalls hinter dem Gateway befindet. Der Administrator muss diese Funktion konfigurieren, da sie standardmäßig nicht aktiviert ist. Weitere Informationen zur Konfiguration finden Sie unter Neue Benutzeroberfläche für lokale Stores (Technische Vorschau).

Die folgende Abbildung zeigt die aktuelle Benutzeroberfläche:


2:07
Hello
Search Workspace
Quick access
Registry Editor
Desktop App
Remote Desktop Connection
Desktop App
Resource Monitor
Desktop App
Windows PowerShell
Desktop App

Die folgende Abbildung zeigt die neue Benutzeroberfläche:


2:11
Favorites
Edit
Registry Editor
Remote Desktop Connection
Resource Monitor
Windows PowerShell

Citrix Gateway

Um Remotebenutzern die Verbindung zu Ihrer Citrix Endpoint Management-Bereitstellung über Citrix Gateway zu ermöglichen, können Sie Zertifikate für die Verwendung mit StoreFront konfigurieren. Die Methode zur Aktivierung des Zugriffs hängt von der Edition von Citrix Endpoint Management in Ihrer Bereitstellung ab.

Wenn Sie Citrix Endpoint Management in Ihrem Netzwerk bereitstellen, ermöglichen Sie Verbindungen von internen oder Remotebenutzern zu StoreFront über Citrix Gateway, indem Sie Citrix Gateway in StoreFront integrieren. Diese Bereitstellung ermöglicht Benutzern die Verbindung zu StoreFront, um auf veröffentlichte Anwendungen von XenApp und virtuelle Desktops von XenDesktop zuzugreifen. Benutzer stellen die Verbindung über die Citrix Workspace-App her.

Sicheres Web-Gateway

Dieses Thema gilt nur für Bereitstellungen, die die Web-Oberfläche verwenden.

Sie können das Secure Web Gateway entweder im Normalmodus oder im Relay-Modus verwenden, um einen sicheren Kommunikationskanal zwischen der Citrix Workspace-App und dem Server bereitzustellen. Wenn Sie das Secure Web Gateway im **Normalmodus** verwenden, ist für die Citrix Workspace-App keine Konfiguration erforderlich. Stellen Sie sicher, dass Endbenutzer über die Web-Oberfläche eine Verbindung herstellen.

Die Citrix Workspace-App verwendet Einstellungen, die remote auf dem Web Interface-Server konfiguriert sind, um eine Verbindung zu Servern herzustellen, auf denen das Secure Web Gateway ausgeführt wird.

Wenn der Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie den Secure Web Gateway Proxy im Relay-Modus verwenden. Wenn Sie den Relay-Modus verwenden, fungiert der Secure Web Gateway-Server als Proxy, und Sie müssen die Citrix Workspace-App für die Verwendung von Folgendem konfigurieren:

- Der vollqualifizierte Domänenname (FQDN) des Secure Web Gateway-Servers.
- Die Portnummer des Secure Web Gateway-Servers.

> **Hinweis:**
>
> Secure Web Gateway Version 2.0 unterstützt den Relay-Modus nicht.

> Der FQDN muss nacheinander die folgenden drei Komponenten auflisten:

- Hostname
- Zwischendomäne
- Top-Level-Domäne

Zum Beispiel ist `my_computer.example.com` ein FQDN, da er nacheinander einen Hostnamen (`my_computer`), eine Zwischendomäne (example) und eine Top-Level-Domäne (`com`) auflistet. Die Kombination aus Zwischen- und Top-Level-Domäne (`example. com`) wird als Domänenname bezeichnet.

Proxyserver

Proxyserver werden verwendet, um den Zugriff auf und von Ihrem Netzwerk zu begrenzen und Verbindungen zwischen der Citrix Workspace-App und Servern zu verwalten. Die Citrix Workspace-App unterstützt sowohl SOCKS- als auch sichere Proxy-Protokolle.

Die Citrix Workspace-App verwendet Proxyservereinstellungen, um mit dem Citrix Virtual Apps and Desktops-Server zu kommunizieren. Die Proxyservereinstellungen werden remote auf dem Web Interface-Server konfiguriert.

Wenn die Citrix Workspace-App mit dem Webserver kommuniziert, verwendet die App die Proxyservereinstellungen. Konfigurieren Sie die Proxyservereinstellungen für den Standard-Webbrowser auf dem Benutzergerät entsprechend.

Firewall

Netzwerk-Firewalls können Pakete basierend auf der Zieladresse und dem Port zulassen oder blockieren. Wenn Sie eine Firewall in Ihrer Bereitstellung verwenden, muss die Citrix Workspace-App in der Lage sein, über die Firewall sowohl mit dem Webserver als auch mit dem Citrix-Server zu kommunizieren. Die Firewall muss HTTP-Datenverkehr für die Kommunikation zwischen Benutzergerät und Webserver zulassen. Normalerweise erfolgt der HTTP-Datenverkehr über den Standard-HTTP-Port 80 oder 443, wenn ein sicherer Webserver verwendet wird. Für die Kommunikation mit dem Citrix-Server muss die Firewall eingehenden ICA-Datenverkehr auf den Ports 1494 und 2598 zulassen.

Wenn die Firewall für Network Address Translation (NAT) konfiguriert ist, können Sie das Web Interface verwenden, um Zuordnungen von internen Adressen zu externen Adressen und Ports zu definieren. Wenn Ihr Citrix Virtual Apps and Desktops- und Citrix DaaS-Server (ehemals Citrix

Virtual Apps and Desktops service) beispielsweise nicht mit einer alternativen Adresse konfiguriert ist, können Sie das Web Interface so konfigurieren, dass es der Citrix Workspace-App für iOS eine alternative Adresse bereitstellt. Die Citrix Workspace-App für iOS stellt dann über die externe Adresse und Portnummer eine Verbindung zum Server her.

TLS

Die Citrix Workspace-App unterstützt TLS 1.2 und 1.3 mit den folgenden Cipher Suites für TLS-Verbindungen zu XenApp und XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Hinweis:**

> Die Citrix Workspace-App, die unter iOS 9 und höher oder Version 21.2.0 ausgeführt wird, unterstützt die folgenden TLS-Cipher-Suites nicht:

> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

> Transport Layer Security (TLS) ist die neueste, standardisierte Version des TLS-Protokolls. Die Internet Engineering Taskforce (IETF) benannte es in TLS um, als sie die Verantwortung für die Entwicklung von TLS als offenen Standard übernahm.

TLS sichert die Datenkommunikation durch Serverauthentifizierung, Verschlüsselung des Datenstroms und Überprüfung der Nachrichtenintegrität. Einige Organisationen, einschließlich US-Regierungsorganisationen, verlangen die Verwendung von TLS zur Sicherung der Datenkommunikation. Diese Organisationen können auch die Verwendung validierter Kryptografie

verlangen, wie z. B. den Federal Information Processing Standard (FIPS) 140. FIPS 140 ist ein Standard für Kryptografie.

Die Citrix Workspace-App unterstützt RSA-Schlüssel mit Längen von 1024, 2048 und 3072 Bit. Root-Zertifikate mit RSA-Schlüsseln von 4096 Bit Länge werden ebenfalls unterstützt.

> **Hinweis:**
>
> - Die Citrix Workspace-App verwendet die iOS-Plattformkryptografie für Verbindungen zwischen der Citrix Workspace-App und StoreFront.

TLS konfigurieren und aktivieren

Es gibt zwei Hauptschritte bei der Einrichtung von TLS:

1. Richten Sie SSL Relay auf Ihrem Citrix Virtual Apps and Desktops™-Server und Ihrem Web Interface-Server ein und beschaffen und installieren Sie das erforderliche Serverzertifikat.
2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Stammzertifikate auf Benutzergeräten installieren

Um die Kommunikation zwischen der TLS-fähigen Citrix Workspace-App und Citrix Virtual Apps and Desktops zu sichern, benötigen Sie ein Stammzertifikat auf dem Benutzergerät. Das Zertifikat kann die Signatur der Zertifizierungsstelle auf dem Serverzertifikat überprüfen.

iOS wird mit etwa 100 vorinstallierten kommerziellen Stammzertifikaten geliefert. Wenn Sie ein anderes Zertifikat verwenden möchten, können Sie eines von der Zertifizierungsstelle erhalten und auf jedem Benutzergerät installieren.

Abhängig von den Richtlinien und Verfahren Ihrer Organisation können Sie das Stammzertifikat auf jedem Benutzergerät installieren, anstatt die Benutzer zur Installation aufzufordern. Der einfachste und sicherste Weg ist, Stammzertifikate zum iOS-Schlüsselbund hinzuzufügen.

So fügen Sie dem Schlüsselbund ein Stammzertifikat hinzu

1. Senden Sie sich selbst eine E-Mail mit der Zertifikatsdatei.
2. Öffnen Sie die Zertifikatsdatei auf dem Gerät. Dadurch wird die Anwendung „Schlüsselbundverwaltung“ automatisch gestartet.
3. Befolgen Sie die Anweisungen, um das Zertifikat hinzuzufügen.

4. Vergewissern Sie sich ab iOS 10, dass das Zertifikat vertrauenswürdig ist, indem Sie zu iOS **Einstellungen** > **Info** > **Zertifikatsvertrauenseinstellungen** navigieren.

   Sehen Sie unter „Zertifikatsvertrauenseinstellungen“ den Abschnitt „VOLLSTÄNDIGES VERTRAUEN FÜR STAMMZERTIFIKATE AKTIVIEREN“. Stellen Sie sicher, dass Ihr Zertifikat für volles Vertrauen ausgewählt wurde.

Das Stammzertifikat ist installiert. Die TLS-fähigen Clients und andere Anwendungen können das Stammzertifikat über TLS verwenden.

Unterstützung für Transport Layer Security 1.3

Ab Version 23.9.0 unterstützt die Citrix Workspace-App für iOS jetzt Transport Layer Security (TLS) 1.3, was die Leistung und Effizienz steigert. TLS 1.3 bietet robuste Sicherheit mit seinen starken Cipher Suites und einmaligen Sitzungsschlüsseln.

Endbenutzer können dies in der Citrix Workspace-App für iOS wie folgt aktivieren.

1. Gehen Sie zu **Erweiterte Einstellungen** > **TLS-Versionen**.
2. Wählen Sie **TLS 1.3-Version**.



Unterstützung für DTLS 1.2

Ab Version 24.7.0 unterstützt die Citrix Workspace-App für iOS das DTLS-Protokoll Version 1.2. DTLS 1.2 bietet Erweiterungen und Verbesserungen gegenüber der vorherigen Version, darunter robuste Verschlüsselungsalgorithmen, bessere Handshake-Protokolle und Schutz vor verschiedenen Angriffen. Dieses Protokoll verbessert die allgemeine Sicherheit.

> **Hinweis:**
>
> Sollte es ein Problem mit dem DTLS-Protokoll Version 1.2 geben, greift die Citrix Workspace-App für iOS nahtlos auf die zuvor unterstützten Versionen zurück.

Unterstützung für den Citrix Device Posture-Dienst

Ab Version 2402 unterstützt die Citrix Workspace™-App für iOS den Citrix Device Posture-Dienst. Der Citrix Device Posture-Dienst ist eine cloudbasierte Lösung, die Administratoren dabei hilft,

bestimmte Anforderungen durchzusetzen, die Endgeräte erfüllen müssen, um Zugriff auf Citrix DaaS (virtuelle Apps und Desktops) oder Citrix Secure Private Access™-Ressourcen zu erhalten.

Für die Citrix Workspace-App für iOS unterstützt die Gerätehaltung nur das Scannen der Citrix Workspace-App-Version und der Betriebssystemversion des iOS-Geräts.

Weitere Informationen finden Sie in der Dokumentation zu Device Posture.

Hinweis

Diese Funktion wird nur für Cloud-Stores unterstützt.

XenApp und XenDesktop® Site

So konfigurieren Sie die XenApp®- und XenDesktop Site:

Wichtig:

- Die Citrix Workspace-App verwendet XenApp- und XenDesktop Sites, die Citrix Secure Gateway 3.x unterstützen.
- Die Citrix Workspace-App verwendet Citrix Virtual Apps-Websites, die Citrix Secure Gateway 3.x unterstützen.
- XenApp and XenDesktop Sites unterstützt nur die Einzelfaktor-Authentifizierung.
- Citrix Virtual Apps™ Websites unterstützen sowohl die Einzelfaktor- als auch die Zweifaktor-Authentifizierung.
- Alle integrierten Browser unterstützen Web Interface 5.4.

Bevor Sie mit dieser Konfiguration beginnen, installieren und konfigurieren Sie Citrix Gateway für den Betrieb mit Web Interface. Sie können diese Anweisungen an Ihre spezifische Umgebung anpassen.

Wenn Sie eine Citrix Secure Gateway-Verbindung verwenden, konfigurieren Sie keine Citrix Gateway-Einstellungen in der Citrix Workspace-App.

Die Citrix Workspace-App verwendet eine XenApp and XenDesktop Site, um Informationen über die Anwendungen abzurufen, für die ein Endbenutzer Berechtigungen besitzt. Dabei werden die Informationen der auf Ihrem Gerät ausgeführten Citrix Workspace-App präsentiert. Ähnlich können Sie das Web Interface für traditionelle SSL-basierte Citrix Virtual Apps-Verbindungen verwenden. Für dieselbe SSL-basierte Verbindung können Sie Citrix Gateway konfigurieren. XenApp and XenDesktop Sites, die auf dem Web Interface 5.x ausgeführt werden, verfügen über diese integrierte Konfigurationsmöglichkeit.

