Citrix Workspace-App für iOS

Contents

Citrix Workspace-App für iOS

July 1, 2024

Die Citrix Workspace-App für iOS ist Clientsoftware, die im App Store zum Download verfügbar ist. Hiermit können Sie auf virtuelle Desktops und gehostete Anwendungen, die mit Citrix Virtual Apps and Desktops bereitgestellt werden, zugreifen und diese ausführen.

iOS ist das Betriebssystem für Mobilgeräte von Apple, wie iPads und iPhones. Die Citrix Workspace-App für iOS kann auf Geräten mit dem iOS-Betriebssystem, wie iPhone X, iPad mini und iPad Pro, ausgeführt werden.

Detaillierte Informationen zu den Features, behobenen Problemen und bekannten Problemen finden Sie auf der Seite Über dieses Release.

Informationen zu veralteten Elementen finden Sie auf der Seite Einstellung von Features und Plattformen.

Sprachunterstützung

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

Referenz

- Tech Brief: Citrix Workspace
- Global App Configuration Service
- Workspace-Benutzeroberfläche
- Optimierung von Microsoft Teams in Citrix Virtual Apps and Desktops-Umgebungen
- Citrix Workspace-App – Releasezeitplan
- Developer Documentation

Neue Features in verwandten Produkten

- Citrix Workspace
- Citrix DaaS
- StoreFront
- Secure Private Access
- Citrix Workspace-App für Mac

Legacy-Dokumentation

Informationen zu Produktversionen, die das Ende der Lebensdauer erreicht haben, finden Sie in der Legacy-Dokumentation.

Info zu diesem Release

July 1, 2024

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

> **Hinweis:**
>
> Suchen Sie nach Technical Previews? Wir haben sie für Sie in einer übersichtlichen Liste zusammengefasst. Sehen Sie sich die Seite Features in Technical Previews an, und teilen Sie uns Ihr Feedback per Podio-Formular mit.

Was ist neu in 24.5.0

Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit Cloudstores

Ab der Version 24.5.0 können sich Benutzer bei der Citrix Workspace App mit FIDO2-basierter kennwortloser Authentifizierung authentifizieren, wenn sie sich mit einem Cloudspeicher verbinden. FIDO2 bietet eine nahtlose Authentifizierungsmethode, mit der Unternehmensmitarbeiter innerhalb virtueller Sitzungen auf Apps und Desktops zugreifen können, ohne dass sie einen Benutzernamen oder ein Kennwort eingeben müssen. Dieses Feature unterstützt sowohl Roaming (nur USB) als auch Plattformauthentifikatoren (PIN-Code, Touch ID und nur Face ID). Dieses Feature ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit On-Premises-Stores.

> **Hinweis:**
>
> Die FIDO2-Authentifizierung wird standardmäßig mit den benutzerdefinierten Chrome-Tabs unterstützt. Wenn Sie daran interessiert sind, die FIDO2-Authentifizierung mit WebView zu verwenden, registrieren Sie Ihr Interesse über Podio-Formular.

Unterstützung für Dokumentenscanner

Ab der Version 24.5.0 unterstützt die Citrix Workspace-App für iOS das Dokumentenscannerfeature. Mit diesem Feature können Sie jetzt mehrere Dokumente innerhalb der Desktopsitzung scannen und

speichern. Dieses Feature ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Unterstützung für Dokumentenscanner.

Ankündigung der Einstellung des DTLS 1.0-Protokolls Citrix plant, die Unterstützung für das DTLS 1.0-Protokoll in zukünftigen Versionen einzustellen. Das alternative Protokoll ist DTLS 1.2. Weitere Informationen finden Sie unter Einstellung von Features und Plattformen.

Technical Preview

- Unterstützung für Single Sign-On für virtuelle Maschinen, die mit Microsoft Entra ID verbunden sind
- Unterstützung der Durchsetzung der biometrischen Authentifizierung für den Zugriff auf die Citrix Workspace-App

Eine Liste aller Features in Technical Previews finden Sie auf der Seite Features in Technical Previews.

Behobene Probleme in 24.5.0

- Möglicherweise stellen Sie fest, dass der Text nicht korrekt gescannt werden kann, wenn Sie den Barcodescanner in der virtuellen Sitzung verwenden. [HDX-63675]

Bekannte Probleme in 24.5.0

Möglicherweise stellen Sie fest, dass das Trackpad auf dem Magic Keyboard in der virtuellen Sitzung auf einem iPad Pro M4-Gerät nicht richtig funktioniert. Um das Problem zu umgehen, können Sie eine externe Maus (entweder kabelgebundener USB-Typ-C-Anschluss oder Bluetooth) verwenden, um in der virtuellen Sitzung auf dem Bildschirm zu navigieren. [HDX-66083]

Frühere Releases

Dieser Abschnitt enthält Informationen zu neuen Features und behobenen Problemen in den früheren Versionen, die wir unterstützen. Weitere Informationen zum Lebenszyklus dieser Releases finden Sie unter Lifecycle Milestones for Citrix Workspace app and Citrix Receiver.

24.4.0

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Ankündigung der Einstellung der Protokolle TLS 1.0 und TLS 1.1 Citrix plant, die Unterstützung für die Protokolle TLS 1.0 und TLS 1.1 in zukünftigen Versionen einzustellen. Das alternative Protokoll ist TLS 1.2 oder TLS 1.3. Weitere Informationen finden Sie unter Einstellung von Features und Plattformen.

Behobene Probleme

- Wenn Sie die Gerätekamera in der Virtual App-Sitzung öffnen, wird die Citrix Workspace-App für iOS möglicherweise unerwartet geschlossen. [CVADHELP-24825]

Bekannte Probleme

Es gibt keine neuen bekannten Probleme.

24.3.5

Was ist neu

Unterstützung für das Twocanoes Smart Card Utility-Lesegerät Ab Version 24.3.5 unterstützt die Citrix Workspace-App für iOS die Lesegeräte für Twocanoes Smart Card Utility. Weitere Informationen zu unterstützten Smartcardlesern finden Sie unter Smartcards.

> **Hinweis:**
>
> Das USB-C-Lesegerät von Twocanoes Smart Card Utility wird sowohl für die Anmeldung in der Citrix Workspace-App als auch für die Anmeldung in virtuellen Sitzungen unterstützt. Das Bluetooth-Lesegerät von Twocanoes Smart Card Utility wird jedoch nur für die Anmeldung in der Citrix Workspace-App und nicht für die Anmeldung in virtuellen Sitzungen unterstützt.

Unterstützung für die Konfiguration des Gerätenamens über UEM Ab der Version 24.3.5 können Administratoren mit der Citrix Workspace-App für iOS Gerätenamen anhand von Benutzergruppen über Unified Endpoint Management (UEM) zuweisen und identifizieren. Weitere Informationen finden Sie unter Unterstützung für die Konfiguration des Gerätenamens über UEM.

Technical Preview

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

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

Behobene Probleme

In dieser Version wurde die allgemeine Leistung und Stabilität verbessert.

Bekannte Probleme

Es gibt keine neuen bekannten Probleme.

24.3.0

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Technical Preview

- Unterstützung für adaptives Audio

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

Behobene Probleme

Nach dem Upgrade von Citrix Workspace-App für iOS auf Version 24.1.0 schlägt die Tastatureingabe über die virtuelle Tastatur in der Sitzung für Anwendungen, die auf der Oracle Java Web Start-Software basieren, möglicherweise fehl. [CVADHELP-24645]

Bekannte Probleme

Es gibt keine neuen bekannten Probleme.

24.2.0

Was ist neu

Unterstützung für das gleichzeitige Löschen mehrerer Stores Ab der Version 24.2.0 unterstützt Citrix Workspace-App für iOS das Auswählen und Löschen mehrerer Stores. Diese Funktion verbessert die Benutzerfreundlichkeit bei der Arbeit mit mehreren Stores. Dieses Feature ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Unterstützung für das gleichzeitige Löschen mehrerer Stores.

Unterstützung für Administratoren, um den Benutzer daran zu hindern, den Storenamen zu ändern Bisher konnten Benutzer den Storenamen mithilfe der Option **Konto bearbeiten** ändern.

Ab 24.2.0 bietet Citrix Workspace-App für iOS Administratoren die Möglichkeit, den Benutzer daran zu hindern, den Storenamen zu ändern. Mit dieser Funktion können Administratoren die Storenamen leicht identifizieren und konsistent halten. Weitere Informationen finden Sie unter Unterstützung für Administratoren, um den Benutzer daran zu hindern, den Storenamen zu ändern.

Storenamen automatisch ausfüllen Ab der Version 24.2.0 unterstützt Citrix Workspace-App für iOS Aktualisierungen von Storenamen durch den Administrator und überträgt die aktualisierten Storenamen automatisch an den Benutzer. Diese Funktion verbessert die Benutzererfahrung, da kein manuelles Eingreifen bei der Aktualisierung des Storenamens erforderlich ist. Weitere Informationen finden Sie unter Storenamen automatisch ausfüllen.

> **Hinweis:**
>
> Dieses Feature kann nur wirksam werden, wenn der Administrator das Ändern des Storenamens durch den Benutzer gesperrt hat.

Technical Preview

- Unterstützung für Bedienungshilfen und VoiceOver

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

Behobene Probleme

In dieser Version wurde die allgemeine Leistung und Stabilität verbessert.

Bekannte Probleme

Es gibt keine neuen bekannten Probleme.

24.1.0

Was ist neu

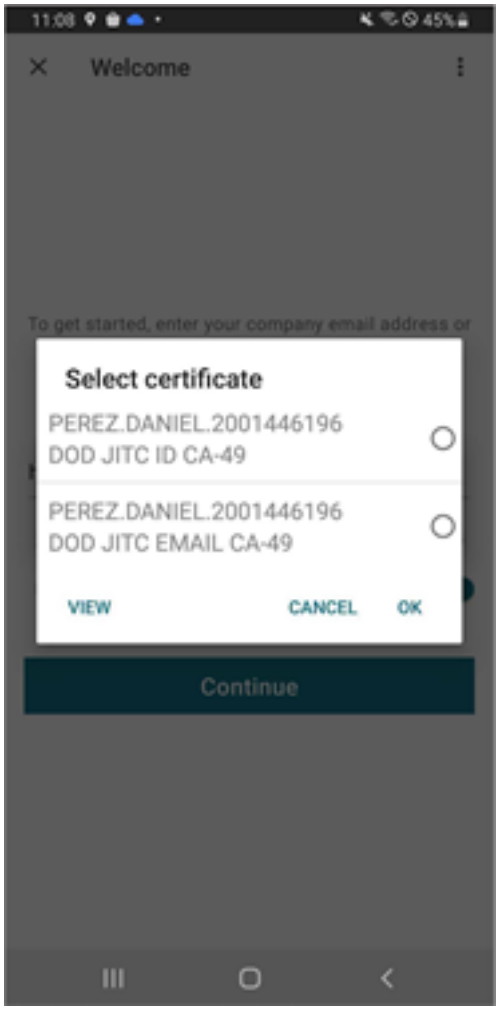
Sicherheitsupdate Diese Version enthält wichtige Sicherheitsupdates und Korrekturen für Sicherheitsprobleme.

Unterstützung für die Konfiguration der Speicherung von Authentifizierungstoken in der On-Premises-Bereitstellung Die Citrix Workspace-App für iOS bietet jetzt die Option, die Speicherung von Authentifizierungstoken auf dem lokalen Datenträger für On-Premises-Stores zu konfigurieren. Mit diesem Feature können Sie die Speicherung des Authentifizierungstokens für die erhöhte Sicherheit deaktivieren. Nach der Deaktivierung müssen Sie sich beim Neustart des Systems oder der Sitzung erneut authentifizieren, um auf die Sitzung zugreifen zu können. Weitere Informationen finden Sie unter Unterstützung für die Konfiguration der Speicherung von Authentifizierungstoken in der On-Premises-Bereitstellung.

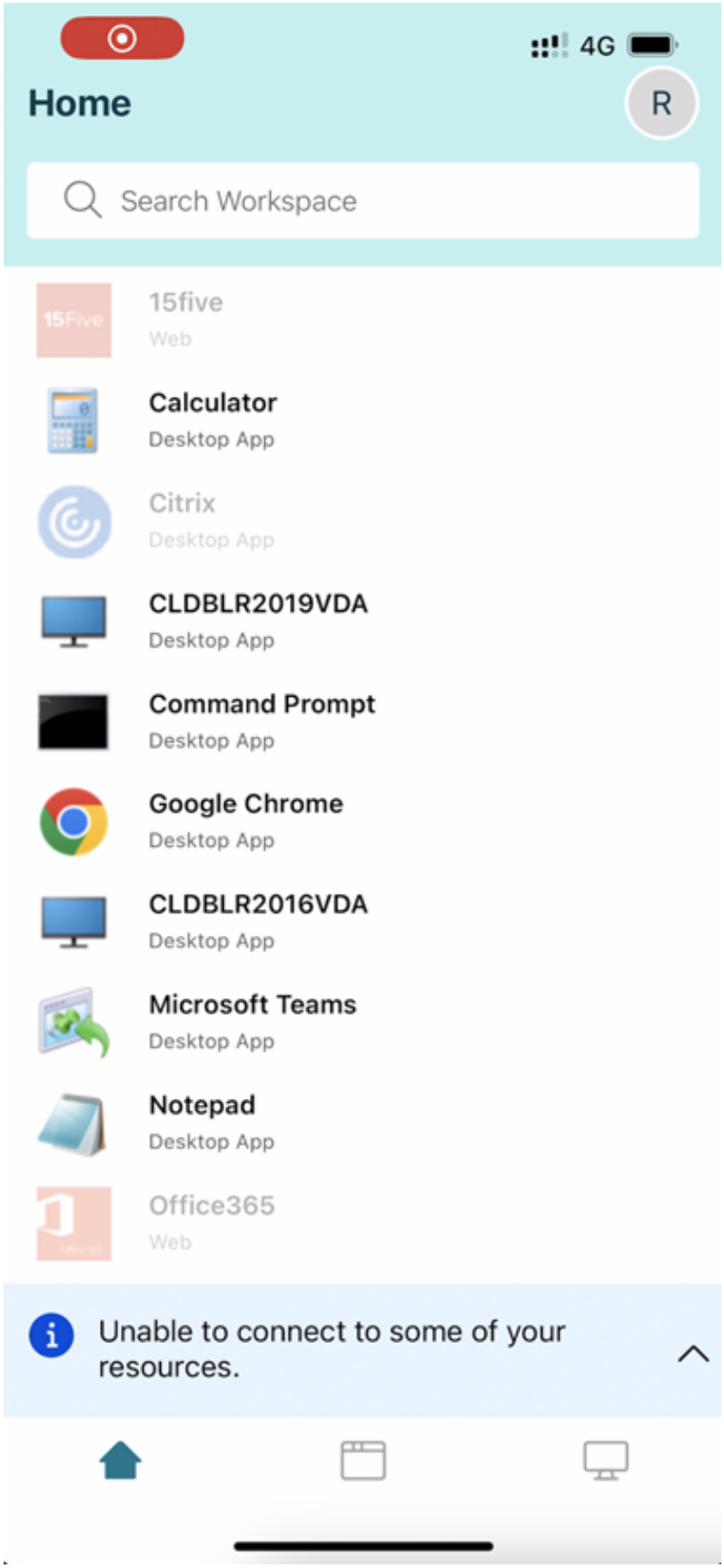
Unterstützung für mehrere Cloudstores Ab Version 24.1.0 können Sie der Citrix Workspace-App für iOS und iPadOS mehrere Cloudstorekonten hinzufügen. Damit können Endbenutzer einfacher mehrere Stores hinzufügen und zwischen ihnen wechseln. Das Feature verbessert die Benutzererfahrung beim Zugriff auf mehrere Stores. Weitere Informationen finden Sie unter Unterstützung für mehrere Cloudstores.

Unterstützung für mehrere Zertifikate bei der Smartcardauthentifizierung Bisher zeigte die Citrix Workspace-App für iOS das Zertifikat an, das auf dem ersten Steckplatz der verbundenen Smartcard verfügbar war.

Ab Version 24.1.0 zeigt die Citrix Workspace-App für iOS jetzt alle auf der Smartcard verfügbaren Zertifikate an und ermöglicht es Ihnen, das erforderliche Zertifikat bei der Authentifizierung über die Smartcardauthentifizierung auszuwählen. Weitere Informationen finden Sie unter Unterstützung für mehrere Zertifikate bei der Smartcardauthentifizierung.



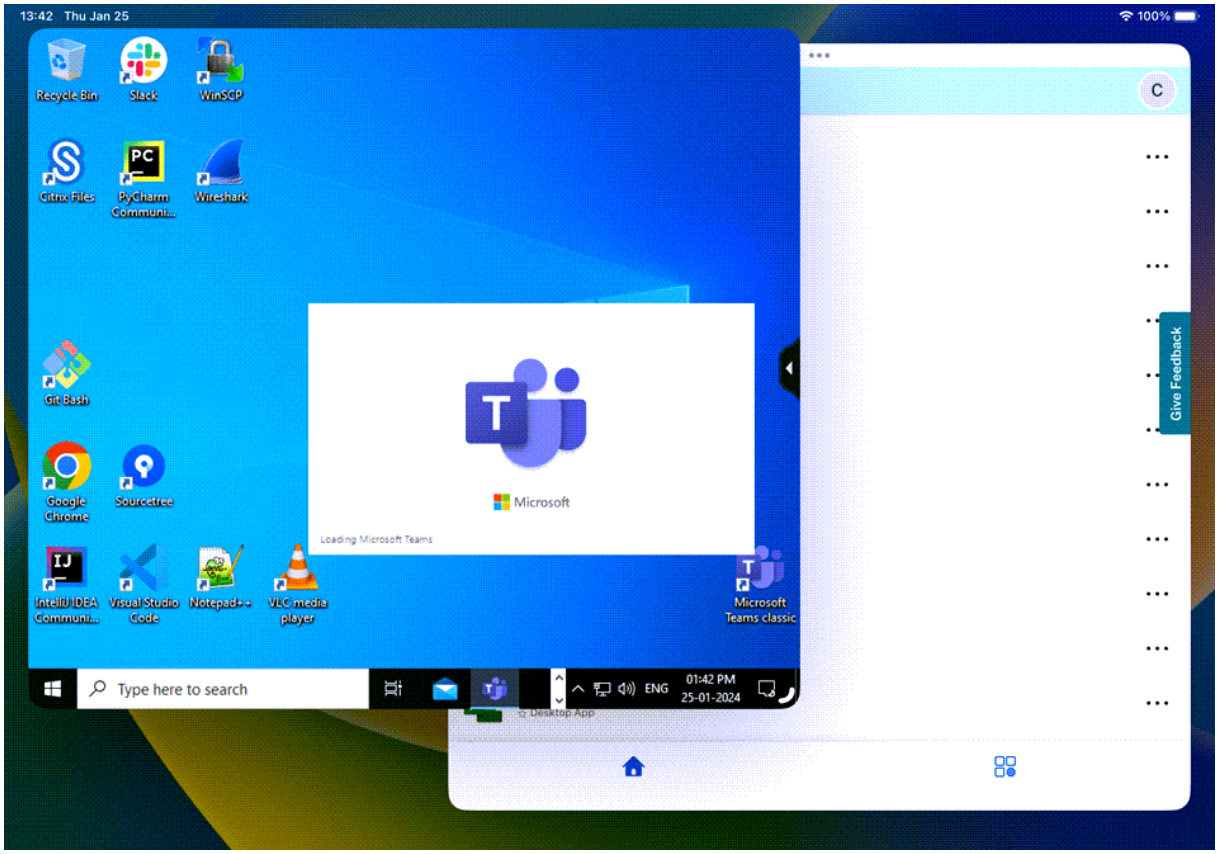
Die Benutzeroberfläche für den Servicekontinuität-Offlinemodus wurde verbessert Ab Version 24.1.0 wurde die Benutzeroberfläche der Citrix Workspace-App für iOS verbessert, um sie informativer und moderner zu gestalten sowie bei Ausfällen von Citrix Workspace ein besseres Benutzererlebnis zu gewährleisten. Die Fuzzy-Suchfunktion steht auch für den Offlinemodus zur Verfügung. Mit dieser Funktion können Sie die Ergebnisse für Apps oder Desktops mit fast übereinstimmendem Text und falsch geschriebenen Suchbegriffen finden. Weitere Informationen zur Servicekontinuität finden Sie unter Servicekontinuität.



Unterstützung für ein separates Sitzungsfenster von der Citrix Workspace-App Ab Version 24.1.0 bietet die Citrix Workspace-App für iOS ein separates Sitzungsfenster, das Multitasking effizienter und benutzerfreundlicher macht. Mit diesem Feature entsteht ein Desktop-ähnliches Erlebnis. Wenn das Feature 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.

> **Hinweis:**
>
> Diese Funktion wird nur auf Geräten unterstützt, die das Stage Manager-Feature unterstützen. Alle iPhone-Geräte und einige iPad-Geräte unterstützen dieses Feature nicht. Weitere Informationen zum State Manager-Feature finden Sie in der Apple Support-Dokumentation unter Stage Manager auf dem iPad ein- oder ausschalten.

Weitere Informationen finden Sie unter Unterstützung für ein separates Sitzungsfenster von der Citrix Workspace-App.



Unterstützung für den Scancode-Eingabemodus Ab Version 24.1.0 können Sie **Scancode** als Tastatureingabemodus auswählen, wenn Sie eine externe physische Tastatur verwenden. Dieses Feature ist hilfreich, wenn Sie iOS-Geräte mit der Standardtastatur eines externen Windows-PCs verwenden.

Mit **Scancode** können Sie das Tastaturlayout des VDA anstelle der iOS-Softtastatur verwenden. Auf diese Weise können Sie dem Eingabestil der externen Windows-Tastatur anstelle von iOS vollständig folgen. Dies ist bei der Eingabe in ostasiatischen Sprachen von Vorteil, da es die allgemeine Benutzererfahrung erheblich verbessert. Die Endbenutzer stellen möglicherweise fest, dass sie das Tastaturlayout des Servers anstelle des Clientlayouts verwenden. Weitere Informationen finden Sie unter Unterstützung für den Scancode-Eingabemodus.

Erweiterung der Unterstützung für externe Tastenkombinationen Mit der Citrix Workspace-App für iOS können Sie jetzt in einer Remotedesktop- oder App-Sitzung mehr Tastenkombinationen von externen Tastaturen verwenden. Die folgenden wichtigen Verbesserungen wurden an externen Tastenkombinationen vorgenommen:

- Unterstützung für Windows-spezifische Tasten wie `Insert`, `Delete` und Ziffernblock.
- Wenn Sie eine Taste gedrückt halten und nicht loslassen, reagiert der Remotedesktop / die App korrekt.
- Unterstützt Tastenkürzel mit mehr als drei Tasten.

Darüber hinaus können Sie jetzt die spezifische Taste für `Alt` konfigurieren, indem Sie die folgenden Optionen über **Einstellungen > Tastaturoptionen > Zuweisen einer bestimmten Taste für Alt** verwenden:

- `Option or Alt (left)`: Sendet `Alt` mit `Option (left)` `or Alt (left)`.
- `Command or Windows (left)`: Sendet `Alt` mit den Tasten `Command (left)` `or Windows (left)`.
- `Option or Alt (left and right)`: Sendet `Alt` mit den Tasten `Option or Alt (left and right)`.

Das Zuweisen einer bestimmten Taste für die Alt-Option hilft, Konflikte zwischen der macOS-Taste "`Option`"und der Windows-Taste "`Alt`"zu vermeiden.

Weitere Informationen finden Sie unter Erweiterung der Unterstützung für externe Tastenkombinationen.

Verbesserte Grafikleistung Ab der Version 24.1.0 unterstützt die Citrix Workspace-App für iOS die hardwarebeschleunigte H.264-Videokodierung oder -dekodierung. Die Multimediaengine von Citrix HDX verwendet jetzt das Video Toolbox-Framework von Apple zur Codierung und Decodierung. Dieses Framework komprimiert und dekomprimiert Video schneller und in Echtzeit. Diese Erweiterung reduziert die CPU-Last bei der Multimedianutzung. Weitere Informationen finden Sie unter Verbesserte Grafikleistung.

Behobene Probleme

In dieser Version wurde die allgemeine Leistung und Stabilität verbessert.

Bekannte Probleme

- Nach dem Upgrade von Citrix Workspace-App für iOS auf Version 24.1.0 schlägt die Tastatureingabe über die virtuelle Tastatur in der Sitzung für Anwendungen, die auf der Oracle Java Web Start-Software basieren, möglicherweise fehl. [CVADHELP-24645]

23.12.1

Neue Features

YubiKey-Unterstützung für Smartcardauthentifizierung Sie können jetzt die Smartcardauthentifizierung mit YubiKey durchführen. Dieses Feature bietet eine Einzelgeräteauthentifizierung für die Citrix Workspace-App, für virtuelle Sitzungen und veröffentlichte Apps in der VDA-Sitzung. Damit wird der Anschluss von Smartcardlesern oder anderen externen Authentifikatoren überflüssig. Für Endbenutzer ist dies benutzerfreundlicher, weil YubiKey eine Vielzahl von Protokollen wie OTP, FIDO usw. unterstützt.

Zum Anmelden bei der Citrix Workspace-App stecken Sie den YubiKey in Ihr iPhone oder iPad, schalten den Smartcardschalter ein und geben ihre Store-URL an.

> **Hinweis:**
>
> Die Citrix Workspace-App für iOS unterstützt nur die YubiKey 5-Serie. Weitere Informationen zu YubiKey finden Sie in der Dokumentation zur YubiKey 5-Serie.

Unterstützung für generische Lesegeräte vom Typ C Die Citrix Workspace-App für iOS unterstützt jetzt Typ-C-CCID-konforme Lesegeräte für die Smartcardauthentifizierung. Bisher wurden nur Lightning-Port-konforme Lesegeräte unterstützt. Die Integration von Typ-C-Smartcardleser 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.

Gerätenamen über UEM konfigurieren Mit dieser Version ist ein neuer Parameter namens deviceName für die Konfiguration über Unified Endpoint Management (UEM) verfügbar. Administratoren können mit diesem Attribut Gerätenamen anhand von Benutzergruppen zuweisen und identifizieren.

Konfigurationsschlüssel	Werttyp	Konfigurationswert
deviceName	Zeichenfolge	Name_des_Geräts

Unterstützung für iOS Version 14 eingestellt Die Citrix Workspace-App für iOS unterstützt iOS-Version 14 oder früher ab 23.12.0 nicht. Sie können über den App Store ein Upgrade auf die neueste Version von iOS ausführen. Weitere Informationen finden Sie in der Tabelle Einstellung von Features und Plattformen.

Technical Preview

- Unterstützung für externe Webcams

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

Behobene Probleme

- Der Start einer Desktopsitzung schlägt fehl, wenn die Sprache der Citrix Workspace-App auf Italienisch eingestellt ist.

23.12.0

Was ist neu

YubiKey-Unterstützung für Smartcardauthentifizierung Sie können jetzt die Smartcardauthentifizierung mit YubiKey durchführen. Dieses Feature bietet eine Einzelgeräteauthentifizierung für die Citrix Workspace-App, für virtuelle Sitzungen und veröffentlichte Apps in der VDA-Sitzung. Damit wird der Anschluss von Smartcardlesern oder anderen externen Authentifikatoren überflüssig. Für Endbenutzer ist dies benutzerfreundlicher, weil YubiKey eine Vielzahl von Protokollen wie OTP, FIDO usw. unterstützt.

Zum Anmelden bei der Citrix Workspace-App stecken Sie den YubiKey in Ihr iPhone oder iPad, schalten den Smartcardschalter ein und geben ihre Store-URL an.

> **Hinweis:**
>
> Die Citrix Workspace-App für iOS unterstützt nur die YubiKey 5-Serie. Weitere Informationen zu YubiKey finden Sie in der Dokumentation zur YubiKey 5-Serie.

Unterstützung für generische Lesegeräte vom Typ C Die Citrix Workspace-App für iOS unterstützt jetzt Typ-C-CCID-konforme Lesegeräte für die Smartcardauthentifizierung. Bisher wurden nur Lightning-Port-konforme Lesegeräte unterstützt. Die Integration von Typ-C-Smartcardleser 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.

Gerätenamen über UEM konfigurieren Mit dieser Version ist ein neuer Parameter namens deviceName für die Konfiguration über Unified Endpoint Management (UEM) verfügbar. Administratoren können mit diesem Attribut Gerätenamen anhand von Benutzergruppen zuweisen und identifizieren.

Konfigurationsschlüssel	Werttyp	Konfigurationswert
deviceName	Zeichenfolge	Name_des_Geräts

Unterstützung für iOS Version 14 eingestellt Die Citrix Workspace-App für iOS unterstützt iOS-Version 14 oder früher ab 23.12.0 nicht. Sie können über den App Store ein Upgrade auf die neueste Version von iOS ausführen. Weitere Informationen finden Sie in der Tabelle Einstellung von Features und Plattformen.

Technical Preview

- Unterstützung für externe Webcams

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

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.12.0

Was ist neu

YubiKey-Unterstützung für Smartcardauthentifizierung Sie können jetzt die Smartcardauthentifizierung mit YubiKey durchführen. Diese Funktion ermöglicht die Einzelgeräteauthentifizierung für Web- und SaaS-Apps sowie virtuelle Sitzungen. Das Anschließen von Smartcardlesern oder anderen externen Authentifikatoren wird damit überflüssig. Für Endbenutzer ist dies benutzerfreundlicher, weil YubiKey eine Vielzahl von Protokollen wie OTP, FIDO usw. unterstützt.

Zum Anmelden bei der Citrix Workspace-App stecken Sie den YubiKey in Ihr iPhone oder iPad, schalten den Smartcardschalter ein und geben ihre Store-URL an.

> **Hinweis:**
>
> Die Citrix Workspace-App für iOS unterstützt nur die YubiKey 5-Serie. Weitere Informationen zu YubiKey finden Sie in der Dokumentation zur YubiKey 5-Serie.

Unterstützung für generische Lesegeräte vom Typ C Die Citrix Workspace-App für iOS unterstützt jetzt Typ-C-CCID-konforme Lesegeräte für die Smartcardauthentifizierung. Bisher wurden nur Lightning-Port-konforme Lesegeräte unterstützt. Die Integration von Typ-C-Smartcardleser 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.

Gerätenamen über UEM konfigurieren Mit dieser Version ist ein neuer Parameter namens deviceName für die Konfiguration über Unified Endpoint Management (UEM) verfügbar. Administratoren können mit diesem Attribut Gerätenamen anhand von Benutzergruppen zuweisen und identifizieren.

Konfigurationsschlüssel	Werttyp	Konfigurationswert
deviceName	Zeichenfolge	Name_des_Geräts

Unterstützung für iOS Version 14 eingestellt Die Citrix Workspace-App für iOS unterstützt iOS-Version 14 oder früher ab 23.12.0 nicht. Sie können über den App Store ein Upgrade auf die neueste Version von iOS ausführen. Weitere Informationen finden Sie in der Tabelle Einstellung von Features und Plattformen.

Technical Preview

- Unterstützung für externe Webcams

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

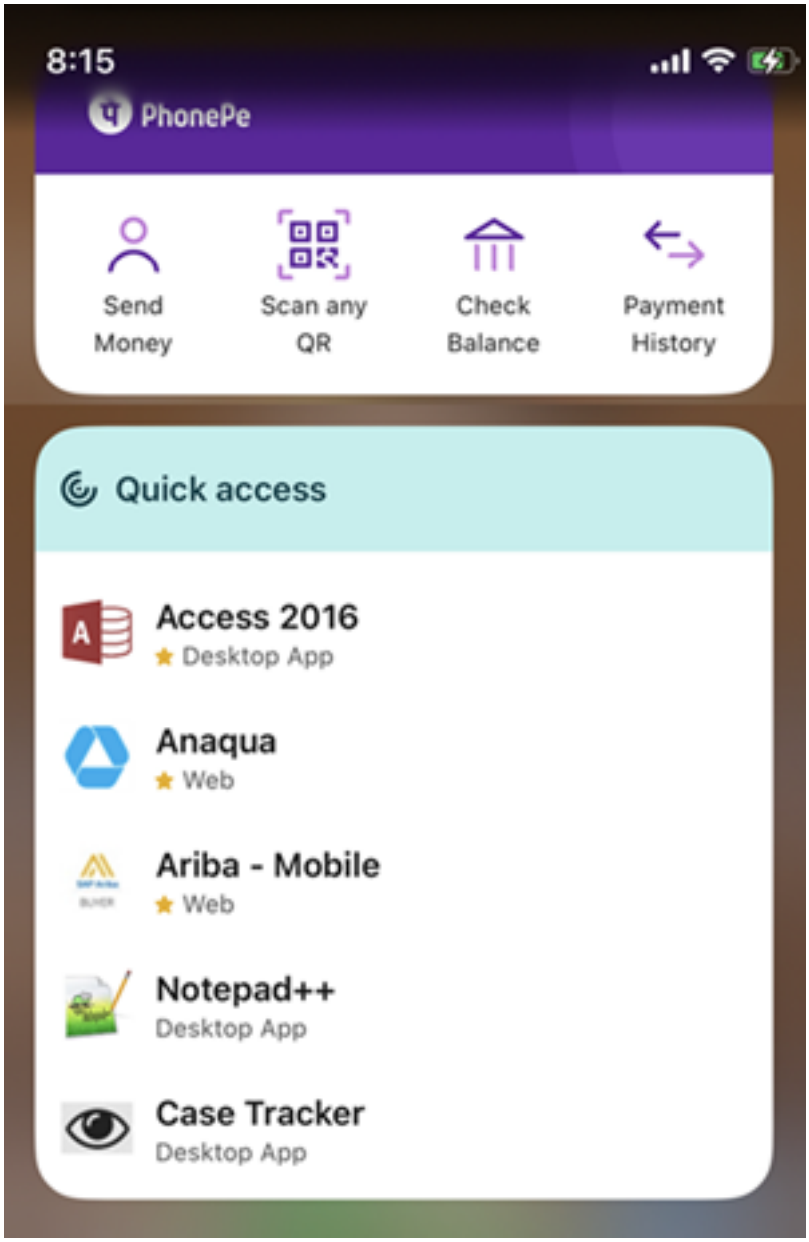
Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.11.0

Apps und Desktops als Widgets anzeigen

Endbenutzer können jetzt virtuelle Apps und Desktops direkt von ihrem iPhone und iPad aus starten. Sie müssen nicht die Citrix Workspace-App öffnen, um eine App- oder Desktopsitzung zu starten. Ein Benutzer kann maximal fünf virtuelle Apps und Desktops als Widgets verwenden.

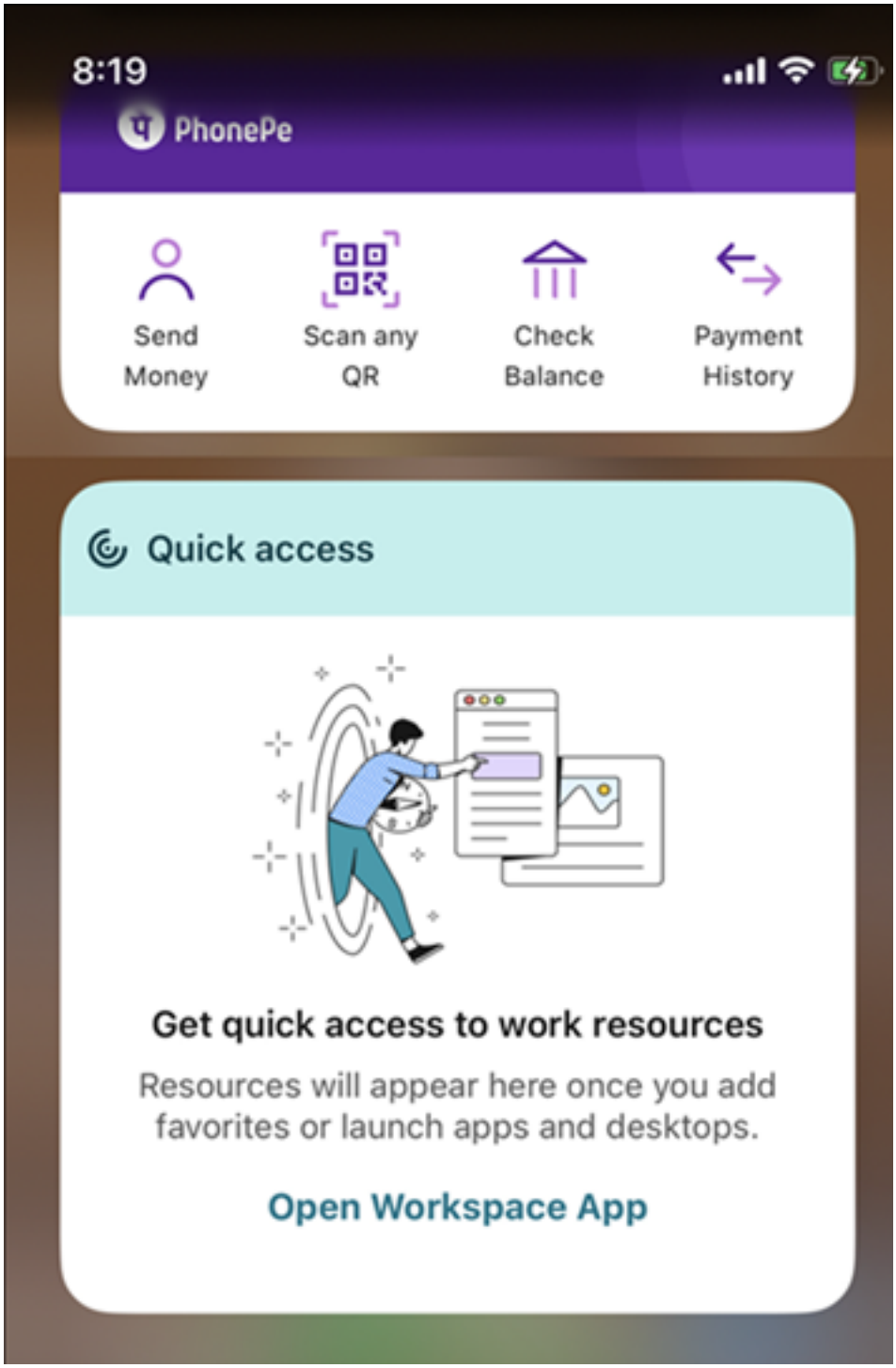


Die Widgets werden automatisch gemäß den folgenden Kriterien erstellt:

- Drei bevorzugte und zwei kürzlich geöffnete Apps oder Desktops werden als Widgets angezeigt
- Sind keine Apps oder -Desktops als Favoriten festgelegt, werden bis zu fünf kürzlich geöffnete

Apps und Desktops als Widgets angezeigt

- Sind keine kürzlich geöffneten Apps oder Desktops vorhanden, werden bis zu fünf als Favoriten festgelegte Apps oder Desktops als Widgets angezeigt
- Wenn keine Apps oder Desktops als Favorit 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.



Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.10.1

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.10.0

Was ist neu

Ankündigung der Einstellung der Unterstützung für iOS-Version 14 Die Citrix Workspace-App unterstützt iOS Version 14 oder früher ab Version 23.12.0 nicht. Sie können über den App Store ein Upgrade auf die neueste Version von iOS ausführen. Weitere Informationen finden Sie in der Tabelle Einstellung von Features und Plattformen.

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.9.0

Was ist neu

Unterstützung für Transport Layer Security 1.3 Die Citrix Workspace-App für iOS unterstützt jetzt TLS (Transport Layer Security) 1.3, was Leistung und Effizienz steigert. Mit seinen starken Verschlüsselungssammlungen und Einmalsitzungsschlüsseln bietet TLS 1.3 robuste Sicherheitsfunktionen.

Endbenutzer können das Feature wie folgt in der Citrix Workspace-App für iOS aktivieren.

1. Gehen Sie zu **Erweiterte Einstellungen** > **TLS-Versionen**.
2. Wählen Sie **Version TLS 1.3**.

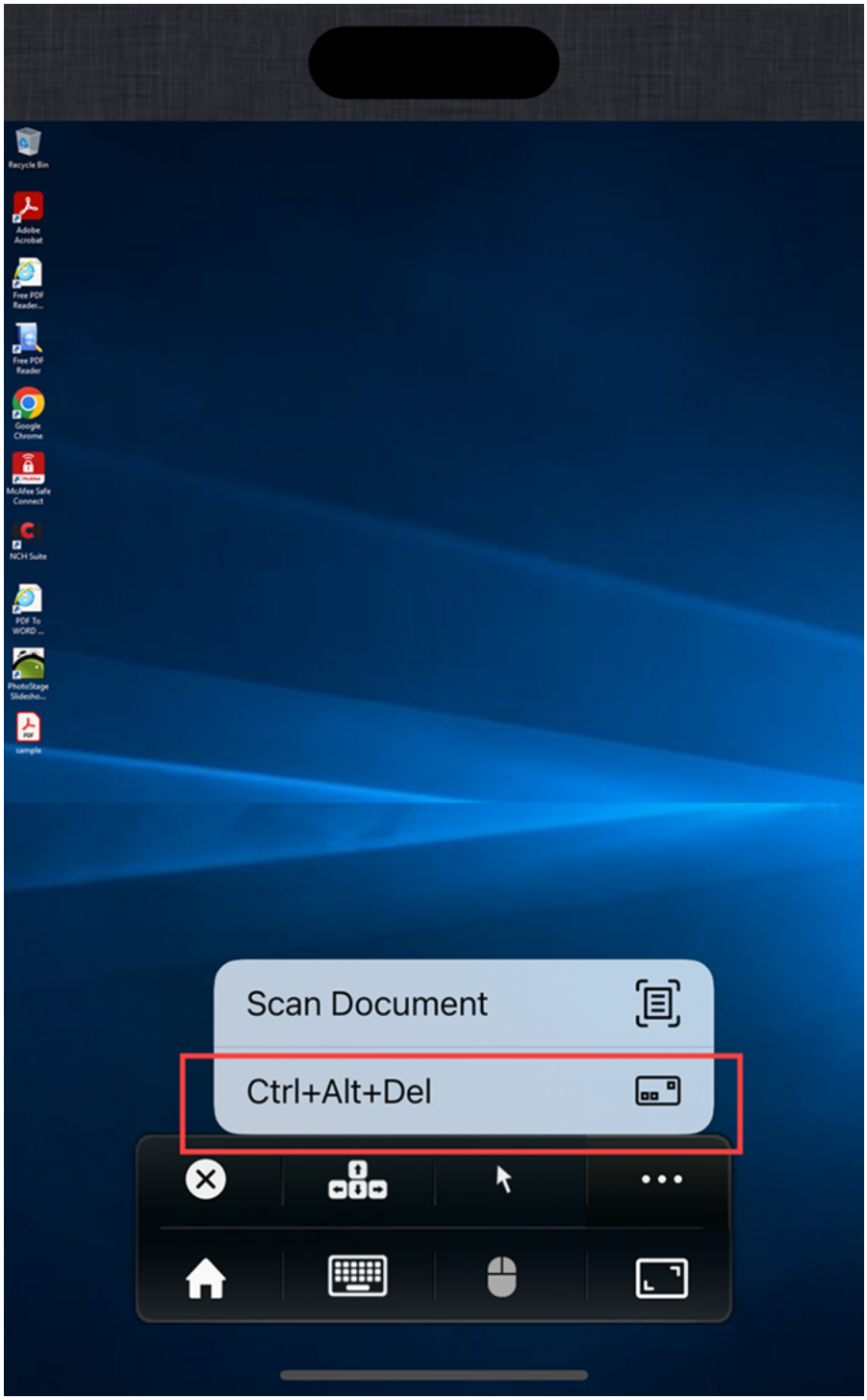
Unterstützung für AirPrint-fähige Drucker Mit AirPrint-fähigen Druckern können Endbenutzer jetzt Dokumente aus ihren aktiven Sitzungen auf iOS-Geräten drucken. Drucker müssen nicht mehr über Kabel oder Netzwerk angeschlossen werden. Sobald Benutzer einen Druckbefehl initiieren, werden AirPrint-fähige Drucker zusammen mit anderen verfügbaren Druckern aufgelistet.

Zur Verwendung eines AirPrint-fähigen Druckers müssen Benutzer Folgendes sicherstellen.

- Der erforderliche Drucker muss AirPrint-kompatibel sein und AirPrint muss aktiviert sein.
- Das Benutzergerät muss mit demselben Wi-Fi-Netzwerk verbunden sein wie der AirPrint-fähige Drucker.

Diese Funktionalität ist für iOS-Plattformen in Cloud- und On-Premises-Umgebungen verfügbar.

Tastenkombination Strg+Alt+Entf zur Sitzungssymbolleiste hinzugefügt Die Sitzungssymbolleiste bietet jetzt die Option, die Funktion **Strg+Alt+Entf** über eine Schaltfläche auszuführen. Über diese Option können Benutzer sich abmelden, Benutzer wechseln, das System sperren oder auf den Task-Manager zugreifen.



FIDO2-basierte Authentifizierung Die Citrix Workspace-App für iOS unterstützt jetzt die kennwortlose Authentifizierung innerhalb einer Citrix Virtual Apps and Desktops-Sitzung mithilfe FIDO2-basierter Authentifizierungsverfahren. Dies ermöglicht Benutzern in Browsern wie Google Chrome oder Microsoft Edge die Anmeldung an einer WebAuthn-fähigen Website mithilfe von

FIDO2-unterstützten Yubico-Sicherheitsschlüsseln. Beim Öffnen einer WebAuthn-fähigen Website wird eine kennwortlose Authentifizierung ausgelöst.

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 mit kennwortloser Authentifizierung wird nicht unterstützt.

Weitere Informationen zu den Voraussetzungen für dieses Feature finden Sie unter Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2 in der Dokumentation zu Citrix Virtual Apps and Desktops.

Technical Preview

- Mehrere Stores mit Unified Endpoint Management (UEM) hinzufügen
- Mehrere Stores mit Unified Endpoint Management (UEM) löschen

Eine Liste aller Features in Technical Previews finden Sie auf der Seite Features in Technical Previews.

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.7.5

Was ist neu

Alle auf der Smartcard verfügbaren Zertifikate anzeigen

In der Citrix Workspace-App für iOS werden jetzt die auf der Smartcard verfügbaren Zertifikate angezeigt und Sie können das Zertifikat für die smartcardbasierte Authentifizierung auswählen. Das erforderliche Zertifikat kann auf der Seite **Zertifikat auswählen** ausgewählt werden, sobald der Smartcardschalter aktiviert wurde.

Auf Webstores zugreifen, die mit Global App Configuration Service aktiviert wurden

Administratoren können jetzt einen Webstore (Webinterface) für die E-Mail-basierte Storediscovery konfigurieren. Basierend auf der E-Mail-Adresse, die Endbenutzer beim Hinzufügen eines Stores (auf dem Willkommensbildschirm) eingegeben haben, hilft der Global App Configuration Service dabei, die vom Administrator definierte benutzerdefinierte Web-URL (Webinterface) zu identifizieren. Endbenutzer werden dann automatisch zu dem vom Administrator konfigurierten Webstore weitergeleitet. Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter Allowed custom web portal.

Ankündigung der Einstellung von PNAgent

Der PNA-Store gilt für die Citrix Workspace-App für iOS ab Version 23.7.5 als veraltet. Ab Version 23.7.5 unterstützt Citrix keine Bugfixes oder Sicherheitspatches für das PNA-Store-Feature.

Behobene Probleme

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

23.6.5

Was ist neu

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

Behobene Probleme

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

23.6.0

Was ist neu

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

Behobene Probleme

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

23.5.0

Was ist neu

Verbesserungen für die erweiterte Tastatur Ab Version 23.5.0 wurde die erweiterte Tastaturfunktionalität verbessert, um eine bessere Benutzererfahrung zu bieten. Folgende Verbesserungen wurden eingeführt:

- Erweiterte Symbolleiste anheften oder lösen.
- Erweiterte Symbolleiste synchron mit der Bildschirmrotation drehen.
- Unterstützung für Tastenkombinationen mit der Windows-Symboltaste und 3-Tasten-Kombinationen.
- Verbesserte Benutzererfahrung bei Anwendungsszenarien mit mehreren Monitoren.
- Automatisches Öffnen oder Reduzieren der erweiterten Symbolleiste.
- Verbesserte Benutzererfahrung im Stage Manager-Modus (auf einem iPad mit M1-Chip).

Behobene Probleme in Release 23.5.0 In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

23.4.5

Was ist neu

Unterstützung für Global App Configuration Service-Kanal Ab Version 23.4.5 können Administratoren mit dem Global App Configuration Service Einstellungen definieren und testen, bevor sie die Konfiguration für alle Endbenutzer bereitstellen. Auf diese Weise wird sichergestellt, dass Funktionen vor Übernahme in die Produktionsumgebung umfassend getestet werden.

> **Hinweis:**
>
> - Die Citrix Workspace-App für iOS unterstützt die Konfigurationen **Standard** und **Testkanal**. Die Standardeinstellung für alle Benutzer ist der Kanal **Standard**.

Weitere Informationen finden Sie in der Dokumentation zum Global App Configuration Service.

Weitere Informationen zur Konfiguration finden Sie unter Unterstützung für Global App Configuration Service-Kanal.

Unterstützung für die Store-Konfiguration mithilfe von MDM-Lösungen Die Citrix Workspace-App für iOS unterstützt jetzt die Remotekonfiguration Ihrer Workspace Store-URL mithilfe von Lösungen zur Mobilgeräteverwaltung (MDM). Weitere Informationen finden Sie unter Workspace-App mit MDM-Lösungen konfigurieren.

Verbesserungen der MDM-Lösungen Die Citrix Workspace-App für iOS unterstützt jetzt weitere Konfigurationen, bei denen AppConfig-basierte Schlüssel-Wert-Paare zur Konfiguration der Citrix Workspace-App verwendet werden. Bisher konnten Administratoren bereits Store-URLs konfigurieren. Jetzt können Administratoren das Anpassen von Store-URLs durch Benutzer einschränken und die App-Anzeige steuern.

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

Details entnehmen Sie den folgenden Angaben:

Konfigurationsschlüssel	Werttyp	Konfigurationswert
`url`	`String`	Die Store-URL. Beispiel: `prodcwa.cloud.com`
`storeType`	`Integer`	• Bei der Einstellung “1” (Standard) können Benutzer die native oder die Standard-Storeanzeige nutzen. - Bei der Einstellung “2”können Benutzer den Store in einem Webinterface anzeigen.

Konfigurationsschlüssel	Werttyp	Konfigurationswert
restrict_user_store_modification	Boolean	• Bei der Einstellung **True** können Benutzer den Store nicht anpassen (hinzufügen/löschen/bearbeiten). - Bei der Einstellung **False** können Benutzer den Store anpassen. **Hinweis:** Bei der Einstellung "True" werden alle vorhandenen Stores gelöscht, bevor ein neuer MDM-konfigurierter Store hinzugefügt wird.

Technical Preview

- Unterstützung für FIDO2-basierte Authentifizierung

Eine Liste aller Features in Technical Previews finden Sie auf der Seite Features in Technical Previews.

Behobene Probleme in 23.4.5

- Wenn Sie den Scrollmodus "Natürliches Scrollen"aktivieren und Ihre Finger auf dem iPad von oben nach unten bewegen, wandern Sie auf der Seite nach unten. Das gleiche Verhalten wird jedoch auch beobachtet, wenn Sie "Natürliches Scrollen"deaktivieren. Das Verhalten tritt außerdem im "Magic Mouse"-Modus auf. [HDX-49267]
- Wenn Sie im Modus "Erweitern"die Auflösung "AutoAnpassen - Mittel"oder "AutoAnpassen - Hoch"auswählen, wird die Bildschirmauflösung automatisch skaliert und die Anzeige ist abgeschnitten. Dieses Problem tritt auf, wenn die Citrix Workspace-App vom Hintergrund in den Vordergrund wechselt. [CVADHELP-19169]

23.3.5

Was ist neu

User-Agent-Zeichenfolge Standardmäßig enthält die User-Agent-Zeichenfolge, die bei einigen über WKWebView initiierten Netzwerkanforderungen verwendet wird, jetzt die ID der Citrix Workspace-App.

Sie wurde 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`

in eine der folgenden Optionen:

`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`
(Beispiel für iPhone)

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`
(Beispiel für iPad)

Technical Previews

- Schnellscan

Eine Liste aller Features in Technical Previews finden Sie auf der Seite Features in Technical Previews.

Behobene Probleme in Release 23.3.5

Nach dem Upgrade der Citrix Workspace-App für iOS auf Version 23.3.0 können Sie sich nicht bei Ihrem Store authentifizieren, wenn er mit der vollständigen Store-Adresse über eine MDM-Lösung konfiguriert ist.

23.3.0

Was ist neu

Unterstützung der Storekonfiguration mithilfe von MDM-Lösungen [Technical Preview]

> **Hinweis:**
>
> Dieses Feature ist als öffentliche Preview verfügbar.

Die Citrix Workspace-App für iOS unterstützt jetzt die Remotekonfiguration Ihrer Workspace Store-URL mithilfe von Lösungen zur Mobilgeräteverwaltung (MDM). Weitere Informationen finden Sie unter Workspace-App mit MDM-Lösungen konfigurieren.

Neuauthentifizierung nach Sitzungstimeout In diesem Release werden Sie jetzt aufgefordert, sich erneut bei der Citrix Workspace-App zu authentifizieren, wenn Ihre Sitzung seit der letzten Anmeldung abgelaufen ist. Sie werden zur Zweifaktorauthentifizierung oder zur Eingabe eines Benutzernamens und Kennworts aufgefordert, wenn Sie über das Web oder einen nativen Client eine Verbindung zur Citrix Workspace-App herstellen.

Technical Preview

- Dokumentenscanner
- Unterstützung für Bild-im-Bild (PiP)

Eine Liste aller Features in Technical Previews finden Sie auf der Seite Features in Technical Previews.

Behobene Probleme

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

23.2.1

Was ist neu

Unterstützung der Rückkamera Citrix Workspace-App für iOS unterstützt 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 auf dem Bildschirm eine unverankerte Kameraschaltfläche, mit der Sie die Kameraposition wechseln können. Sie können die unverankerte Schaltfläche auch frei auf dem Bildschirm bewegen und an einer beliebigen Stelle platzieren.

Gehen Sie wie folgt vor, um die Kameraposition in den virtuellen Sitzungen zwischen vorne und hinten zu wechseln:

1. Öffnen Sie eine Client-App, die Videos aufnimmt.
2. Starten Sie die Videoaufnahme.
3. Tippen Sie auf die unverankerte Kameraschaltfläche, die auf dem Bildschirm erscheint, um zwischen der vorderen und hinteren Kamera zu wechseln.

> **Hinweis:**
>
> Die Einstellungen der Client-App haben innerhalb einer HDX-Sitzung keine Auswirkung auf die Kamera. Sie müssen die von Citrix aktivierte unverankerte Schaltfläche für die Kamera verwenden, um die Kameraposition zu ändern.

Bekannte Probleme:

Die unverankerte Schaltfläche ist teilweise oder vollständig verdeckt, wenn das Casting-Feature oder das Feature "Dokument scannen"aktiviert ist.

Unterstützung für das automatische Ausfüllen der Store-URL Wenn Sie auf die umbenannte Citrix Workspace-App für iOS zugreifen, können Sie festlegen, dass die Store-URL automatisch ausgefüllt wird. Diese Funktion reduziert manuelle Eingriffe und ermöglicht einen schnellen Zugriff auf die App. Weitere Informationen zur App-Personalisierung finden Sie unter App Personalization.

Unterstützung eines Wechsels des Webbrowsers für die Authentifizierung Auf iOS- oder iPad-Geräten können Administratoren jetzt den für den Authentifizierungsprozess verwendeten Browser vom eingebetteten Browser zum Systembrowser wechseln, wenn eine erweiterte Authentifizierungsrichtlinie für das on-premises Citrix Gateway und StoreFront-Bereitstellung konfiguriert ist. Weitere Informationen finden Sie unter Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren.

Behobene Probleme

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

23.2.0

Was ist neu

Unterstützung der Rückkamera Citrix Workspace-App für iOS unterstützt 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 auf dem Bildschirm eine unverankerte Kameraschaltfläche, mit der Sie die Kameraposition wechseln können. Sie können die unverankerte Schaltfläche auch frei auf dem Bildschirm bewegen und an einer beliebigen Stelle platzieren.

Gehen Sie wie folgt vor, um die Kameraposition in den virtuellen Sitzungen zwischen vorne und hinten zu wechseln:

1. Öffnen Sie eine Client-App, die Videos aufnimmt.
2. Starten Sie die Videoaufnahme.
3. Tippen Sie auf die unverankerte Kameraschaltfläche, die auf dem Bildschirm erscheint, um zwischen der vorderen und hinteren Kamera zu wechseln.

> **Hinweis:**
>
> Die Einstellungen der Client-App haben innerhalb einer HDX-Sitzung keine Auswirkung auf die Kamera. Sie müssen die von Citrix aktivierte unverankerte Schaltfläche für die Kamera verwenden, um die Kameraposition zu ändern.

Bekannte Probleme:

Die unverankerte Schaltfläche ist teilweise oder vollständig verdeckt, wenn das Casting-Feature oder das Feature "Dokument scannen"aktiviert ist.

Unterstützung für das automatische Ausfüllen der Store-URL Wenn Sie auf die umbenannte Citrix Workspace-App für iOS zugreifen, können Sie festlegen, dass die Store-URL automatisch ausgefüllt wird. Diese Funktion reduziert manuelle Eingriffe und ermöglicht einen schnellen Zugriff auf die App. Weitere Informationen zur App-Personalisierung finden Sie unter App Personalization.

Unterstützung eines Wechsels des Webbrowsers für die Authentifizierung Auf iOS- oder iPad-Geräten können Administratoren jetzt den für den Authentifizierungsprozess verwendeten Browser vom eingebetteten Browser zum Systembrowser wechseln, wenn eine erweiterte Authentifizierungsrichtlinie für das on-premises Citrix Gateway und StoreFront-Bereitstellung konfiguriert ist. Weitere Informationen finden Sie unter Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren.

Behobene Probleme

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

Einschränkungen

- Wir empfehlen Ihnen, die Tasten **Strg + C** und **Strg + V** auf der Bildschirmtastatur Ihres Geräts zum Kopieren und Einfügen zu verwenden. Die Tasten **Cmd + C** und **Cmd + V** auf einer externen Tastatur funktionieren möglicherweise nicht. [HDX-32431]
- Versuche, eine App durch Tippen auf die ICA-Datei im Download-Manager zu starten, schlagen fehl, wenn Sie den Safari-Webbrowser verwenden.
  Stellen Sie sicher, dass die neueste Version der Citrix Workspace-App oder Citrix Receiver für iOS (aber nicht beide) auf dem Gerät vorhanden ist, um einen erfolgreichen Start der App in Safari sicherzustellen. [RFIOS-5502]
- Nach der Migration von StoreFront zu Citrix Workspace flackert der Bildschirm kurzzeitig, wenn Sie in der Pendo-Anleitung auf die Schaltfläche **Weiter** tippen.
- Wenn beim Starten von Web- und SaaS-Apps innerhalb der Citrix Workspace-App Google IdP verwendet wird und der Benutzer sich anmelden muss, schlägt die Authentifizierung mit der Fehlermeldung “Zugriff verweigert”fehl. [RFIOS-11904]

Einstellung von Features und Plattformen

Informationen zu veralteten Elementen finden Sie auf der Seite Einstellung von Features und Plattformen.

Features in Technical Previews

July 1, 2024

Kunden haben die Möglichkeit, Technical Previews in ihren Umgebungen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, zu nutzen und Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Features in Technical Previews, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor.

Liste der Features in Technical Previews

Die folgende Tabelle enthält die Features, die als Technical Preview erhältlich sind. Bei diesen Funktionen handelt es sich um Preview Features, die nur auf Anfrage angefordert werden können. Füllen Sie die entsprechenden Formulare aus, um eines dieser Features zu aktivieren und Feedback dafür zu geben.

Titel	Verfügbar ab Version	Aktivierungsformular (auf das Symbol klicken)	Feedbackformular (auf das Symbol klicken)
Unterstützung der Durchsetzung der biometrischen Authentifizierung für den Zugriff auf die Citrix Workspace-App	2405		
Unterstützung für Single Sign-On für virtuelle Maschinen, die mit Microsoft Entra ID verbunden sind	2405		
Unterstützung für die Konfiguration der Citrix Workspace-App-Einstellungen per UEM	24.3.5		
Unterstützung für adaptives Audio	24.3.0		
Unterstützung für Bedienungshilfen und VoiceOver	24.2.0		
Unterstützung für externe Webcams	23.12.0		
Mehrere Stores mit Unified Endpoint Management (UEM) hinzufügen	23.9.0		

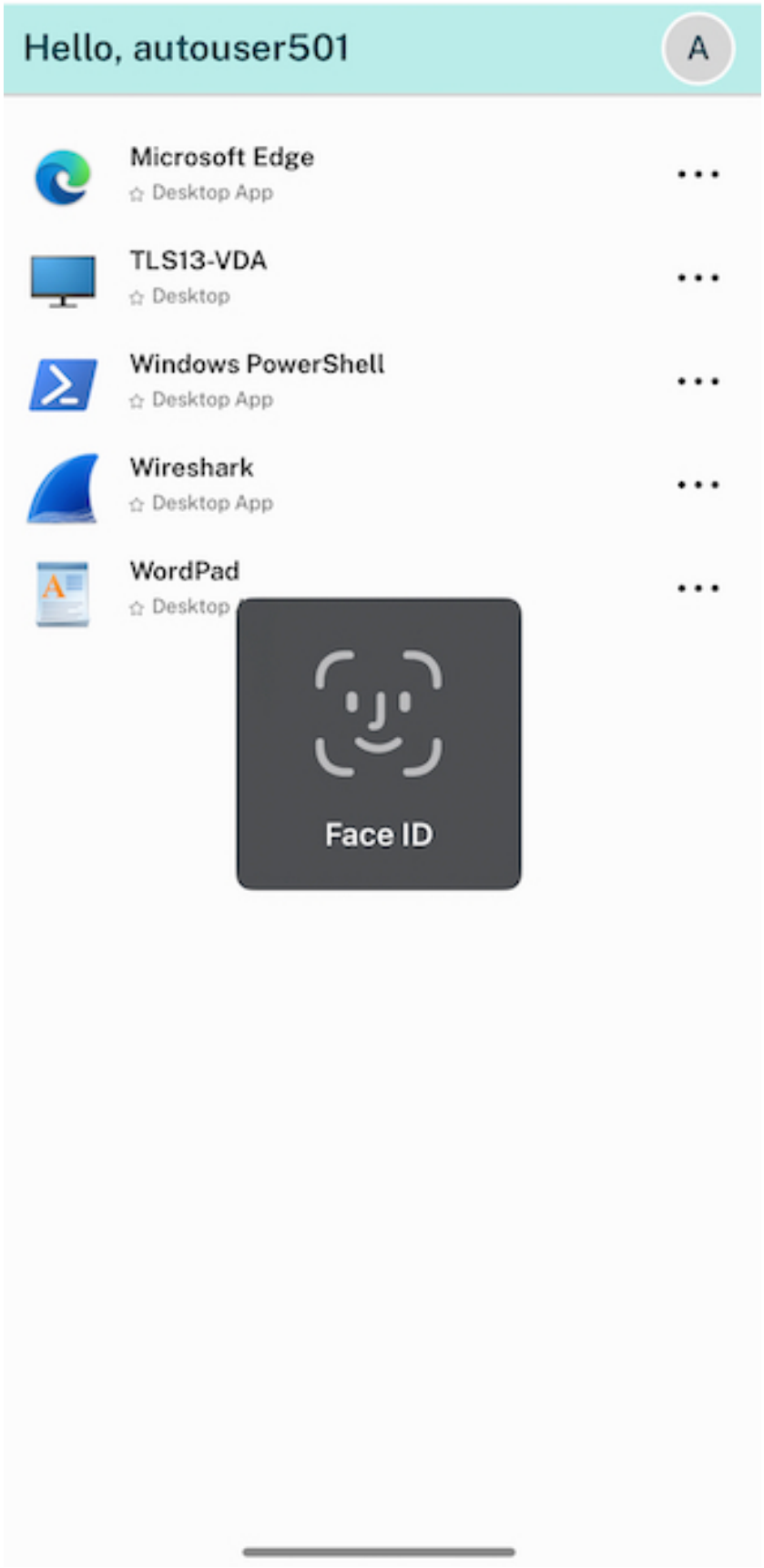
Titel	Verfügbar ab Version	Aktivierungsformular (auf das Symbol klicken)	Feedbackformular (auf das Symbol klicken)
Mehrere Stores mit Unified Endpoint Management (UEM) löschen	23.9.0		
Schnellscan	23.3.5		
Unterstützung für Bild-im-Bild (Picture-in-Picture, PiP)	23.3.0		
Unterstützung für den nativen Nicht-Spiegeln-Modus von Apple	23.3.0		
Unterstützung für besseres Single Sign-On (SSO) bei Web- und SaaS-Apps	23.3.0		

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

Technical Preview ab Version	Aktivierungsformular	Feedback-Formular
2405		

Ab Version 24.5.0 können Administratoren jetzt die biometrische Authentifizierung eines Geräts erzwingen, um ihren Benutzern den Zugriff auf die Citrix Workspace-App zu ermöglichen. Wenn Sie mit diesem Feature die Citrix Workspace-App öffnen, nachdem Sie sie geschlossen haben, oder sie nach dem Minimieren in den Vordergrund rücken, wird eine Aufforderung zur Face ID- oder Touch ID-Überprüfung angezeigt, um die Sperre zu entsperren und sich anzumelden. Wenn

das Gerät keine biometrische Authentifizierung unterstützt, wird die Kennwort- oder Passcode-Authentifizierungsmethode für den Zugriff auf die App verwendet. Wenn der Passcode auf dem Gerät nicht aktiviert ist, wird das Konto abgemeldet, sodass sich der Benutzer erneut anmelden muss, um auf die Citrix Workspace-Anwendung zuzugreifen.



Administratoren können dieses Feature mit der Unified Endpoint Management-Lösung mit den folgenden Schlüssel-Wert-Paaren konfigurieren:

- **Schlüssel**: verify_biometric_on_app_foreground_transition
- **Werttyp:**: boolesch
- **Wert**: “true”oder “false”
  - Wenn der Wert auf **true** gesetzt ist, ist eine biometrische Authentifizierung erforderlich, damit Endbenutzer auf die Citrix Workspace-App zugreifen können.
  - Wenn der Wert auf **false** gesetzt ist, wird die biometrische Authentifizierung für den Zugriff auf die Citrix Workspace-App nicht erzwungen. Benutzer haben die Möglichkeit, die biometrische Authentifizierung zu deaktivieren.

Unterstützung für Single Sign-On für virtuelle Maschinen, die mit Microsoft Entra ID verbunden sind

Technical Preview ab Version 2405	Aktivierungsformular	Feedback-Formular

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

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

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

Technical Preview ab Version 24.3.5	Aktivierungsformular	Feedback-Formular

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

Ab Version 24.3.5 können Sie auch die Citrix Workspace-App-Einstellungen auf den verwalteten Geräten mit jeder UEM-Lösung konfigurieren, die in Ihrer Infrastruktur bereitgestellt wird.

> **Hinweis:**
>
> Wenn Sie als Administrator die Einstellungen der Citrix Workspace-App mit UEM und mit dem Global App Configuration Service (GACS) konfigurieren können, ist UEM stets bevorzugt zu verwenden.

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>
<!--NeedCopy-->
```


> **Hinweis:**
>
> Das Flag `userOverride` ermöglicht es dem Benutzer, die Einstellungen der Citrix Workspace-App zu ändern. Wenn das Flag `userOverride` auf "true"gesetzt ist, kann der Benutzer die Einstellungen ändern. Wenn das Flag `userOverride` für eine Einstellung auf "false"gesetzt ist, kann der Benutzer sie in den Einstellungen der Citrix Workspace-App nicht ändern.

Tabelle mit Schlüssel-Wert-Paaren

Die folgende Tabelle enthält 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
Audio	Audio	Bietet Benutzern Zugriff zum Ein- und Ausschalten des Audios über die virtuelle App oder den Desktop.	settings_audio_redirection	true/false	Boolescher Wert	TRUE
Tastatur	Unicode-Tastatur verwenden	Ermöglicht Benutzern die Verwendung einer Unicode-Standardtastatur.	settings_use_unicode_keyboard	true/false	Boolescher Wert	TRUE

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Tastatur	Automatische Tastatur	Aktiviert oder deaktiviert die automatische Anzeige der Tastatur in einer Sitzung.	settings_automatic_keyboard	true/false	Boolescher Wert	TRUE
Tastatur	Tastaturlayoutsynchronisierung	Ermöglicht Benutzern, auf dem Gerät zu ihrem bevorzugten Tastaturlayout zu wechseln.	settings_keyboard_layout_sync	true/false	Boolescher Wert	FALSE
Tastatur	Benutzerdefinierte Tastaturen verwenden	Ermöglicht es Benutzern, heruntergeladene Tastaturen von Drittanbietern in der virtuellen Sitzung zu verwenden.	settings_allow_keyboard_extensions	true/false	Boolescher Wert	FALSE
display	Sitzungsauflösung	Ermöglicht es Benutzern, die Bildschirmauflösung auszuwählen.	settings_resolution	0–9	Ganzzahl	5 (iPad) 3 (iPhone)

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
display	Präsentationsmodus	Ermöglicht es Ihnen, Ihr iOS-Gerät als Touchpad für die Sitzungssteuerung zu verwenden, wenn Sie eine externe Anzeige verwenden.	settings_presentation_mode	true/false	Boolescher Wert	FALSE
display	Externe Anzeige	Verbindet eine externe Anzeige mit dem Gerät.	settings_external_display	true/false	Boolescher Wert	TRUE
Erweitert	Strikte Zertifikatvalidierung	Erzwingt eine strengere Kontrolle bei der Validierung von Serverzertifikaten.	settings_strictCertValidation	true/false	Boolescher Wert	FALSE
Erweitert	TLS-Versionen	Ermöglicht Benutzern, ihre TLS-Einstellungen für die Problembehandlung zu ändern.	settings_tlsVersion	0–3	Ganzzahl	0

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Erweitert	Natives Kombinationsfeld verwenden	Ermöglicht die Verwendung des nativen iOS-Auswahlfeatures.	settings_native_combobox	true/false	Boolescher Wert	TRUE
Erweitert	Toucheingabe aktivieren (nur iPad)	Aktiviert die Toucheingabe für alle Apps und Desktops, einschließlich derer, für die die Toucheingabeoption nicht nativ aktiviert ist.	settings_multitouch	true/false	Boolescher Wert	true (iPad) false (iPhone)
Erweitert	Vollbildansicht	Ermöglicht es Ihnen, Ihre Apps und Desktops im Vollbildmodus anzuzeigen.	settings_mobile_view_full_screen	true/false	Boolescher Wert	true (iPad) false (iPhone)

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Erweitert	Bei Anmeldung wieder verbinden	Ermöglicht die automatische Wiederverbindung einer Sitzung, wenn ein neues Konto hinzugefügt wird oder während der Anmeldung.	settings_reconnect_login	true/false	Boolescher Wert	FALSE
Erweitert	Wiederverbindung beim Aktualisieren	Automatische Wiederverbindung zu einer Sitzung, die auf einem anderen Gerät gestartet wurde, wenn Apps und Desktops auf dem zweiten Gerät aktualisiert werden.	settings_reconnect_refresh	true/false	Boolescher Wert	FALSE

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Erweitert	HTTP-Proxy aktivieren	Ermöglicht die Verwendung des HTTP-Proxys für eine Sitzung.	settings_use_local_proxy	true/false	Boolescher Wert	TRUE
Erweitert	Abgeleitete Anmeldeinformationen verwenden	Ermöglicht die Verwendung abgeleiteter Anmeldeinformationen.	setting_useDerivedCredentials	true/false	Boolescher Wert	FALSE
Erweitert	Smartcard in Sitzung	Ermöglicht die Verwendung eines Smartcardgeräts innerhalb einer Sitzung. Diese Einstellung ermöglicht es Benutzern nicht, sich für die Sitzung zu authentifizieren.	settings_usesSmartCardInsideSession	true/false	Boolescher Wert	FALSE

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Erweitert	EDT zulassen	Aktiviert die Unterstützung für den adaptiven Transport.	settings_allow_edt	true/false	Boolescher Wert	TRUE
Erweitert	Autom. Tablet-modus	Ermöglicht das Starten der virtuellen Sitzung im Tablet-modus, wenn keine externe Tastatur oder Maus erkannt wird.	settings_enable_tablet_mode	true/false	Boolescher Wert	TRUE
Erweitert	Anzeige nicht abschalten	Lässt den Bildschirm eingeschaltet.	settings_stay_awake	true/false	Boolescher Wert	FALSE
Erweitert	iPad-Speicher verwenden	Ermöglicht den Zugriff auf lokale Laufwerke auf Ihrem Gerät.	settings_client_drive	true/false	Boolescher Wert	false
X1-Maus	X1-Maus zulassen	Ermöglicht Ihnen das Umschalten für den Zugriff auf Ihre Citrix X1-Maus.	settings_allow_x1_mouse	true/false	Boolescher Wert	FALSE

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	Ganzzahl	200 (iPadPro) 100 (alle anderen Geräte)
X1-Maus	Remotecursorhalt für Citrix X1-Maus verwenden	Hält den Cursor innerhalb einer Sitzung an die App oder den Desktop an. Wenn sich der Cursor beispielsweise über einem Textfeld befindet, passt er sich dem Textfeld an.	settings_X1_mouse_use_server_side_cursor	true/false	Boolescher Wert	TRUE

Kategorie	Einstellung	Beschreibung	Schlüssel	Wert	Werttyp	Standardwert
Authentifizierung	Webbrowser für die Authentifizierung	Ermöglicht Ihnen die Identifizierung der Verwendung von SafariViewController anstelle von WKWeb auf dem Gerät.	settings_auth_system_browser	System browser/embedded	Zeichenfolge	Eingebettet
thirdPartyServices	LaunchDarkly	Aktiviert das LaunchDarkly-Flag für Features der Citrix Workspace-App.	enableLaunchDarkly	true/false	Boolescher Wert	true (Nicht-EU-Regionen)

Unterstützung für adaptives Audio

Technical Preview ab Version 24.3.0	Aktivierungsformular	Feedback-Formular

Ab 24.3.0 unterstützt die Citrix Workspace-App für iOS adaptives HDX-Audio. Diese Funktion verbessert die Benutzererfahrung, indem sie eine verbesserte Audioqualität und eine niedrige Latenz bietet.

Weitere Informationen finden Sie unter Audio - Richtlinieneinstellungen in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung für Bedienungshilfen und VoiceOver

Technical Preview ab Version 24.2.0	Aktivierungsformular	Feedback-Formular

Ab der Version 24.2.0 unterstützt Citrix Workspace-App für iOS die Features Bedienungshilfen und VoiceOver. Dieses Feature unterstützt sehbehinderte Endbenutzer bei der Verwendung der Benutzeroberfläche. Eine Sprachausgabe liest die Bildschirmelemente laut vor, wenn ein Benutzer Citrix Workspace und die Benutzeroberfläche für virtuelle Sitzungen verwendet.

Um das VoiceOver-Feature zu aktivieren, navigieren Sie zu iOS **Einstellungen > Bedienungshilfen > VoiceOver** und schalten Sie es ein.

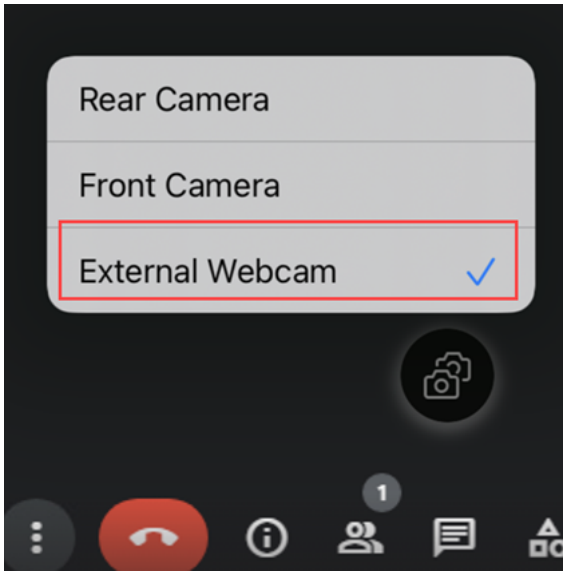
Sie müssen die von iOS bereitgestellten Standardgesten für Bedienungshilfen verwenden, um mit der Citrix Workspace-App zu interagieren. Sie können beispielsweise auf dem Bildschirm nach links und rechts wischen, um zwischen den Menüs zu navigieren, während das Voiceover für jedes Objekt abgespielt wird.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

Unterstützung für externe Webcams

Technical Preview ab Version 23.12.0	Aktivierungsformular	Feedback-Formular

Die Citrix Workspace-App für iOS unterstützt jetzt extern verbundene Webcams in Ihren DaaS-Sitzungen. Schließen Sie über USB eine Webcam an und verwenden Sie sie für Videokonferenzen, indem Sie auf das Kamerasymbol klicken und dann die Option **Externe Webcam** auswählen. Damit können Ressourcen genutzt werden, die den Endbenutzern zur Verfügung stehen.

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



Das System merkt sich die Kameraeinstellungen und verwendet sie, wenn Sie das nächste Mal eine Videokonferenz-App verwenden. Wenn Sie beispielsweise den letzten Videoanruf mit der Einstellung **Externe Webcam** abgeschlossen haben, wird beim nächsten Mal standardmäßig die externe Webcam ausgewählt.

Sie können Ihre Kameraeinstellungen ändern, indem Sie auf dem Bildschirm auf das Kamerasymbol tippen. Die Kameraeinstellungen können auch während Ihrer Anrufe geändert werden.

Dieses Feature ist für Kunden in Cloudstores und On-Premises-Stores verfügbar.

Mehrere Stores mit Unified Endpoint Management (UEM) hinzufügen

Technical Preview ab Version 23.12.0	Aktivierungsformular	Feedback-Formular

Mit Lösungen zur einheitlichen Endpunktverwaltung (Unified Endpoint Management, UEM) können Administratoren mehrere Stores für verwaltete iOS-Geräte hinzufügen und konfigurieren. Die Details für jeden Store können einer XML-Datei hinzugefügt werden. Die XML-Datei kann dann beim Konfigurieren der App-Konfigurationsrichtlinie hochgeladen werden.

> **Hinweis:**
>
> Die XML-Datei muss im Format mit Schlüssel/Wert-Paar vorliegen.

Konfigurationsschlüssel	Werttyp	Beschreibung
haben,	Zeichenfolge	Die Store-URL. Beispiel: example.cloud.com
storeType (optional)	Ganzzahl	Bei der Einstellung **1** können Benutzer die native oder die Standard-Storeanzeige nutzen. Bei der Einstellung **2** können Benutzer den Store in einem Webinterface anzeigen.
displayName (optional)	Zeichenfolge	Der Name des Stores.
restrict_user_store_modification (optional)	Boolescher Wert	Wenn dieser Wert auf **true** gesetzt ist, können Benutzer den Store nicht ändern (d. h. hinzufügen, löschen oder bearbeiten). Wenn der Wert auf **false**gesetzt ist, 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 vorhandenen Stores gelöscht, bevor ein neuer, mit UEM konfigurierter Store hinzugefügt wird.
> - Wenn storeType nicht festgelegt ist, gilt die Standardschnittstelle als native Schnittstelle.

XML-Beispielkonfiguration zum Hinzufügen von Stores

Weitere Informationen finden Sie in dieser XML-Beispieldatei.

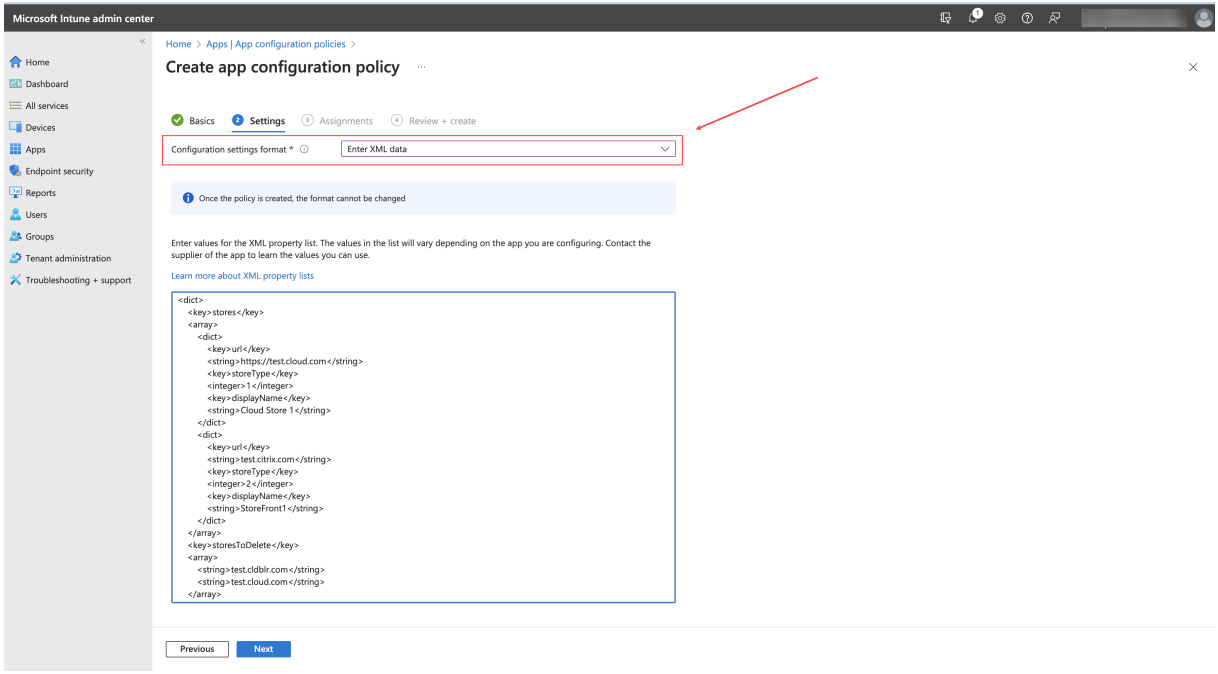
```
    <dict>
        <key>stores</key>
        <array>
            <dict>
                <key>url</key>
                <string>test.cloud.com</string>
                <key>storeType</key>
                <integer>1</integer>
                <key>displayName</key>
                <string>Cloud Store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