Konfigurieren Sie die XenApp and XenDesktop Site so, dass sie Verbindungen von einer Citrix Secure Gateway-Verbindung unterstützt:

1. Wählen Sie in der XenApp and XenDesktop Site **Sicheren Clientzugriff verwalten** > **Einstellungen für sicheren Clientzugriff bearbeiten**.
2. Ändern Sie die Zugriffsmethode in **Gateway Direct**.
3. Geben Sie den FQDN des Secure Web Gateway ein.
4. Geben Sie die Informationen zur Secure Ticket Authority (STA) ein.

> **Hinweis:**
>
> Für das Citrix Secure Gateway empfiehlt Citrix die Verwendung des Citrix Standardpfads (//XenAppServerName/Citrix/PNAgent). Der Standardpfad ermöglicht es den Endbenutzern, den FQDN des Secure Web Gateway anzugeben, mit dem sie sich verbinden. Verwenden Sie nicht den vollständigen Pfad zur Datei config.xml, die sich auf der XenApp and XenDesktop Site befindet. Zum Beispiel (//XenAppServerName/CustomPath/config.xml).

So konfigurieren Sie das Citrix Secure Gateway

1. Verwenden Sie den Konfigurationsassistenten des Citrix Secure Gateway, um das Gateway zu konfigurieren.

   Das Citrix Secure Gateway unterstützt den Server im sicheren Netzwerk, der die XenApp Service Site hostet.

   Nach Auswahl der Option **Indirekt** geben Sie den FQDN-Pfad Ihres Secure Web Gateway Servers ein und fahren Sie mit den Assistentenschritten fort.
2. Testen Sie eine Verbindung von einem Benutzergerät, um zu überprüfen, ob das Secure Web Gateway korrekt für die Netzwerkverbindung und Zertifikatszuweisung konfiguriert ist.

So konfigurieren Sie das Mobilgerät

1. Beim Hinzufügen eines Citrix Secure Gateway-Kontos geben Sie den passenden FQDN Ihres Citrix Secure Gateway-Servers im Feld **Adresse** ein:

    - Wenn Sie die XenApp- und XenDesktop-Site mit dem Standardpfad (/Citrix/PNAgent) erstellt haben, geben Sie den Secure Web Gateway FQDN ein: FQDNofSecureGateway.companyName.com
    - Wenn Sie den Pfad der XenApp- und XenDesktop-Site angepasst haben, geben Sie den vollständigen Pfad der Datei config.xml ein, z. B.: FQDNofSecureGateway.companyName.com/CustomPath/config.xml

2. Wenn Sie das Konto manuell konfigurieren, deaktivieren Sie die Option Citrix Gateway im Dialogfeld **Neues Konto**.

Sitzungserlebnis

Der EDT-Lossy-Modus unterstützt jetzt SecureHDX (SecureICA 2.0)-Verbindungen

Bisher:

- EDT Lossy (unzuverlässiger Subkanal) funktioniert nur mit DTLS-Verschlüsselung.
- SecureHDX-Verbindungen sind nur auf zuverlässigen Transport beschränkt.
- Die Audio- und Videoleistung könnte bei SecureHDX-Verbindungen beeinträchtigt sein.

Aktuell:

- EDT Lossy funktioniert jetzt sowohl mit DTLS- als auch mit SecureHDX-Verbindungen.
- Die Echtzeitleistung für Audio, Video und andere latenzempfindliche Kanäle verbessert sich bei Verwendung von SecureICA 2.0.
- Besseres Benutzererlebnis mit reduzierter Latenz bei SecureHDX-Verbindungen.

Technischer Überblick

Diese Verbesserung modifiziert die Netzwerktransportschicht, um unzuverlässige UDP-Subkanäle bei Verwendung der SecureHDX (SecureICA 2.0)-Verschlüsselung zu ermöglichen. Der unzuverlässige Subkanal überträgt latenzempfindliche Daten, wie Audio- und Videoframes, bei denen gelegentlicher Paketverlust akzeptabel ist. Dieser Ansatz priorisiert die Echtzeitlieferung anstelle der erneuten Übertragung verlorener Pakete.

Voraussetzungen

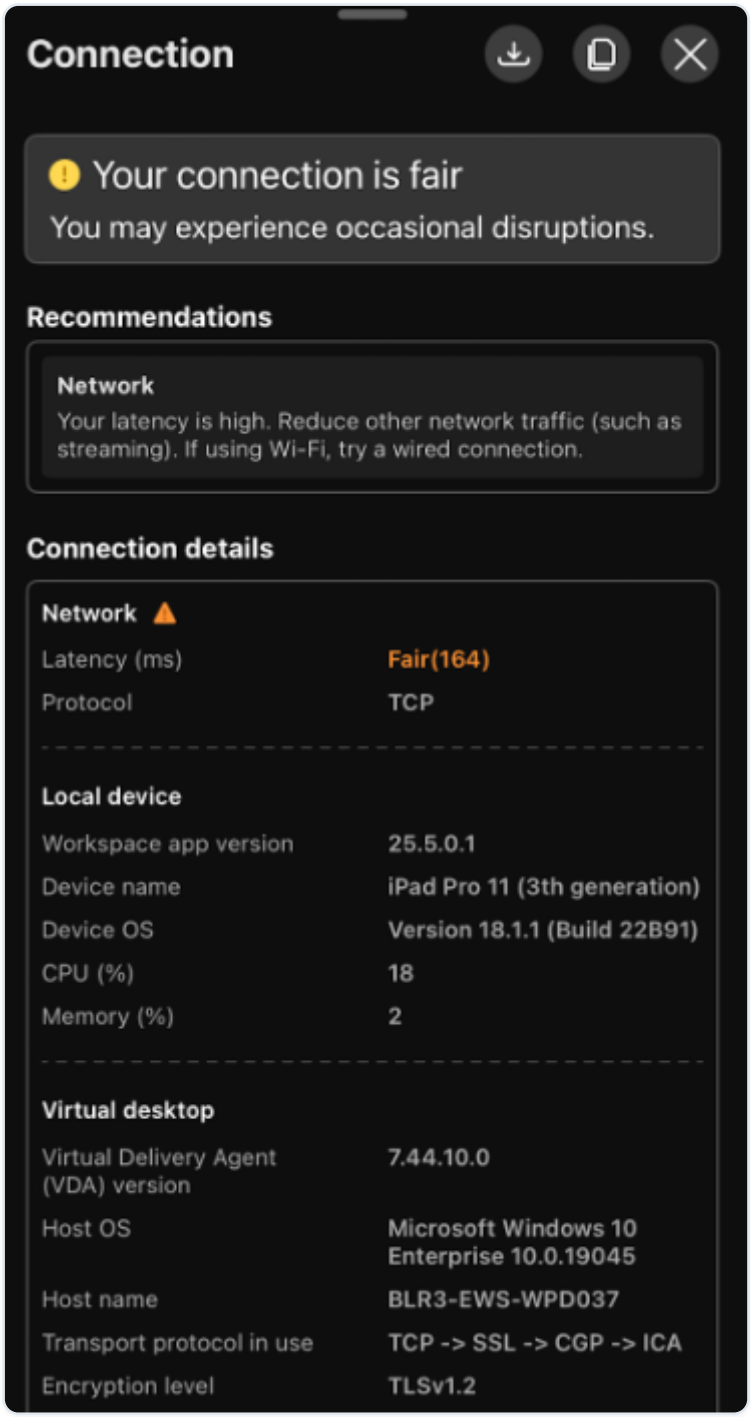
- Aktivieren Sie SecureICA 2.0 sowohl auf dem Server als auch auf dem Client. Weitere Informationen finden Sie unter Secure HDX™ Citrix Virtual Apps and Desktops™ 7 2511.
- Aktivieren Sie EDT Lossy sowohl auf dem Server als auch auf dem Client. Weitere Informationen finden Sie unter Adaptive transport Citrix Virtual Apps and Desktops™ 7 2511

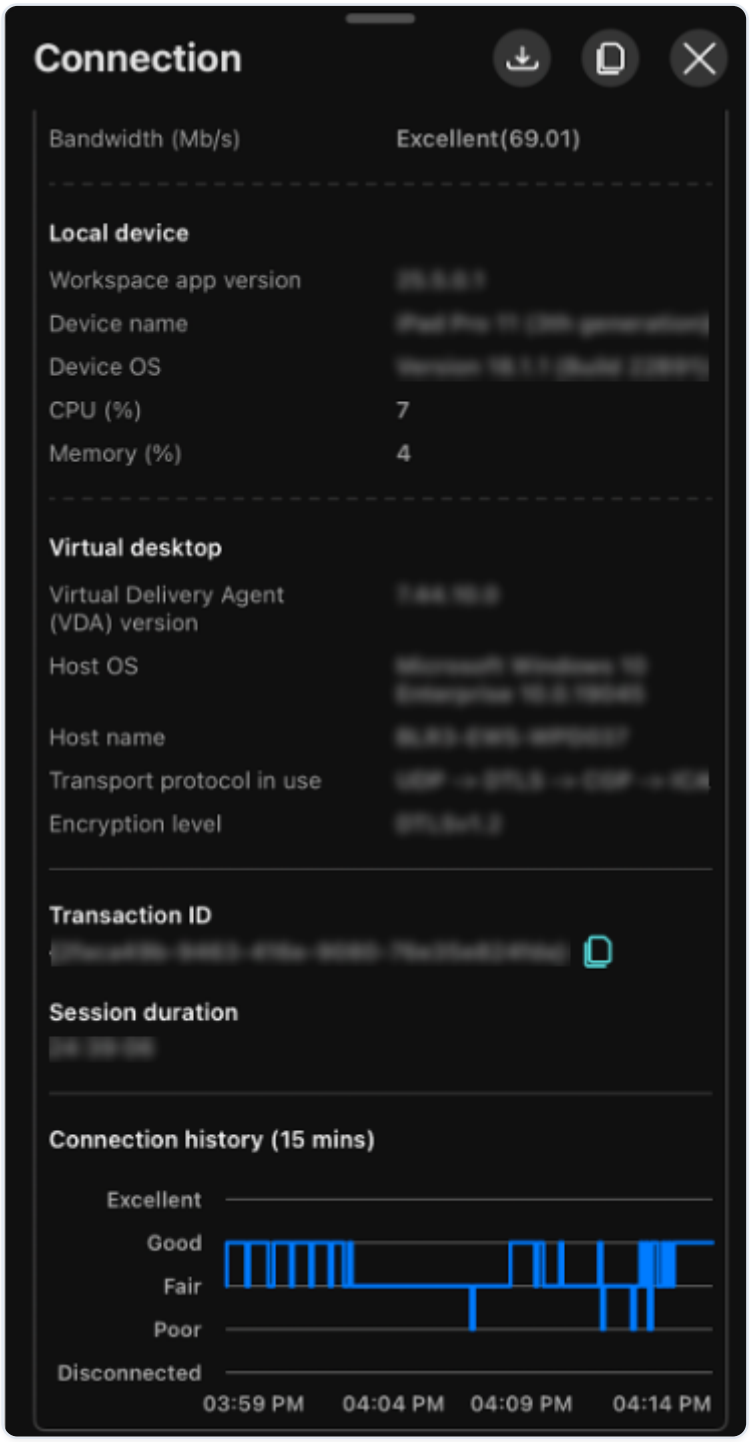
Verbesserte Anzeige der Verbindungsstärke

Ab Version 25.7.2 haben wir die Anzeige der Verbindungsstärke verbessert. Diese Verbesserung bietet Echtzeit-Einblicke in Ihre Verbindungsqualität und hilft bei der Selbstbehebung von Verbindungsproblemen. Diese Funktion ist über die Symbolleiste zugänglich und standardmäßig aktiviert.

Voraussetzungen:

- Um diese Funktion zu nutzen, aktivieren Sie die erweiterte Desktop Viewer-Symbolleiste. Administratoren müssen die neue Symbolleistenfunktion über den Global App Configuration Service aktivieren. Diese Funktion ist nur in VDA 2407 oder höher verfügbar.
- Der Supportability Virtual Channel muss clientseitig aktiviert sein, was in der Citrix Workspace-App für iOS 24.12.0 standardmäßig aktiviert ist.


Connection
Your connection is fair
You may experience occasional disruptions.
Recommendations
Network
Your latency is high. Reduce other network traffic (such as streaming). If using Wi-Fi, try a wired connection.
Connection details
Network
Latency (ms) Fair(164)
Protocol TCP
Local device
Workspace app version 25.5.0.1
Device name iPad Pro 11 (3th generation)
Device OS Version 18.1.1 (Build 22B91)
CPU (%) 18
Memory (%) 2
Virtual desktop
Virtual Delivery Agent (VDA) version 7.44.10.0
Host OS Microsoft Windows 10 Enterprise 10.0.19045
Host name BLR3-EWS-WPD037
Transport protocol in use TCP -> SSL -> CGP -> ICA
Encryption level TLSv1.2



Vorteile:

- **Sofortiges Feedback:** Das Netzwerksymbol benachrichtigt Benutzer, wenn Netzwerkprobleme erkannt werden.
- **Verbesserte Fehlerbehebung:** Echtzeitstatistiken und Diagnosen unterstützen Benutzer und IT-Teams bei der Identifizierung und Behebung von Verbindungsproblemen.