<!--NeedCopy-->
```

Sobald die XML-Datei mit der Storekonfiguration fertiggestellt ist, können Administratoren sie auf der Seite zum **Erstellen einer App-Konfigurationsrichtlinie** hochladen. In Microsoft Intune müssen Administratoren beispielsweise in der Dropdownliste für **Format für Konfigurationseinstellungen** die Option **XML-Daten eingeben** auswählen.



Mehrere Stores mit Unified Endpoint Management (UEM) löschen

Technical Preview ab Version	Aktivierungsformular	Feedback-Formular
23.12.0		

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

XML-Beispielkonfiguration zum Löschen von Stores

Weitere Informationen finden Sie in dieser XML-Beispieldatei.

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

<!--NeedCopy-->
```

Die folgende Datei ist eine XML-Beispieldatei, die Konfigurationsangaben zum 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>

<!--NeedCopy-->
```

Schnellscan

Technical Preview ab Version 23.3.5 | Aktivierungsformular | Feedback-Formular

Wenn Sie auf mehreren Geräten bei der Citrix Workspace-App angemeldet sind, können Sie per Schnellscan mehrere Dokumente mit einem iOS-Gerät scannen. Sie können diese gescannten Dokumente dann auf ein iOS-Gerät übertragen.

Führen Sie folgende Schritte aus, um Dokumente mit dem Schnellscan-Feature zu scannen:

1. Klicken Sie auf dem Mac-Gerät mit der rechten Maustaste auf das Symbol der Citrix Workspace-App in Ihrer Desktopsitzung und klicken Sie dann auf **Schnellscan**. Ein QR-Code wird angezeigt.
2. Klicken Sie auf Ihrem iOS-Gerät auf **Einstellungen** > **Schnellscan**.
3. Scannen Sie den auf dem Mac-Gerät angezeigten QR-Code, um Mac-Gerät und iOS-Gerät miteinander zu verbinden.
4. Scannen Sie ein beliebiges Dokument und senden Sie es an Ihr Mac-Gerät.
5. In der Desktopsitzung auf dem Mac-Gerät können Sie die gescannten Dokumente im Finder aufrufen.

Voraussetzungen

- Die Clientlaufwerkzuordnung (CDM) muss für den Store aktiviert sein.
- Sie müssen auf dem iOS- und Mac-Gerät mit demselben Konto in der Citrix Workspace-App angemeldet sein.
- Sie müssen mit demselben WLAN verbunden sein.
- Die erforderliche Mindestversion der Citrix Workspace-App für Mac ist 2304.
- Der Schnellscan erfordert Lese- und Schreibzugriff auf Ihrem Gerät. Führen Sie folgende Schritte aus, um den Zugriff zu aktivieren:

  1. Klicken Sie in Ihrem Profil auf **Anwendungseinstellungen** > **Storeeinstellungen**.
  2. Klicken Sie auf Ihren aktuellen Store.
  3. Klicken Sie auf **Gerätespeicher** und wählen Sie **Lese- und Schreibzugriff**.

Unterstützung für Bild-im-Bild (Picture-in-Picture, PiP)

Technical Preview ab Version 23.3.0 | Aktivierungsformular | Feedback-Formular

Die Citrix Workspace-App für iOS unterstützt den Bild-im-Bild-Modus. Damit können Sie Ihre Desktopsitzung, SaaS-App oder Web-App auf ein unverankertes Fenster verkleinern. Sie können dieses Fen-

ster frei auf dem Bildschirm bewegen und überall platzieren. Der Bild-im-Bild-Modus gibt den Homebildschirm der Citrix Workspace-App frei, sodass Sie andere Aufgaben erledigen können. Klicken Sie in Ihrer Desktopsitzung in der Symbolleiste der Sitzung auf die **Hometaste** oder wählen Sie **Dreipunktmenü (…)** > **Minimieren** in Ihrer SaaS-App oder Web-App, um den Bildschirm zu minimieren. Klicken Sie auf das unverankerte Fenster, um die App im Vollbildmodus anzuzeigen. Klicken Sie auf das **X-Symbol** im unverankerten Fenster, um die App zu schließen. Das unverankerte Fenster wird automatisch im Vollbildmodus angezeigt, wenn Sie eine andere App minimieren.

Das Feature wird in On-Premises- und in Cloud-Bereitstellungen unterstützt. In Cloud-Bereitstellungen können Web-Apps allerdings auf PiP minimiert werden. Sie können auch zwischen einer Desktopsitzung und einer Web-App wechseln, indem Sie auf das unverankerte Fenster klicken.

> **Hinweis:**
>
> Es können nur zwei Apps gleichzeitig aktiv sein. Eine App im Vollbildmodus und eine zweite minimiert als Bild-im-Bild:
>
> - 2 Web- oder SaaS-Apps
> - 1 Web- oder SaaS-App und 1 virtuelle App oder Desktopsitzung

Bekannte Einschränkungen:

- Der Bild-im-Bild-Modus ist nicht verfügbar, wenn externe Peripheriegeräte wie eine Maus oder Tastatur oder ein externer Monitor angeschlossen sind.
- Wenn Ihr Gerät bei aktiviertem Bild-im-Bild-Modus an einen externen Monitor angeschlossen wird, reagiert die Citrix Workspace-App nicht und die Zurück-Schaltfläche ist in den **Anzeigeeinstellungen** innerhalb der Desktopsitzung nicht verfügbar.

Unterstützung für den nativen Nicht-Spiegeln-Modus von Apple

Technical Preview ab Version 22.12.0	Aktivierungsformular	Feedback-Formular

Sie können die Anzeige auf dem iPad OS 16.2 jetzt im Nicht-Spiegeln-Modus von Apple erweitern. Sie können mehrere Aufgaben ausführen, indem Sie die Citrix Workspace-App, virtuelle Apps und virtuelle Desktops auf dem externen Bildschirm ausführen und den iPad-Bildschirm leer lassen, um andere native Apps auszuführen.

> **Hinweis:**
>
> Die Unterstützung für die Anzeige im Nicht-Spiegeln-Modus von Apple ist nur für ausgewählte

> iPad-Modelle verfügbar. Weitere Informationen finden Sie in der Dokumentation von Apple.

Wenn Sie dieses Technical Preview-Feature nicht verwenden möchten, können Sie die Citrix Workspace-App jederzeit im Vollbildmodus verwenden.

Unterstützung für besseres Single Sign-On (SSO) bei Web- und SaaS-Apps

Technical Preview ab Version 22.3.5	Aktivierungsformular	Feedback-Formular

Diese Funktion vereinfacht die Konfiguration von SSO für interne Web-Apps und SaaS-Apps bei Verwendung von externen Identitätsanbietern (IdP). Die verbesserte SSO-Erfahrung reduziert den gesamten Prozess auf einige Befehle. Es entfällt die Voraussetzung, Citrix Secure Private Access in der IdP-Kette konfigurieren zu müssen, um SSO einzurichten. Zudem ist die Benutzererfahrung verbessert, vorausgesetzt, derselbe IdP wird für die Authentifizierung bei der Workspace-App und bei der zu startenden Web- oder SaaS-App verwendet.

Von Technical Preview zu allgemeiner Verfügbarkeit

Dienst oder Feature	Allgemein verfügbare Version
Unterstützung für Dokumentenscanner	24.5.0
Unterstützung für FIDO2-basierte Authentifizierung	23.9.0

Systemanforderungen und Kompatibilität

March 27, 2024

Geräteanforderungen

- Die Citrix Workspace-App für iOS Version 23.9.0 und höher unterstützt iOS 17 und iPadOS 17.
- Die Citrix Workspace-App für iOS Version 22.9.0 und höher unterstützt iOS 16 und iPadOS 16.
- Die Citrix Workspace-App für iOS Version 21.9.1 und höher unterstützt iOS 15 und iPadOS 15.

- Die Citrix Workspace-App für iOS Version 20.9.0 und höher unterstützt iOS 14 und iPadOS 14.
- Dieses Softwareupdate wurde für die folgenden Geräte validiert:
  - iPhone 7x-Modelle, iPhone 8x-Modelle und nur iPhone X-Modelle.
  - Alle iPad-Modelle, einschließlich iPad Pro. Ausnahmen: iPad 1 und iPad 2 werden nicht unterstützt.
- Unterstützung externer Bildschirme
  - iPhone, soweit vom iOS unterstützt.
  - iPad: Gemäß Unterstützung von iOS (nicht der ganze Bildschirm wird verwendet).

Serveranforderungen

Installieren Sie alle aktuellen Hotfixes für die Server.

- Für Verbindungen mit virtuellen Desktops und Apps unterstützt die Citrix Workspace-App Citrix StoreFront und das Webinterface.

  StoreFront:

  - StoreFront 3.6 oder höher (empfohlen). Die Citrix Workspace-App wurde für die aktuelle StoreFront-Version validiert. Unterstützte Vorversionen sind StoreFront 2.6 und höher.

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

    > **Hinweis:**
    >
    > In XenApp und XenDesktop 7.8 führte Citrix Unterstützung für den Framehawk Virtual Channel und 3D Pro ein. Diese Funktionalität wurde auf die Citrix Workspace-App ausgeweitet.

  - StoreFront wurde mit einer Workspace für Website konfiguriert.

    Bietet Zugriff auf StoreFront-Stores über einen Safari-Webbrowser. Benutzer müssen die ICA-Datei manuell im Browser öffnen. Weitere Informationen zu den Einschränkungen in dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

  Webinterface:

  - Webinterface 5.4 mit Webinterface-Sites
  - Webinterface 5.4 mit XenApp und XenDesktop-Sites
  - Webinterface auf Citrix Gateway (browserbasierter Zugriff nur mit Safari)

    Aktivieren Sie die Rewrite-Richtlinien, die vom Citrix Gateway bereitgestellt werden.

- **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 und 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 bei Workspace für Web (Browser)	Citrix Gateway bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zweistufige 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 mit oder ohne installiertem zugeordneten Plug-In auf dem Gerät enthalten.

> **Hinweis:**
>
> Das Citrix Gateway Plug-In für die Endpunktanalyse (EPA) wird für Citrix Workspace unterstützt. In der nativen Citrix Workspace-App wird es nur unterstützt, wenn die nFactor-Authentifizierung verwendet wird. Weitere Informationen finden Sie unter Konfigurieren des EPA-Scans für die Vor- und Nachauthentifizierung als Faktor in der Multifaktorauthentifizierung (nFactor) in der Dokumentation zu Citrix ADC.

Für Verbindungen mit dem Webinterface 5.4 unterstützt die Citrix Workspace-App die folgenden Authentifizierungsmethoden:

> **Hinweis:**
>
> Im Webinterface wird der Begriff "Explizit"für die Domänen- und Sicherheitstokenauthentifizierung verwendet.

	Webinterface (Browser)	Webinterface XenApp- und XenDesktop-Site	Citrix Gateway bei Webinterface (Browser)	Citrix Gateway bei Webinterface XenApp und XenDesktop-Site
Anonym	Ja			
Domäne	Ja	Ja	Ja*	
Domänen-Passthrough	Ja			
Sicherheitstoken			Ja*	
Zweistufige 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 für die Zertifizierungsstelle der Organisation auf dem Gerät installiert ist.

> **Hinweis:**
>
> Wenn das Zertifikat des Remotegateways sich beim Herstellen der Verbindung nicht verifizieren lässt, wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Dieses Problem liegt daran, dass das Stammzertifikat nicht im lokalen Keystore enthalten ist. Wenn der Benutzer weiterarbeitet, wird eine Liste der Anwendungen angezeigt; die Anwendungen können jedoch nicht gestartet werden.

Manuell installiertes Zertifikat In iOS 10.3 und höher wird einem Zertifikat, das Sie manuell in einem Profil installiert haben, nicht automatisch für SSL vertraut. Vertrauen von manuell installierten Zertifikatprofilen in iOS:

1. Stellen Sie sicher, dass das Zertifikatprofil auf dem Gerät installiert ist.
2. Navigieren Sie zu **Einstellungen** > **Allgemein** > **Info** > **Zertifikatsvertrauenseinstellungen**.

   Jedes Stammzertifikat (Root-Zertifikat), das über ein Profil installiert wurde, wird unter **Volles Vertrauen für Root-Zertifikate aktivieren** angezeigt.
3. Sie können das Vertrauen für jedes Stammzertifikat ein- und ausschalten.

Importieren von Stammzertifikaten auf iPad- und iPhone-Geräten Erwerben Sie das Stammzertifikat des Zertifikatausstellers und senden es per E-Mail an ein E-Mail-Konto, das auf dem Gerät konfiguriert ist. Wenn Sie auf den Anhang klicken, werden Sie zum Importieren des Stammzertifikats aufgefordert.

Zertifikate mit Platzhalterzeichen Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate und Citrix Gateway Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Zertifikat des Citrix Gateway- oder Access Gateway-Servers angehängt werden. Informieren Sie sich für Access Gateway-Installationen unter Install, link, and update certificates in der Citrix ADC-Dokumentation über Zertifikate, die Ihren Anforderungen entsprechen.

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

Die Citrix Workspace-App unterstützt alle Authentifizierungsmethoden, die von Access Gateway unterstützt werden.

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate Releases der Citrix Workspace-App haben eine strengere Validierungsrichtlinie für Serverzertifikate.

> **Wichtig!**
>
> Bestätigen Sie vor der Installation der Citrix Workspace-App, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:
>
> - Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat
> - Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
> - Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
> - Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet die Citrix Workspace-App jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases überprüft die Citrix Workspace-App dann, ob die Zertifikate vertrauenswürdig sind. Wenn nicht alle Zertifikate vertrauenswürdig sind, schlägt die Verbindung fehl.

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

Der Server bzw. das Gateway muss mit den richtigen Zertifikaten konfiguriert sein. Sind nicht die richtigen Zertifikate vorhanden, schlagen Verbindungen mit der Citrix Workspace-App u. U. fehl.

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

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Beispielstammzertifikat

Die Citrix Workspace-App überprüft dann, ob alle Zertifikate gültig sind. Die Citrix Workspace-App überprüft auch, ob das **Beispielstammzertifikat** bereits vertrauenswürdig ist.

> **Hinweise:**
>
> - Wenn die Citrix Workspace-App das **Beispielstammzertifikat** nicht als vertrauenswürdig einstuft, schlägt die Verbindung fehl.
> - Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Stellen Sie sicher, dass

> Ihre Konfiguration das entsprechende Stammzertifikat verwendet, wenn Sie eine strengere Validierung benötigen.

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 eins verfügbar (**DigiCert Baltimore Root**/**Baltimore CyberTrust Root**).

Wenn Sie **GTE CyberTrust Global Root** auf dem Gateway konfigurieren, schlagen die Verbindungen mit der Citrix Workspace-App auf diesen Benutzergeräten fehl. Aus der Dokumentation der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat verwendet werden muss. Beachten Sie außerdem, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.

Die Citrix Workspace-App verwendet dann diese beiden Zertifikate. Die App sucht nach einem Stammzertifikat auf dem Benutzergerät. Wenn die App ein gültiges Zertifikat findet, das auch vertrauenswürdig ist (z. B. **Beispielstammzertifikat**), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl.

Diese Konfiguration stellt das von der Citrix Workspace-App benötigte Zwischenzertifikat zur Verfügung, ermöglicht der Citrix Workspace-App aber auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats.

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

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Falsches Stammzertifikat

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

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall ist das Gateway normalerweise wie folgt mit allen Zwischenzertifikaten konfiguriert, jedoch nicht mit dem Stammzertifikat:

- Beispielserverzertifikat
- Beispielzwischenzertifikat 1
- Beispielzwischenzertifikat 2

> **Wichtig!**
>
> Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat. Diese Zertifikate sind für Situationen vorgesehen, wenn mehr als ein Stammzertifikat vorhanden ist und ein früher ausgestelltes Stammzertifikat zur gleichen Zeit wie ein später ausgestelltes Stammzertifikat verwendet wird. In diesen Fällen existieren mindestens zwei Zwischenzertifikate.

Beispielsweise hat das früher ausgestellte Stammzertifikat **Class 3 Public Primary Certification Authority** das entsprechende übergreifende Zwischenzertifikat **Verisign Class 3 Public Primary Certification Authority – G5**. Ein entsprechendes später ausgestelltes Stammzertifikat **Verisign Class 3 Public Primary Certification Authority - G5** ist ebenfalls verfügbar und es ersetzt **Class 3 Public Primary Certification Authority**. Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.

> **Hinweis:**
>
> Das übergreifende Zwischenzertifikat und das Stammzertifikat haben denselben Antragstellernamen (Ausgestellt für), das übergreifende Zwischenzertifikat hat jedoch einen anderen Ausstellernamen (Ausgestellt von). Durch den Antragstellernamen unterscheidet sich das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat wie **Beispielzwischenzertifikat 2**.

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

- Beispielserverzertifikat
- Beispielzwischenzertifikat

Konfigurieren Sie das Gateway nicht für die Verwendung des übergreifenden Zwischenzertifikats, weil die Citrix Workspace-App sonst das früher ausgestellte Stammzertifikat auswählt:

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Übergreifendes Beispielzwischenzertifikat [nicht empfohlen]

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

- Beispielserverzertifikat

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

Installation und Upgrade

November 8, 2023

Sie können die neueste Version der Citrix Workspace-App aus dem Apple Store zum Installieren bzw. für ein Upgrade herunterladen.

- Erstbenutzer können die Citrix Workspace-App aus dem Apple Store herunterladen und auf ihrem Gerät installieren.
- Benutzer mit vorhandener App können über den Apple Store ein Upgrade auf die neueste Version der Citrix Workspace-App ausführen.

Informationen zum Konfigurieren der Citrix Workspace-App finden Sie unter Konfigurieren.

Informationen zu den Features in der Citrix Workspace-App für iOS finden Sie unter Citrix Workspace-App –Featurematrix.

Erste Schritte

March 27, 2024

Setup

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

- XenApp und XenDesktop-Sites
- Citrix Virtual Apps and Desktops- und Citrix DaaS-Sites (früher Citrix Virtual Apps and Desktops Service).

Mit Webinterface-Sites können Clientgeräte eine Verbindung mit der Serverfarm herstellen. Die Authentifizierung zwischen Citrix Workspace-App für iOS und einer Webinterface-Site kann mit verschiedenen Lösungen gehandhabt werden, u. a. Citrix Secure Web Gateway.

Außerdem können Sie StoreFront so konfigurieren, dass Authentifizierungs- und Ressourcenbereitstellungsdienste für die Citrix Workspace-App bereitgestellt werden; Sie können dann zentralisierte Unternehmensstores erstellen, die Benutzern Desktops, Anwendungen und anderen Ressourcen bereitstellen.

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

Konfigurieren Sie die folgenden Komponenten in der Bereitstellung, wie hier beschrieben, bevor Benutzer auf Anwendungen zugreifen, die in der Citrix Virtual Apps and Desktops- und Citrix DaaS-Umgebung ausgeführt werden.

- Ziehen Sie die folgenden Optionen in Betracht, wenn Sie Anwendungen in den Farmen veröffentlichen, um die Erfahrung für die Benutzer zu steigern, die über StoreFront-Stores auf die Anwendungen zugreifen.
  - Verwenden Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen, da diese Beschreibungen Benutzern in der Citrix Workspace-App angezeigt werden.
  - Sie können veröffentlichte Anwendungen für mobile Benutzer hervorheben. Sie können die Anwendungen in der Liste "Highlights"auflisten. Bearbeiten Sie die Eigenschaften der Anwendungen, die auf Ihren Servern veröffentlicht sind, um diese Liste in der Citrix Workspace-App aufzufüllen. Sie können jetzt die Zeichenfolge "KEYWORDS: Featured"an den Wert des Felds **Anwendungsbeschreibung** anhängen.
  - Der AutoAnpassen-Bildschirmmodus passt die Anwendung an die Bildschirmgröße von Mobilgeräten an. Um diesen Modus zu aktivieren, bearbeiten Sie die Eigenschaften der Anwendungen, die auf Ihren Servern veröffentlicht sind, und hängen Sie die mobile Zeichenfolge "KEYWORDS:"an den Wert des Felds für die Anwendungsbeschreibung an. Mit diesem Schlüsselwort wird auch der automatische Bildlauf für die Anwendung aktiviert.
  - Sie können eine Anwendung automatisch für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge "KEYWORDS: Auto"an die Beschreibung anhängen, wenn Sie die Anwendung in Citrix Virtual Apps veröffentlichlen. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Wenn das Webinterface in der Citrix Virtual Apps and Desktops- und Citrix DaaS-Bereitstellung keine Site hat, erstellen Sie eine Site. Der Name und die Erstellung der Site hängen von der installierten Webinterface-Version ab.

Manuelles Setup

Wenn die Citrix Workspace-App eine Verbindung mit einem Citrix Gateway herstellt, sucht die Citrix Workspace-App nach der Authentifizierung im Allgemeinen nach einer XenApp und XenDesktop-Site oder Citrix Virtual Apps-Website. Wenn keine Site gefunden wird, zeigt die Citrix Workspace-App für iOS einen Fehler an. Konfigurieren Sie ein Konto manuell, um diese Situation zu vermeiden, damit die Citrix Workspace-App für iOS eine Verbindung mit Citrix Gateway herstellen kann.

1. Tippen Sie auf das Symbol **Konten** > **Bildschirm "Konten"** > **Pluszeichen (+)**. Der Bildschirm "Neues Konto"wird angezeigt.
2. Tippen Sie links unten im Bildschirm auf das Symbol links neben **Optionen** und tippen Sie auf **Manuelles Setup**. Andere Felder werden auf dem Bildschirm angezeigt.

3. Geben Sie im Feld **Adresse** die sichere URL der Site oder des Citrix Gateways an (z. B. agee.mycompany.com).
4. Wählen Sie eine der folgenden Verbindungsoptionen. Die übrigen Felder auf dem Bildschirm werden entsprechend der Auswahl geändert.

    - **Webinterface**: Bei Auswahl zeigt die Citrix Workspace-App eine Citrix Virtual Apps-Website an, die einem Webbrowser ähnelt. Diese Benutzeroberfläche wird auch Webansicht genannt.
    - **XenApp Services**: Bei Auswahl sucht die Citrix Workspace-App für iOS eine bestimmte XenApp und XenDesktop-Site, für die eine Authentifizierung über Citrix Gateway nicht konfiguriert ist. Geben Sie für die zusätzlichen Optionen, die auf diesem Bildschirm angezeigt werden, die Anmeldeinformationen für die Site an.
        - \<StoreFront-FQDN\>: Bei mehreren Stores wird eine Liste angezeigt und der Benutzer kann den Store auswählen, der hinzugefügt wird.
        - <StoreFront-FQDN>/citrix/<Storename>: Mit dieser Option wird der StoreFront-Store <Storename> hinzugefügt.
        - \<StoreFront-FQDN\>/citrix/PnAgent/config.xml: Mit dieser Option wird der Standard-PNAgent-Legacystore hinzugefügt.
        - <StoreFront-FQDN>/citrix/<Storename>/PnAgent/config.xml: Mit dieser Option wird der PNAgent-Legacystore, der <Storename> zugeordnet ist, hinzugefügt.
    - Citrix Gateway: Bei Auswahl stellt die Citrix Workspace-App für iOS eine Verbindung mit einer XenApp und XenDesktop-Site über einen bestimmten Citrix Gateway her. Wählen Sie in den zusätzlichen Optionen auf diesem Bildschirm die Serveredition und die Anmeldeinformationen aus, einschließlich des ggf. erforderlichen Sicherheitstokens für die Authentifizierung.

5. Verwenden Sie für die Zertifikatssicherheit die Einstellung im Feld "Zertifikatwarnungen" ignorieren und legen Sie fest, ob eine Verbindung mit dem Server hergestellt wird, selbst wenn das Zertifikat ungültig, selbstsigniert oder abgelaufen ist. Die Standardeinstellung ist AUS.
   Wichtig: Wenn Sie diese Option aktivieren, müssen Sie eine Verbindung mit dem richtigen Server herstellen. Citrix empfiehlt dringend, dass alle Server ein gültiges Zertifikat haben, um Benutzergeräte vor Onlinesicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt, dass die Zertifikatsicherheit nicht ausgelassen wird.
6. Tippen Sie auf Speichern.
7. Geben Sie den Benutzernamen und das Kennwort (oder das Token, wenn Sie die zweistufige Authentifizierung ausgewählt haben) ein und tippen Sie dann auf "Anmelden". Der Citrix Workspace-App für iOS-Bildschirm wird angezeigt, von dem Sie auf die Desktops zugreifen und die Anwendungen 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 die Citrix Gateway-Versionen bis 13.
> - Die Citrix Workspace-App für iOS unterstützt nur XenApp und XenDesktop-Site auf dem Webinterface.
> - Die Citrix Workspace-App für iOS unterstützt das Starten von Sitzungen über Workspace für Web, sofern der verwendete Browser mit Workspace für Web funktioniert. Wenn die Starts nicht erfolgen, konfigurieren Sie Ihr Konto direkt über die Citrix Workspace-App für iOS. Benutzer müssen die ICA-Datei mit der Browserfunktion zum Öffnen in Workspace manuell öffnen. Weitere Informationen zu den Einschränkungen in dieser Bereitstellung finden Sie in der StoreFront-Dokumentation.

Mit StoreFront bestehen die 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 folgenden Sites zählen und zusammenfassen:

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

1. Installieren und konfigurieren Sie StoreFront. Weitere Informationen finden Sie in der StoreFront-Produktdokumentation. Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für die Citrix Workspace-App für iOS erstellen.
2. Stores für StoreFront konfigurieren Sie genauso wie andere Citrix Virtual Apps and Desktops und Citrix DaaS-Anwendungen. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich. Weitere Informationen finden Sie unter "Benutzerzugriffsoptionen" im StoreFront-Abschnitt der Produktdokumentation. Verwenden Sie für Mobilgeräte eine dieser Methoden:
    - Provisioningdateien: Sie können Benutzern Provisioningdateien (.cr) bereitstellen, die Verbindungsdetails für die Stores enthalten. Nach der Installation öffnen Benutzer die Datei auf dem Gerät, um die Citrix Workspace-App für iOS automatisch zu konfigurieren. Workspace für Websites bieten Benutzern standardmäßig eine Provisioningdatei für den einen Store, für den die Site konfiguriert ist. Alternativ können Sie mit der Citrix StoreFront-Verwaltungskonsole Provisioningdateien für einen oder viele Stores generieren und manuell an die Benutzer verteilen.
    - Manuelle Konfiguration: Sie können Benutzern die Citrix Gateway- oder Store-URL, mit der sie auf ihre Desktops und Anwendungen zugreifen können, direkt mitteilen. Für Verbindungen über Citrix Gateway benötigen Benutzer außerdem die Produktedition und erforderliche Authentifizierungsmethode. Nach der Installation geben Benutzer diese

Informationen in der Citrix Workspace-App ein. Die Citrix Workspace-App fordert die Benutzer auf, sich anzumelden, falls die Verbindung erfolgreich überprüft werden konnte.

- Automatische Konfiguration: Tippen Sie auf dem Willkommenbildschirm auf **Konto hinzufügen** und geben Sie die URL des StoreFront-Servers in das Feld "Adresse"ein. Das Konto wird beim Hinzufügen automatisch konfiguriert.

Konfigurieren von Citrix Gateway

Wenn Benutzer sich von außerhalb mit dem internen Netzwerk verbinden, konfigurieren Sie die Authentifizierung über Citrix Gateway. Dies können zum Beispiel Benutzer sein, die über das Internet von einem Remotestandort eine Verbindung herstellen.

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

Webinterface

Zum Konfigurieren der Webinterface-Site können Benutzer mit iPhone- und iPad-Geräten Anwendungen über die Webinterface-Site und den integrierten Safari-Browser auf dem Mobilgerät starten. Konfigurieren Sie die Webinterface-Site genauso wie andere Citrix Virtual Apps-Anwendungen. Wenn keine XenApp und XenDesktop-Site für das Mobilgerät konfiguriert ist, verwendet die Citrix Workspace-App für iOS automatisch die Webinterface-Site. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich.

Der integrierte Safari-Browser unterstützt das Webinterface 5.x.

Starten von Anwendungen auf dem iOS-Gerät

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

Automatisches Provisioning für mobile Geräte

In StoreFront können Sie mit den Aufgaben **Multistore-Provisioningdatei exportieren** und **Provisioningdatei exportieren** Dateien mit Verbindungsinformationen für Stores generieren, z. B. für Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden. Stellen Sie diese Dateien Benutzern zur Verfügung, damit diese die Citrix Workspace-App für iOS automatisch mit den Details der Stores konfigurieren können. Benutzer können auch Citrix Workspace-App für iOS-Provisioningdateien von Workspace für Websites erhalten.

> **Wichtig:**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Suchen Sie auf dem Windows-Startbildschirm oder Apps-Bildschirm nach der Citrix StoreFront-Kachel und klicken Sie darauf. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores.
2. Um eine Provisioningdatei mit Details für mehrere Stores zu generieren, klicken Sie im Bereich "Aktionen"auf Multistore-Provisioningdatei exportieren und wählen Sie die Stores aus, die der Datei hinzugefügt werden sollen.
3. Klicken Sie auf "Exportieren"und speichern Sie die Provisioningdatei mit der Erweiterung `.cr` an einem geeigneten Speicherort im Netzwerk.

Benutzerzugriffsinformationen

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

- Konfigurieren der e-mail-basierten Kontenermittlung
- Bereitstellen einer Provisioningdatei für Benutzer
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

Konfigurieren der e-mail-basierten Kontenermittlung

Sie können die Citrix Workspace-App für iOS für die e-mail-basierte Kontenermittlung konfigurieren. Nach der Konfiguration geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration der Citrix Workspace-App für iOS ein. Die Citrix Workspace-App ermittelt auf der Basis von DNS-Dienstdatensätzen den Access Gateway- oder StoreFront-Server oder das virtuelle Endpoint Management-Gerät, der bzw. das der E-Mail-Adresse zugeordnet ist, und fordert die Benutzer zur Anmeldung auf, sodass sie auf ihre gehosteten Anwendungen, Desktops und Daten zugreifen können.

> **Hinweis:**
>
> Die e-mail-basierte Kontenermittlung wird nicht unterstützt, wenn die Citrix Workspace-App für iOS eine Verbindung zu einer Webinterface-Bereitstellung herstellt.

DNS Service Location (SRV)-Datensatz hinzufügen, um die E-Mail-basierte Discovery zu ermöglichen Während der Erstkonfiguration kann die Citrix Workspace-App Active Directory DNS-Server (Domain Name System) kontaktieren, um Details zu den für Benutzer verfügbaren Stores zu erhalten. Dies bedeutet, dass Benutzer die Zugriffsinformationen 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 Informationen zur Domäne aus der E-Mail-Adresse abrufen.

Schrittfolge zum Auffinden verfügbarer Stores in der Citrix Workspace-App, basierend auf den E-Mail-Adressen der Benutzer:

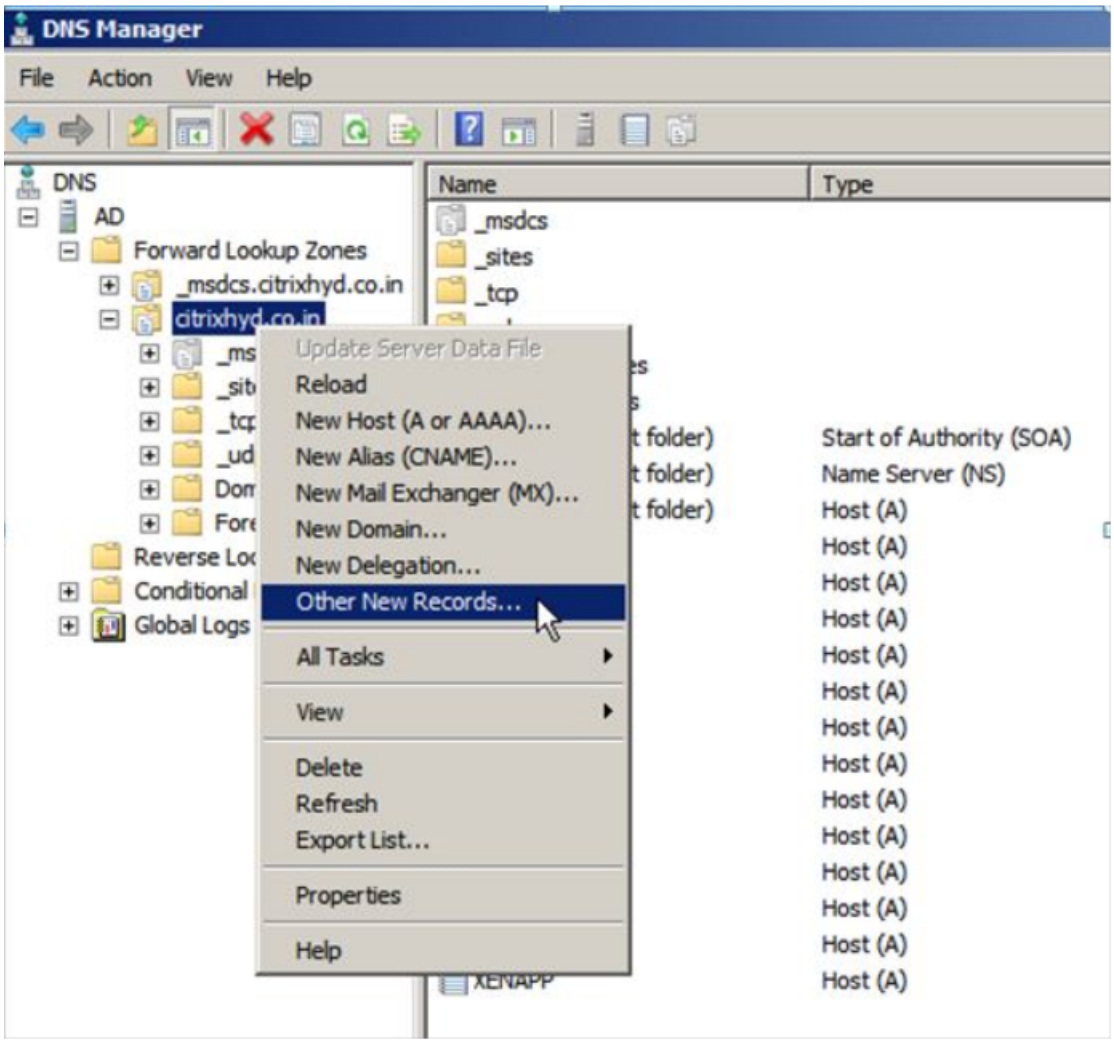
- Konfigurieren von SRV-Ressourceneinträgen für Access Gateway.
- Konfigurieren der StoreFront- oder AppController-Verbindungen auf Ihrem DNS-Server.

Sie müssen ein gültiges Serverzertifikat auf dem Access Gateway-Gerät und dem StoreFront- oder AppController-Server installieren, um die e-mail-basierte Kontenermittlung zu aktivieren. Des Weiteren muss die vollständige Kette zum Stammzertifikat gültig sein. Zum Optimieren der Benutzerfreundlichkeit installieren Sie ein Zertifikat entweder mit:

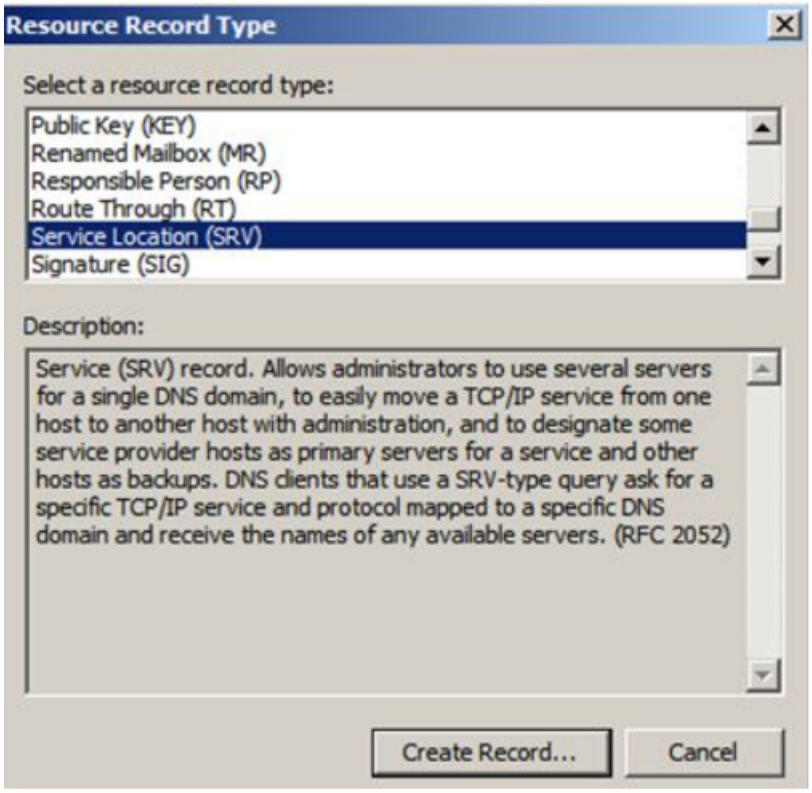
- einem Antragsteller
- einem alternativen Antragstellernamen: *discoverReceiver.domain*
- einem Platzhalterzertifikat für die Domäne, die die E-Mail-Konten Ihrer Benutzer enthält.

Um Benutzern die Konfiguration der Citrix Workspace-App für iOS mit einer E-Mail-Adresse zu ermöglichen, fügen Sie Ihrer DNS-Zone einen SRV-Eintrag wie folgt hinzu:

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



4. Das Dialogfeld **Ressourceneintragstyp** wird angezeigt.
5. Unter **Wählen Sie einen Ressourceneintragstyp** wählen Sie die Option **Dienstidentifizierung (SRV)** aus.
6. Wählen Sie **Eintrag erstellen** aus.



7. Das Dialogfeld "Eigenschaften"wird angezeigt.
8. Wählen Sie die Registerkarte **Dienstidentifizierung** aus.
9. Geben Sie unter **Service** 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 Ihr Access Gateway-Gerät (zur Unterstützung von lokalen Benutzern und Remotebenutzern) oder den StoreFront- oder AppController-Server an (um nur Benutzer im lokalen Netzwerk zu unterstützen).
12. Klicken Sie auf "OK".

> **Hinweis:**
>
> Ihr StoreFront-FQDN muss eindeutig sein und sich vom FQDN des virtuellen Access Gateway-Servers unterscheiden. Das Verwenden desselben FQDN für StoreFront und den virtuellen Access Gateway-Server wird nicht unterstützt. Die Citrix Workspace-App erfordert eine eindeutige Adresse als StoreFront-FQDN, 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 Kontenermittlung nicht verwenden.

Bereitstellen einer Provisioningdatei für Benutzer

Sie können mit StoreFront ein Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, um eine automatische Konfiguration der Citrix Workspace-App für iOS zu ermöglichen. Nach der Installation der Citrix Workspace-App für iOS öffnen Benutzer die Datei mit der Erweiterung `.cr` auf dem Gerät, um die Citrix Workspace-App für iOS zu konfigurieren. Wenn Sie Workspace für Websites konfigurieren, können Benutzer die Citrix Workspace-App für iOS-Provisioningdateien auch von diesen Seiten abrufen.

Weitere Informationen finden Sie in der StoreFront-Dokumentation.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

Wenn Sie Benutzern Kontoangaben für die manuelle Eingabe bereitstellen, müssen Sie folgende Informationen übermitteln, damit die Benutzer erfolgreich eine Verbindung zu den gehosteten Desktops herstellen können:

- Die StoreFront-URL oder die XenApp and XenDesktop-Site mit den gehosteten Ressourcen, z. B.: `servername.company.com`.
- Stellen Sie für den Zugriff mit Citrix Gateway die Citrix Gateway-Adresse und die erforderliche Authentifizierungsmethode bereit.

Wenn ein Benutzer Angaben für ein neues Konto macht, versucht die Citrix Workspace-App, die Verbindung zu überprüfen. Im Erfolgsfall fordert die Citrix Workspace-App für iOS den Benutzer auf, sich bei dem Konto anzumelden.

Citrix Workspace-App konfigurieren

March 27, 2024

In diesem Artikel werden Aufgaben aufgeführt, die Ihnen beim Konfigurieren der Citrix Workspace-App für iOS helfen.

Featureflags verwalten

Wenn ein Problem mit der Citrix Workspace-App in der Produktion auftritt, kann das betroffene Feature dynamisch in der Citrix Workspace-App deaktiviert werden. Dies ist selbst nach der Bereitstellung des Features möglich. Wir verwenden Featureflags und den Drittanbieterdienst “LaunchDarkly”. Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den

ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen.

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

Datenverkehr für folgende URLs zulassen

- app.launchdarkly.com
- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com

IP-Adressen in einer Positivliste auflisten

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

LaunchDarkly-Systemanforderungen

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

- LaunchDarkly-Dienst.
- APNs-Listenerdienst

Provisioning zum Deaktivieren des LaunchDarkly-Diensts:

Sie können den LaunchDarkly-Dienst sowohl in On-Premises- als auch in Cloudstores deaktivieren.

In der Cloud können Sie den LaunchDarkly-Dienst deaktivieren, indem Sie das Attribut enableLaunchDarkly auf “false”setzen. Sie können hierfür den Global App Configuration Service verwenden.

```
{

    "assignedTo": [
        "AllUsersNoAuthentication"
    ],
```



```
    "category": "Third Party Services",
    "settings": [
        {

        "name": "Enable Launch Darkly",
        "value": "true"
         }

    ],
    "userOverride": false
 }

<!--NeedCopy-->
```

Weitere Informationen finden Sie in der Dokumentation zum Global App Configuration Service.

Führen Sie in der On-Premises-Bereitstellung folgende Schritte aus:

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

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

   Vor dem Tag navigieren Sie zu den Eigenschaften des Benutzerkontos:

   ```
   <properties>
   <clear/>
   </properties>
   <!--NeedCopy-->
   ```

3. Fügen Sie das Tag “enableLaunchDarkly”mit dem Wert “false”hinzu.
4. Fügen Sie das Tag “enableLaunchDarkly”mit dem Wert “false”hinzu.

   `<property name="enableLaunchDarkly"value="false"/>`

> **Hinweis:**
>
> Die meisten Features unterliegen einem Featureflag, das von LaunchDarkly gesteuert wird. In Umgebungen, in denen es deaktiviert ist, müssen Sie mindestens 90 Tage warten.

Inaktivitätstimeout für die Citrix Workspace-App

Administratoren können angeben, wie viel Leerlaufzeit zulässig ist. Nach dem Timeout wird eine Authentifizierungsaufforderung angezeigt.

Der Wert für das Inaktivitätstimeout kann zwischen einer Minute und 24 Stunden liegen. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert. Administratoren können die Eigenschaft “inac-

tivityTimeoutInMinutesMobile"mit einem PowerShell-Modul konfigurieren. Klicken Sie hier, um die PowerShell-Module für die Konfiguration der Citrix Workspace-App herunterzuladen.

Wenn Sie den angegebenen Timeoutwert erreicht haben, ist die Benutzererfahrung je nach konfiguriertem Authentifizierungstyp wie folgt:

- Nach dem Inaktivitätstimeout werden Sie zur biometrischen Authentifizierung aufgefordert, um wieder auf die Citrix Workspace-App zugreifen zu können.
- Wenn Sie die biometrische Authentifizierungsaufforderung abbrechen, wird die folgende Meldung angezeigt:

  Die Citrix Workspace-App ist gesperrt.

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

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

> **Hinweis:**
>
> Dieses Feature ist nur für Kunden in Workspace (Cloud) verfügbar.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

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

Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix. Die Daten sind gemäß der Anlage zur Sicherheit von Citrix Diensten 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 sammeln. Informieren Sie sich, wie Google die für Google Firebase gesammelten Daten verwendet.

Deaktivieren der Übertragung von CEIP-Daten an Citrix und Google Firebase:

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

> **Hinweis:**
>
> Es werden keine Daten für Benutzer in der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK) gesammelt.

Folgende CEIP-Datenelemente werden von Google Firebase erfasst:

Sitzungsinformationen und Sitzungsstartmethode	Citrix Stores und Store-Konfiguration	Authentifizierungstyp und Authentifizierungskonfiguration	ICA-Verbindungen
HDX-Sitzungsstart	Store-App-Sitzung	WebView-Aktion “Öffnen”	WebView-Aktion “Kopieren”
WebView-Aktion “Teilen”	Bewertung der Workspace-App	Verbindungsstatus, Verbindungsfehler, Connection Center-Nutzung	Externe Anzeige
Socketstatus	Sitzungsdauer	HDX über UDP	Startzeit der Sitzung
Geräteinformationen	Info zum Gerätemodell	Nutzungsstatistiken senden	App-Sprache, Workspace-App-Sprache
Sprache der Tastatur	Type des Citrix Store	Citrix Store-Kombination	Protokolltyp des Store
Store-Anzahl	HDX-UDP-Status	RSA-Tokeninstallationen	

Bekannte Einschränkungen

- In VDA 7.18 und früheren Versionen erfordert das Casting auf einen Workspace Hub, dass für den verwendeten Desktop oder die verwendete Ressource die h.264-Vollbildrichtlinie aktiviert und die Richtlinie für Legacygrafiken deaktiviert ist.

Sitzungsfreigabe

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

- **Trennen:** Abmelden vom Konto; die Windows-Anwendung bzw. der -Desktop wird weiter auf dem Server ausgeführt. Der Benutzer kann dann ein anderes Gerät starten, die Citrix Workspace-App für iOS öffnen und sich mit dem letzten Zustand wiederverbinden, bevor er die Verbindung mit dem iOS-Gerät trennt. Mit dieser Option können sich Benutzer von einem Gerät mit einem anderen Gerät wiederverbinden und in den ausgeführten Anwendungen weiterarbeiten.
- **Abmelden:** Abmeldung vom Konto und Schließen der Windows-Anwendung. Es erfolgt auch eine Abmeldung von Citrix Virtual Apps and Desktops und dem Citrix DaaS-Server. Mit dieser Option können Benutzer die Verbindung zum Server trennen und sich vom Konto abmelden. Wenn sie die Citrix Workspace App für iOS erneut starten, wird sie im Standardzustand geöffnet.

Cloudstores

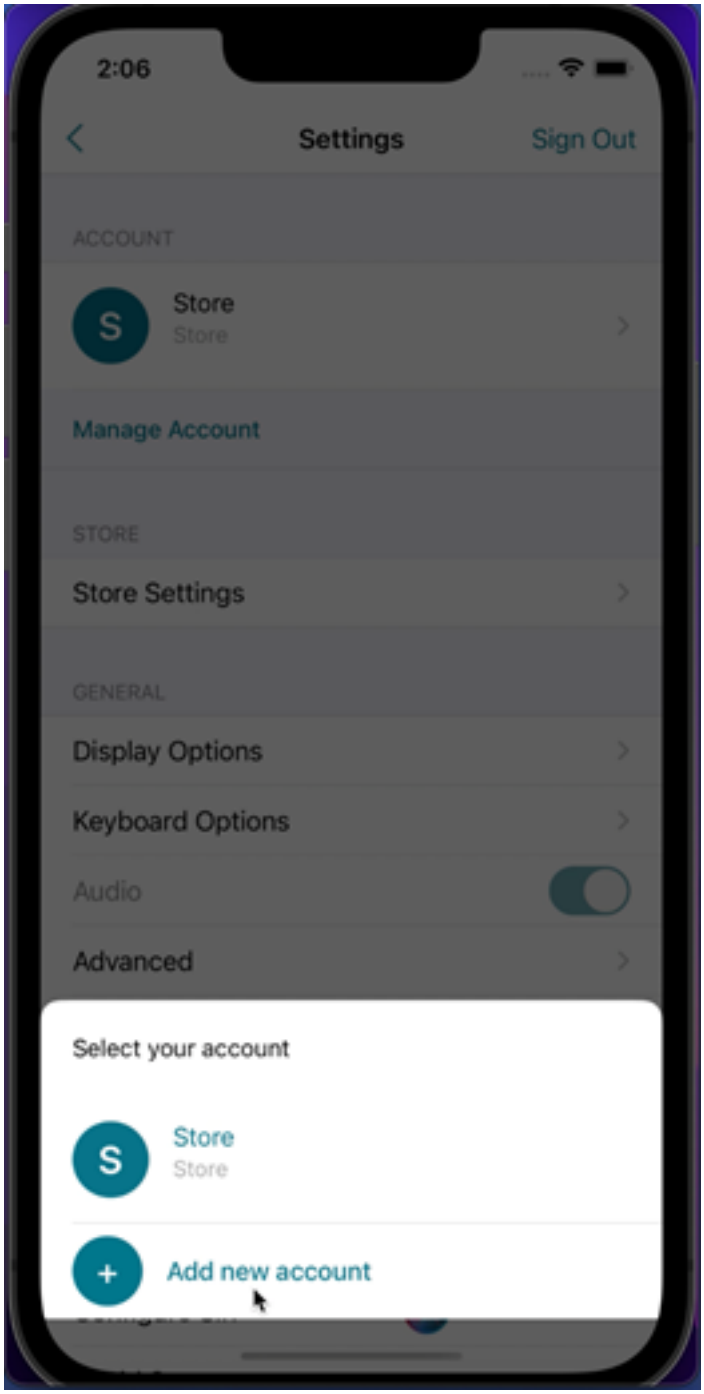
Sie können unabhängig von Ihrem Zugriffsort auf das Internet, SaaS-Apps und Websites zugreifen, die von Ihrer Organisation gehostet werden. Dieses Feature ist nur für Kunden in Cloudstores verfügbar.

Unterstützung für mehrere Cloudstores

Ab Version 24.1.0 können Sie der Citrix Workspace-App für iOS und iPadOS mehrere Cloudstorekonten hinzufügen. Damit können Endbenutzer einfacher mehrere Stores hinzufügen und zwischen ihnen wechseln. Das Feature verbessert die Benutzererfahrung beim Zugriff auf mehrere Stores.

Gehen Sie wie folgt vor, um ein weiteres Konto hinzuzufügen:

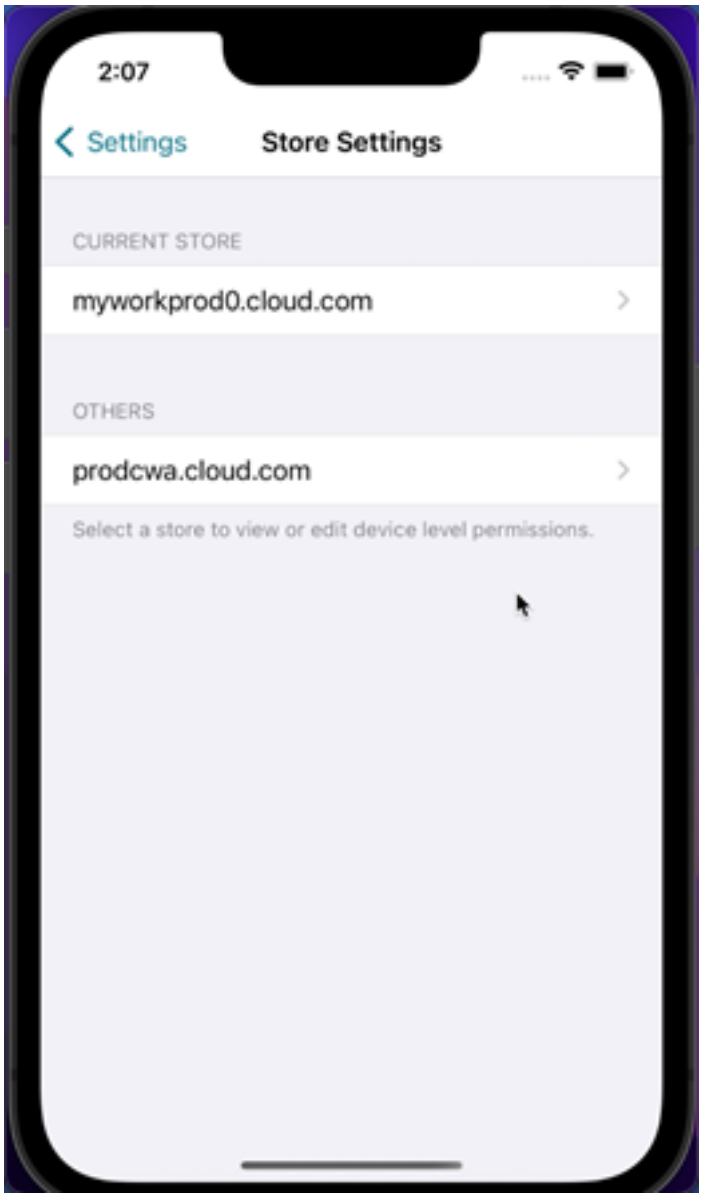
1. Navigieren Sie zu **Einstellungen > Konto verwalten**. Unten erscheint ein Dialogfeld mit der Liste Ihrer Konten.
2. Tippen Sie auf **Neues Konto hinzufügen**.



3. Geben Sie die URL oder E-Mail-Adresse ein, die Sie von Ihrem IT-Administrator erhalten haben. Zur Verwendung einer (optionalen) Smartcard für die Anmeldung tippen Sie auf **Smartcard verwenden**.
4. Tippen Sie auf **Weiter**. Das Dialogfeld **Anmelden** mit Feldern für Benutzernamen, Kennwort, Domäne und Passcode wird angezeigt.
5. Geben Sie die Informationen ein. Weitere Informationen zu den Feldern erhalten Sie von Ihrem

IT-Administrator.

6. Tippen Sie auf **Anmelden**. Ihr Konto ist jetzt eingerichtet.



Store-URL automatisch ausfüllen

Wenn Sie auf die umbenannte Citrix Workspace-App für iOS zugreifen, können Sie festlegen, dass die Store-URL automatisch ausgefüllt wird. Diese Funktion reduziert manuelle Eingriffe und ermöglicht einen schnellen Zugriff auf die App. Weitere Informationen zur App-Personalisierung finden Sie unter App Personalization.

Unterstützung für das gleichzeitige Löschen mehrerer Stores

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

Gehen Sie wie folgt vor, um auf dem Bildschirm **Stores** mehrere Stores gleichzeitig zu löschen:

1. Tippen Sie auf dem Bildschirm **Stores** auf **Auswählen**.
2. Wählen Sie Stores aus, die gelöscht werden sollen. Um alle Stores zu löschen, tippen Sie auf **Alle auswählen**.
3. Tippen Sie auf **Löschen**.

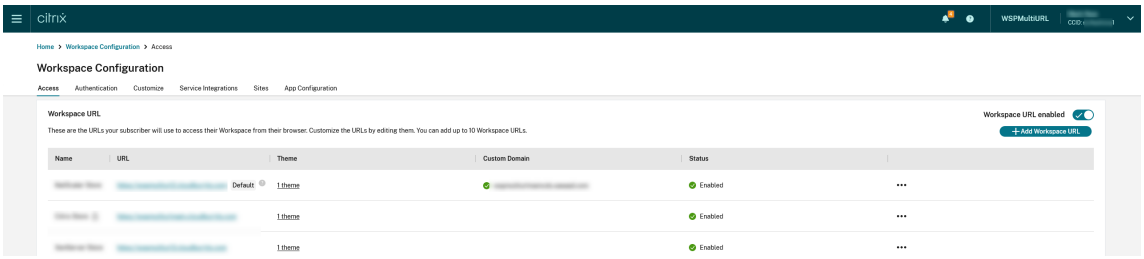
Unterstützung für Administratoren, um den Benutzer daran zu hindern, den Storenamen zu ändern

Bisher konnten Benutzer den Storenamen mithilfe der Option **Konto bearbeiten** ändern.

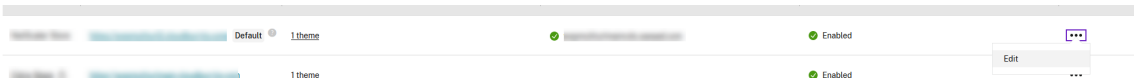
Ab 24.2.0 bietet Citrix Workspace-App für iOS Administratoren die Möglichkeit, den Benutzer daran zu hindern, den Storenamen zu ändern. Mit dieser Funktion können Administratoren die Storenamen leicht identifizieren und konsistent halten.

Gehen Sie wie folgt vor, um den Endbenutzern zu ermöglichen, den Storenamen zu ändern:

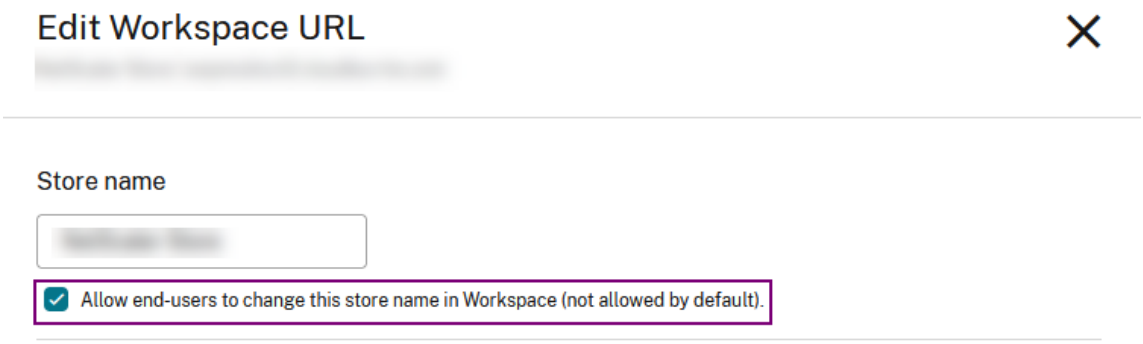
1. Melden Sie sich mit Ihren Anmeldeinformationen bei Citrix Cloud an.
2. Navigieren Sie zu **Workspace-Konfiguration > Zugriff**. Unter **Workspace-URL** finden Sie eine Liste der vorhandenen Store-URLs.



3. Klicken Sie auf die Auslassungspunkte bei dem Store, dessen Name von Endbenutzern von nun an geändert werden darf.
4. Wählen Sie **Bearbeiten**.



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



6. Klicken Sie auf **Speichern**.

Storenamen automatisch ausfüllen

Ab der Version 24.2.0 unterstützt Citrix Workspace-App für iOS Aktualisierungen von Storenamen durch den Administrator und überträgt die aktualisierten Storenamen automatisch an den Benutzer. Diese Funktion verbessert die Benutzererfahrung, da kein manuelles Eingreifen bei der Aktualisierung des Storenamens erforderlich ist.

> **Hinweis:**
>
> Dieses Feature kann nur wirksam werden, wenn der Administrator das Ändern des Storenamens durch den Benutzer gesperrt hat.

Verbesserung von End User Experience Monitoring

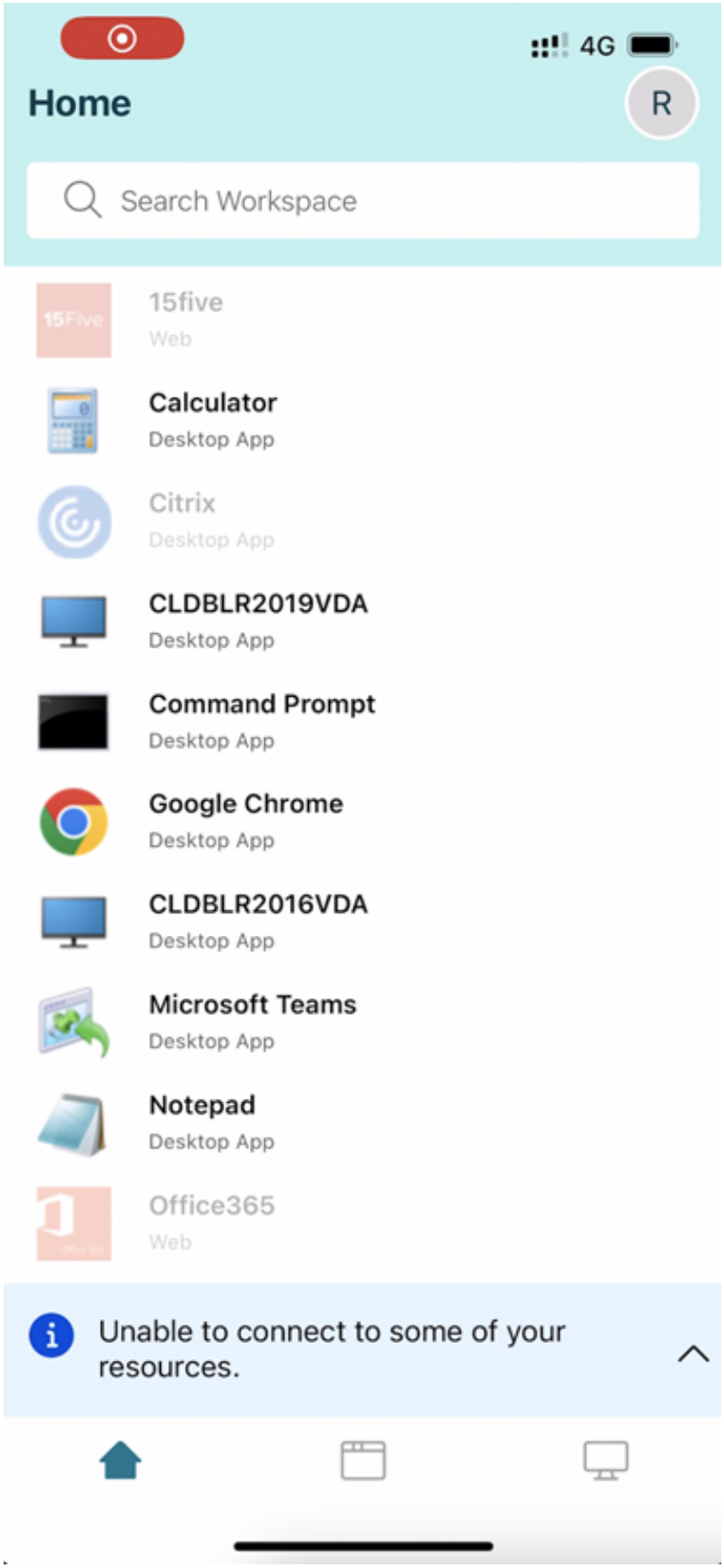
Wir unterstützen jetzt Client-Startwerte für EUEM (End User Experience Monitoring). EUEM dient zum Sammeln von sehr detaillierten Überwachungsdaten für die Sitzungserfahrung in Echtzeit. Die Daten werden an das Director-Dashboard gesendet, damit der Administrator die Benutzererfahrung überwachen kann. Die Daten werden über den auf dem VDA vorhandenen Session Experience Monitoring Service (SEMS) gesammelt. Zu den für die Überwachung im Dashboard verfügbaren Client-Startwerten gehören Folgende:

- Dauer des ICA-Dateidownloads
- Sitzungserstellungsdauer auf Client “Sitzungserstellungsdauer auf Client”gibt die Zeit an, die zum Erstellen einer Sitzung benötigt wird. Sie wird ab dem Starten der ICA-Datei bis zum Verbindungsaufbau berechnet.
- Sitzungslookupdauer auf Client “Sitzungslookupdauer auf Client”gibt die Zeit an, die benötigt wird, um jede Sitzung zum Hosten der angeforderten veröffentlichten Anwendung abzufragen. Die Überprüfung wird auf dem Client durchgeführt, um festzustellen, ob eine bestehende Sitzung die Anforderung zum Starten der Anwendung verarbeiten kann.

- Citrix Echtzeit-Aufzeichnung der ICA-Roundtripzeit, auch ICA RTT genannt. ICA RTT ist die Zeit, die ab dem Drücken einer Taste durch den Benutzer vergeht, bis die Antwort am Endpunkt angezeigt wird.

Die Benutzeroberfläche für den Servicekontinuität-Offlinemodus wurde verbessert

Ab Version 24.1.0 wurde die Benutzeroberfläche der Citrix Workspace-App für iOS verbessert, um sie informativer und moderner zu gestalten sowie bei Ausfällen von Citrix Workspace ein besseres Benutzererlebnis zu gewährleisten. Die Fuzzy-Suchfunktion steht auch für den Offlinemodus zur Verfügung. Mit dieser Funktion können Sie die Ergebnisse für Apps oder Desktops mit fast übereinstimmendem Text und falsch geschriebenen Suchbegriffen finden. Weitere Informationen zur Servicekontinuität finden Sie unter Servicekontinuität.



Workspace-App mit Lösungen zur einheitlichen Endpunktverwaltung konfigurieren

April 17, 2024

Die Citrix Workspace-App für iOS unterstützt die Administratorkonfiguration der Workspace-App über AppConfig-basierte Schlüssel/Wert-Paare unter Verwendung von Lösungen zur einheitlichen Endpunktverwaltung (Unified Endpoint Management, UEM).

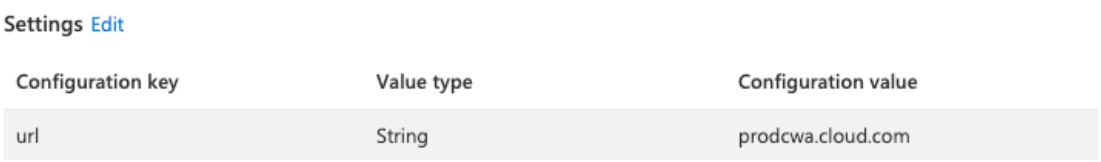
Informationen zur Konfiguration

Gehen Sie folgendermaßen vor, um Ihre Workspace-Store-URL mit Lösungen zur einheitlichen Endpunktverwaltung zu konfigurieren:

> **Hinweis:**
>
> Zu Demonstrationszwecken wird in diesem Beispiel Microsoft Intune als UEM-Lösung verwendet. Schritte und Benutzeroberfläche können je nach UEM-Anbieter unterschiedlich sein.

1. Melden Sie sich bei Ihrem UEM-Anbieter an.
2. Fügen Sie die Citrix Workspace-App hinzu, die Sie über Ihren UEM-Anbieter verwalten möchten. Sie können die App über das Portal Ihres UEM-Anbieters hochladen, um die Verwaltung durch Ihren UEM-Anbieter zu ermöglichen. Alternativ können Sie einen Link zur App im App-Store einrichten.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.
4. Fügen Sie der XML-Eigenschaftsliste ein Schlüssel- und Wertepaar hinzu und geben Sie die folgenden Werte ein:

    - **Schlüssel**: `url`
    - **Werttyp**: `String`
    - **Wert**: Ihre Store-URL (z. B. `prodcwa.cloud.com`)



Einschränkungen

- Wenn bereits ein Cloudstore eingerichtet ist und der Administrator einen neuen Cloudstore konfiguriert, wird Ihr vorhandener Cloudstore gelöscht. Außerdem werden alle zugehörigen Daten oder Einstellungen des vorhandenen Cloudstores gelöscht. Sie erhalten eine Benachrichtigung in Citrix Workspace. Sie müssen sich dann erneut anmelden, damit der neue Cloudstore zu Citrix Workspace hinzugefügt wird.
  - Die obige Aussage gilt nur für bestehende Cloudstores. Wenn bereits ein On-Premises-Store konfiguriert ist und der Administrator einen neuen Cloud- oder On-Premises-Store konfiguriert, wird der neue Store hinzugefügt und es erfolgt kein Löschen.
- Um neue Konfigurationen anzuwenden, müssen Sie die Citrix Workspace-App schließen und dann neu starten.

Verbesserungen an Lösungen zur einheitlichen Endpunktverwaltung (UEM)

Die Citrix Workspace-App für iOS unterstützt jetzt weitere Konfigurationen, bei denen AppConfig-basierte Schlüssel-Wert-Paare zur Konfiguration der Citrix Workspace-App verwendet werden. Bisher konnten Administratoren bereits Store-URLs konfigurieren. Jetzt können Administratoren das Anpassen von Store-URLs durch Benutzer einschränken und die App-Anzeige steuern.

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

Details entnehmen Sie den folgenden Angaben:

Konfigurationsschlüssel	Werttyp	Konfigurationswert
`url`	`String`	Die Store-URL. Beispiel: `prodcwa.cloud.com`

Konfigurationsschlüssel	Werttyp	Konfigurationswert
storeType	Integer	• Bei der Einstellung “1” (Standard) können Benutzer die native oder die Standard-Storeanzeige nutzen. - Bei der Einstellung “2”können Benutzer den Store in einem Webinterface anzeigen.
restrict_user_store_modification	Boolean	• Bei der Einstellung **True** können Benutzer den Store nicht anpassen (hinzufü- gen/löschen/bearbeiten). - Bei der Einstellung **False** können Benutzer den Store anpassen. **Hinweis:** Bei der Einstellung “True” werden alle vorhandenen Stores gelöscht, bevor ein UEM-konfigurierter Store hinzugefügt wird.

Unterstützung für die Konfiguration des Gerätenamens über UEM

Ab der Version 24.3.5 können Administratoren mit der Citrix Workspace-App für iOS Gerätenamen anhand von Benutzergruppen über Unified Endpoint Management (UEM) zuweisen und identifizieren.

Gehen Sie wie folgt vor, um den Gerätenamen mithilfe von UEM zu konfigurieren:

> **Hinweis:**
>
> Zu Demonstrationszwecken wird in diesem Beispiel Microsoft Intune als UEM-Lösung verwendet. Schritte und Benutzeroberfläche können je nach UEM-Anbieter unterschiedlich sein.

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

2. Fügen Sie die Citrix Workspace-App hinzu, die Sie über Ihren UEM-Anbieter verwalten möchten. Sie können die App über das Portal Ihres UEM-Anbieters hochladen, um die Verwaltung durch Ihren UEM-Anbieter zu ermöglichen. Alternativ können Sie einen Link zur App im App-Store einrichten.
3. Erstellen Sie eine App-Konfigurationsrichtlinie für Ihre App.
4. Fügen Sie der XML-Eigenschaftsliste ein Schlüssel- und Wertepaar hinzu und geben Sie die folgenden Werte ein:

    - Schlüssel: deviceName
    - Werttyp: Zeichenfolge
    - Wert: Name des Geräts (z. B. MY_IPHONE_Device)

Peripheriegeräte

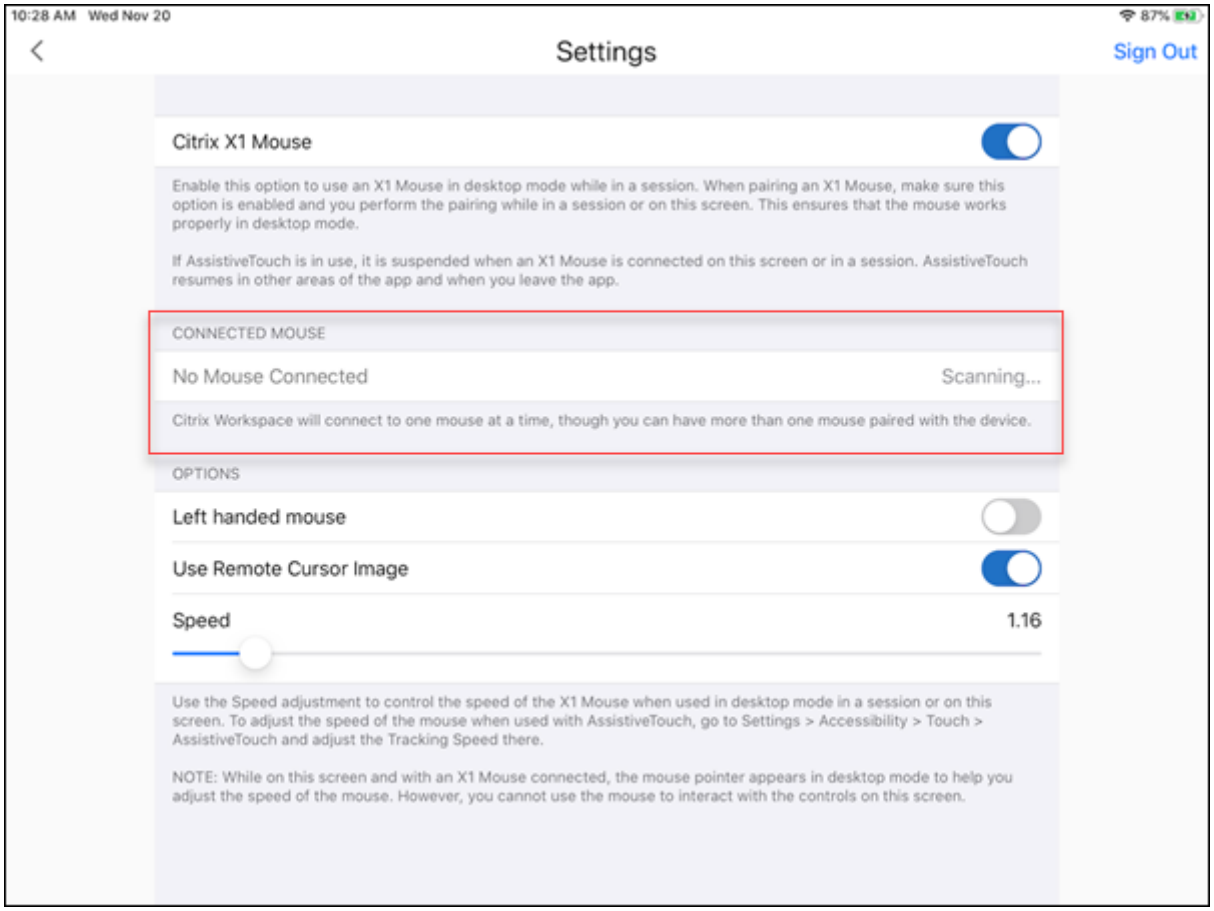
July 1, 2024

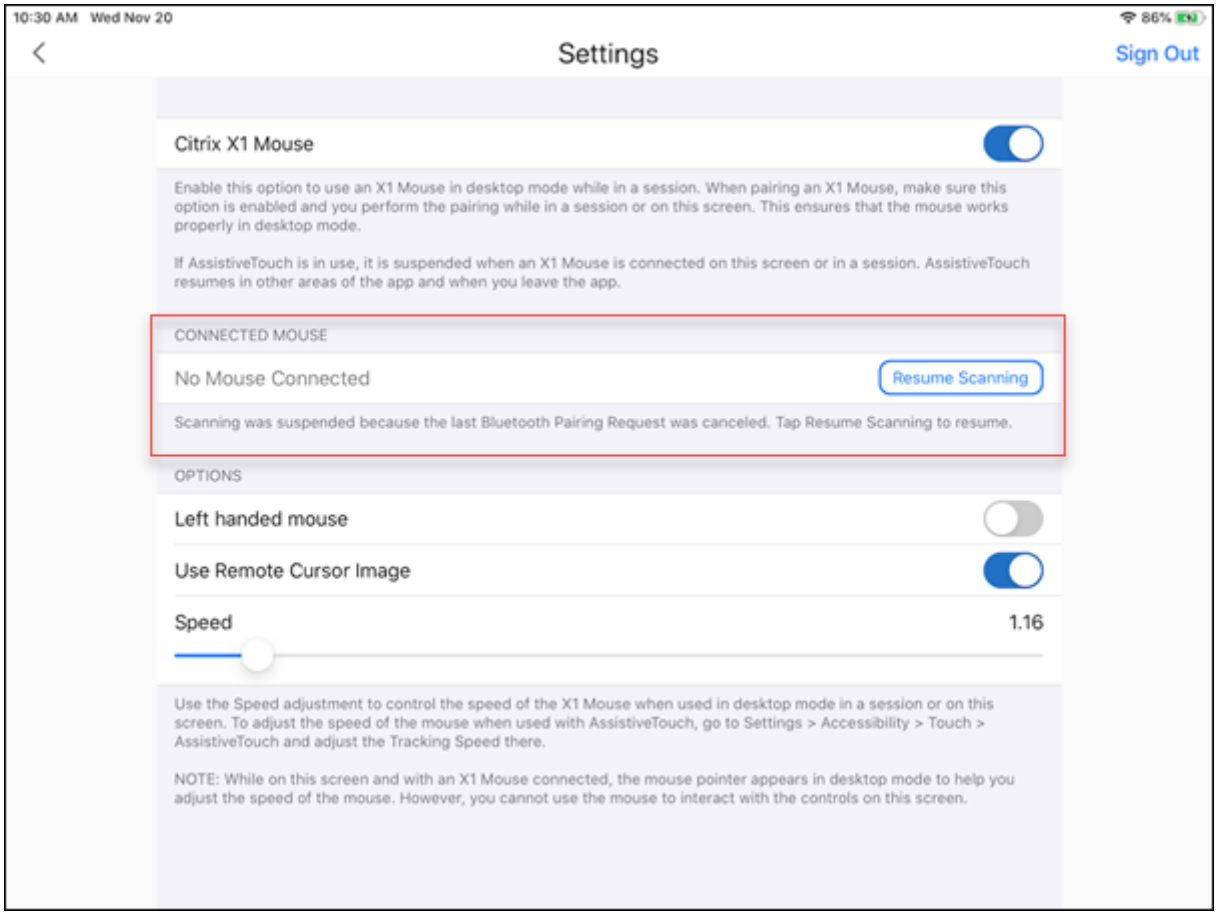
Citrix X1-Maus

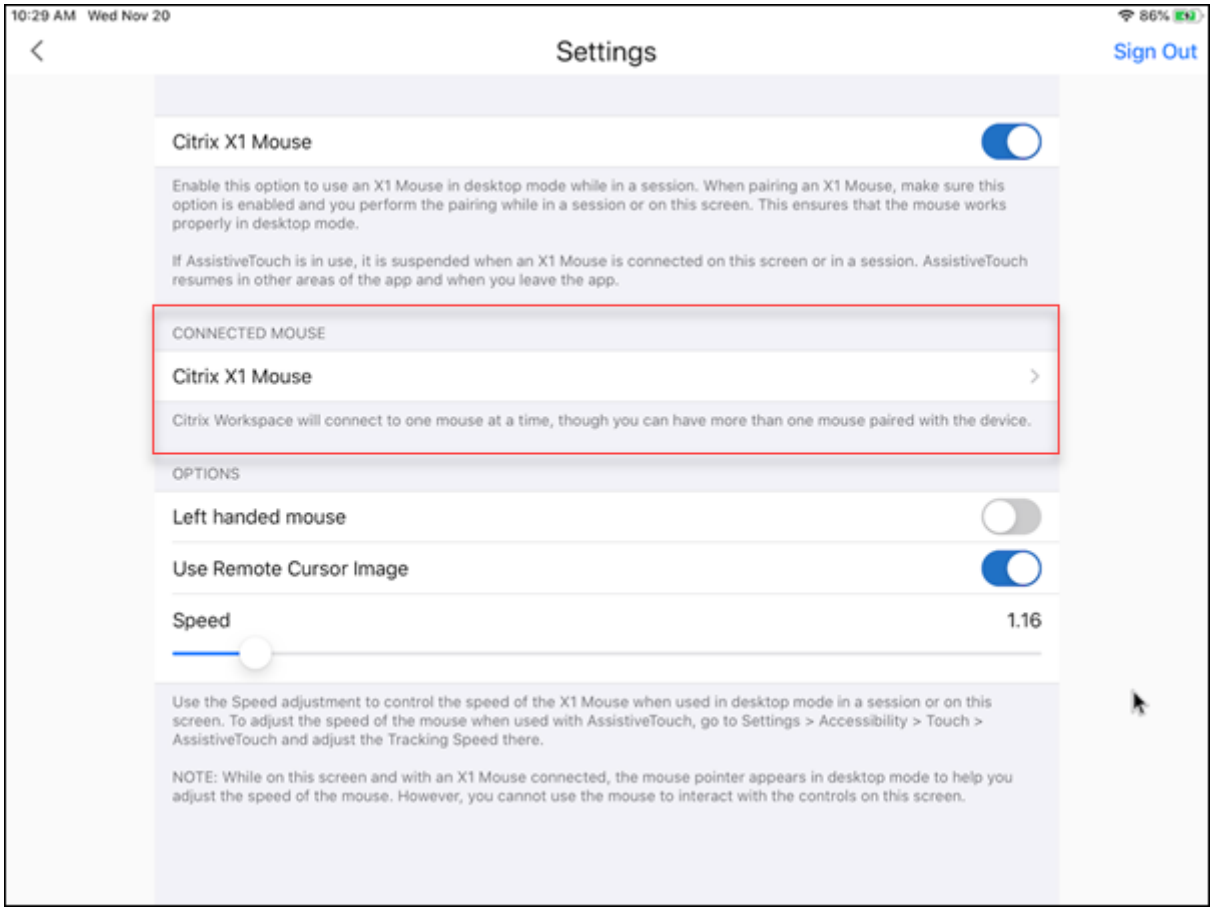
Citrix X1-Mauskopplung und Verbindungsstatus

Mit dieser Funktion haben Sie mehr Kontrolle über den Kopplungsprozess der Citrix X1-Maus. Der Bildschirm **Einstellungen** bietet folgende Optionen:

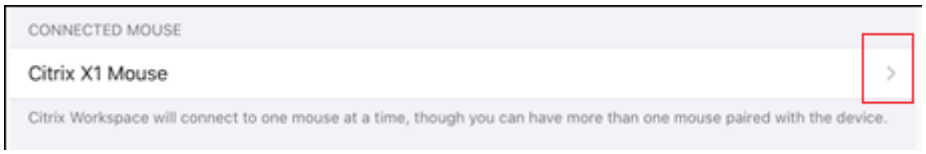
- Koppeln der Citrix X1-Maus. Sie können eine X1-Maus auch koppeln, wenn Sie in einer Sitzung sind.
- Anzeigen des Verbindungsstatus.







- Anzeigen von Eigenschaften der Citrix X1-Maus, z. B. **Name**, **UUID**, **Firmwareversion**und **Akkustand**. Tippen Sie dazu unter **VERBUNDENE MAUS** auf “Citrix X1-Maus”.



Eigenschaften der verbundenen Maus:

AssistiveTouch Wenn die AssistiveTouch-Funktion unter iOS 13 oder höher aktiviert ist, können Sie den AssistiveTouch-Cursor sehen, wenn Sie zwischen Desktopmodus und 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:

- Beim Verlassen einer Sitzung
- Beim Wechseln zum iOS App Switcher-Bildschirm
- Beim Wechseln zum iOS-Startbildschirm oder zu einer anderen App

Der Desktopmodus wird fortgesetzt, wenn Sie zurück zur Citrix Workspace-App navigieren und wenn Sie in einer Sitzung sind.

Unterstützung für externen Bildschirm und Symbolleiste

Sie können die Citrix X1-Maus verwenden, um die Symbolleiste auf einem externen Bildschirm zu bedienen. Sie können die Symbolleistenverankerung auch horizontal verschieben, während die Symbolleiste geschlossen ist. Wenn Sie Ihr iOS-Gerät mit dem externen Bildschirm verbinden, erkennt die Citrix Workspace-App automatisch die Bildschirmauflösung des externen Bildschirms. Sie können die Schaltfläche **Anzeige** in der Symbolleiste verwenden, um eine bestimmte Bildschirmauflösung auszuwählen. Sie können auf die Option **Anzeige** zugreifen, ohne vorher ein Konto hinzufügen oder sich anmelden zu müssen.

Generische Maus

Unterstützung für generische Mäuse und Trackpads

Sie können eine generische Maus oder ein Trackpad verwenden, um in HDX-Sitzungen mit der rechten Maustaste zu klicken, zu scrollen und den Mauszeiger zu verwenden. Die Aktionen ähneln der Citrix X1-Maus. Der Stil des lokalen Mauszeigers ändert sich und gleicht dem des Remotecursors.

> **Hinweise:**
>
> - Dieses Feature ist auf iPadOS 13.4 und höher verfügbar.
> - Dieses Feature wird auf iPhones nicht unterstützt.

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

Generische Mausunterstützung auf externen Bildschirmen

Sie können eine generische Maus auf externen Bildschirmen verwenden, die mit einem iPad verbunden sind. Generische Mäuse werden auf Geräten mit iOS 13.4 oder höher unterstützt.

> **Wichtig:**
>
> Um eine generische Maus mit externen Bildschirmen zu verwenden, stellen Sie sicher, dass der Modus **Präsentation** in Ihrer Citrix Workspace-App deaktiviert ist. Navigieren Sie dazu zu **Einstellungen** > **Anzeigeoptionen**.

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

Erweiterte Multimonitorunterstützung mit generischer Maus für iPad

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

> **Hinweis:**
>
> - Dieses Feature kann in früheren Versionen teilweise verfügbar sein. Um das vollständige Feature zu nutzen, aktualisieren Sie auf Version 22.1.0.
> - Deaktivieren Sie AssistiveTouch in iOS unter **Settings** > **Accessibility** > **Touch** > **AssistiveTouch**, damit die Citrix Workspace-App primäre Mausklicks empfängt.

Konfigurieren des Modus "Erweitern" Modus **Erweitern** aktivieren:

1. Verbinden Sie den externen Bildschirm über ein HDMI-Kabel und die erforderlichen Adapter mit dem iPad.

   > **Hinweis:**
   >
   > Das Einrichten funktioniert am besten mit einem USB-C-auf-Digital-AV-Multiport-Adapter oder einem Lightning Digital AV-Adapter von Apple.

2. Navigieren Sie in der Anwendung zu **Einstellungen** > **Anzeigeoptionen** und wählen Sie für **Externe Anzeige** die Einstellung **Ein**. Es werden verschiedene Anzeigemodi angezeigt. Im Spiegel- und Präsentationsmodus wird auch die generische Mouse verwendet, wenn die iPadOS-Version 14.0 und höher vorliegt.
3. Wählen Sie die Option **Erweitern**.

   Sie können einen der folgenden Anzeigemodi wählen:

   - Spiegeln: Ermöglicht das Spiegeln der Anzeige auf dem externen Monitor, der an das iPad angeschlossen ist.
   - Präsentation: Ermöglicht es Ihnen, Ihren externen Monitor auf Trackpad umzustellen.
   - Erweitern: Ermöglicht die Anzeige verschiedener Ansichten oder Bildschirme auf jedem Display.

> **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.

Konfigurieren der Anzeigeanordnung Schrittfolge zum Konfigurieren der Anzeigeanordnung:

1. Wählen Sie den Modus **Erweitern**. Die Option **Anzeigeanordnung** wird angezeigt.

2. Positionieren Sie die Kachel **Externe Anzeige** neu (links, oberhalb, rechts oder unterhalb der iPad-Anzeige).

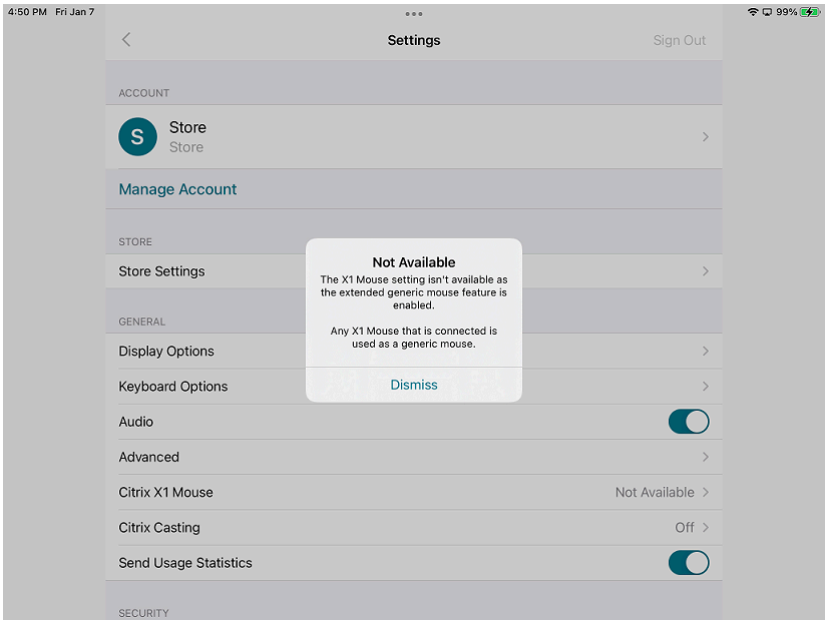
> **Hinweis:**
>
> Während einer Sitzung können Sie die Anzeigeanordnung auf der sitzungseigenen Symbolleiste über das Symbol **Anzeige** anpassen.

> **Hinweis:**
>
> Die externe Bildschirmauflösung ist abhängig von:
>
> - Adaptern
> - iPad
> - anderer verwendeter Hardware

Generischer Mausmodus und Citrix X1-Mausmodus im Vergleich

Der generische Mausmodus hat automatisch Vorrang vor dem Citrix X1-Mausmodus. Wenn Sie eine X1-Maus anschließen, wird sie als generische Maus verwendet. Daher sind die Einstellungen der X1-Maus nicht verfügbar, wenn das Featureflag für die generische Maus aktiviert ist.

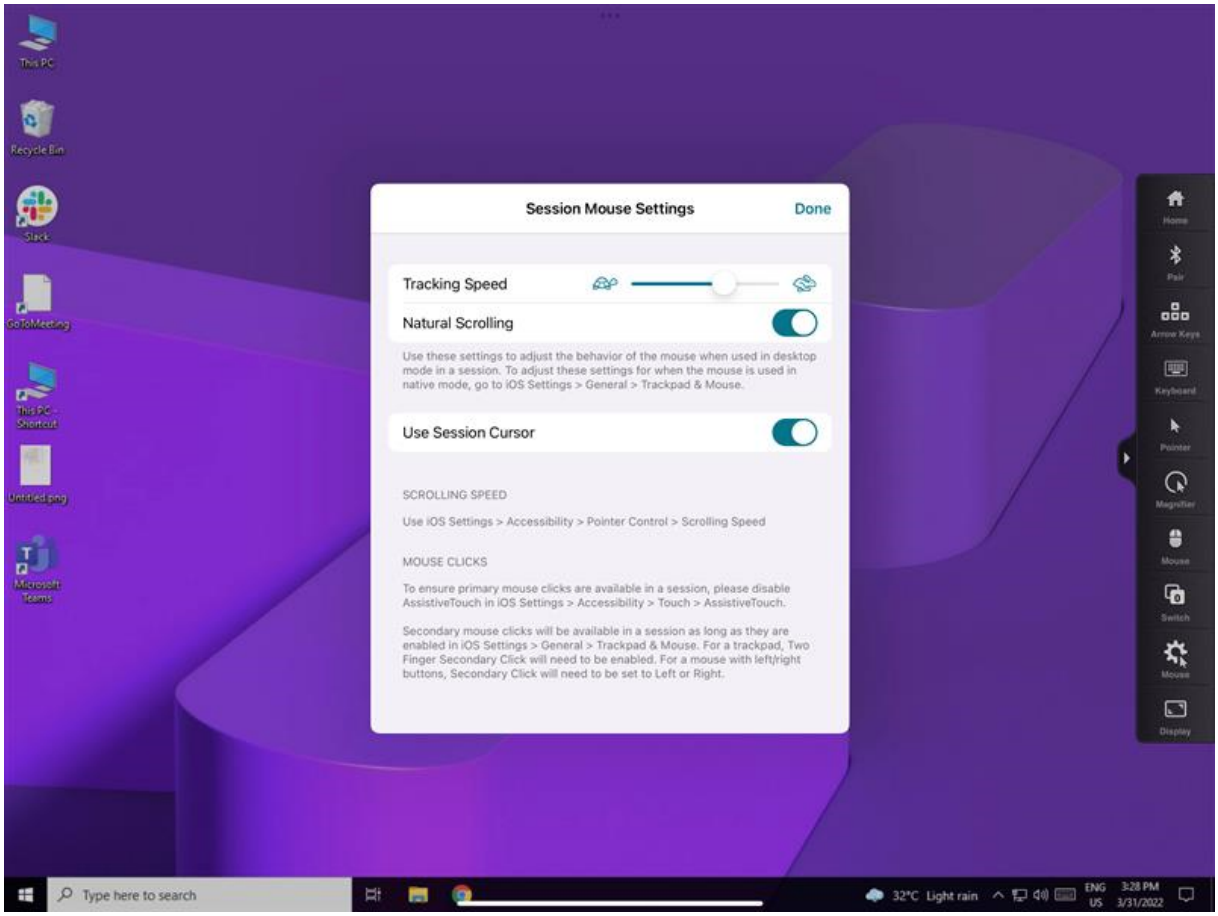
> **Hinweis:**
>
> Bei Geräten mit iPadOS Version 14.0 und höher verhält sich jede mit dem iPad verbundene X1-Maus wie eine Bluetooth-Maus.



Symbol für generische Maus

Das Symbol für die **Maus**-Einstellungen wird in der sitzungseigenen Symbolleiste neben dem Symbol **Anzeige** hinzugefügt. Mit den **Maus**-Einstellungen können Sie während einer Sitzung die Trackinggeschwindigkeit der generischen Maus anpassen. Außerdem können Sie "Remotecursorbild verwenden"ein- bzw. ausschalten.

> **Hinweis:**
>
> Die Trackinggeschwindigkeit der nativen Maus können Sie in den iOS-Einstellungen anpassen.



Funktionseinschränkungen

- Um sicherzustellen, dass die Citrix Workspace-App primäre Mausklicks empfängt, deaktivieren Sie AssistiveTouch in iOS unter **Settings** > **Accessibility** > **Touch** > **AssistiveTouch**.
- Die Optionen für Trackinggeschwindigkeit und natürliches Scrollen in den iOS-Einstellungen wirken sich nicht auf die generische Maus in der Sitzung aus. Die Scrollgeschwindigkeit kann jedoch über die **Einstellungen** in iOS gesteuert werden.