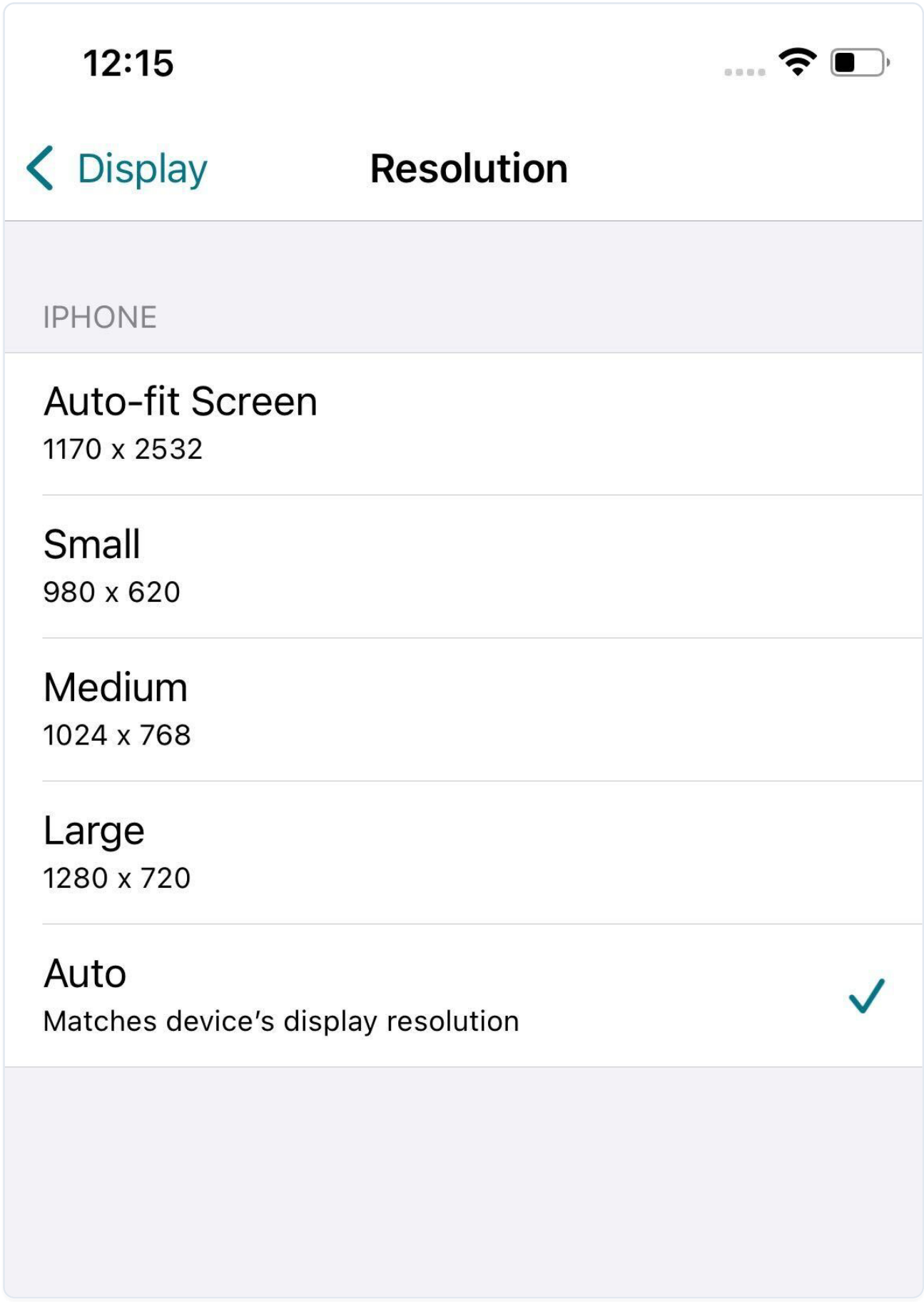
Verbesserungen der Anzeige der Verbindungsstärke

- **Brandneue Benutzeroberfläche:** Die Benutzeroberfläche wurde für verbesserte Klarheit und ein besseres Benutzererlebnis neu gestaltet.
- **Zusätzliche Verbindungsdetails:** Die Anzeige zeigt jetzt die aktuelle CPU- und Speicherauslastung des Geräts an.
- **Bewertete Metriken und Empfehlungen:** Latenz- und Bandbreitenwerte werden berechnet und angezeigt. Wenn ein Wert „Mittelmäßig“ oder „Schlecht“ ist, wird eine Empfehlung zur Behebung des Problems angezeigt.
- **Verbindungsverlauf:** Die Verbindungsbewertungen der letzten 15 Minuten werden aufgezeichnet und in einem Diagramm am unteren Rand des Layouts angezeigt. Dieser Gesamtscore basiert auf Bandbreite und Latenz, und historische Daten werden beim Kopieren oder Herunterladen in die Protokolle aufgenommen.
- **Details herunterladen:** Alle Verbindungsmetriken, einschließlich Latenz, Bandbreite, CPU- und Speicherauslastung, werden aufgezeichnet. Der Verbindungsverlauf der letzten 15 Minuten ist ebenfalls in den herunterladbaren Protokollen enthalten.

Verbesserte Sitzungsauflösung

Ab Version 25.3.0 bietet die Citrix Workspace-App für iOS Verbesserungen bei der Sitzungsauflösung für ein nahtloseres Benutzererlebnis. Die **DPI**-Einstellungen, die standardmäßig auf „Auto“ stehen, passen sich automatisch an, wenn ein Benutzer eine Sitzung startet, was das Gesamterlebnis verbessert.

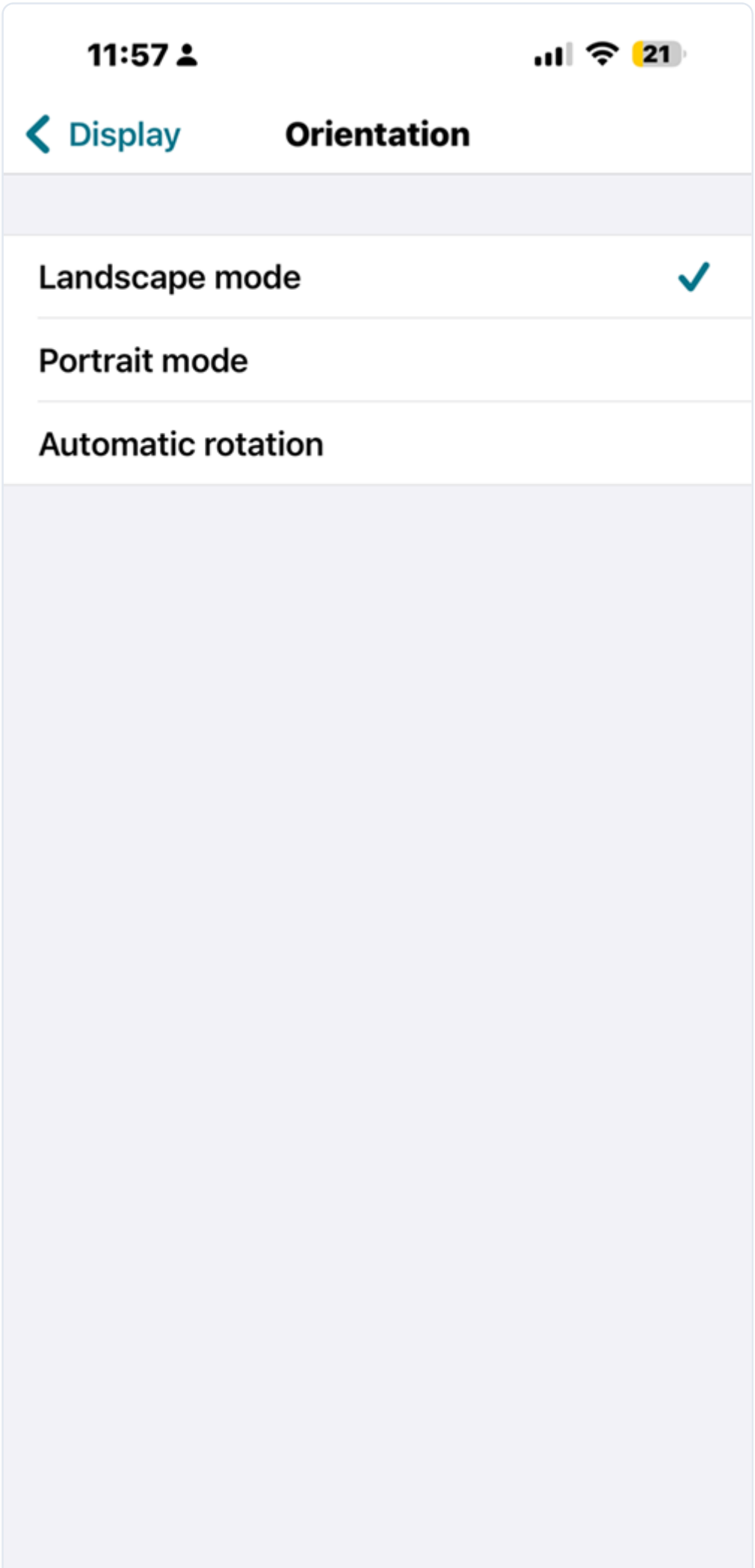
Um ein konsistentes und benutzerfreundliches Erlebnis zu gewährleisten, werden virtuelle Desktops standardmäßig im Querformat gestartet. Dies berücksichtigt Breitbildanwendungen und Multitasking-Anforderungen. Diese Funktion ist standardmäßig aktiviert.


12:15
Display
Resolution
IPHONE
Auto-fit Screen
1170 x 2532
Small
980 x 620
Medium
1024 x 768
Large
1280 x 720
Auto
Matches device's display resolution

Standard-Querformatausrichtung für virtuelle Desktops

Ab Version 25.1.0 erzwingt die Citrix Workspace-App standardmäßig die Querformatausrichtung, wenn ein virtueller Desktop auf iPhone-Geräten gestartet wird. Dies gewährleistet eine optimale und konsistente Benutzererfahrung für Breitbildanwendungen und Multitasking. Benutzer können die Ausrichtungseinstellungen über die App oder die HDX-Symbolleiste konfigurieren, um das Querformat zu sperren, das Hochformat zu sperren, die Ausrichtung basierend auf Anwendungsmetadaten automatisch anzupassen oder der Bildschirmausrichtung des Geräts zu folgen. Diese Flexibilität berücksichtigt verschiedene Workflows, einschließlich Apps, die für den Hochformatmodus entwickelt wurden, und sorgt gleichzeitig für eine nahtlose und benutzerfreundliche Erfahrung.

Um die Standardausrichtung zu konfigurieren, navigieren Sie zu **Einstellungen** > **Anzeige** > **Ausrichtung** > **Querformatmodus**.


11:57
21
Display
Orientation
Landscape mode
Portrait mode
Automatic rotation

Verbessertes gesichertes ICA®

Ab Version 25.1.0 verbessert die neue ICA-Verschlüsselungsfunktion die Sicherheit durch die Verwendung moderner Verschlüsselungsalgorithmen. Dies erhöht die Sicherheitslage unseres Produkts und bietet unseren Kunden eine Möglichkeit, die Sicherheitslage ihrer Umgebungen auf einfache und zuverlässige Weise zu verbessern. Es vereinfacht die Einrichtung, indem es eine komplexe Zertifikatsverwaltung überflüssig macht, und ermöglicht eine einfache Konfiguration über Citrix-Richtlinieneinstellungen. Die Funktion funktioniert nahtlos auf allen unterstützten Plattformen.

Voraussetzungen:

- Stellen Sie sicher, dass die Bereitstellung entweder für den CVAD-Dienst oder für die lokale Nutzung konfiguriert ist.
- Zu den unterstützten Plattformen gehören Windows, Linux, Mac, Android, iOS, HTML5 und Chrome OS.
- Administrativer Zugriff auf Citrix Studio ist erforderlich.

Konfiguration

Die Funktion kann über eine einzige Richtlinie oder Delivery Group-Eigenschaft aktiviert oder deaktiviert werden. Greifen Sie auf den Delivery Controller™ (DDC) zu und nehmen Sie die folgenden Änderungen vor:

1. Navigieren Sie zu **Einstellungen** > **Computereinstellung – ICA**, um die erforderliche Richtlinie zu konfigurieren.
2. Führen Sie den folgenden Befehl aus, um die Gruppenrichtlinie zu aktualisieren: `gpupdate/force`
3. Starten Sie die Sitzung neu, um die Änderungen zu übernehmen.