Über den Bildschirm **Mauseinstellungen** in der Sitzungssymbolleiste können Sie auf die Optionen "Trackinggeschwindigkeit"und "Natürliches Scrollen"zugreifen.

- Wenn ein iPad im Splitscreen-Modus verwendet wird und der Bildschirm 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, also vor dem Sitzungsstart, werden die Mausereignisse nicht empfangen.
  Um dieses Problem zu umgehen, rufen Sie die Mitteilungszentrale auf, bewegen den nativen Zeiger an eine andere Stelle und schließen die Mitteilungszentrale.
- Die Audioumleitung schlägt fehl, wenn Sie ein iPad an einen externen Bildschirm anschließen. Die Audio-Wiedergabe erfolgt über die iPad-Lautsprecher. [HDX-39159]

Bekannte Probleme des Features

- Während einer aktiven Sitzung wird das Desktopimage, das auf einem iPad oder externen Bildschirm angezeigt wird, gestört, wenn Sie Folgendes ändern:
  - Anzeigeanordnung
  - Auflösung
  - Ausrichtung oder
  - Anzeigemodi

  Um dieses Problem zu umgehen, trennen Sie den Bildschirm und schließen ihn erneut an. Wenn das Problem weiterhin besteht, trennen Sie die Sitzung und starten Sie sie erneut. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].
- In seltenen Fällen ist die Audio-Wiedergabe um einige Sekunden verzögert, wenn das Video auf dem externen Bildschirm wiedergeben wird. [HDX-39159]
- In seltenen Fällen ist das VDA-Display auf einem iPad und auf dem externen Bildschirm abgeschnitten. Um dieses Problem zu umgehen, trennen Sie den Bildschirm und schließen ihn erneut an. Wenn das Problem weiterhin besteht, trennen Sie die Sitzung und starten Sie sie erneut. [HDX-37100]
- Wenn Sie das Video auf dem externen Bildschirm auf Vollbild maximieren, können Probleme mit der Videoqualität auftreten. [HDX-39159]
- In seltenen Fällen gelingt es in einer Desktopsitzung nicht, die Apps vom iPad auf den externen Bildschirm zu verschieben. Um dieses Problem zu umgehen, trennen Sie den Bildschirm und schließen ihn erneut an. Wenn das Problem weiterhin besteht, trennen Sie die Sitzung und starten Sie sie erneut. [HDX-36981]
- In seltenen Fällen sind unter "Anzeigeoptionen"die Anzeigemodi nicht sichtbar, wenn Sie ein iPad mithilfe von Drittanbieteradaptern an einen externen Bildschirm anschließen. [HDX-39713]

- Gelegentlich ist in der VDA-Sitzung unter dem Mauszeiger eine Linie zu sehen. [RFIOS-9569]

Tastaturunterstützung

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung ermöglicht es Benutzern, zu bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert.

Um die Synchronisierung des Tastaturlayouts zu aktivieren, gehen Sie zu **Einstellungen** > **Tastatur-optionen** und aktivieren Sie die Option **Synchronisierung des Tastaturlayouts**.

> **Hinweis:**
>
> Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Sie Japanisch, Chinesisch oder Koreanisch verwenden und den Server-IME bevorzugen, deaktivieren Sie die Option für das lokale Tastaturlayout, indem Sie die entsprechende Option unter **Einstellungen** > **Tastatur** deaktivieren.

Voraussetzungen

- Für Linux VDA aktivieren Sie die Richtlinie Client-Tastaturlayoutsynchronisierung und Verbesserung des IME.
- Für Windows VDA aktivieren Sie die Richtlinien Unicode-Tastaturlayoutzuordnung, Client-Tastaturlayoutsynchronisierung und Verbesserung des IME.
- Der VDA muss Version 7.16 oder höher sein.

Tastaturlayoutunterstützung für Windows VDA und Linux VDA

Tastaturlayout unter iOS	Sprache der Tastatur	Tastaturlayout unter Windows	Tastaturlayout unter Linux
Belarussisch (Belarus)	Belarussisch (Belarus)	Belarussische Tastatur (Belarus)	by
Bulgarisch	Bulgarisch	Bulgarische Tastatur (Schreibmaschine)	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

Tastaturlayout unter iOS	Sprache der Tastatur	Tastaturlayout unter Windows	Tastaturlayout unter Linux
Tschechisch	Tschechisch	Tschechische Tastatur	cz
Dänisch	Dänisch	Dänische Tastatur	df
Niederländisch	Niederländisch (Niederlande)	Tastatur für USA – International	us
Niederländisch (Belgien)	Niederländisch	Belgische Tastatur (Punkt)	be
Englisch (Australien)	Englisch (Australien)	US-Tastatur	us
Englisch (Kanada)	Englisch (Kanada)	US-Tastatur	us
Englisch (UK)	Englisch (Großbritannien)	Tastatur für Großbritannien	gb
Englisch (USA)	Englisch (USA)	US-Tastatur	us
Estnisch	Estnisch	Estnische Tastatur	ee
Finnisch	Finnisch	Finnische Tastatur	fi
Französisch (Kanada)	Französisch (Kanada)	Französische Tastatur	fr
Französisch (Schweiz)	Französisch (Frankreich)	Französische Tastatur (Schweiz)	ch
Französisch (Französisch)	Französisch (Frankreich)	Französische Tastatur	fr
Deutsch (Österreich)	Deutsch (Österreich)	Deutsche Tastatur	at
Deutsch (Schweiz)	Deutsch (Schweiz)	Schweizerdeutsche Tastatur	ch
Deutsch (Deutschland)	Deutsch (Deutschland)	Deutsche Tastatur	at
Griechisch	Griechisch	Griechische Tastatur	gr
Ungarisch	Ungarisch	Ungarische Tastatur	hu
Isländisch	Isländisch	Isländische Tastatur	is
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	no

Tastaturlayout unter iOS	Sprache der Tastatur	Tastaturlayout unter Windows	Tastaturlayout unter Linux
Polnisch	Polnisch	Polnische Tastatur (Programmierer)	pl
Portugiesisch (Brasilien)	Portugiesisch (Brasilien)	Portugiesische Tastatur (Brasilien, ABNT)	br
Portugiesisch (Portugal)	Portugiesisch (Portugal)	Portugiesische Tastatur	pt
Rumänisch	Rumänisch (Rumänien)	Rumänische Tastatur (alt)	ro
Russisch (Russland)	Russisch	Russische Tastatur	ru
Slowakisch	Slowakisch	Slowakische Tastatur	sk
Slowenisch	Slowenisch	Slowenische Tastatur	si
Spanisch (Mexiko)	Spanisch (Mexiko)	Lateinamerikanische Tastatur	latam
Spanisch (Spanien)	Spanisch (Spanien)	Spanische Tastatur	es
Schwedisch (Schweden)	Schwedisch (Schweden)	Schwedische Tastatur	se
Türkisch	Türkisch	Türkische Tastatur (F)	tr
Ukrainisch	Ukrainisch	Ukrainische Tastatur	ua

Unterstützung für Sondertasten

Unterstützung für die folgenden Einzeltasten auf einer externen Tastatur ab iOS 13.4 und höher:

- Bild auf
- Bild ab
- Home
- Ende
- 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 hinzu:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + STRG + S
- Windows + T
- Windows + U
- Windows + Ziffer
- Windows + Aufwärts
- Windows + Abwärts
- Windows + Nach links
- Windows + Nach rechts
- Windows + X
- Windows + K
- STRG + ESC

Verbesserungen für die erweiterte Tastatur

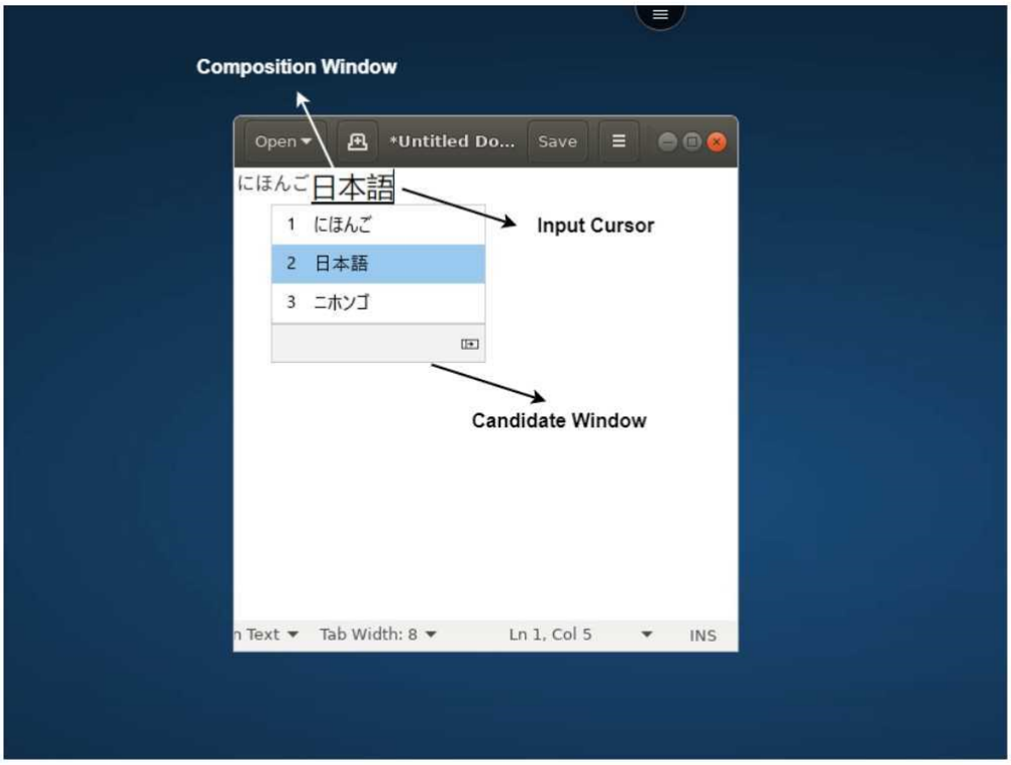
Ab Version 23.5.0 wurde die erweiterte Tastaturfunktionalität verbessert, um eine bessere Benutzererfahrung zu bieten. Folgende Verbesserungen wurden eingeführt:

- Erweiterte Symbolleiste anheften oder lösen.
- Erweiterte Symbolleiste synchron mit der Bildschirmrotation drehen.
- Unterstützung für Tastenkombinationen mit der Windows-Symboltaste und 3-Tasten-Kombinationen.
- Verbesserte Benutzererfahrung bei Anwendungsszenarien mit mehreren Monitoren.
- Automatisches Öffnen oder Reduzieren der erweiterten Symbolleiste.

- Verbesserte Benutzererfahrung im Stage Manager-Modus (auf einem iPad mit M1-Chip).

IME-Benutzeroberfläche

Die Benutzeroberfläche des IME bietet Komponenten wie das Kandidatenfenster und das Kompositionsfenster. Das Kompositionsfenster enthält die Kompositionszeichen und Elemente der Kompositionsbenutzeroberfläche, beispielsweise Unterstreichungen und Hintergrundfarbe. Im Kandidatenfenster wird die Kandidatenliste angezeigt.



Im Kompositionsfenster können Sie zwischen den bestätigten Zeichen und den zu verfassenden Zeichen unterscheiden. Das Kompositionsfenster und das Kandidatenfenster bewegen sich mit dem Eingabecursor.

Daher bietet das Feature Folgendes:

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

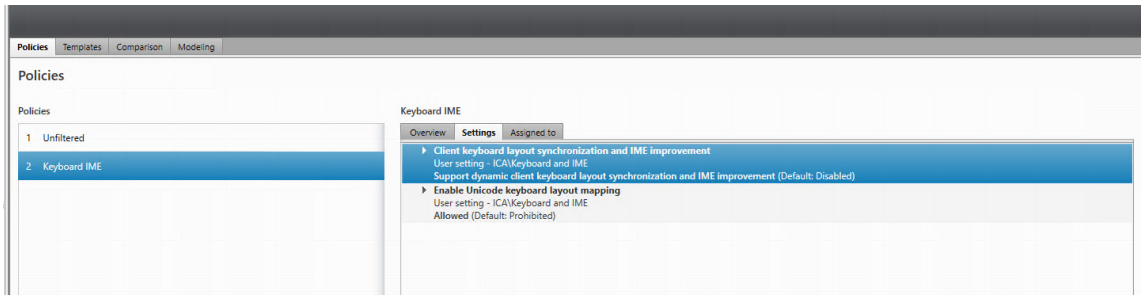
Derzeit können Sie dieses Feature in Sitzungen verwenden, die auf Windows VDAs gehostet werden. Es werden Bildschirmtastatur und externe physische Tastaturen unterstützt.

Generischer Client-Eingabemethoden-Editor für ostasiatische Sprachen

Der generische Client-Eingabemethoden-Editor (Input Method Editor, IME) verbessert die Eingabe- und Anzeigeerfahrung bei chinesischen, japanischen und koreanischen (CJK) Sprachzeichen auf iOS-Geräten. Mit diesem Feature können Sie in einer Sitzung mit Ihrem Client-IME CJK-Zeichen an der Cursorposition verfassen. Dieses Feature ist für Windows VDA-Umgebungen verfügbar. Für eine bessere Benutzererfahrung wird empfohlen, den Client-IME anstelle des VDA-seitigen Eingabemethoden-Editors zu verwenden.

Voraussetzungen

- Aktivieren Sie auf dem Windows VDA mit der Gruppenrichtlinie die Richtlinien "Client-Tastaturlayoutsynchronisierung und IME-Verbesserung"und "Unicode-Tastaturlayoutzuordnung aktivieren".



Weitere Informationen finden Sie im Knowledge Center-Artikel CTX312404.

Sie können die Optionen auch mit den folgenden Registrierungen auf dem 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 in der Citrix Workspace-App **Einstellungen** > **Tastaturoptionen** > **Tastaturlayoutsynchronisierung**.

Unterstützung für den Scancode-Eingabemodus

Ab Version 24.1.0 können Sie **Scancode** als Tastatureingabemodus auswählen, wenn Sie eine externe physische Tastatur verwenden. Dieses Feature ist hilfreich, wenn Sie iOS-Geräte mit der Standardtastatur eines externen Windows-PCs verwenden. Mit **Scancode** können Sie das Tastaturlayout des VDA anstelle der iOS-Softtastatur verwenden. Auf diese Weise können Sie dem Eingabestil der externen Windows-Tastatur anstelle von iOS vollständig folgen. Dies ist bei der Eingabe in ostasiatischen Sprachen von Vorteil, da es die allgemeine Benutzererfahrung erheblich verbessert. Die Endbenutzer

stellen möglicherweise fest, dass sie das Tastaturlayout des Servers anstelle des Clientlayouts verwenden. Weitere Informationen finden Sie im Abschnitt Anwendungsfall in diesem Artikel.

Führen Sie folgende Schritte aus, um das **Scancode**-Feature zu verwenden:

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, welcher das entsprechende Zeichen generiert. Wendet serverseitiges Tastaturlayout an.
   - **Unicode:** Sendet die Taste von der clientseitigen Tastatur an den VDA, welcher das gleiche Zeichen auf dem VDA generiert. Wendet clientseitiges Tastaturlayout an.

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

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

Anwendungsfall Es kann zum Beispiel vorkommen, dass Sie ein internationales US-amerikanisches Tastaturlayout verwenden, das mit Ihrem iOS-Gerät verbunden ist.
Wenn Sie **Scancode** auswählen und die Taste neben der Feststelltaste auf Ihrer externen Tastatur drücken, 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 drücken, wird das Zeichen **a** an den VDA gesendet. Selbst wenn der VDA ein anderes Tastaturlayout mit einem anderen Zeichen an derselben Position verwendet, wird das Zeichen **a** auf dem Bildschirm angezeigt.

> **Hinweis:**
>
> **Unicode** ist der bevorzugte Modus für die Eingabe, wenn Sie eine Touchtastatur auf Ihren Mobilgeräten verwenden. Die Tasten einer Touchtastatur generieren nämlich im Allgemeinen keinen Scancode.

Erweiterung der Unterstützung für externe Tastenkombinationen

Mit der Citrix Workspace-App für iOS können Sie jetzt in einer Remotedesktop- oder App-Sitzung mehr Tastenkombinationen von externen Tastaturen verwenden. Die folgenden wichtigen Verbesserungen wurden an externen Tastenkombinationen vorgenommen:

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

Darüber hinaus können Sie jetzt die spezifische Taste für **Alt** konfigurieren, indem Sie die folgenden Optionen über **Einstellungen > Tastaturoptionen > Zuweisen einer bestimmten Taste für Alt** verwenden:

- **Wahltaste oder Alt-Taste (links)**: Sendet **Alt**-Taste mit **Wahltaste(links) oder Alt-Taste (links)**.
- **Befehl oder Windows (links)**: Sendet die **Alt**-Taste mit der **Befehlstaste (links) oder der Windows-Taste (links)**.
- **Wahltaste oder Alt-Taste (links und rechts)**: Sendet **Alt** mit der **Wahltaste oder Alt-Taste (links und rechts)**.

Das Zuweisen einer bestimmten Taste für Alt hilft, Konflikte zwischen der macOS-**Optionstaste** und der Windows-**Alt-Taste** zu vermeiden.

Einschränkungen Die folgenden iOS-Tastenkombinationen werden derzeit nicht unterstützt:

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

Zugriff auf Mikrofon und Kamera

Sie können jetzt über eine VDA-Sitzung auf Ihr Mikrofon und Ihre Kamera für Audio-/Videokonferenzen zugreifen. Die Citrix Workspace-App fordert Ihre Genehmigung an, um auf das Mikrofon oder die Kamera zuzugreifen. Sie gewähren die Genehmigung, indem Sie auf Ihrem Gerät zu **Einstellungen** navigieren und die Kamera oder das Mikrofon aktivieren.

Außerdem wurde der Mikrofon- und Kamerazugriff pro Store als Teil des clientselektiven Vertrauens im Rahmen der Sicherheitsfunktion integriert, damit die Citrix Workspace-App dem Zugriff von einer VDA-Sitzung aus vertrauen kann.

Die Citrix Workspace-App benötigt die Berechtigung des Benutzers, um auf das Mikrofon oder die Kamera zuzugreifen.

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

Unterstützung der Rückkamera

Mit der Citrix Workspace-App für iOS können Sie jetzt innerhalb der VDA-Sitzung die Kameraposition von Front- auf Rückkamera ändern (und umgekehrt).

Beim Aufrufen der Kamera wird eine unverankerte Schaltfläche angezeigt. Tippen Sie einmal auf diese Schaltfläche, um zwischen der Front- und Rückkamera zu wechseln.

Sie können die unverankerte Schaltfläche auch frei auf dem Bildschirm bewegen und an einer beliebigen Stelle platzieren.

Bekannte Probleme:

Die unverankerte Schaltfläche ist teilweise oder vollständig verdeckt, wenn das Casting-Feature oder das Feature “Dokument scannen”aktiviert ist.

Grafik und Display

Verbesserte Grafikleistung

Ab der Version 24.1.0 unterstützt die Citrix Workspace-App für iOS die hardwarebeschleunigte H.264-Videokodierung oder -dekodierung. Die Multimediaengine von Citrix HDX verwendet jetzt das Video Toolbox-Framework von Apple zur Codierung und Decodierung. Dieses Framework komprimiert und dekomprimiert Video schneller und in Echtzeit. Diese Erweiterung reduziert die CPU-Last bei der Multimedianutzung.

Clientlaufwerkzuordnung (Clientlaufwerkzuordnung)

Sie können für jeden konfigurierten Store einen bestimmten Gerätespeicherzugriff auswählen. Die folgenden Optionen sind für den Gerätespeicherzugriff verfügbar.

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

Wenn Sie **Jedes Mal fragen** auswählen, wird bei jedem Start eine Eingabeaufforderung zum Auswählen des Gerätespeicherzugriffs angezeigt. Standardmäßig ist die Option **Kein Zugriff** ausgewählt.

> **Hinweis:**
>
> Dieses Feature gilt nur für direkte ICA-Starts und für Citrix Gateway konfigurierte Stores. Stores ohne End-to-End-SSL-Setup werden nicht unterstützt.

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

Citrix Ready Workspace Hub

Der Citrix Ready Workspace Hub verbindet die digitale und die physische Umgebung zur Bereitstellung von Apps und Daten in einem sicheren, intelligenten Bereich. Das System verbindet Geräte (oder auch Dinge, z. B. mobile Apps und Sensoren) zur Schaffung einer intelligenten und reaktionsfähigen Umgebung.

Citrix Ready Workspace Hub baut auf der Raspberry Pi 3-Plattform auf. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, stellt eine Verbindung zum Citrix Ready Workspace Hub her und ermöglicht die Anzeige von Apps und Desktops auf einem größeren Display.

Informationen zu Citrix Ready Workspace Hub finden Sie in der Dokumentation zu Citrix Ready Workspace Hub.

Zur Sicherheit unterstützt Citrix Ready Workspace Hub eine SSL-Verbindung (Secure Sockets Layer) zwischen Mobilgeräten und dem Hub. Legen Sie einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) entweder manuell oder automatisch fest, um jedes Gerät eindeutig zu identifizieren. Weitere Informationen finden Sie unter Sichere Verbindung in der Dokumentation zu Citrix Ready Workspace Hub.

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

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

Citrix Ready Workspace Hub konfigurieren

Um die Citrix Ready Workspace Hub-Features zu aktivieren, navigieren Sie zu **Einstellungen** und tippen Sie auf **Citrix Casting**, damit das Feature auf Ihrem Gerät verfügbar ist. Weitere Informationen finden Sie in der Hilfedokumentation zu iOS-Geräten.

Die Citrix Workspace-App integriert ein neues Verfahren zum Hinzufügen oder Entfernen eines Workspace Hubs aus der Liste vertrauenswürdiger Geräte auf iOS-Geräten. Weitere Informationen finden Sie unter Sichere Verbindung.

Unterstützung für Dokumentenscanner

Ab der Version 24.5.0 unterstützt die Citrix Workspace-App für iOS das Dokumentenscannerfeature. Mit diesem Feature können Sie jetzt mehrere Dokumente innerhalb der Desktopsitzung scannen und speichern. Dieses Feature ist standardmäßig aktiviert.

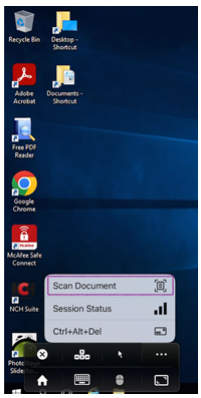
Voraussetzungen

- Die Clientlaufwerkzuordnung (CDM) muss für den Store aktiviert sein.
- Der Dokumentscanner erfordert Lese- und Schreibzugriff auf Ihr Gerät. Führen Sie folgende Schritte aus, um den Zugriff zu aktivieren:

    1. Tippen Sie in Ihrem Profil auf **Anwendungseinstellungen > Storeeinstellungen**.
    2. Tippen Sie auf Ihren aktuellen Store.
    3. Tippen Sie auf **Gerätespeicher** und wählen Sie **Vollzugriff**.

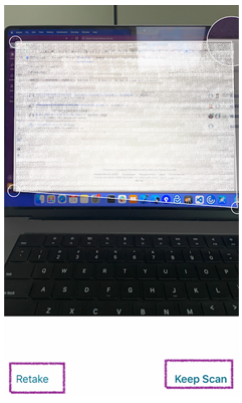
Gehen Sie wie folgt vor, um Dokumente mit dem Dokumentenscanner zu scannen:

1. Tippen Sie in der Symbolleiste während der Sitzung auf das Dreipunktemenü und wählen Sie **Dokument scannen** aus. Die Kamera-App wird geöffnet.

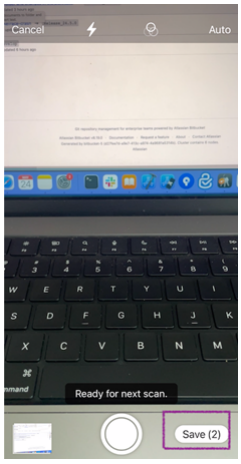


2. Tippen Sie auf den Auslöser, um das Foto aufzunehmen. Für eine weitere Aufnahme tippen Sie auf **Erneut aufnehmen**.

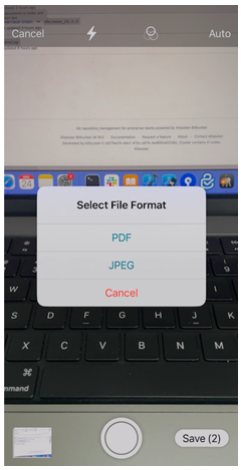
3. Optional: Gescanntes Dokument zuschneiden. Tippen Sie nach dem Zuschneiden auf die gewünschte Größe auf **Scan beibehalten**. Die Kamera-App wird erneut geöffnet, damit Sie mehr Bilder aufnehmen können.



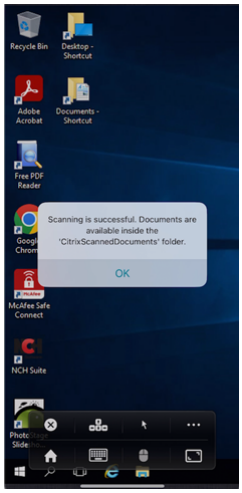
4. Nachdem Sie die erforderlichen Bilder aufgenommen haben, tippen Sie auf **Speichern**.



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

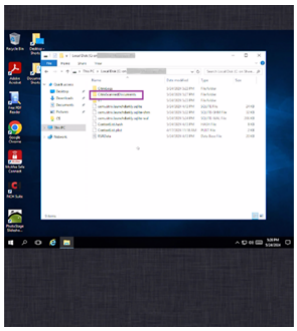


6. Tippen Sie auf **OK**.



Auf alle gescannten Dokumente kann im Ordner **CitrixScannedDocuments** im lokalen Speicher des Geräts zugegriffen werden. Sie können auch im Sitzungsdateimanager auf **CitrixScannedDocu-**

ments zugreifen.

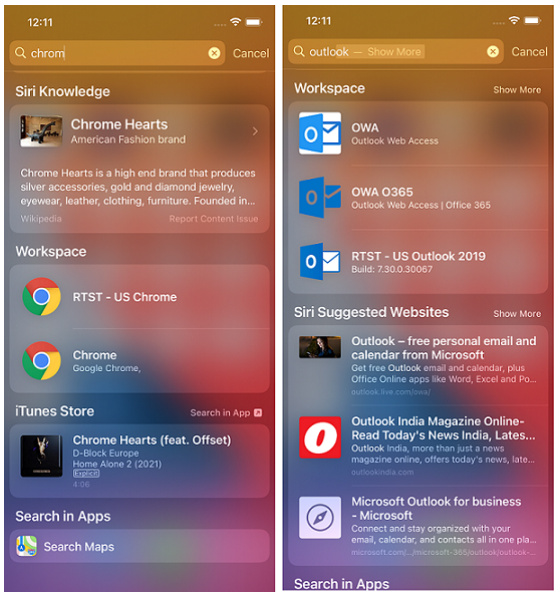


Benutzererfahrung

March 27, 2024

Erweiterung der Spotlight-Suche

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



Zugriff auf aktuelle Apps per 3D-Touch-Geste

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

Akkustatusanzeige

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

Dieses Feature wird nur für VDA-Versionen ab 7.18 unterstützt.

> **Hinweis:**
>
> In Sitzungen auf VDAs mit Microsoft Windows 10 kann es 1 bis 2 Minuten dauern, bis die Akkustatusanzeige angezeigt wird.

Langes Drücken für den Zugriff auf Ressourcen

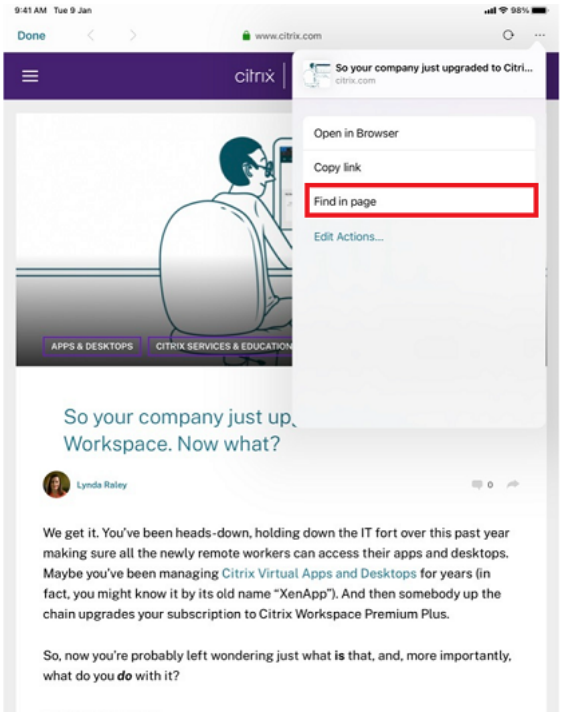
Sie können jetzt lange auf das Citrix Workspace-App-Symbol drücken und auf Ihre zuletzt gestartete Ressource zugreifen. Sie können jetzt die Citrix Workspace-App beenden und auf Ihre zuletzt gestartete Ressource zugreifen.

Verbesserung “Auf Seite suchen”

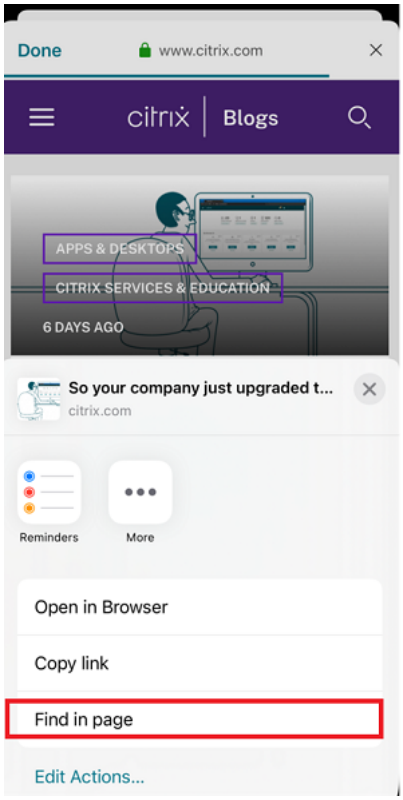
Mit dem Feature “Auf Seite suchen”können Sie besser nach Wörtern oder Wortgruppen suchen. Dieser verbesserte Benutzerkomfort ist in Web-Apps und SaaS-Apps (Software as a Service) anwendbar.

Ausführen der Suche:

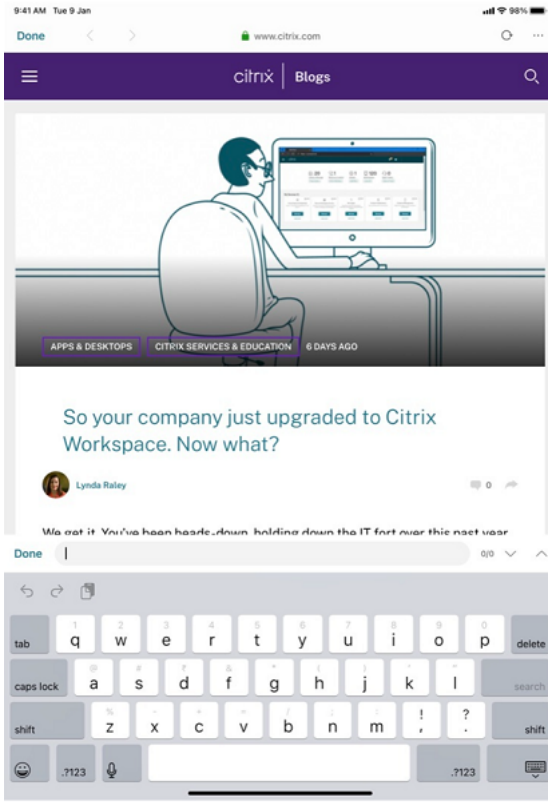
1. Tippen Sie auf dem iPad rechts oben in der Ecke auf die drei Punkte (…) und wählen Sie **Auf Seite suchen**.



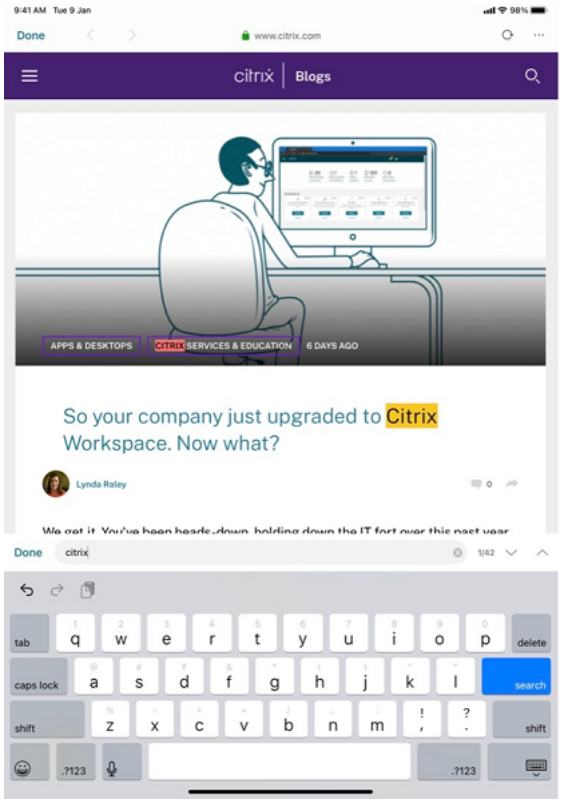
Tippen Sie auf dem iPhone rechts oben in der Ecke auf die drei Punkte (…) und wählen Sie **Auf Seite suchen**.



Die Bildschirmtastatur wird angezeigt.



1. Geben Sie den Suchtext in das Textfeld ein (zum Beispiel Citrix). Die Suchergebnisse werden angezeigt.



Neupositionieren der Sitzungssymbolleiste

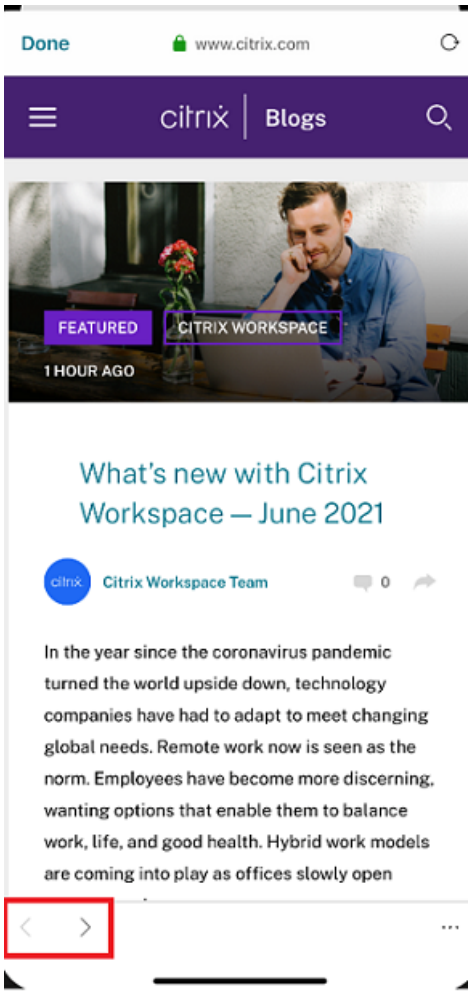
Sie können die sitzungseigene Symbolleiste entweder oben oder rechts im Bildschirm positionieren. Wenn Sie die Kerbe der Symbolleiste vom Rand der Symbolleiste wegziehen, werden die Rechteck-Ziehen-Anzeige und das Ablageziel angezeigt. Legen Sie die Ziehen-Anzeige über das Ablageziel, um die Symbolleiste neu zu positionieren

> **Hinweise:**
>
> - Das Feature gilt nur für iPad-Benutzer.
> - Das Feature funktioniert mit Touch oder Maus.
> - Das Feature funktioniert mit einem iPad oder auf einem externen Display.
> - Die letzte Symbolleistenposition bleibt für die nächste Sitzung oder nach dem Anwendungsstart erhalten.

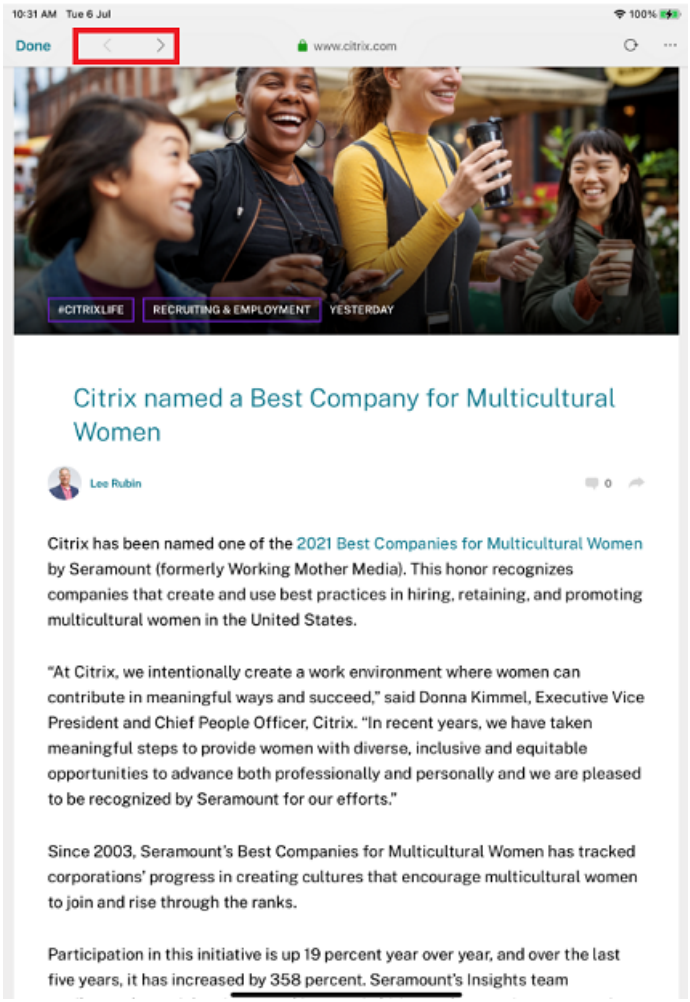
Zwischen SaaS- und Web-Apps wechseln

Mit der Verbesserung der Benutzerfreundlichkeit können Sie zwischen Web- und SaaS-Apps hin und her navigieren.

Die Navigationsschaltflächen werden unten links in den Workspace-Web- und SaaS-App-Sitzungen auf Ihrem iPhone angezeigt.



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



Migration vom On-Premises- zum Cloudkonto

Administratoren können die Endbenutzer nahtlos von einer on-premises StoreFront-Store-URL zu einer Workspace-URL migrieren. Administratoren können die Migration mit minimaler Endbenutzerinteraktion über den Global App Configuration Service durchführen.

Schrittfolge zum Konfigurieren:

1. Navigieren Sie zur URL der Global App Configuration Service Settings API und geben Sie die Cloudstore-URL ein.
   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** und klicken Sie auf **POST**.
3. Klicken Sie auf **INVOKE API**.

4. Geben Sie die Nutzlastdaten ein und laden Sie sie hoch. Geben Sie das Verfallsdatum des StoreFront-Stores im Unixzeit-Format (Millisekunden) ein.

   Beispiel:

```
"migrationUrl": [
{


"url": "<cloud store url>"
"StoreFrontValidUntil": "<epoch timestamp in milliseconds>",
 }

]   ,
<!--NeedCopy-->
```

5. Klicken Sie auf **EXECUTE**, um den Dienst per Push zu übermitteln.

Endbenutzererlebnis

Wenn Sie als Endbenutzer die Citrix Workspace-App zum ersten Mal verwenden, wird nach erfolgreicher Authentifizierung der Migrationsbildschirm **Der neue Citrix Workspace** angezeigt (sofern Berechtigung vorliegt). Tippen Sie auf die Option **Testen Sie jetzt den neuen Citrix Workspace**, um die Migration zu starten. Nach erfolgreicher Migration können Sie auf den Workspace-Store (Cloudstore) zugreifen.

> **Hinweis:**
>
> Sie können die Migration dreimal überspringen. Danach wird die Migration ohne Option zum Überspringen erzwungen.

Nach der Migration zum Workspace-Store (Cloudstore) können Sie unter **Einstellungen** StoreFront und den Workspace-Store anzeigen. Wenn Sie von einem Cloudstore zum on-premises bereitgestellten StoreFront-Store wechseln, wird ein Bildschirm für Ihr Feedback angezeigt.

> **Hinweis:**
>
> Der StoreFront-Store hat ein Verfallsdatum. Nach Ablauf des Verfallsdatums wird der Store gelöscht.

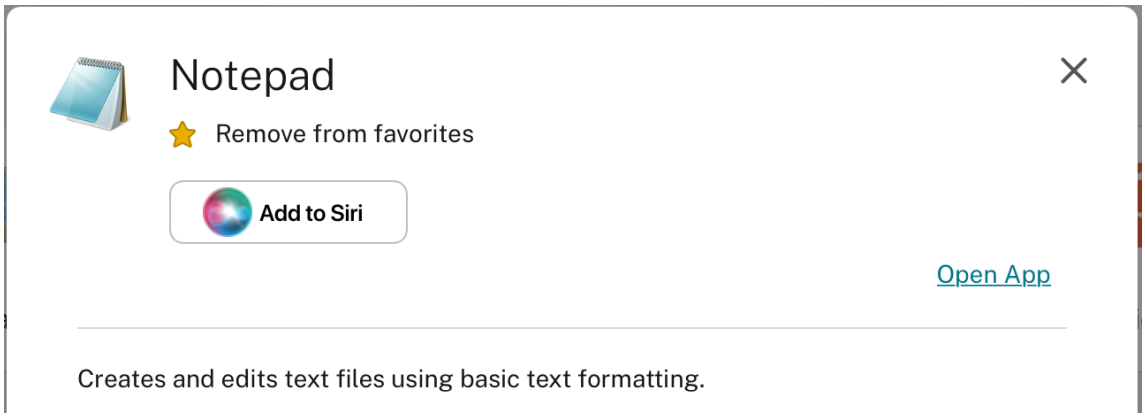
Siri-Integration

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

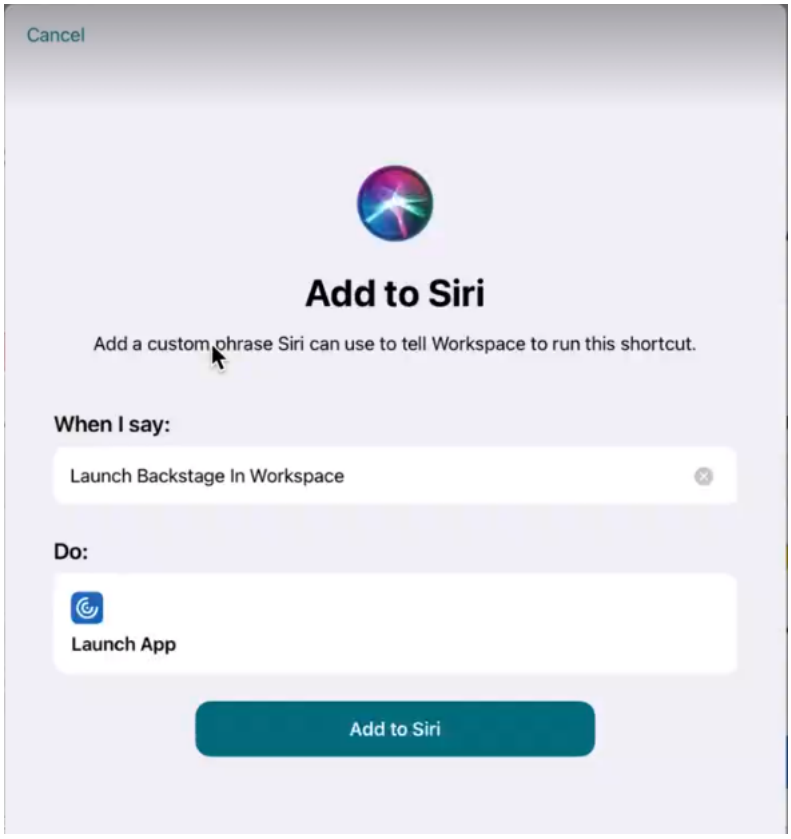
Konfiguration

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 das Dreipunktmenü (…). Ein Dialogfenster wird angezeigt.

   > **Hinweis:**
   >
   > Als iPhone- oder iPad-Desktopbenutzer tippen Sie auf das **Dreipunktmenü (…)** > **App-Details** > **Details anzeigen**. Ein Dialogfenster wird angezeigt. Fahren Sie mit Schritt 3 fort.

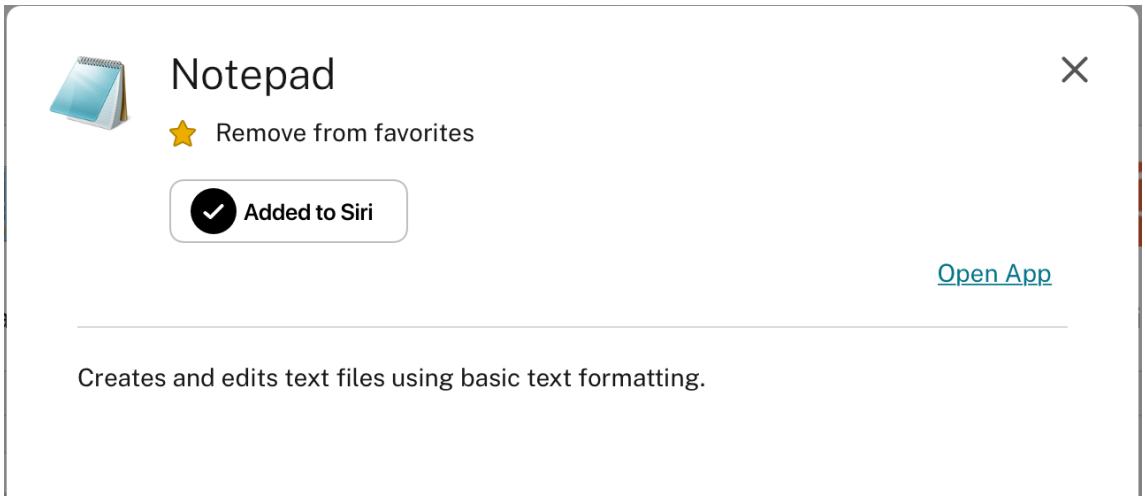
   

3. Tippen Sie auf **Zu Siri hinzufügen**. Das Dialogfenster **Zu Siri hinzufügen** wird angezeigt.



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

> **Hinweis:**
>
> Einige Geräte unterstützen das Aufzeichnen des benutzerdefinierten Sprachbefehls zum Aufrufen von Siri.



Anwendungseinstellungen

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

Sie können die Ressource jetzt per Spracheingabe starten.

Bearbeiten oder Löschen der Verknüpfung

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

Unterstützung für ein separates Sitzungsfenster von der Citrix Workspace-App

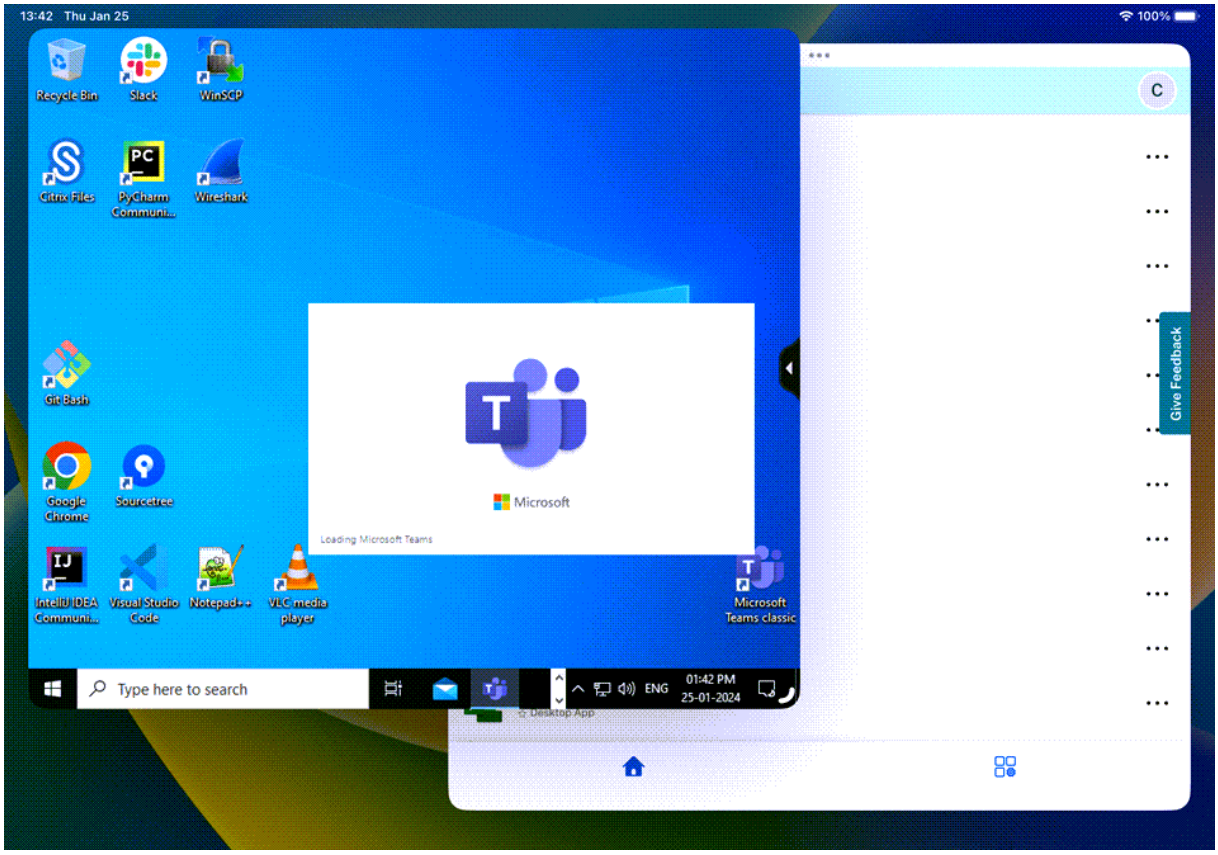
Ab Version 24.1.0 bietet die Citrix Workspace-App für iOS ein separates Sitzungsfenster, das Multitasking effizienter und benutzerfreundlicher macht. Mit diesem Feature entsteht ein Desktop-ähnliches Erlebnis. Wenn das Feature für separate Sitzungsfenster aktiviert ist, können Sie Sitzungen einfach per 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 diesem Feature enthalten:

- Wenn Sie in der Sitzungsmenüleiste auf die Schaltfläche **Home** klicken, wird das Citrix Workspace-Benutzeroberflächenfenster geöffnet, anstatt das HDX-Sitzungsfenster zu schließen. Mit dieser Verbesserung können Sie die Citrix Workspace-Benutzeroberfläche und die HDX-Sitzung gleichzeitig verwenden. Wenn Sie eine neue Sitzung über die Citrix Workspace-Benutzeroberfläche starten, wird die bestehende automatisch getrennt.
- Wenn Sie in der Sitzungsmenüleiste auf die Schaltfläche **Anzeigeoptionen** klicken, wird ein Einstellungsfenster über der HDX-Sitzung angezeigt. In diesem Fenster können Sie die Sitzungsauflösung anstelle der Citrix Workspace-Benutzeroberflächeneinstellungen anpassen.

> **Hinweis:**
>
> Diese Funktion wird nur auf Geräten unterstützt, die das Stage Manager-Feature unterstützen. Alle iPhone-Geräte und einige iPad-Geräte unterstützen dieses Feature nicht. Weitere Informationen zum State Manager-Feature finden Sie in der Apple Support-Dokumentation unter Stage Manager auf dem iPad ein- oder ausschalten.

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



Webansicht für Web- und SaaS-Apps

December 11, 2023

Webseite

Externe Freigabe von Webseiten

Sie können die Webseiten, die Sie über die Citrix Workspace-App öffnen, für andere freigeben. Sie haben folgende Möglichkeiten:

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

Zur Freigabe tippen Sie auf das Symbol **...** oben rechts in der Webansicht oder tippen Sie lange auf einen beliebigen Link in der Webansicht und tippen Sie dann auf die gewünschte Option.

Webansicht

Erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps

Sie können eine erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps verwenden. Diese Erweiterung ermöglicht Folgendes:

- Anzeigen der URL Ihrer Apps.
- Anzeigen der Sicherheitsinformationen Ihrer Apps.
- Teilen von Apps.

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

Webviewer für mobile Citrix Workspace-Apps

Der Webviewer ist eine In-App-Browsing-Lösung, die in der Citrix Workspace-App ausgeführt wird. Es ermöglicht Benutzern, Web- oder SaaS-Apps über die Citrix Workspace-App auf sichere Weise zu öffnen. Der Webviewer vereinheitlicht die Benutzeroberfläche beim Zugriff auf verschiedene Web- oder SaaS-Apps. Er erhöht die Produktivität und bietet eine bessere Leistung beim Rendern der Apps.

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

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

Administratoren können Secure Private Access (SPA) einschließlich Download, Zwischenablage, Navigationsbeschränkungen, Dateiupload und Wasserzeichen in unterschiedlichen Kombinationen auf Pro-URL-Basis aktivieren.

Kennwortverwaltung

March 27, 2024

Kennwörter speichern

In der Citrix Webinterface-Verwaltungskonsole konfigurieren Sie die Authentifizierungsmethode, damit Benutzer ihre Kennwörter speichern können. Wenn Sie das Benutzerkonto konfigurieren, wird das verschlüsselte Kennwort gespeichert, bis der Benutzer das erste Mal eine Verbindung herstellt. Beachten Sie Folgendes:

- Wenn Sie das Speichern des Kennworts aktivieren, speichert die Citrix Workspace-App für iOS das Kennwort für zukünftige Anmeldungen auf dem Gerät und fordert nicht zur Kennworteingabe auf, wenn Benutzer eine Verbindung zu Anwendungen herstellen.

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

- Wenn Sie das Speichern des Kennworts deaktivieren (Standardeinstellung), fordert die Citrix Workspace-App für iOS Benutzer jedes Mal zur Kennworteingabe auf, wenn sie eine Verbindung herstellen.

> **Hinweis:**
>
> Für direkte StoreFront-Verbindungen können Kennwörter nicht gespeichert werden.

Überschreiben der Kennwortspeicherung

Wenn der Server Kennwörter speichert, können Benutzer, die eine Kennworteingabe bei der Anmeldung bevorzugen, das Speichern des Kennworts überschreiben:

- Machen Sie beim Erstellen des Kontos keine Eingabe in das Feld “Kennwort”.
- Löschen Sie beim Bearbeiten eines Kontos das Kennwort und speichern Sie das Konto.

Verwendung

Die Citrix Workspace-App hat ein Feature, mit dem das Herstellen einer Verbindung optimiert wird, da Sie das Kennwort speichern können. Damit entfällt der zusätzliche Schritt zur Authentifizierung einer Sitzung bei jedem Öffnen der Citrix Workspace-App.

> **Hinweis:**
>
> Die Funktionalität **Kennwort speichern** unterstützt das PNA-Protokoll. Der *native* Store-

> Front wird nicht unterstützt. Diese Funktionalität funktioniert jedoch, wenn StoreFront den *PNA-Legacymodus* aktiviert.

StoreFront zum Speichern von Kennwörtern konfigurieren

Konfigurieren von StoreFront zum Aktivieren der Funktionalität **Kennwort speichern**:

1. Wenn Sie einen vorhandenen Store konfigurieren, gehen Sie zu Schritt 3.
2. Zum Konfigurieren einer neuen StoreFront-Bereitstellung halten Sie sich an die bewährten Methoden, die unter Installieren, Einrichten, Upgrade durchführen 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 beim Generieren des SSL-Zertifikats angegeben wurde.
4. Wählen Sie den Store aus, den Sie konfigurieren möchten.
5. Klicken Sie auf **XenApp Services-Support konfigurieren**.
6. Aktivieren Sie **XenApp Services-Support**, wählen Sie den **Standardstore** (optional) aus und klicken Sie auf **OK**.
7. Navigieren Sie zur Vorlagenkonfigurationsdatei in c:\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\.
8. Erstellen Sie ein Backup der Datei Config.aspx.
9. Öffnen Sie die Originaldatei Config.aspx.
10. Bearbeiten Sie die Zeile <EnableSavePassword>**false**</EnableSavePassword> und ändern Sie den Wert **false** in **true**.
11. Speichern Sie die bearbeitete Datei Config.aspx.
12. Führen Sie PowerShell auf dem StoreFront-Server 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 Folgendes ein: “Set-DSServiceMonitorFeature –ServiceUrl”`https://localhost:443/StoreFrontMonitor`
14. Bei einer StoreFront-Gruppe müssen Sie dieselben Befehle für alle Mitgliedern der Gruppe ausführen.

Citrix Gateway zum Speichern von Kennwörtern konfigurieren

> **Hinweis:**
>
> Diese Konfiguration verwendet Citrix Gateway-Server mit Lastausgleich.

Konfigurieren von Citrix Gateway für die Unterstützung der Kennwortspeicherung:

1. Melden Sie sich bei der Citrix Gateway-Verwaltungskonsole an.
2. Halten Sie sich an die bewährten Citrix-Methoden beim Erstellen eines Zertifikats für die virtuellen Server mit Lastausgleich.
3. Navigieren Sie auf der Registerkarte "Configuration"auf **Traffic Management** > **Load Balancing** > **Servers** und klicken Sie auf **Add**.
4. Geben Sie den Servernamen und die IP-Adresse des StoreFront-Servers ein.
5. Klicken Sie auf **Erstellen**. Wiederholen Sie für eine StoreFront-Gruppe Schritt 5 für alle Server in der Gruppe.
6. Navigieren Sie auf der Registerkarte "Configuration"auf **Traffic Management** > **Load Balancing** > **Monitor** und klicken Sie auf **Add**.
7. Geben Sie einen Namen für den Monitor ein. Wählen Sie als Typ **StoreFront**. Wählen Sie unten auf der Seite **Secure** (erforderlich, da der StoreFront-Server HTTPS verwendet).
8. Klicken Sie auf die Registerkarte **Special Parameters**. Geben Sie den vorher konfigurierten StoreFront-Namen ein, wählen Sie **Check Backed Services** und klicken Sie auf**Create**.
9. Navigieren Sie auf der Registerkarte **Configuration** auf **Traffic Management** > **Load Balancing** > **Service Groups** und klicken Sie auf **Add**.
10. Geben Sie einen Namen für die Dienstgruppe ein und legen Sie für das Protokoll **SSL** fest und klicken Sie auf **OK**.
11. Klicken Sie auf der rechten Seite des Bildschirms unter "Advanced Settings"auf **Settings**.
12. Aktivieren Sie die Client-IP und geben Sie Folgendes für den Headerwert ein: **X-Forwarded-For**. Klicken Sie dann auf **OK**.
13. Wählen Sie unter "Advanced Settings"auf der rechten Seite des Bildschirms **Monitors**. Klicken Sie auf den Pfeil und fügen Sie neue Monitore hinzu.
14. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann das Dropdownmenü **Select Monitor** aus. Eine Liste der auf dem Citrix Gateway konfigurierten Bildschirme wird angezeigt.
15. Klicken Sie auf das Optionsfeld neben dem zuvor erstellten Bildschirm und klicken Sie auf **Select** und dann auf **Bind**.

16. Wählen Sie unter "Advanced Settings"auf der rechten Seite des Bildschirms **Members** aus. Klicken Sie auf den Pfeil und fügen Sie neue Dienstgruppenmitglieder hinzu.
17. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann die Dropdownliste **Select Member** aus.
18. Aktivieren Sie das Optionsfeld **Server Based**. Eine Liste der auf dem Citrix Gateway konfigurierten Servermitglieder wird angezeigt. Klicken Sie auf das Optionsfeld neben dem zuvor erstellten StoreFront-Server.
19. Geben Sie für die Portnummer 443 und für die Hash-ID eine eindeutige Zahl ein. Klicken Sie dann auf **Create** und auf **Done**. Wenn alles richtig konfiguriert wurde, sollte **Effective State** ein grünes Licht anzeigen, d. h. das Monitoring funktioniert richtig.
20. Navigieren Sie auf **Traffic Management -> Load Balancing -\ > Virtual Servers** und klicken Sie auf **Add**. Geben Sie den Namen für den Server ein und wählen Sie als Protokoll **SSL**.
21. Geben Sie die IP-Adresse für den StoreFront-Lastausgleichsserver ein und klicken Sie auf **OK**.
22. Wählen Sie die Bindung **Load Balancing Virtual Server Service Group**, klicken Sie auf den Pfeil und fügen Sie die vorher erstellte Dienstgruppe hinzu. Klicken Sie zwei Mal auf **OK**.
23. Weisen Sie das für den virtuellen Lastausgleichsserver erstellte SSL-Zertifikat zu. Wählen Sie **No Server Certificate**.
24. Wählen Sie das Zertifikat des Lastausgleichsservers aus der Liste aus und klicken Sie auf **Bind**.
25. Fügen Sie das Domänenzertifikat dem Lastausgleichsserver hinzu. Klicken Sie auf **No CA certificate**.
26. Wählen Sie das Domänenzertifikat aus und klicken Sie auf **Bind**.
27. Wählen Sie auf der rechten Seite des Bildschirms **Persistence**.
28. Ändern Sie "Persistence"in **SOURCEIP** und stellen Sie das Timeout auf **20** ein. Klicken Sie auf **Save** und anschließend auf **Done**.
29. Fügen Sie den Lastausgleichsserver (wenn er noch nicht erstellt ist) dem Domänen-DNS-Server hinzu.
30. Starten Sie die Citrix Workspace-App für iOS auf dem iOS-Gerät und geben Sie die vollständige XenApp-URL ein.

Authentifizieren

July 1, 2024

Clientzertifikatauthentifizierung

> **Wichtig:**
>
> - Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App Folgendes:
>   - 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 Clientzertifikatauthentifizierung.
> - Nur Access Gateway Enterprise Edition 9.x und 10.x (und spätere Releases) unterstützen die Clientzertifikatauthentifizierung.
> - Die Zweiquellenauthentifizierungstypen müssen CERT und LDAP sein.
> - Die Citrix Workspace-App unterstützt auch die optionale Clientzertifikatauthentifizierung.
> - Nur Zertifikate im P12-Format werden unterstützt.

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

Mit folgendem Verfahren können Administratoren Endbenutzer auf der Basis der Clientzertifikatattribute authentifizieren:

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

Wenn Benutzer sich am virtuellen Citrix Gateway-Server anmelden, können sie nach der Authentifizierung den Benutzernamen und die Domäne aus dem Feld **SubjectAltName:OtherName:MicrosoftUniversal** des Zertifikats extrahieren. Das Format lautet `username@domain`.

Die Authentifizierung ist abgeschlossen, wenn der Benutzer den Benutzernamen und die Domäne extrahiert und die benötigten Informationen (beispielsweise ein Kennwort) eingibt. Wenn der Benutzer kein gültiges Zertifikat und keine gültigen Anmeldeinformationen bereitstellt oder wenn der Benutzername bzw. die Domäne nicht extrahiert werden kann, schlägt die Authentifizierung fehl.

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

Konfigurieren der XenApp-Farm

Erstellen Sie in der Citrix Virtual Apps-Konsole oder Webinterface-Konsole eine XenApp-Farm für mobile Geräte. Die verwendete Konsole hängt davon ab, welche Version von Citrix Virtual Apps installiert ist.

Die Citrix Workspace-App verwendet eine XenApp-Farm, um Informationen über die Anwendungen abzurufen, für die ein Benutzer Rechte besitzt. Diese Informationen werden für die Apps freigegeben, die auf dem Gerät ausgeführt werden. Dieses Verfahren ähnelt der Verwendung des Webinterface für traditionelle SSL-basierte Citrix Virtual Apps-Verbindungen, für die das Citrix Gateway konfiguriert werden kann.

Konfigurieren Sie die XenApp-Farm für die Citrix Workspace-App für Mobilgeräte, um Citrix Gateway-Verbindungen zu ermöglichen:

1. Wählen Sie in der XenApp-Farm **Manage secure client access** > **Edit secure client access settings**.
2. Ändern Sie die Zugriffsmethode in Gateway Direct.
3. Geben Sie den FQDN des Citrix Gateway-Geräts ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.

Konfigurieren des Citrix Gateway-Geräts

Für die Clientzertifikatauthentifizierung konfigurieren Sie das Citrix Gateway mit zweistufiger Authentifizierung und den Authentifizierungsrichtlinien Cert und LDAP. Konfigurieren des Citrix Gateway-Geräts:

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

    - Erstellen Sie eine Sitzungsrichtlinie, mit der Sie angeben, dass die Verbindung von der Citrix Workspace-App für Mobilgeräte ist. Konfigurieren Sie beim Erstellen der Sitzungsrichtlinie den folgenden Ausdruck und wählen Sie “Match All Expressions”als Operator aus:

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

    - Stellen Sie in der zugeordneten Profilkonfiguration für die Sitzungsrichtlinie auf der Registerkarte **Security** den Eintrag **Default Authorization** auf **Allow**.

      Wenn die Einstellung auf der Registerkarte **Published Applications** keine globale Einstellung ist (das Kontrollkästchen “Override Global”ist aktiviert), muss das Feld **ICA-Proxy** auf **ON** eingestellt sein.

Geben Sie im Webinterface im Feld **Adresse** die URL einschließlich 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 den virtuellen Server.
- Erstellen Sie Authentifizierungsrichtlinien für Cert und LDAP.