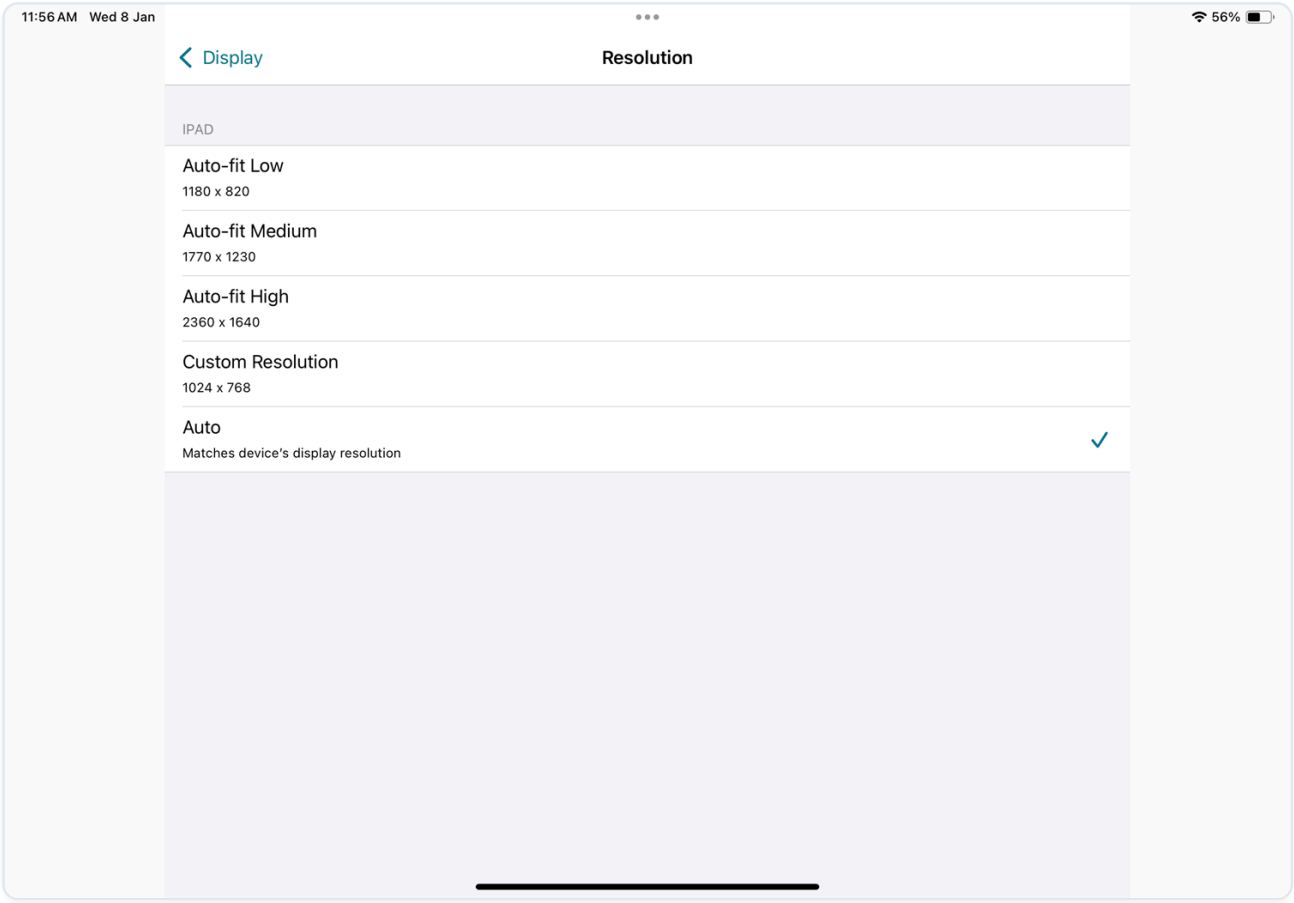
DPI-Anpassung

Die DPI-Anpassungsfunktion stellt sicher, dass die virtuelle Sitzung entsprechend der DPI des Geräts gerendert wird. Ab Version 25.1.0 verbessert eine neue Anzeigeeinstellung die DPI-Anpassungsfunktionen:

- Automatische Auflösungserkennung: Die App identifiziert automatisch die Auflösung des Gerätebildschirms.

- Dynamische DPI-Anpassung: Die DPI der virtuellen Desktopsitzung passt sich dynamisch an die erkannte Auflösung des Displays an. Dies gewährleistet optimale Klarheit, Lesbarkeit und Benutzerfreundlichkeit auf dem jeweiligen Display.
- Reibungslose Skalierung: UI-Elemente, Schriftarten und Bilder werden bei der DPI-Anpassung reibungslos und ohne Verzerrung oder Pixelbildung skaliert.
- Unterstützt Auflösungen bis zu 4K.

Die Option „Auto (DPI-Anpassung)“ ermöglicht eine automatische DPI-Anpassung für ein nahtloses Anzeigeerlebnis. Die DPI-Einstellungen sind in der App unter **Einstellungen** > **Anzeige** > **Auflösung** zugänglich.

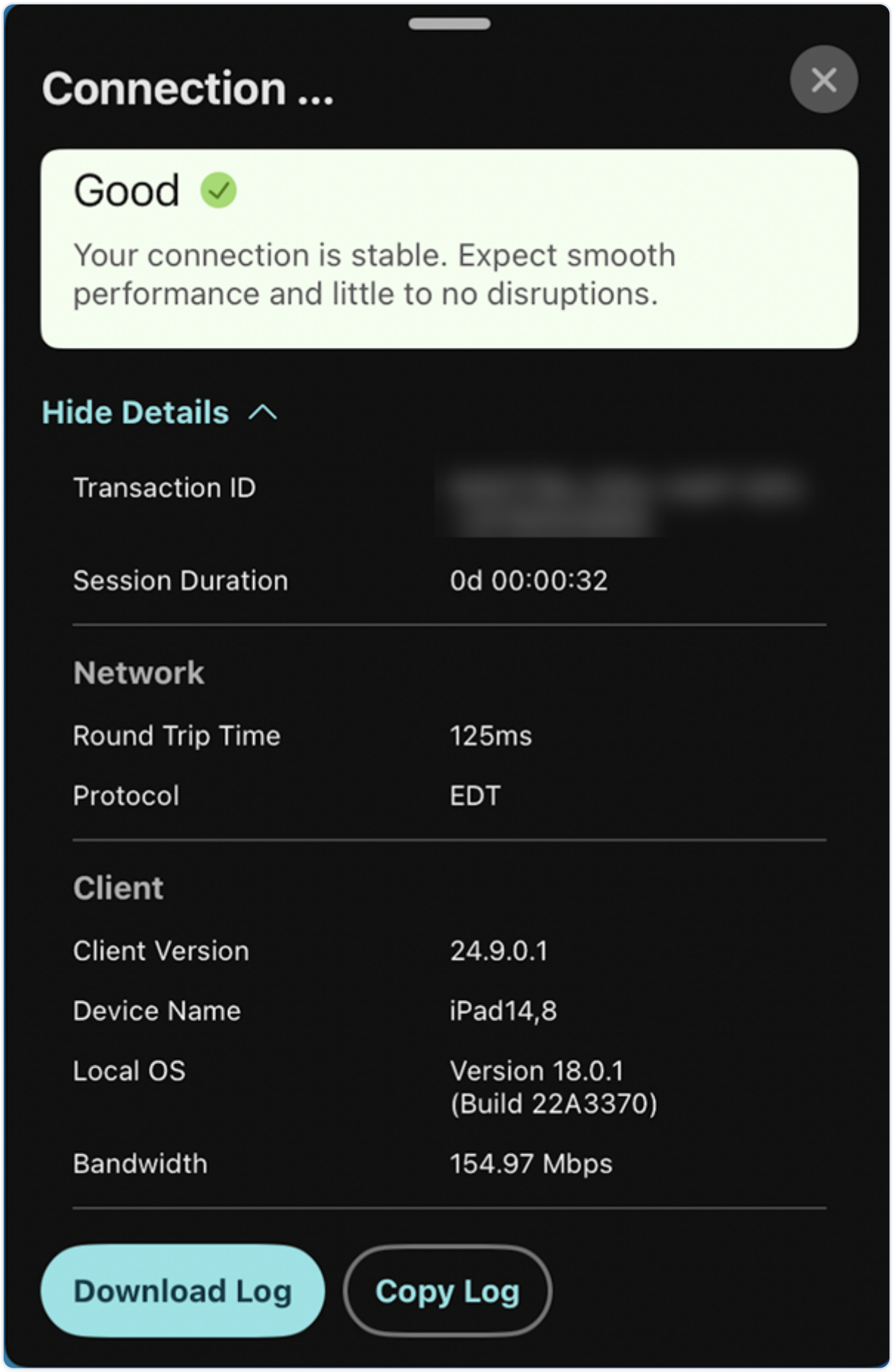


Anzeige der Verbindungsstärke

Ab Version 24.12.0 unterstützt die Citrix Workspace-App für iOS die Anzeige der Verbindungsstärke in der Symbolleiste des **Desktop Viewer**. Diese Funktion zeigt ein Netzwerksymbol an, das Sie auf Netzwerkprobleme aufmerksam macht. Durch Klicken auf das Symbol können Sie Echtzeit-Verbindungsstatistiken für Client, Gateway und VDA anzeigen und Diagnoseinformationen kopieren, um sie zur erweiterten Fehlerbehebung mit der IT zu teilen.

Voraussetzungen:

- Um diese Funktion zu nutzen, aktivieren Sie die erweiterte Desktop Viewer-Symbolleiste. Administratoren müssen die neue Symbolleistenfunktion über den Global App Configuration Service aktivieren. Diese Funktion ist nur in VDA 2405 oder höher verfügbar.
- Der Supportability Virtual Channel muss auf Clientseite aktiviert sein, was in der Citrix Workspace-App für iOS 24.12.0 standardmäßig der Fall ist.


Connection ...
Good
Your connection is stable. Expect smooth performance and little to no disruptions.
Hide Details
Transaction ID
Session Duration
0d 00:00:32
Network
Round Trip Time
125ms
Protocol
EDT
Client
Client Version
24.9.0.1
Device Name
iPad14,8
Local OS
Version 18.0.1 (Build 22A3370)
Bandwidth
154.97 Mbps
Download Log
Copy Log

Einführung der In-Memory ICA-Lösung

Ab Version 24.12.0 verbessert die Citrix Workspace-App für iOS die Unterstützung für In-Memory-Hybridstarts mithilfe des Citrix Workspace Launchers. Diese Verbesserung ermöglicht eine effizientere und sicherere Benutzererfahrung, da das Herunterladen von ICA-Dateien entfällt.

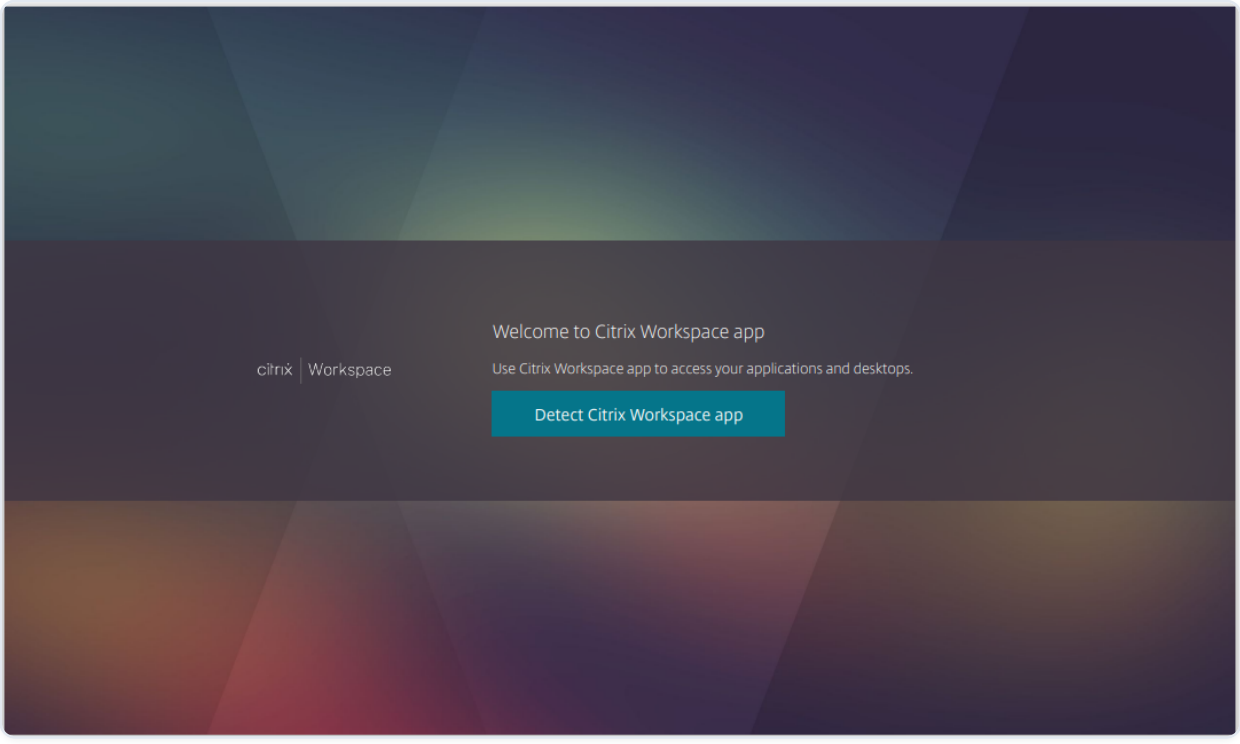
Voraussetzungen:

Citrix Workspace-App für iOS 24.12.0 oder höher.