- Binden Sie die Authentifizierungsrichtlinien an den virtuellen Server.
- Konfigurieren Sie den virtuellen Server, Clientzertifikate im TLS-Handshake anzufordern. Navigieren Sie dafür zu **Certificate**, öffnen Sie **SSL Parameters** > **Client Authentication**, und setzen Sie **Client Certificate** auf **Mandatory**.

> **Wichtig:**
>
> Es muss beachtet werden, ob das Serverzertifikat, das auf dem Citrix Gateway verwendet wird, Teil einer Zertifikatskette ist. Wenn es sich beispielsweise um ein Zwischenzertifikat handelt, installieren Sie die Zertifikate auf dem Citrix Gateway. Weitere Informationen zur Installation von Zertifikaten finden Sie in der Citrix Gateway-Dokumentation.

Konfigurieren des Mobilgeräts

Wenn die Clientzertifikatauthentifizierung in 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 spezielle Richtlinien anwenden.

1. Öffnen Sie in der Citrix Workspace-App das **Konto** und geben Sie im Feld "Server"den entsprechenden FQDN des Citrix Gateway-Servers ein. Zum Beispiel "GatewayClientCertificateServer.organization.com". Die Citrix Workspace-App erkennt automatisch, dass das Clientzertifikat benötigt wird.
2. Benutzer können entweder ein neues Zertifikat installieren oder eines aus der Liste der bereits installierten Zertifikate auswählen. Für die iOS-Clientzertifikatauthentifizierung erfolgen Download und Installation des Zertifikats nur von der Citrix Workspace-App.
3. Nachdem Sie ein gültiges Zertifikat ausgewählt haben, sind die Felder für Benutzernamen und Domäne im Anmeldebildschirm mit dem Benutzernamen aus dem Zertifikat vorausgefüllt. Ein Endbenutzer kann andere Details eingeben, einschließlich des Kennworts.
4. Wenn die Clientzertifikatauthentifizierung optional ist, können Benutzer die Zertifikatauswahl überspringen, wenn sie auf der Zertifikatseite auf "Back"klicken. In diesem Fall stellt die Citrix Workspace-App die Verbindung her und zeigt dem Benutzer einen Anmeldebildschirm.

5. Nachdem Benutzer die Erstanmeldung abgeschlossen haben, können sie Anwendungen ohne erneute Angabe des Zertifikats starten. Die Citrix Workspace-App speichert das Zertifikat für das Konto und verwendet es automatisch für weitere Anmeldungen.

Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren

Administratoren können den für die Authentifizierung verwendeten Browser ändern und vom eingebetteten Browser auf den Systembrowser wechseln. Dies ist nur möglich, wenn eine erweiterte Authentifizierungsrichtlinie auf der On-Premises-Bereitstellung von Citrix Gateway- und StoreFront konfiguriert ist. Um eine erweiterte Authentifizierungsrichtlinie zu konfigurieren, konfigurieren Sie die NetScaler Rewrite-Richtlinie mithilfe der 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_p -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Durch einen Wechsel auf den Systembrowser werden u. a. die folgenden Zusatzfunktionen bereitgestellt:

- Bessere Nutzung der zertifikatbasierten Authentifizierung.
- Verwendbarkeit des vorhandenen Benutzerzertifikats aus dem Geräteschlüsselspeicher zur Authentifizierung.
- Unterstützung für einige Authentifikatoren von Drittanbietern wie SITHS eID.

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

In dieser Tabelle sind die Browser aufgeführt, die, basierend auf der Konfiguration auf dem NetScaler Gateway und im Global App Config Service, für die Authentifizierung verwendet werden:

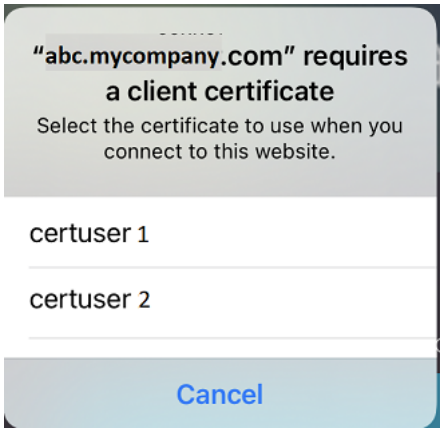
NetScaler Gateway	Global App Configuration Service	Zur Authentifizierung verwendeter Browser
System	System	System
System	Eingebettet	System
Eingebettet	System	System
Eingebettet	Eingebettet	Eingebettet

NetScaler Gateway	Global App Configuration Service	Zur Authentifizierung verwendeter Browser
Keine Konfiguration	System	System
Keine Konfiguration	Eingebettet	Eingebettet

Unterstützung der zertifikatsbasierten Authentifizierung für On-Premises-Stores

Endbenutzer können jetzt die zertifikatbasierte Authentifizierung nutzen, bei der die Zertifikate im Geräte-Schlüsselbund gespeichert werden. Während der Anmeldung erkennt die Citrix Workspace-App die Liste der Zertifikate auf Ihrem Gerät, und Sie können ein Zertifikat für die 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 in den iOS-Geräteeinstellungen "Reset Safari"auswählen oder die Citrix Workspace-App neu installieren.



> **Hinweis:**
>
> Dieses Feature unterstützt On-Premises-Bereitstellungen.

Schrittfolge zum Konfigurieren:

1. Navigieren Sie zur URL der Global App Configuration Service Settings API und geben Sie die Cloudstore-URL ein.
   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** und klicken Sie auf **POST**.

3. Klicken Sie auf **INVOKE API**.
4. Geben Sie die Nutzlastdaten ein und laden Sie sie hoch. Wählen Sie einen der folgenden Werte aus:

   - "Embedded": Sie können WKWebView verwenden. Diese Option ist standardmäßig eingestellt.
   - "system": Sie können den Safari View-Controller verwenden.

   Beispiel:

   ```
   "category": "Authentication",
   "userOverride": false,
   "settings": [
   {
     "name": "Web Browser to use for Authentication", "value": "*
        Embedded*/*System*"  }
    ,
   <!--NeedCopy-->
   ```

   Auf iOS- oder iPad-Geräten können Administratoren den für den Authentifizierungsprozess verwendeten Browser wechseln. Sie können vom eingebetteten Browser zum Systembrowser wechseln, wenn eine erweiterte Authentifizierungsrichtlinie auf der On-Premises-Bereitstellung von Citrix Gateway und StoreFront konfiguriert ist. Weitere Informationen finden Sie unter Rewrite-Richtlinie für den Authentifizierungsprozess konfigurieren.
5. Klicken Sie auf **EXECUTE**, um den Dienst per Push zu übermitteln.

Smartcards

Die Citrix Workspace-App unterstützt SITHS-Smartcards, jedoch nur für Verbindungen innerhalb von Sitzungen.

Wenn Sie FIPS Citrix Gateway-Geräte verwenden, sollten Sie die Systeme so konfigurieren, dass SSL-Neuaushandlungen abgelehnt werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123680.

Die folgenden Produkte und Konfigurationen werden unterstützt:

- Unterstützte Smartcardleser:
  - Precise Biometrics Tactivo für iPad Mini Firmwareversion 3.8.0
  - Precise Biometrics Tactivo für iPad (4. Generation) und Tactivo für iPad (3. Generation) und iPad 2 Firmwareversion 3.8.0
  - BaiMobile® 301MP und 301MP-L Smartcardleser
  - Thursby PKard USB-Lesegerät
  - Feitian iR301 USB-Lesegerät

  - CCID-konforme Lesegeräte vom Typ C
  - Twocanoes Smart Card Utility-Lesegerät
- Unterstützte VDA-Smartcard-Middleware
  - ActiveIdentity
- Unterstützte Smartcards:
  - PIV-Karten
  - Common Access Card (CAC)
- Unterstützte Konfigurationen:
  - Smartcardauthentifizierung bei Citrix Gateway mit StoreFront 2.x und XenDesktop 7.x und höher oder XenApp 6.5 und höher

Konfigurieren der Citrix Workspace-App für den App-Zugriff

1. Wenn Sie die Citrix Workspace-App so konfigurieren möchten, dass sie beim Erstellen eines Kontos automatisch auf Apps zugreift, geben Sie im Feld “Adresse”die entsprechende URL des Stores ein. Beispiel:
   - StoreFront.organization.com
   - netscalervserver.organization.com
2. Wählen Sie die Option **Smartcard verwenden**, wenn Sie die Authentifizierung mit Smartcard durchführen.

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

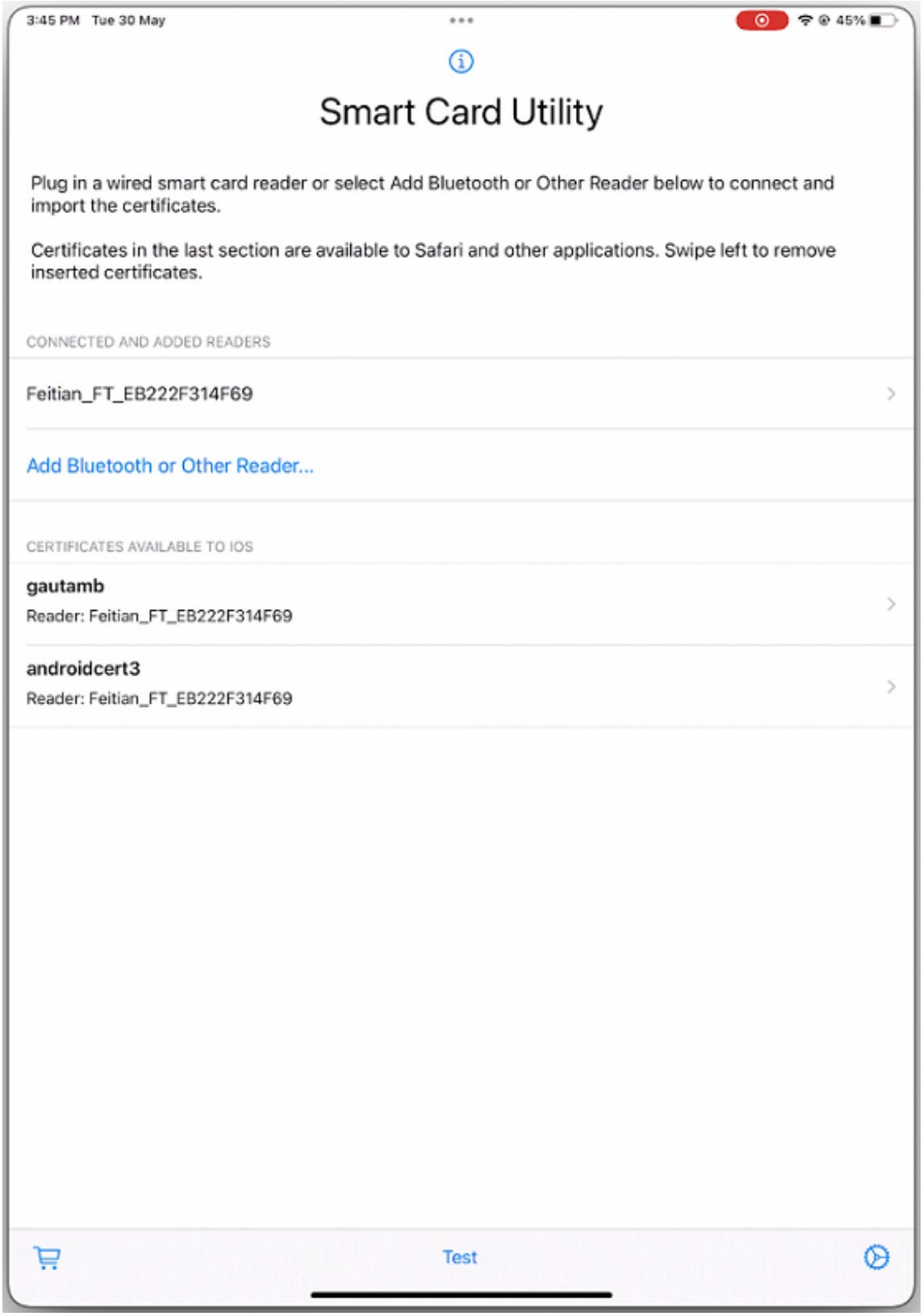
Unterstützung für das Twocanoes Smart Card Utility-Lesegerät

Ab Version 24.3.5 unterstützt die Citrix Workspace-App für iOS die Lesegeräte für Twocanoes Smart Card Utility. Weitere Informationen zu unterstützten Smartcardlesern finden Sie unter Smartcards.

> **Hinweis:**
>
> Das USB-C-Lesegerät von Twocanoes Smart Card Utility wird sowohl für die Anmeldung in der Citrix Workspace-App als auch für die Anmeldung in virtuellen Sitzungen unterstützt. Das Bluetooth-Lesegerät von Twocanoes Smart Card Utility wird jedoch nur für die Anmeldung in der Citrix Workspace-App und nicht für die Anmeldung in virtuellen Sitzungen unterstützt.

Gehen Sie wie folgt vor, um das Bluetooth-Lesegerät von Twocanoes Smart Card Utility zu konfigurieren:

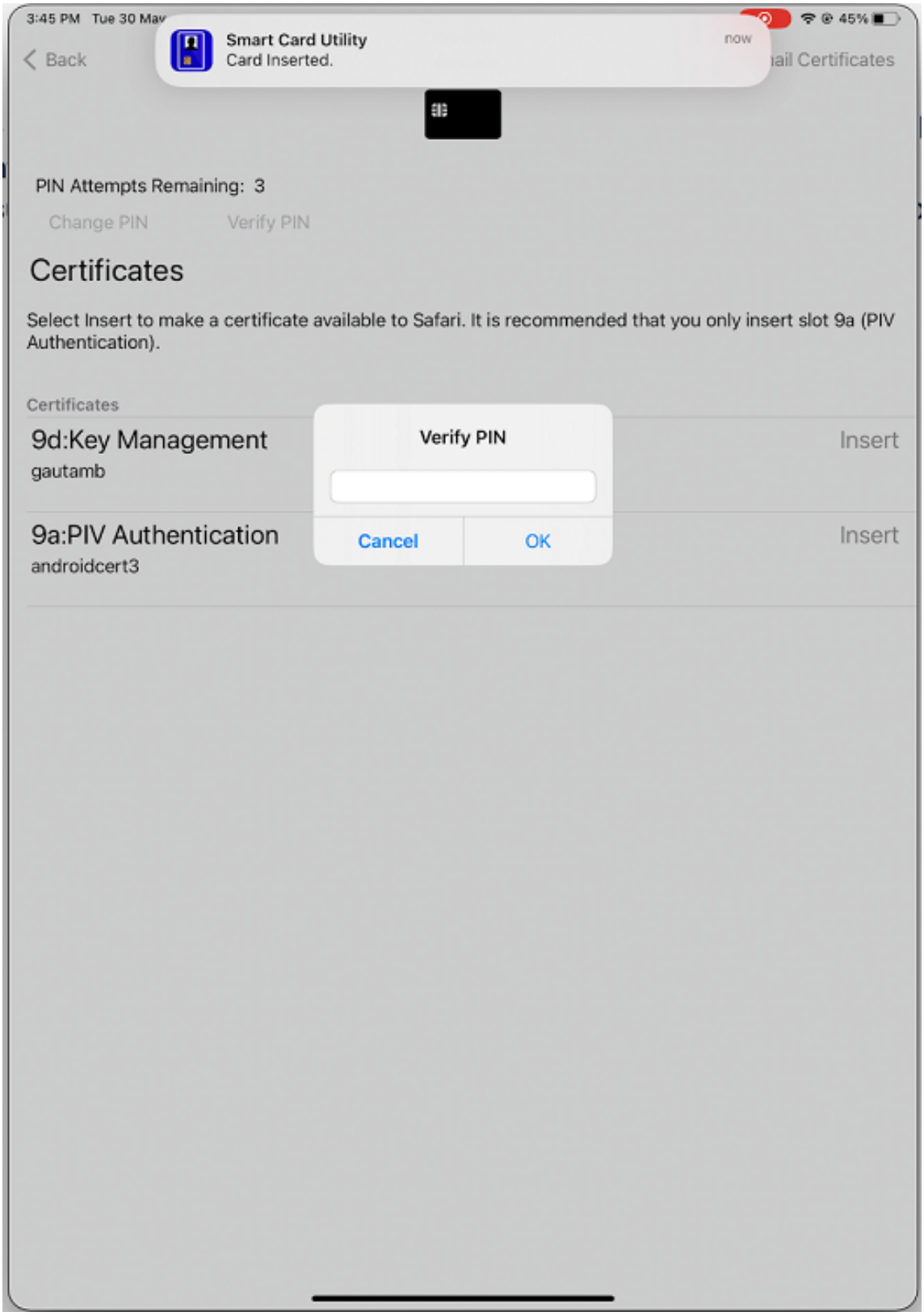
1. Laden Sie die Smart Card Utility-App aus dem App Store herunter und installieren Sie sie. Weitere Informationen finden Sie in der Twocanoes-Knowledge Base unter Smart Card Utility Bluetooth Reader Quick Start.
2. Vergewissern Sie sich, dass Bluetooth auf Ihrem Gerät eingeschaltet ist und die Smartcard in das Lesegerät eingesteckt ist.
3. Öffnen Sie die Smart Card Utility-App.



4. Wenn Sie das Bluetooth-Lesegerät verwenden, tippen Sie auf **Add Bluetooth or Other Reader**

... und wählen Sie Ihr Lesegerät aus, mit dem Sie eine Verbindung herstellen möchten.

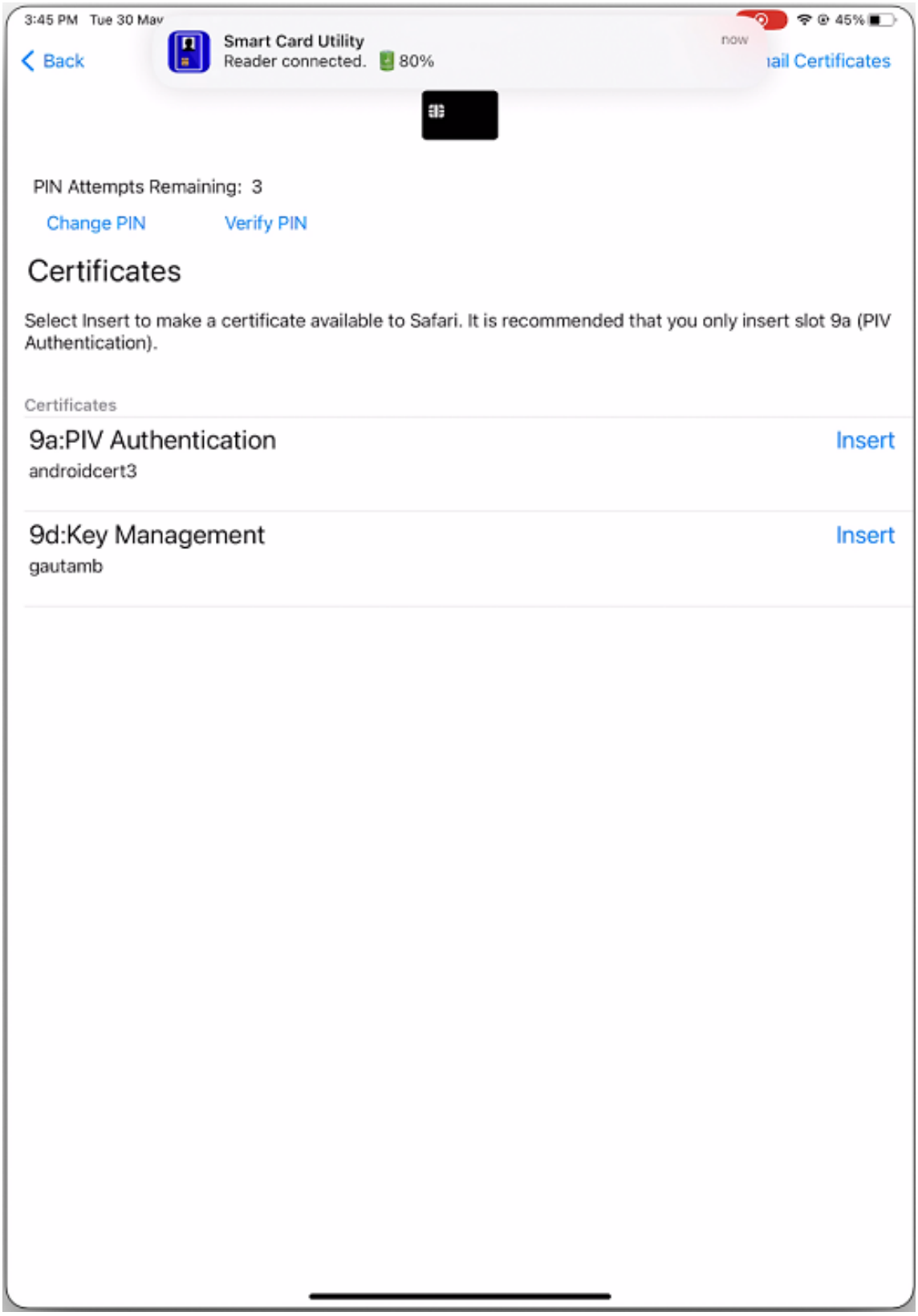
> **Hinweis:**
>
> Wenn das Lesegerät mit Pin-Pairing aktiviert ist, müssen Sie die **PIN** eingeben, wenn Sie dazu aufgefordert werden. Die **PIN** befindet sich auf der Rückseite des Lesegeräts.



5. Tippen Sie auf dem erforderlichen Zertifikat auf **Insert**, um es in die Schlüsselbundoberfläche

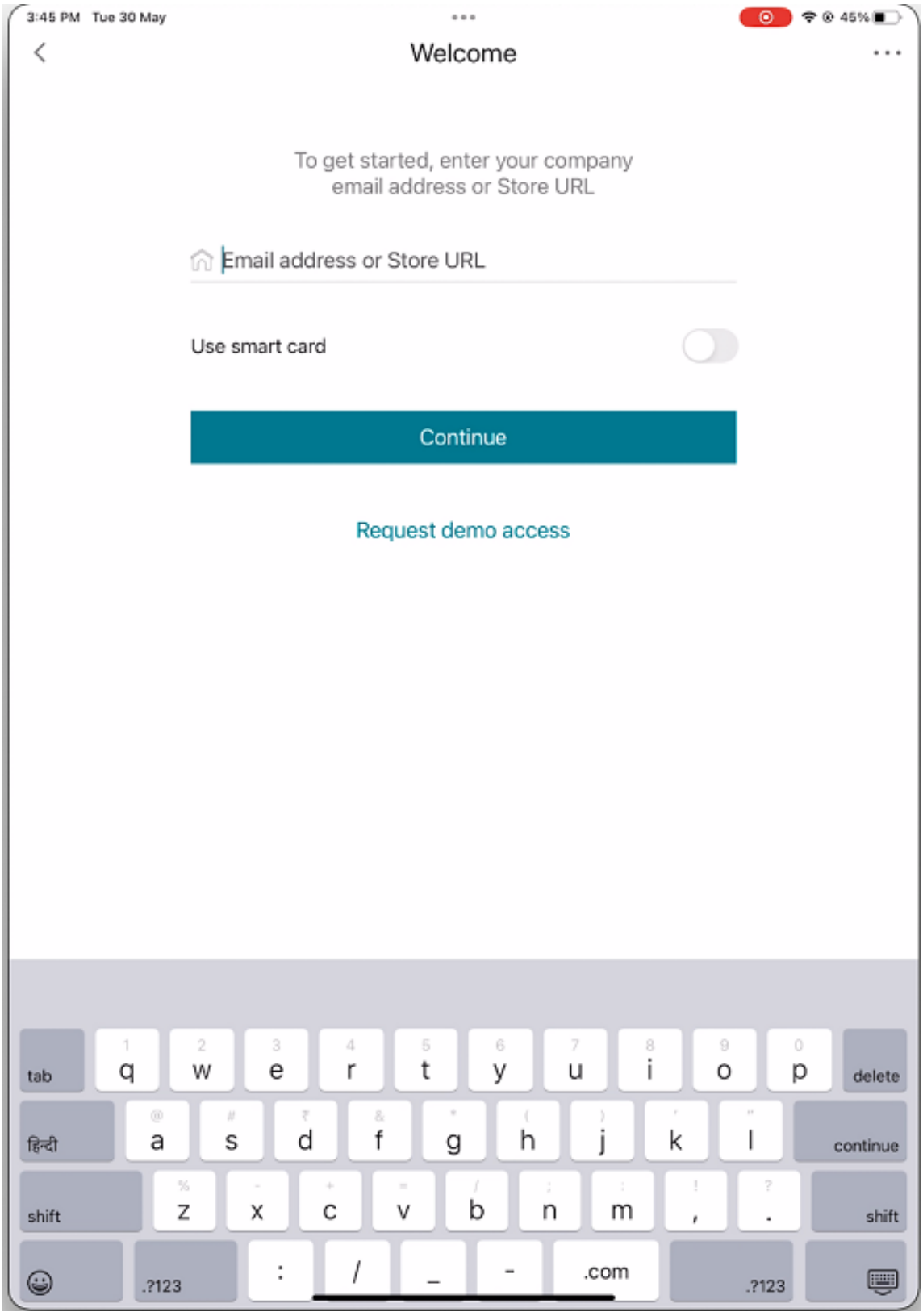
zu kopieren.

> **Hinweis:**
>
> Die Smart Card Utility-App hat eine von Apple bereitgestellte Cryptokit-Erweiterung implementiert, um Zertifikate in Form von Tokens in die Schlüsselbundoberfläche zu schreiben. Weitere Informationen finden Sie in der Apple-Entwicklerdokumentation unter Configuring Smart Card Authentication .

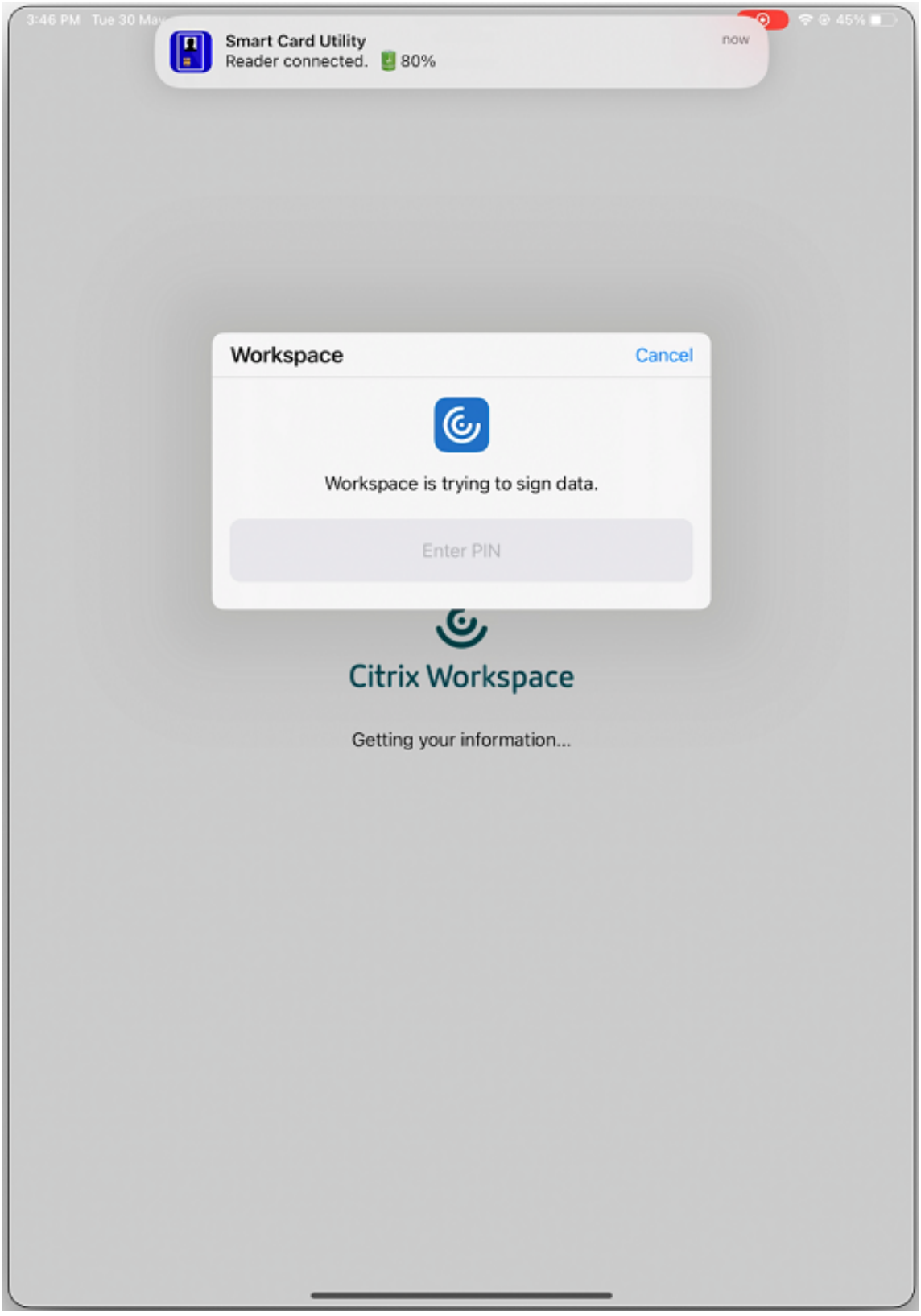


6. Vergewissern Sie sich, dass das Lesegerät mit dem Gerät verbunden bleibt.

7. Öffnen Sie die Citrix Workspace-App und geben Sie die Store-URL ein, die mit Smartcard-Authentifizierung konfiguriert ist.

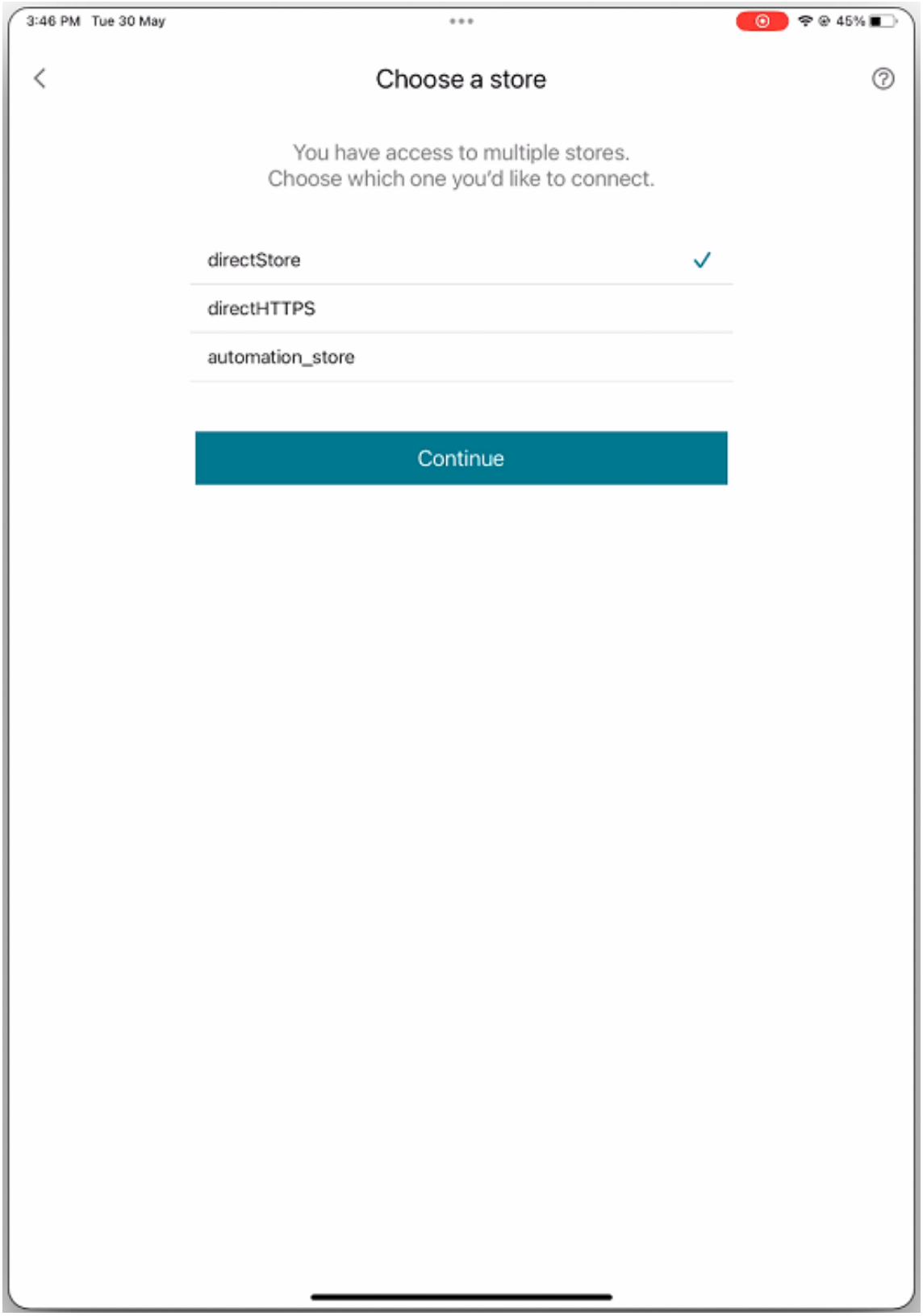


8. Wählen Sie auf dem Bildschirm “Zertifikate”das erforderliche Zertifikat aus und geben Sie die Smartcard-PIN ein, die Sie von Ihrem IT-Administrator für die Anmeldung erhalten haben.



9. Wenn Sie Zugriff auf mehrere Stores haben, wählen Sie den gewünschten Store aus und tippen

Sie auf **Weiter**.



10. Nach erfolgreicher Authentifizierung werden Sie bei der Citrix Workspace-App angemeldet.

YubiKey-Unterstützung für Smartcardauthentifizierung

Sie können jetzt die Smartcardauthentifizierung mit YubiKey durchführen. Dieses Feature bietet eine Einzelgeräteauthentifizierung für die Citrix Workspace-App sowie für die virtuellen Sitzungen und veröffentlichten Apps in der VDA-Sitzung. Damit wird der Anschluss von Smartcardlesern oder anderen externen Authentifikatoren überflüssig. Für Endbenutzer ist dies benutzerfreundlicher, weil YubiKey eine Vielzahl von Protokollen wie OTP, FIDO usw. unterstützt.

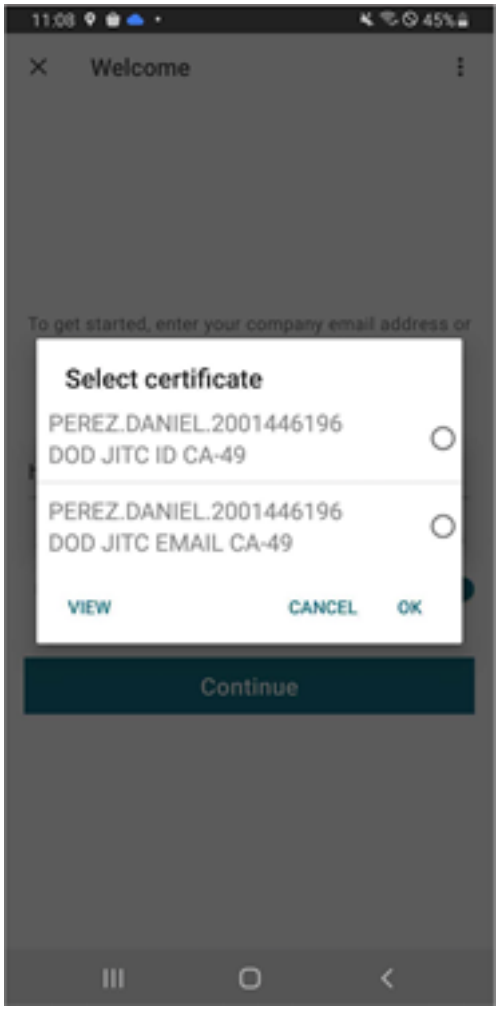
Zum Anmelden bei der Citrix Workspace-App müssen Endbenutzer den YubiKey in ihr iPhone oder iPad stecken, den Smartcardschalter einschalten und ihre Store-URL angeben.

> **Hinweis:**
>
> Dieses Feature unterstützt nur die direkte Verbindung zur Citrix Workspace-App in StoreFront-Bereitstellungen und nicht die Verbindung über Citrix Gateway. Die YubiKey-Unterstützung für die Smartcard-Authentifizierung über Citrix Gateway wird in der zukünftigen Version verfügbar sein.
> Die Citrix Workspace-App für iOS unterstützt nur die YubiKey 5-Serie. Weitere Informationen zu YubiKey finden Sie in der Dokumentation zur YubiKey 5-Serie.

Unterstützung für mehrere Zertifikate bei der Smartcardauthentifizierung

Bisher zeigte die Citrix Workspace-App für iOS das Zertifikat an, das auf dem 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. Mit dieser Funktion können Sie das erforderliche Zertifikat auswählen, während Sie sich über die Smartcard-Authentifizierung authentifizieren.



RSA SecurID-Authentifizierung

Die Citrix Workspace-App unterstützt die RSA SecurID-Authentifizierung für Konfigurationen mit Secure Web Gateway. Die Konfigurationen erfolgen über das Webinterface und gelten für alle Citrix Gateway-Konfigurationen.

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

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

Importieren eines RSA SecurID-Softwaretokens

Um einen RSA-Softwaretoken mit der Citrix Workspace-App zu verwenden, müssen Sie als Administrator sicherstellen, dass Endbenutzer folgende Vorgaben befolgen:

- die Richtlinie für die PIN-Länge
- die Art der PIN (nur numerisch und alphanumerisch)
- die Beschränkungen bei der Wiederverwendung von PINs

Nachdem der Endbenutzer erfolgreich am RSA-Server authentifiziert wurde, muss er die PIN nur einmal einrichten. Nach der Überprüfung der PIN wird der Endbenutzer auch am StoreFront-Server authentifiziert. Nach Abschluss der gesamten Überprüfung zeigt die Workspace-App verfügbare veröffentlichte Anwendungen und Desktops an.

Verwenden eines RSA-Softwaretokens

1. Importieren Sie den RSA-Softwaretoken, den Ihre Organisation bereitgestellt hat.
2. Wählen Sie in der E-Mail mit der angehängten SecurID-Datei **In Workspace öffnen** als Importzielort aus. Nach dem Import des Softwaretokens wird die Citrix Workspace-App automatisch geöffnet.
3. Falls Ihre Organisation ein Kennwort für den Abschluss des Imports bereitgestellt hat, geben Sie das bereitgestellte Kennwort ein und klicken Sie auf **OK**. Nach dem Klicken auf **OK** gibt eine Meldung den erfolgreichen Import des Tokens an.
4. Schließen Sie die Importmeldung und tippen Sie in der Citrix Workspace-App auf **Konto hinzufügen**.
5. Geben Sie die URL des von der Organisation bereitgestellten Stores ein und klicken Sie auf **Weiter**.
6. Geben Sie auf dem Anmeldebildschirm Ihre Anmeldeinformationen ein: Benutzername, Kennwort und Domäne. Geben Sie im Feld "PIN"**0000** ein, wenn Ihnen keine andere Standard-PIN bereitgestellt wurde. Die PIN 0000 ist ein RSA-Standard; Ihre Organisation hat sie ggf. geändert, um eigene Sicherheitsrichtlinien einzuhalten.
7. Klicken Sie oben links auf **Anmelden**. Sie werden aufgefordert, eine PIN zu erstellen.
8. Geben Sie eine PIN mit 4 bis 8 Stellen ein und klicken Sie auf **OK**. Sie werden aufgefordert, Ihre neue PIN zu verifizieren.
9. Geben Sie Ihre PIN erneut ein und klicken Sie auf **OK**. Sie können jetzt auf Ihre Apps und Desktops zugreifen.

Nächster Tokencode

Die Citrix Workspace-App unterstützt "Nächster Tokencode", wenn Sie Citrix Gateway mit RSA SecurID-Authentifizierung konfigurieren. Wenn Sie das Kennwort dreimal falsch eingeben, wird im Citrix Gateway-Plug-in eine Fehlermeldung angezeigt. Warten Sie auf den nächsten Token, um sich anzumelden. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers, der sich zu oft mit einem falschen Kennwort anmeldet, deaktiviert wird.

Abgeleitete Anmeldeinformationen

Die Citrix Workspace-App unterstützt die Verwendung abgeleiteter Anmeldeinformationen mit Purebred. Beim Herstellen einer Verbindung mit einem Store, der abgeleitete Anmeldeinformationen zulässt, können Benutzer sich mithilfe einer virtuellen Smartcard bei der Citrix Workspace-App anmelden. Dieses Feature wird nur bei On-Premises-Bereitstellungen unterstützt.

> **Hinweis:**
>
> Citrix Virtual Apps and Desktops 7 1808 oder höher ist für dieses Feature erforderlich.

Aktivieren von abgeleiteten Anmeldeinformationen in der Citrix Workspace-App:

1. Navigieren Sie zu **Einstellungen** > **Erweitert** > **Abgeleitete Anmeldeinformationen**.
2. Tippen Sie auf **Abgeleitete Anmeldeinformationen verwenden**.

Schrittfolge zum Erstellen einer virtuellen Smartcard, die mit abgeleiteten Anmeldeinformationen verwendet werden kann:

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 PIN ein (nur Zahlen) und bestätigen Sie sie.
4. Tippen Sie auf **Weiter**.
5. Tippen Sie unter "Authentifizierungszertifikat"auf **Zertifikat importieren…**
6. Das Dokumentauswahlfenster wird angezeigt. Tippen Sie auf **Durchsuchen**.
7. Tippen Sie unter "Speicherort"auf **Purebred Key Chain**.
8. Wählen Sie das passende Authentifizierungszertifikat in der Liste aus.
9. Tippen Sie auf **Schlüssel importieren**.
10. Wiederholen Sie ggf. die Schritte 5 bis 9 für das digitale Signaturzertifikat und das Verschlüsselungszertifikat.
11. Tippen Sie auf **Speichern**.

Sie können bis zu drei Zertifikate für Ihre virtuelle Smartcard importieren. Das Authentifizierungszertifikat ist erforderlich, damit die virtuelle Smartcard ordnungsgemäß funktioniert. Das Verschlüs-

selungszertifikat und das digitale Signaturzertifikat 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 jeweils nur eine aktive Karte haben.
- Wenn eine virtuelle Smartcard erstellt wurde, kann sie nicht mehr bearbeitet werden. Sie müssen die Karte löschen und erstellen.
- Sie haben bis zu 10 Eingabeversuche für eine PIN. 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-Zeichenfolge für WKWebView

Standardmäßig enthält die User-Agent-Zeichenfolge, die bei einigen über WKWebView initiierten Netzwerkanforderungen verwendet wird, jetzt die ID der Citrix Workspace-App.

Sie wurde 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
```