Konfiguration

Um die Citrix Workspace-App zu starten, ohne eine ICA-Datei herunterzuladen, führen Sie die folgenden Schritte auf Ihrem iOS-Gerät aus:

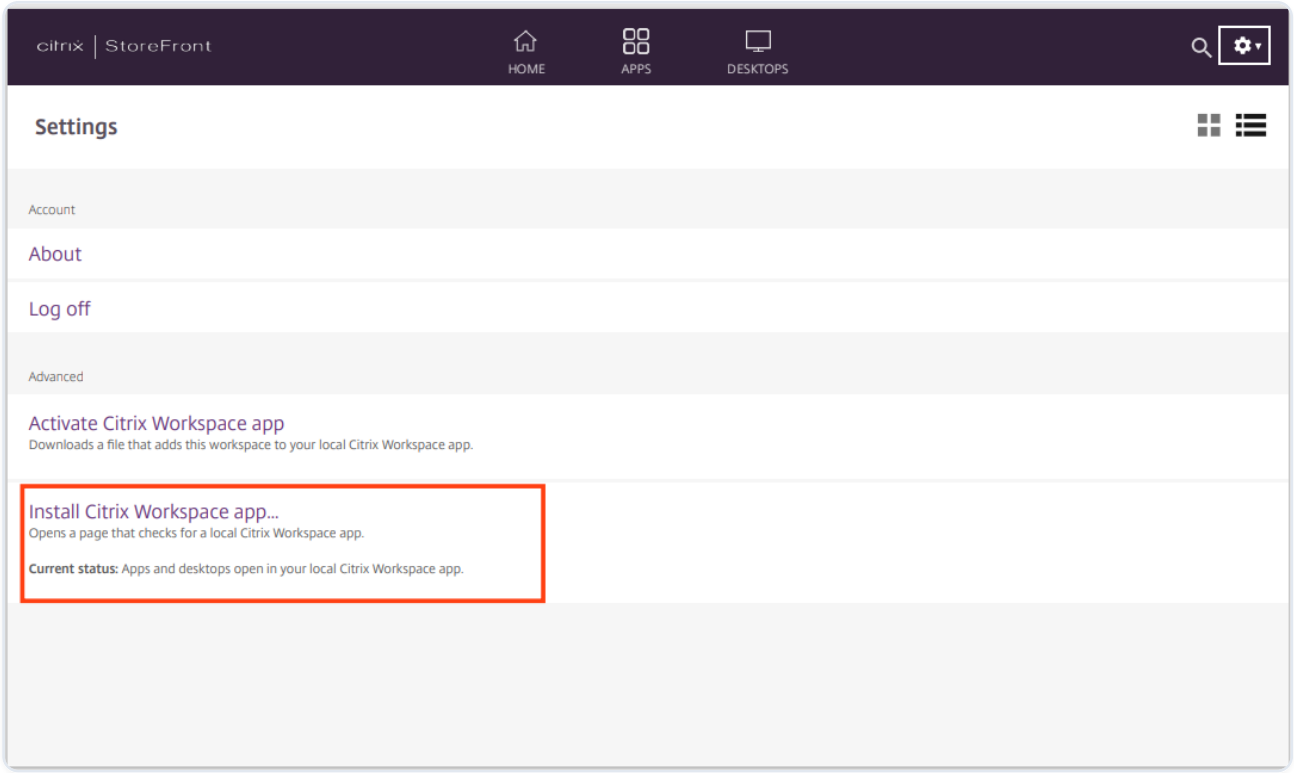
1. Öffnen Sie einen unterstützten Webbrowser (Safari, Chrome oder Firefox).
2. Rufen Sie die Store-URL Ihrer Organisation auf und melden Sie sich mit Ihren Anmeldeinformationen an.
3. Suchen und tippen Sie auf dem Begrüßungsbildschirm auf **Citrix Workspace-App erkennen**. Dadurch wird der Client-Erkennungsprozess gestartet, der die Citrix Workspace-App öffnet.



4. Kehren Sie nach der Erkennung zum Browser zurück. Sie befinden sich nun auf dem Startbildschirm des Organisations-Stores.

Sie können Ihre Apps und Desktops jetzt direkt über die Oberfläche des Organisations-Stores aufrufen und öffnen, ohne eine ICA-Datei herunterladen zu müssen.

Wenn Sie die Client-Erkennung während der ersten Anmeldung überspringen, können Sie über **Einstellungen > Citrix Workspace-App installieren > Client-Erkennung** navigieren.



Einschränkung:

Wenn die Client-Erkennung fehlschlägt, lädt das System automatisch eine ICA-Datei herunter, und die Sitzung wird aus der heruntergeladenen Datei gestartet.

Unterstützung für Rapid Scan

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS die Rapid Scan-Funktion. Mit dieser Funktion können Sie mehrere Dokumente mit einem iOS-Gerät scannen und diese gescannten Dokumente dann mithilfe der Citrix Workspace-App für Mac und iOS auf ein Mac-Gerät übertragen.

Wenn Sie sowohl auf Ihrem Mac als auch auf Ihrem iOS-Gerät bei Citrix Workspace angemeldet sind, können Sie Rapid Scan verwenden, um Dokumente mit Ihrem iPhone oder iPad zu scannen. Die gescannten Dateien werden auf Ihrem Mac gespeichert, und Sie können auch remote über einen virtuellen Desktop mithilfe von Client Drive Mapping darauf zugreifen. Diese Funktion funktioniert sowohl für Cloud- als auch für lokale Stores.

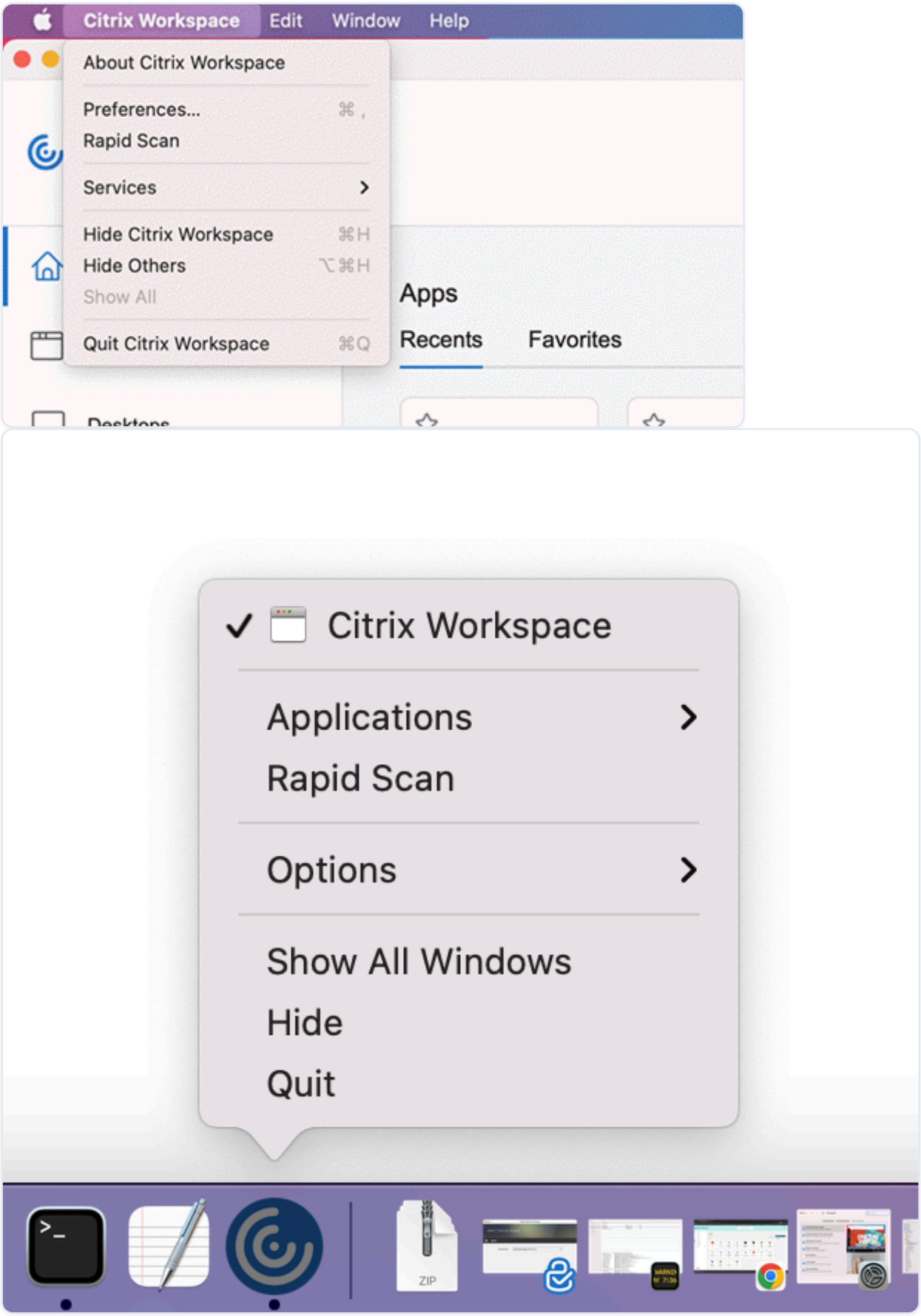
Voraussetzungen:

- Stellen Sie sicher, dass beide Geräte mit demselben Citrix Workspace-Konto angemeldet sind.

- Beide Geräte müssen mit demselben WLAN-Netzwerk verbunden sein.
- Die Citrix Workspace-App für Mac muss Version 24.9.0 oder höher sein.

So verwenden Sie Rapid Scan:

1. Öffnen Sie die Citrix Workspace-App auf Ihrem Mac.
2. Drücken Sie lange (oder klicken Sie mit der rechten Maustaste) auf das Citrix Workspace-Symbol im Dock oder in der Menüleiste.



3. Wählen Sie im Menü **Rapid Scan** aus. Ein QR-Code wird auf Ihrem Mac-Bildschirm angezeigt.
4. Gehen Sie auf Ihrem iOS-Gerät zu **Einstellungen** und tippen Sie auf **Rapid Scan**.

5. Scannen Sie den auf Ihrem Mac angezeigten QR-Code mit Ihrem iOS-Gerät.
6. Wenn das Bestätigungsfenster auf Ihrem Mac angezeigt wird, klicken Sie auf **Ja**, um die Verbindung herzustellen. Sie können Ihr iOS-Gerät nun zum Scannen von Dokumenten verwenden.
7. Wählen Sie, ob die gescannten Dateien im PDF- oder JPEG-Format gespeichert werden sollen.
8. Standardmäßig werden die gescannten Dokumente im Ordner **Downloads** auf Ihrem Mac gespeichert.
9. Nach Abschluss des Downloads klicken Sie auf Ihrem Mac auf **In Finder öffnen**, um die gescannten Dokumente zu finden.

Zugriff auf gescannte Dokumente von einem virtuellen Desktop:

1. Client Drive Mapping (CDM) muss aktiviert sein, um auf die Speicherlaufwerke Ihres Macs innerhalb des virtuellen Desktops zugreifen zu können. Dadurch können Sie Dateien zwischen Ihrem Mac und dem virtuellen Desktop übertragen. Bitte wenden Sie sich an Ihren Administrator, um diese Funktion zu aktivieren.
2. Sobald CDM aktiviert ist, sind Ihre lokalen Laufwerke im virtuellen Desktop sichtbar.
3. Wenn Sie dazu aufgefordert werden, erteilen Sie **Lese- und Schreibberechtigungen**, um vom virtuellen Desktop auf Ihre lokale Festplatte zuzugreifen.
4. Navigieren Sie zu dem Ordner, in dem die gescannten Dokumente gespeichert sind (standardmäßig der Ordner **Downloads**), und kopieren Sie die Dateien in den Speicher des virtuellen Desktops.

Unterstützung für Apples nativen Nicht-Spiegelmodus

Sie können die Anzeige jetzt mit Apples Nicht-Spiegelmodus erweitern, der mit iPadOS 16.2 verfügbar ist. Sie können Multitasking betreiben, indem Sie die Citrix Workspace-App, virtuelle Apps und virtuelle Desktops auf dem externen Monitor ausführen und den iPad-Bildschirm für andere native Apps freihalten.

> **Hinweis:**

> Die Unterstützung für die erweiterte Anzeige im Nicht-Spiegelmodus von Apple ist nur auf ausgewählten iPad-Modellen verfügbar. Weitere Informationen finden Sie in der Apple-Dokumentation.

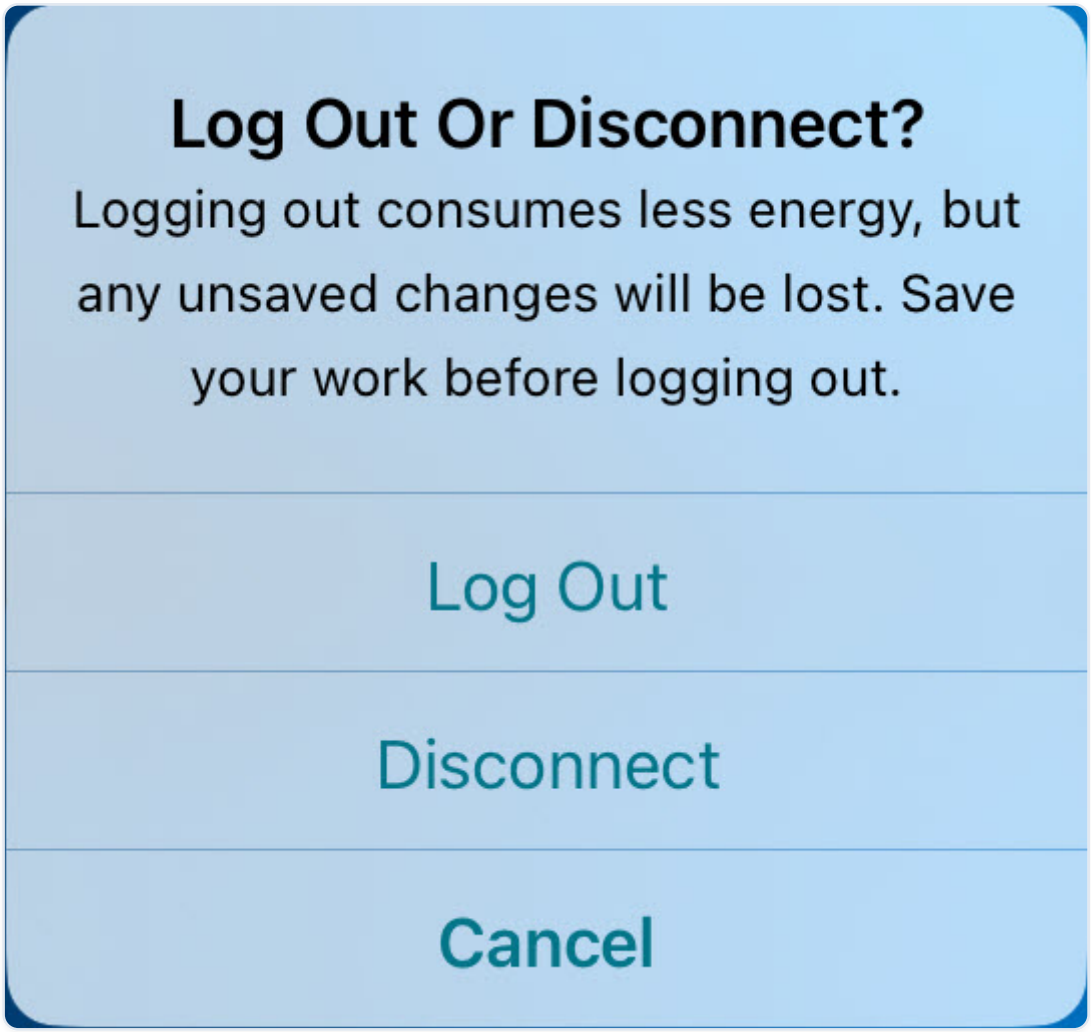
> Wenn Sie diese technische Vorschaufunktion nicht nutzen möchten, können Sie die Citrix Workspace-App jederzeit im Vollbildmodus verwenden.

Unterstützung für Nachhaltigkeitsinitiative

Ab Version 24.9.0 sehen Benutzer eine Aufforderung, sich von ihrer Desktopsitzung abzumelden, wenn sie einen virtuellen Desktop schließen. Diese Funktion hilft, Energie zu sparen, indem sie sich von VMs abmeldet, wenn diese nicht benötigt werden. Zuvor blieben diese Sitzungen in einem getrennten Zustand, was zu unnötigem Energieverbrauch führte.

Beim Trennen einer Sitzung, ohne dass die Nachhaltigkeitsfunktion aktiviert ist, sehen Benutzer eine Aufforderung mit der Option **trennen und Nicht erneut fragen** für automatische zukünftige Trennungen. Dieser Standardtext ist lokalisiert.

Wenn Benutzer bei aktivierter Nachhaltigkeitsfunktion die Verbindung trennen, fordert das System sie auf, sich **abzumelden**, um Energie zu sparen. Als Administrator können Sie die Nachhaltigkeitsmeldung anpassen.



Administratoren können wählen, ob sie die Nachhaltigkeitswarnung, die ein Blattsymbol enthält, anzeigen und den Titel sowie die Aufforderung anpassen möchten. Wenn der Administrator keinen Titel oder keine Aufforderung angibt und das Blattsymbol deaktiviert, während die Nachhaltigkeitsfunktion aktiviert ist, erscheint eine Standardmeldung: **trennen Desktop? Ihre Arbeit bleibt so erhalten, wie Sie sie verlassen haben, wenn Sie sich das nächste Mal mit dem verwalteten %@ Desktop verbinden**. Das **%@** wird durch den Namen der Virtual Desktop-App ersetzt. Diese Standardmeldungen sind lokalisiert.

Beachten Sie, dass von Administratoren konfigurierte Nachrichten nicht lokalisiert werden. Administratoren müssen daher für Klarheit und Genauigkeit in ihren Texten sorgen.

Weitere Informationen zum Aktivieren und Anpassen dieser Funktion finden Sie unter Nachhaltigkeitsinitiative der Citrix Workspace-App in der Dokumentation zur Citrix Workspace-App für Windows.

Verbesserte Multi-App-Fensterverwaltung

Ab Version 24.9.0 unterstützt die Citrix Workspace-App für iOS jetzt eine nahtlose Multi-App-Fensterverwaltung für iPads, die an externe Monitore angeschlossen sind. Diese Funktion verbessert Multitasking und Produktivität, indem sie native Multi-App-Erlebnisse ermöglicht. Sie kann auch aktiviert werden, wenn das iPad-Gerät nicht an externe Monitore angeschlossen ist.

Mit dieser Funktion können Sie:

- Wechseln Sie zwischen Anwendungen und öffnen Sie eine einzelne App in separaten Fenstern, um den Workflow und die Produktivität zu verbessern.
- Verwenden Sie mehrere Apps in einer Sitzung, während Sie mit externen Monitoren verbunden sind.

Um die nahtlose Multi-App zu aktivieren, führen Sie die folgenden Schritte aus:

1. Gehen Sie zu **Anwendungseinstellungen** > **Erweitert** > **Multitasking**.
2. Aktivieren Sie **Separates Sitzungsfenster**.
3. Aktivieren Sie **Mehrere Fenster für nahtlose App-Sitzung**.

Einschränkung:

- Stage Manager muss auf Geräten aktiviert sein und während der Nutzung aktiviert bleiben.

- Nach dem Start wird möglicherweise eine graue Überlagerung angezeigt und das HDX-Sitzungsfenster erscheint. Dies geschieht, während der Server gestartet wird. Nach ein paar Sekunden/Minuten können die Benutzer das App-Bild sehen und normal verwenden.
- Diese Funktion ist nur auf Stage Manager-unterstützten Geräten wie z. B. mit Apple Silicon Chip ausgestatteten iPads verfügbar.

Problembehandlung

So überprüfen Sie die App-Version

Um Ihre Citrix Workspace-App-Version zu überprüfen, öffnen Sie die App. Tippen Sie auf **Einstellungen** > **Info**. Die Versionsinformationen werden auf Ihrem Bildschirm angezeigt.



So aktualisieren Sie die Citrix Workspace-App auf die neueste Version

Sie können die Citrix Workspace-App im App Store auf die neueste Version aktualisieren. Suchen Sie nach der Citrix Workspace-App und tippen Sie auf die Schaltfläche **Aktualisieren**.

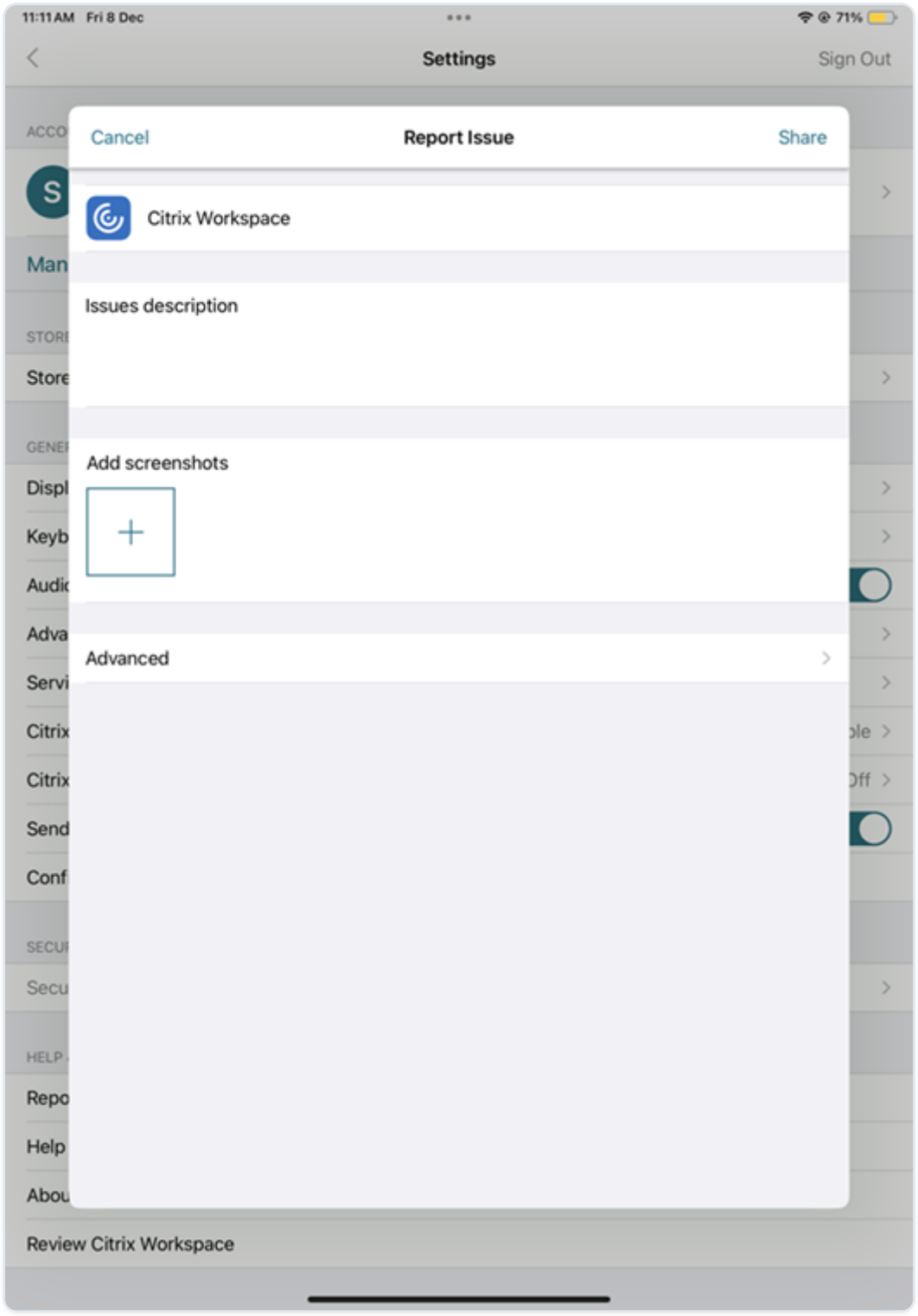
So setzen Sie die Citrix Workspace-App zurück

Sie können Ihre Citrix Workspace-App mit einer der folgenden Methoden zurücksetzen:

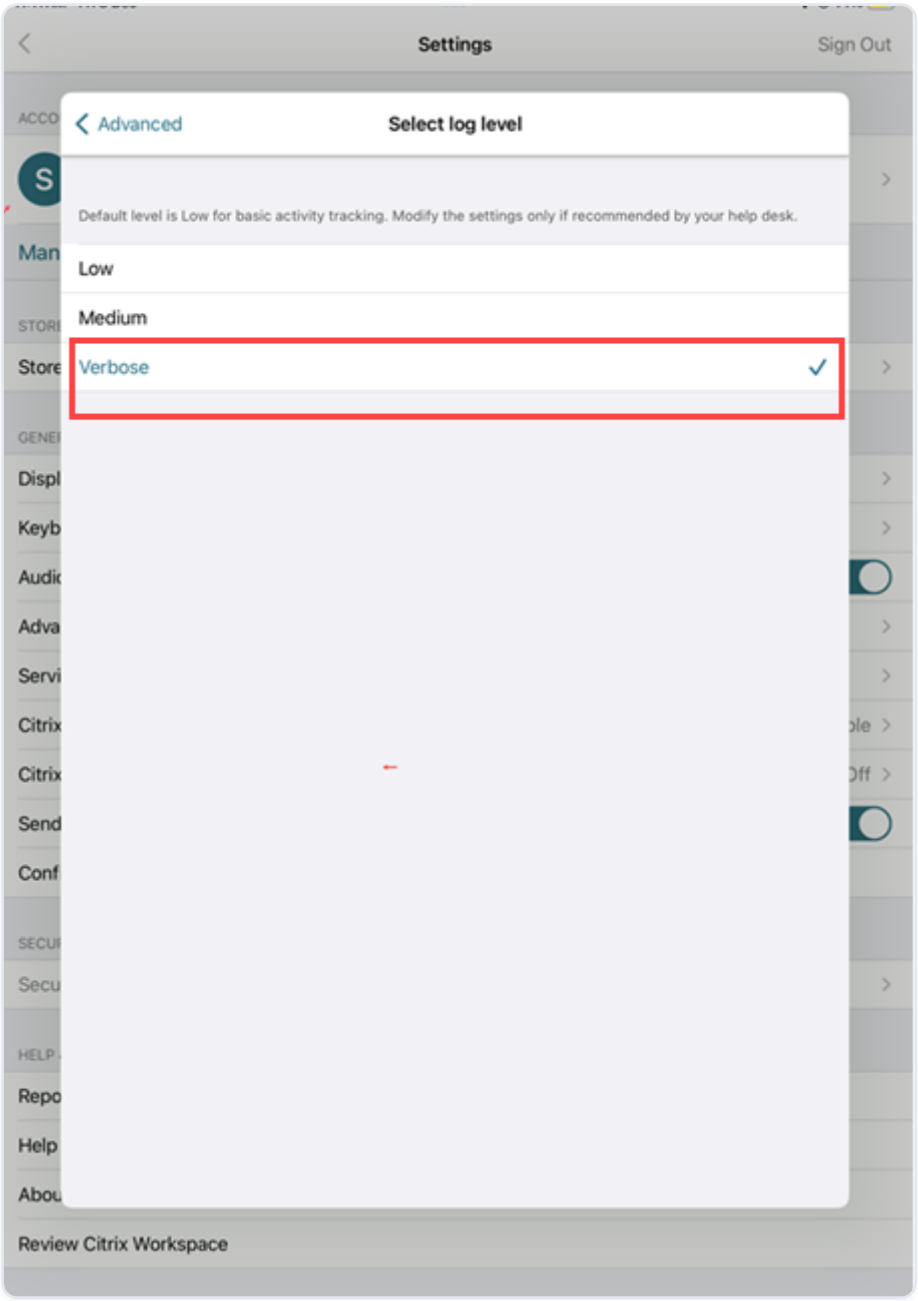
- Löschen Sie alle vorhandenen Konten aus der Citrix Workspace-App
- Löschen Sie die Speicherdaten der Citrix Workspace-App
- Deinstallieren Sie die Citrix Workspace-App und installieren Sie die neueste Citrix Workspace-App für iOS, die den neuesten Fix enthält.

So erfassen Sie Protokolle

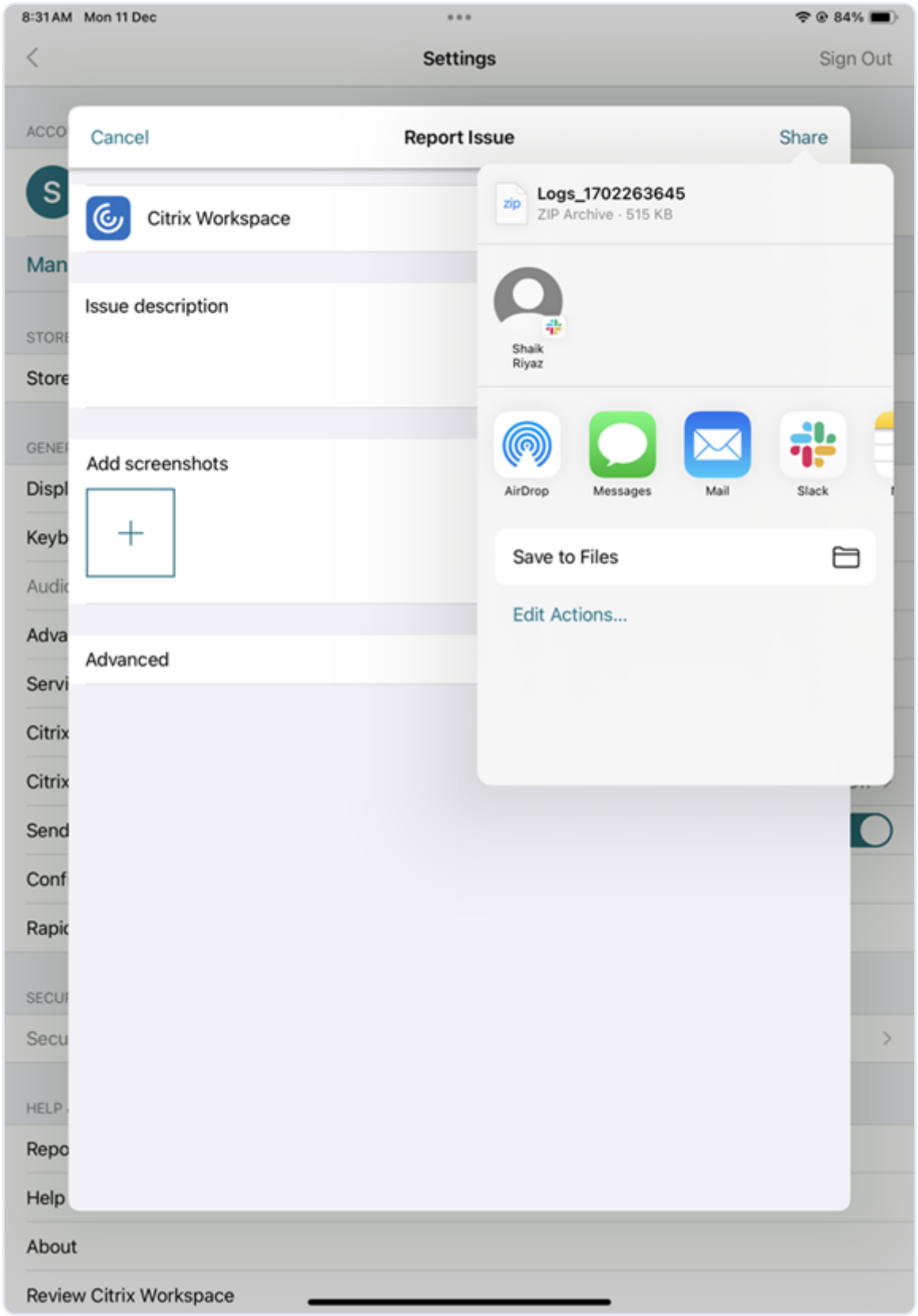
1. Öffnen Sie Ihre Citrix Workspace-App und navigieren Sie zu **Einstellungen**.
2. Wählen Sie unter **Hilfe & Support** die Option **Problem melden**.



3. Reproduzieren Sie Ihr Problem.
4. Wählen Sie auf der Seite „Protokollierungsstufe auswählen“ die Option **Ausführlich**.



5. Wählen Sie auf der Seite **Protokollspeicherort auswählen** die Option **Konsole & Datei**.
6. Teilen Sie die ZIP-Datei mit Citrix.



So fordern Sie Verbesserungen an

Sie können Ihre Anfragen für Verbesserungen per E-Mail an <ios_ear_support@citrix.com> senden.

So greifen Sie auf technische Vorschaufunktionen zu

Sie können technische Vorschaufunktionen per E-Mail unter <ios_ear_support@citrix.com> anfordern, die für jede Funktion einzigartig ist. Dieses Formular finden Sie als Anhang zur Ankündigung der technischen Vorschau in der Produktdokumentation.

So geben Sie Feedback zu EAR

Sie können EAR-Feedback per E-Mail an <ios_ear_support@citrix.com> geben.

Häufige Probleme und Tipps zur Fehlerbehebung

Getrennte Sitzungen

Benutzer können sich auf folgende Weisen von einer Citrix Workspace-App für iOS-Sitzung trennen (aber nicht abmelden):

- Beim Anzeigen einer veröffentlichten App oder eines Desktops in der Sitzung:
  - Tippen Sie auf den Pfeil oben auf dem Bildschirm, um das Dropdown-Menü in der Sitzung anzuzeigen.
  - Tippen Sie auf die Schaltfläche **Home**, um zum Launchpad zurückzukehren.
  - Beachten Sie den weißen Schatten unter dem Symbol einer der veröffentlichten Apps, die sich noch in einer aktiven Sitzung befinden; tippen Sie auf das Symbol.
  - Tippen Sie auf trennen.
- Citrix Workspace-App für iOS schließen:
  - Doppeltippen Sie auf die **Home**-Taste des Geräts.
  - Suchen Sie die Citrix Workspace-App für iOS in der iOS-App-Umschalteransicht.
  - Tippen Sie im angezeigten Dialogfeld auf trennen.
- Drücken der Home-Taste auf ihrem Mobilgerät.
- Tippen auf Home oder Switch im Dropdown-Menü der App.

Die Sitzung bleibt in einem getrennten Zustand. Obwohl der Benutzer später wieder eine Verbindung herstellen kann, können Sie überprüfen, ob getrennte Sitzungen nach einem bestimmten Intervall als inaktiv angezeigt werden.

Um die App im inaktiven Modus anzuzeigen, konfigurieren Sie ein Sitzungs-Timeout für die ICA-TCP-Verbindung in der Remote-Desktop-Sitzungshostkonfiguration (früher bekannt als „Terminaldienste-Konfiguration“).

Weitere Informationen zum Konfigurieren von Remotedesktopdiensten (früher bekannt als „Terminaldienste“) finden Sie in der Produktdokumentation von Microsoft Windows Server.

Abgelaufene Kennwörter

Die Citrix Workspace-App für iOS unterstützt die Möglichkeit für Benutzer, ihre abgelaufenen Kennwörter zu ändern. Es werden Aufforderungen angezeigt, in denen Benutzer die erforderlichen Informationen eingeben müssen.

Jailbroken-Geräte

Ihre Benutzer können die Sicherheit Ihrer Bereitstellung gefährden, indem sie sich mit Jailbreak-iOS-Geräten verbinden. Jailbreak-Geräte sind Geräte, die von ihren Besitzern modifiziert wurden, meist mit dem Ziel, bestimmte Sicherheitsvorkehrungen zu umgehen.

Wenn die Citrix Workspace-App für iOS ein Jailbreak-iOS-Gerät erkennt, zeigt die Citrix Workspace-App für iOS dem Benutzer eine Warnmeldung an.

Um Ihre Umgebung zusätzlich zu schützen, können Sie StoreFront oder Web Interface konfigurieren, um zu verhindern, dass erkannte Jailbreak-Geräte Apps ausführen.

Anforderungen

- Citrix Receiver für iOS 6.1 oder höher
- StoreFront 3.0 oder Web Interface 5.4 oder höher
- Zugriff auf StoreFront oder Web Interface über ein Administratorkonto

> **Hinweis:**

> Die Citrix Workspace™ App deaktiviert sich selbst, wenn sie ein Jailbreak-Gerät erkennt, um Daten zu schützen und die Sicherheit zu gewährleisten. Dadurch wird sichergestellt, dass die App nicht auf Geräten mit nicht autorisierten Modifikationen verwendet werden kann.

Verlust der HDX™-Audioqualität

Bei Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) kann die HDX-Audioqualität zur Citrix Workspace-App für iOS beeinträchtigt werden. Das Problem tritt auf, wenn Sie Audio und Video gleichzeitig verwenden.

Das Problem tritt auf, wenn die HDX-Richtlinien von Citrix Virtual Apps and Desktops™ und Citrix DaaS die Menge der Audiodaten zusammen mit den Videodaten nicht verarbeiten können.

Vorschläge zur Erstellung von Richtlinien zur Verbesserung der Audioqualität finden Sie im Knowledge Center-Artikel CTX123543.

Starten von Desktop- und App-Sitzungen für angepasste Store-Erfahrung fehlgeschlagen

Das Starten von Desktop- und App-Sitzungen über die Citrix Workspace-App kann fehlschlagen, wenn Sie eine angepasste Store-Erfahrung haben. Die automatische Erkennung des Store-Typs wird nur für E-Mail-Adressen und nicht für Store-URLs unterstützt. Es wird empfohlen, eine E-Mail-Adresse oder den Web-Interface-Anmeldemodus zu verwenden, wenn Sie einen angepassten Store haben. Weitere Informationen finden Sie unter Manuelle Einrichtung und Konfigurieren der E-Mail-basierten Kontoerkennung.

Um ein Konto manuell über den Web-Interface-Anmeldemodus zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Tippen Sie auf das **Kontosymbol > Kontobildschirm > Pluszeichen (+)**. Der Bildschirm **Neues Konto** wird angezeigt.
2. Tippen Sie in der unteren linken Ecke des Bildschirms auf das Symbol links neben **Optionen** und tippen Sie auf **Manuelle Einrichtung**. Andere Felder werden auf dem Bildschirm angezeigt.
3. Geben Sie im Feld **Adresse** die sichere URL der Site oder des Citrix Gateways ein (zum Beispiel agee.mycompany.com).
4. Wählen Sie die Verbindung **Webinterface** aus. Dieser Verbindungsmodus zeigt eine Citrix Virtual Apps™-Website an, die einem Webbrowser ähnelt. Diese Benutzeroberfläche ist auch als Web View bekannt.

   Webinterface(/en-us/citrix-workspace-app-for-ios/media/web-interface.png)
5. Verwenden Sie für die Zertifikatssicherheit die Einstellung im Feld **Zertifikatswarnungen ignorieren**, um festzulegen, ob Sie eine Verbindung zum Server herstellen möchten, selbst

wenn dieser ein ungültiges, selbstsigniertes oder abgelaufenes Zertifikat besitzt. Die Standardeinstellung ist AUS.

> **Wichtig:**
>
> Wenn Sie diese Option aktivieren, stellen Sie sicher, dass Sie eine Verbindung zum richtigen Server herstellen. Citrix empfiehlt dringend, dass alle Server über ein gültiges Zertifikat verfügen, um Benutzergeräte vor Online-Sicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt nicht, die Zertifikatssicherheit zu umgehen.

6. Tippen Sie auf **Speichern**.
7. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein (oder Token, wenn Sie die Zwei-Faktor-Authentifizierung ausgewählt haben), und tippen Sie dann auf Anmelden. Der Bildschirm der Citrix Workspace-App für iOS wird angezeigt, auf dem Sie auf Ihre Desktops zugreifen und Ihre Apps hinzufügen und öffnen können.

> **Hinweis:**
>
> Sie müssen die Benutzeranmeldeinformationen für jede Verbindung eingeben, da diese im Anmeldemodus des Webinterfaces nicht gespeichert werden.

Citrix Verbindungsproblembehandlung

Die Funktion Citrix Verbindungsproblembehandlung wurde entwickelt, um Endbenutzern die Möglichkeit zu geben, potenzielle Fehler beim Starten von Desktops oder Anwendungen effektiv selbst zu beheben. Diese Verbesserung zielt darauf ab, Benutzern klare Diagnosen, potenzielle Empfehlungen und die Möglichkeit zu bieten, Korrekturen mit einem einfachen Klick auszuführen.

Funktionsweise

Die Funktion liefert granularere und verbesserte Fehlermeldungen, um Benutzern zu helfen, die Grundursache von Startfehlern klar zu verstehen. Die Funktion Verbindungsproblembehandlung analysiert Verbindungsprobleme mit dem Virtual Delivery Agent (VDA) in Echtzeit während des Startvorgangs. Anschließend werden benutzerfreundliche Fehlermeldungen und Empfehlungen

angezeigt, die es Benutzern ermöglichen, das Problem entweder direkt zu beheben oder bei Bedarf Protokolle für ein Support-Ticket zu sammeln.

Analysierte Verbindungspfade

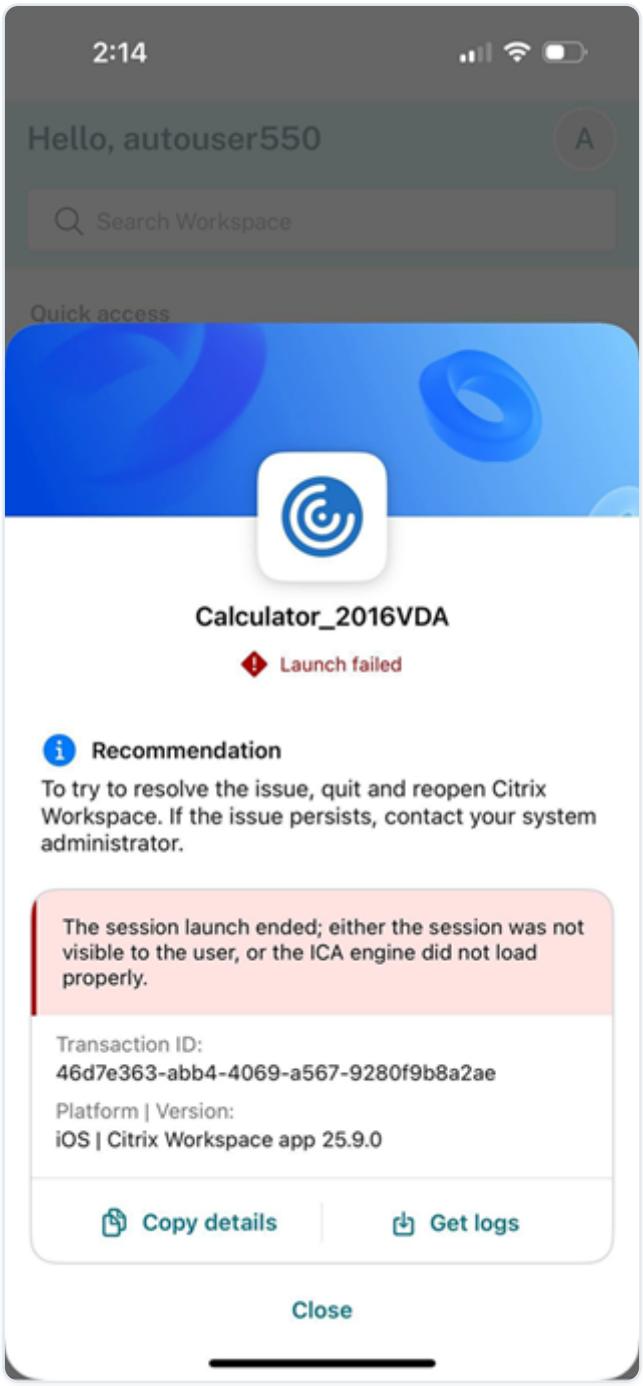
Die Funktion diagnostiziert potenzielle Startprobleme bei virtuellen Apps und Desktops über kritische Verbindungspunkte hinweg, einschließlich:

- Netzwerkkonnektivität vom Client zum Gateway.
- Verbindung vom Gateway zum StoreFront-Server.
- Verbindung vom StoreFront-Server zum Broker.
- Verbindung vom Broker zum VDA.

Verbesserte Fehlermeldungen und Diagnosen

Im Falle von Startfehlern zeigt Citrix jetzt klare, benutzerfreundliche Fehlermeldungen an, die spezifische Verbindungsprobleme wie Netzwerkfehler, Server-Nichtverfügbarkeit oder VDA-Fehler genau identifizieren. Für Administratoren werden detaillierte Fehlercodes in den Protokollen bereitgestellt, die in serverseitige und clientseitige Fehler kategorisiert sind und als wertvolle Referenzen für eine tiefere Untersuchung dienen.





Selbstwiederherstellung und Korrekturmaßnahmen

Die Funktion „Citrix Troubleshoot Connection“ enthält Schritte, die Benutzer unternehmen können, um sich automatisch von häufigen Problemen zu erholen und so den Bedarf an Support-Interventionen zu minimieren. Im Folgenden sind die potenziellen Probleme aufgeführt, die mit geführter Behebung gelöst werden können:

- VDA neu starten
- Citrix Workspace-App (CWA) neu starten – erneute Anmeldung bei CWA
- Ressourcenliste aktualisieren

- App aktualisieren und erneut versuchen
- Store neu konfigurieren
- CWA aktualisieren
- CWA neu installieren
- Netzwerk überprüfen
- Warten und erneut versuchen

Systemanforderungen

Um die Funktion zur Problembehandlung bei Verbindungen zu verwenden, benötigen Sie die folgenden Versionen der Citrix Workspace-App:

- **Citrix Workspace-App für iOS:** Version 2509 und höher

> **Hinweis:**

> Die Fehlermeldungen enthalten auch Serverfehlercodes. Details dazu für On-Premises und Cloud finden Sie im Abschnitt Fehlercodes

> Die Funktion zur Problembehandlung bei Verbindungen ist in DaaS-Umgebungen standardmäßig aktiviert. Detaillierte Fehlermeldungen und Empfehlungen sind sowohl für im Browser gestartete Sitzungen als auch für mit der Citrix Workspace-App gestartete Sitzungen verfügbar. Fehlercodes und Transaktions-IDs werden zu Referenzzwecken für Administratoren in Protokollen aufgezeichnet. Fehlercodes werden als serverseitig oder clientseitig kategorisiert. Für bestimmte Fehler wird eine Behebungsoption zum Neustart des Virtual Delivery Agent (VDA) bereitgestellt. Diese Funktion unterstützt keine Sitzungen im Hybridmodus. Sie kann beispielsweise nicht verwendet werden, wenn Sie eine ICA-Datei in einem Browser herunterladen und diese Datei dann mit der Citrix Workspace-App öffnen.

FAQs

So verbessern Sie die Videoleistung in virtuellen Apps und auf virtuellen Desktops für Geräte mit geringer Leistung oder mobile Geräte

Informationen zum Verbessern und Konfigurieren der Videoleistung virtueller Desktops mithilfe des Registrierungswerts MaxFramesPerSecond oder mithilfe von HDX-Richtlinien, abhängig von Ihrer Citrix Virtual Apps and Desktops-Version, finden Sie im Knowledge Center-Artikel CTX123543.

Ich kann meine Apps oder Desktops nach der Anmeldung bei der Citrix Workspace-App nicht sehen

Wenden Sie sich für weitere Unterstützung an den Helpdesk Ihres Unternehmens oder an den Administrator Ihres IT-Supportteams.

So beheben Sie Probleme mit langsamen Verbindungen

Wenn eines der folgenden Probleme auftritt, befolgen Sie die Schritte, die im folgenden Abschnitt **Problemumgehung** beschrieben sind.

- Langsame Verbindungen zur Citrix Virtual Apps and Desktops Site
- Fehlende App-Symbole
- Wiederkehrende Protokolltreiber-Fehlermeldungen

Problemumgehung

Deaktivieren Sie die Eigenschaften des Citrix PV Ethernet Adapters für die Netzwerkschnittstelle auf dem Citrix Virtual Apps-Server, Citrix Secure Web Gateway™ und dem Web Interface-Server. Die Eigenschaften des Citrix PV Ethernet Adapters umfassen die folgenden Eigenschaften, die standardmäßig aktiviert sind. Sie müssen alle diese Eigenschaften deaktivieren.

- Large Send Offload
- Offload IP-Prüfsumme
- Offload TCP-Prüfsumme
- Offload UDP-Prüfsumme

> **Hinweis:**
>
> Ein Serverneustart ist nicht erforderlich. Diese Problemumgehung gilt für Windows Server 2003 und 2008 (32-Bit). Dieses Problem betrifft Windows Server 2008 R2 nicht.

Problembehandlung bei numerischen Tasten und Sonderzeichen

Wenn numerische Tasten oder chinesische IME-Zeichen nicht wie erwartet funktionieren, müssen Sie die Option „Unicode-Tastatur“ deaktivieren. So deaktivieren Sie die Option „Unicode-Tastatur“:

1. Navigieren Sie zu **Einstellungen** > **Tastaturoptionen**.
2. Stellen Sie **Unicode-Tastatur verwenden** auf **Aus**.

Citrix Workspace-App für iOS

Die Citrix Workspace-App für iOS ist eine Client-Software, die im App Store zum Download verfügbar ist. Sie ermöglicht Ihnen den Zugriff und die Ausführung virtueller Desktops und gehosteter Anwendungen, die von Citrix Virtual Apps and Desktops bereitgestellt werden.

iOS ist das Betriebssystem für mobile Apple-Geräte wie iPads und iPhones. Die Citrix Workspace-App für iOS läuft auf Geräten mit dem iOS-Betriebssystem, wie iPhone X, iPad mini und iPad Pro.

Sprachunterstützung

Die Citrix Workspace-App für iOS ist für die Verwendung in anderen Sprachen als Englisch angepasst. Eine Liste der von der Citrix Workspace-App für iOS unterstützten Sprachen finden Sie unter Sprachunterstützung.

Einstellung

Die Ankündigung in diesem Artikel informiert Sie vorab über Plattformen, Citrix®-Produkte und Funktionen, die eingestellt werden, damit Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Kundennutzung und das Feedback, um zu bestimmen, wann diese zurückgezogen werden. Ankündigungen können sich in nachfolgenden Releases ändern und möglicherweise nicht jede veraltete Funktion oder Funktionalität umfassen.

Veraltete Elemente werden nicht sofort entfernt. Citrix unterstützt sie in diesem Release weiterhin, aber sie werden in Zukunft entfernt.

ELEMENT	EINSTELLUNG ANGEKÜNDIGT IN	ENTFERNT IN	ALTERNATIVE
iOS-Betriebssystemversion 17	Citrix Workspace-App für iOS Version 26.9.0	Citrix Workspace-App für iOS Version 26.9.0	Upgrade auf die neueste verfügbare iOS-Version
Auto-Configure, XenApp Services und Access Gateway	Citrix Workspace-App für iOS Version 26.7.0	Citrix Workspace-App für iOS 26.11.0	-

CITRIX WORKSPACE™-APP FÜR IOS

ELEMENT	EINSTELLUNG ANGEKÜNDIGT IN	ENTFERNT IN	ALTERNATIVE
EDT-Einstellung zulassen	Citrix Workspace-App für iOS Version 26.7.0	Citrix Workspace-App für iOS 27.3.0	Als Admin-Einstellung verfügbar
Citrix X1-Maus	Citrix Workspace-App für iOS Version 25.9.0	Citrix Workspace-App für iOS 26.3.0	-
Citrix Casting	Citrix Workspace-App für iOS Version 25.9.0	Citrix Workspace-App für iOS 26.3.0	-
iOS-Betriebssystem Version 16	Citrix Workspace-App für iOS Version 25.7.2	Citrix Workspace-App für iOS 25.7.2	Upgrade auf die neueste verfügbare iOS-Version
iOS-Betriebssystem Version 15	Citrix Workspace-App für iOS Version 24.7.0	Citrix Workspace-App für iOS 24.12.0	Upgrade auf die neueste verfügbare Version von iOS
Unterstützung für DTLS 1.0-Protokoll	Citrix Workspace-App für iOS Version 24.5.0	-	DTLS 1.2-Protokoll
Unterstützung für TLS 1.0- und TLS 1.1-Protokolle	Citrix Workspace-App für iOS Version 24.4.0	Citrix Workspace-App für iOS Version 25.3.0	TLS 1.2- oder TLS 1.3-Protokoll
XenApp Services (auch bekannt als PNAgent)	Citrix Workspace-App für iOS Version 23.7.5	-	Innerhalb der Citrix Workspace-App stellen Sie eine Verbindung zu Stores her, indem Sie die Store-URL anstelle der XenApp Services-URL verwenden.

CITRIX WORKSPACE™-APP FÜR IOS

ELEMENT	EINSTELLUNG ANGEKÜNDIGT IN	ENTFERNT IN	ALTERNATIVE
iOS-Betriebssystem Version 14	Citrix Workspace-App für iOS Version 23.10.0	Ziel: Citrix Workspace-App für iOS 23.12.0	Auf die neueste verfügbare iOS-Version aktualisieren
iOS-Betriebssystemversion 13.x	Citrix Workspace-App für iOS Version 22.9.5	Ziel: Dezember 2022 und Version 22.12.0	Auf die neueste verfügbare iOS-Version aktualisieren
iOS-Betriebssystemversion 11.x und 12.x	Citrix Workspace-App für iOS Version 21.12.0	Ziel: August 2022 und Version 22.8.0	Auf die neueste verfügbare iOS-Version aktualisieren
iOS-Betriebssystemversion 10.x	Citrix Workspace-App für iOS Version 21.1.5	Release nach 21.1.5	Verwenden Sie die Citrix Workspace-App für iOS Version 21.1.5 oder früher

Hinweise:

- Bestehende Benutzer der Citrix Workspace™-App auf veralteten Plattformversionen können nicht auf die neueste Version (aus dem App Store) der Citrix Workspace-App aktualisieren.
- Neue Benutzer der Citrix Workspace-App auf veralteten Plattformversionen können nur eine ältere kompatible Version aus dem App Store herunterladen.
- Benutzer auf veralteten Plattformversionen erhalten keine neuen Funktionen oder Sicherheitspatches, die mit jeder neueren Version der Citrix Workspace-App einhergehen.