in eine der folgenden Optionen:

```
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
```

(Beispiel für iPhone)

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
```

(Beispiel für iPad)

nFactor-Authentifizierung

Unterstützung für Multifaktorauthentifizierung (nFactor)

Die Multifaktorauthentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Mit der Multifaktorauthentifizierung können Authentifizierungsschritte und die zugehörigen Anmeldeinformationsformulare vollständig vom Administrator konfiguriert werden.

Die native Citrix Workspace-App kann dieses Protokoll über die unterstützten Anmeldeformulare nutzen, die bereits für StoreFront implementiert sind. Die webbasierte Anmeldeseite für virtuelle Citrix Gateway- und Traffic Manager-Server verwendet ebenfalls dieses Protokoll.

Weitere Informationen finden Sie unter SAML-Authentifizierung und Multifaktorauthentifizierung (nFactor).

Einschränkungen:

- Wenn die Unterstützung für Multifaktorauthentifizierung (nFactor) aktiviert ist, können Sie keine biometrische Authentifizierung, wie Touch ID und Face ID, verwenden.

Unterstützung für erweiterte nFactor-Authentifizierungsrichtlinie

Wir unterstützen jetzt die zertifikatbasierte Authentifizierung in der Citrix Workspace-App, wenn sie über erweiterte nFactor-Authentifizierungsrichtlinien auf Citrix Gateway konfiguriert wird. Die nFactor-Authentifizierung erleichtert das Konfigurieren flexibler und agiler mehrstufiger Schemas.

User-Agent-Zeichenfolge:

Bei der Durchführung der erweiterten Authentifizierung (nFactor-Authentifizierung) für die Citrix Workspace-App auf dem iPhone oder iPad wird der Authentifizierungsprozess an eine eingebettete Webansicht umgeleitet. Die resultierende User-Agent-Zeichenfolge kann je nach Betriebssystemversion, CWA-Build-Version, Gerätemodell und AuthManager-Version geringfügig variieren. Im Folgenden sehen Sie Beispiele für User-Agent-Zeichenfolgen für iPhone und iPad.

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
```

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
```

Dieses Feature ist als Preview verfügbar. Es kann auf Anfrage über diesen Podio-Link oder durch Kontaktaufnahme mit dem technischen Support von Citrix aktiviert werden. Nach Abschluss der Previewphase erfolgt der allgemeine Rollout für alle Kunden.

> **Hinweis:**
>
> - Die Versions- oder Gerätemodellinformationen hängen von der Umgebung ab.
> - Mit folgenden Schlüsselwörtern können Sie bei der Authentifizierung die Citrix Workspace-App für iOS-spezifische benutzeragentbasierte Richtlinien verwenden.
>   - iOS
>   - CWA
>   - CWACapable

Unterstützung für FIDO2-basierte Authentifizierung beim Herstellen einer Verbindung zur HDX-Sitzung

Die Citrix Workspace-App für iOS unterstützt jetzt die kennwortlose Authentifizierung innerhalb einer Citrix Virtual Apps and Desktops-Sitzung mithilfe FIDO2-basierter Authentifizierungsverfahren. Dieses Feature ermöglicht Benutzern in Browsern wie Google Chrome oder Microsoft Edge die Anmeldung an einer WebAuthn-fähigen Website mithilfe von FIDO2-unterstützten Yubico-Sicherheitsschlüsseln. Beim Öffnen einer WebAuthn-fähigen Website wird eine kennwortlose Authentifizierung ausgelöst. 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 mit kennwortloser Authentifizierung wird nicht unterstützt.

Weitere Informationen zu den Voraussetzungen finden Sie unter Lokale Autorisierung und virtuelle Authentifizierung mit FIDO2 in der Dokumentation zu Citrix Virtual Apps and Desktops.

Unterstützung der Authentifizierung mit FIDO2 beim Verbinden mit Cloudstores

Ab der Version 24.5.0 können sich Benutzer bei der Citrix Workspace App mit FIDO2-basierter kennwortloser Authentifizierung authentifizieren, wenn sie sich mit einem Cloudspeicher verbinden. FIDO2 bietet eine nahtlose Authentifizierungsmethode, mit der Unternehmensmitarbeiter innerhalb virtueller Sitzungen auf Apps und Desktops zugreifen können, ohne dass sie einen Benutzernamen oder ein Kennwort eingeben müssen. Dieses Feature unterstützt sowohl Roaming (nur USB) als auch Plattformauthentifikatoren (PIN-Code, Touch ID und nur Face ID). Dieses Feature ist standardmäßig aktiviert.

> **Hinweis:**
>
> Die FIDO2-Authentifizierung wird standardmäßig mit den benutzerdefinierten Chrome-Tabs unterstützt. Wenn Sie daran interessiert sind, die FIDO2-Authentifizierung mit WebView zu verwenden, registrieren Sie Ihr Interesse über Podio-Formular.

Unterstützung für die Konfiguration der Speicherung von Authentifizierungstoken in der On-Premises-Bereitstellung

Die Citrix Workspace-App für iOS bietet jetzt die Option, die Speicherung von Authentifizierungstoken auf dem lokalen Datenträger für On-Premises-Stores zu konfigurieren. Mit diesem Feature können Sie die Speicherung des Authentifizierungstokens für die erhöhte Sicherheit deaktivieren. Nach der Deaktivierung müssen Sie sich beim Neustart des Systems oder der Sitzung erneut authentifizieren, um auf die Sitzung zugreifen zu können.

Gehen Sie wie folgt vor, um die Speicherung von Authentifizierungstoken der On-Premises-Bereitstellung in der Verwaltungskonfigurationsdatei zu deaktivieren:

1. Öffnen Sie die Datei web.config mit einem Texteditor. Die Datei ist normalerweise unter `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkonto-Element in der Datei (Store ist der Kontoname Ihrer Bereitstellung).
   Beispiel: `<account id=... name="Store">`
3. Navigieren Sie vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

```
    <properties>
        <property name="TokenPersistence" value="false" />
    </properties>
<!--NeedCopy-->
```

Dies 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>
<!--NeedCopy-->
```

Sicherheit

January 7, 2024

Zum Sichern der Kommunikation zwischen der Serverfarm und der Citrix Workspace-App integrieren Sie Verbindungen zur Serverfarm mit zahlreichen Sicherheitsverfahren, einschließlich Citrix Gateway.

> **Hinweis:**
>
> Citrix empfiehlt das Schützen der Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit Citrix Gateway.

- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver).

  Mit Proxyservern schränken Sie den eingehenden und ausgehenden Zugriff auf das Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.

- Secure Web Gateway.

  Secure Web Gateway stellt zusammen mit dem Webinterface einen einzigen sicheren und verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit.

Sie können Secure Web Gateway mit Webinterface 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.

  Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden.

  Wenn Sie die Citrix Workspace-App mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.

Citrix Gateway

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

Wenn Sie Citrix Endpoint Management im Netzwerk bereitstellen, lassen Sie Verbindungen von internen oder Remotebenutzern mit StoreFront über Citrix Gateway zu, indem Sie Citrix Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf von XenApp veröffentliche Anwendungen und auf von XenDesktop virtualisierte Desktops zu. Benutzer stellen eine Verbindung über die Citrix Workspace-App her.

Secure Web Gateway

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können Secure Web Gateway im Modus "Normal" oder "Relay" verwenden, um einen sicheren Kommunikationskanal zwischen der Citrix Workspace-App und dem Server bereitzustellen. Wenn Sie Citrix Secure Web Gateway im Modus **Normal** verwenden, muss die Citrix Workspace-App nicht konfiguriert werden. Stellen Sie sicher, dass Endbenutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Secure Web Gateway-Servern verwendet die Citrix Workspace-App Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden.

Wenn der Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie den Secure Web Gateway Proxy im Relaymodus verwenden. Wenn Sie den Relaymodus verwenden, fungiert der Secure Web Gateway-Server als Proxy und die Citrix Workspace-App muss Folgendes verwenden:

- Vollqualifizierter Domänenname (FQDN) des Secure Web Gateway-Servers.

- Portnummer des Secure Web Gateway-Servers.

> **Hinweis:**
>
> Secure Web Gateway Version 2.0 unterstützt den Relaymodus nicht.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

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

Proxyserver

Proxyserver beschränken den eingehenden und ausgehenden Netzwerkzugriff und verwalten Verbindungen zwischen der Citrix Workspace-App und Servern. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Citrix Virtual Apps and Desktops-Server verwendet die Citrix Workspace-App die Proxyservereinstellungen. Diese Proxyservereinstellungen werden remote auf dem Webinterface-Server konfiguriert.

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

Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss die Citrix Workspace-App über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können. Die Firewall muss HTTP-Verkehr für die Kommunikation zwischen Benutzergerät und Webserver zulassen. Bei Verwendung eines sicheren Webservers verläuft der HTTP-Verkehr normalerweise über den HTTP-Standardport 80 oder 443. Für die Kommunikation mit dem Citrix-Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

Wenn die Firewall für die Netzwerkadressenübersetzung konfiguriert ist, verwenden, können Sie im Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports definieren.

Beispiel: Wenn der Citrix Virtual Apps and Desktops- und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)-Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface der Citrix Workspace-App für iOS eine alternative Adresse bereitstellen. Die Citrix Workspace-App für iOS stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her.

TLS

Die Citrix Workspace-App unterstützt TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen für TLS-Verbindungen mit 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 auf iOS 9 und höher oder Version 21.2.0 ausgeführt wird, unterstützt nicht die folgenden TLS-Verschlüsselungssammlungen:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

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

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

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

> **Hinweis:**
>
> - Die Citrix Workspace-App verwendet plattformeigene Kryptografie (iOS) für Verbindungen

> zwischen der Citrix Workspace-App und StoreFront.

Konfigurieren und Aktivieren von TLS

Das Setup von TLS besteht aus zwei Hauptschritten:

1. Setup von SSL-Relay auf dem Citrix Virtual Apps and Desktops-Server und dem Webinterface-Server und Abrufen und Installieren des benötigten Serverzertifikats.
2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Installieren von Stammzertifikaten auf Benutzergeräten Für das Sichern der Kommunikation zwischen TLS-aktivierter Citrix Workspace-App und Citrix Virtual Apps and Desktops muss auf dem Clientgerät ein Stammzertifikat vorhanden sein. Das Stammzertifikat überprüft die Signatur der Zertifizierungsstelle im Serverzertifikat.

iOS wird mit hunderten kommerziellen Stammzertifikaten geliefert, die vorinstalliert sind. Wenn Sie jedoch ein anderes Zertifikat verwenden möchten, können Sie eines von der Zertifizierungsstelle abrufen und auf jedem Benutzergerät installieren.

Abhängig von den Richtlinien und Abläufen in Ihrem Unternehmen können Sie das Stammzertifikat ggf. auf jedem Benutzergerät installieren und die Installation nicht den Benutzern überlassen. Am einfachsten und sichersten ist es, wenn Sie die Stammzertifikate der iOS-Schlüsselkette hinzufügen.

Hinzufügen eines Stammzertifikats zur Schlüsselkette

1. Senden Sie sich selbst eine E-Mail mit der Zertifikatdatei.
2. Öffnen Sie die Zertifikatdatei auf dem Gerät. Durch diese Aktion wird die Anwendung für die Schlüsselbundverwaltung automatisch gestartet.
3. Folgen Sie die Anweisungen, um das Zertifikat hinzuzufügen.
4. Ab iOS 10 stellen Sie in den iOS-Einstellungen unter **Allgemein** > **Info** > **Zertifikatvertrauenseinstellungen** sicher, dass das Zertifikat als vertrauenswürdig angesehen wird.

   Überprüfen Sie unter “Zertifikatvertrauenseinstellungen”den Abschnitt “VOLLES VERTRAUEN FÜR ROOT-ZERTIFIKATE AKTIVIEREN”. Stellen Sie sicher, dass für Ihr Zertifikat volles Vertrauen aktiviert ist.

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

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 und XenDesktop-Sites unterstützen nur die einstufige Authentifizierung.
> - Citrix Virtual Apps-Websites unterstützen die einstufige und die zweistufige Authentifizierung.
> - Alle integrierten Browser unterstützen das Webinterface 5.4.

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

Konfigurieren Sie keine Citrix Gateway-Einstellungen auf der Citrix Workspace-App, wenn Sie eine Citrix Secure Gateway-Verbindung verwenden.

Die Citrix Workspace-App verwendet eine XenApp und XenDesktop-Site, um Informationen über die Anwendungen abzurufen, für die ein Benutzer Rechte besitzt. Dabei werden die Informationen der Citrix Workspace-App bereitgestellt, die auf Ihrem Gerät ausgeführt wird. In ähnlicher Weise können Sie das Webinterface für herkömmliche SSL-basierte Citrix Virtual Apps-Verbindungen verwenden. Für dieselbe SSL-basierte Verbindung können Sie Citrix Gateway konfigurieren. Diese Konfiguration ist in XenApp und XenDesktop-Sites integriert, die auf einem Server mit dem Webinterface 5.x ausgeführt werden.

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

1. Wählen Sie in der XenApp und XenDesktop-Site **Sicheren Clientzugriff verwalten** > **Einstellungen für sicheren Clientzugriff verwalten**.
2. Ändern Sie die Zugriffsmethode in **Gateway Direct**.
3. Geben Sie den FQDN von Secure Web Gateway ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.

> **Hinweis:**
>
> Citrix empfiehlt, für Citrix Secure Gateway den Citrix Standardpfad (//XenAppServerName/Citrix/PNAgent) zu verwenden. Der Standardpfad ermöglicht es Endbenutzern, den FQDN des Secure Web Gateway anzugeben, mit dem sie eine Verbindung herstellen. Verwenden Sie nicht

> den vollständigen Pfad zur Datei config.xml, die sich auf der XenApp und XenDesktop-Site befindet. Zum Beispiel //XenAppServerName/CustomPath/config.xml).

Konfigurieren von Citrix Secure Gateway

1. Konfigurieren Sie das Gateway mit dem Konfigurationsassistenten von Citrix Secure Gateway.

   Das Citrix Secure Gateway unterstützt den Server in dem sicheren Netzwerk, das die XenApp Service-Site hostet.

   Nachdem Sie die Option **Indirect** ausgewählt haben, geben Sie den FQDN-Pfad Ihres Secure Web Gateway-Servers ein und setzen Sie den Assistenten fort.
2. Testen Sie eine Verbindung von einem Benutzergerät aus, um sicherzustellen, dass Netzwerk und Zertifikatzuteilung für Secure Web Gateway richtig konfiguriert sind.

Konfigurieren des Mobilgeräts

1. Geben Sie beim Hinzufügen eines Citrix Secure Gateway-Kontos den FQDN des Citrix Secure Gateway-Servers in das 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 zur Datei config.xml an, z. B.: FQDNofSecureGateway.companyName.com/CustomPath/config.xml
2. Wenn Sie das Konto manuell konfigurieren, deaktivieren Sie die Citrix Gateway-Option **Neues Konto**.

Problembehandlung

March 27, 2024

So überprüfen Sie die Version der App

Um Ihre Citrix Workspace-App-Version zu überprüfen, öffnen Sie Ihre 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 ein Upgrade auf die neueste Version der Citrix Workspace-App über den Apple Store durchführen. Suchen Sie nach der Citrix Workspace-App und tippen Sie auf die Schaltfläche **Upgrade**.

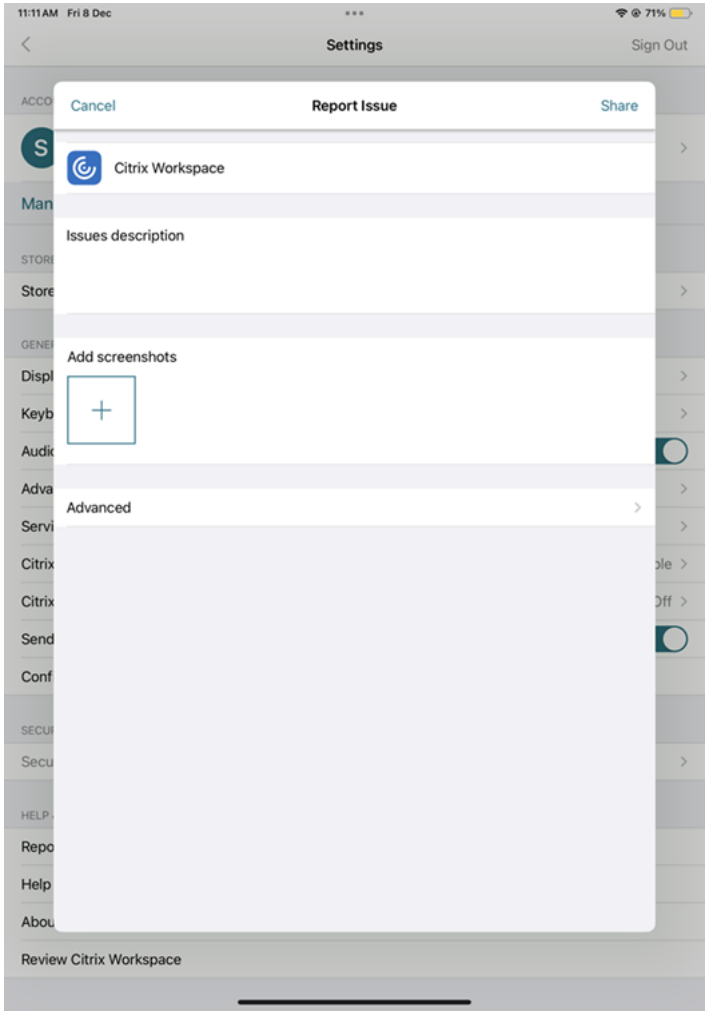
So setzen Sie die Citrix Workspace-App zurück

Sie können Ihre Citrix Workspace-App mit einer der folgenden Methoden zurücksetzen:

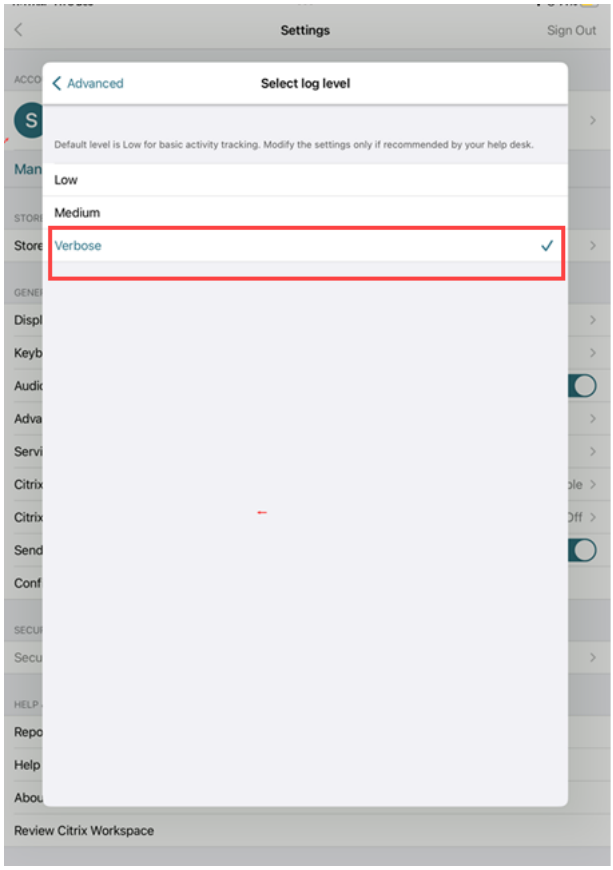
- Löschen Sie alle vorhandenen Konten aus der Citrix Workspace-App
- Löschen Sie die Speicherdaten der Citrix Workspace-App
- Deinstallieren Sie die Citrix Workspace-App und installieren Sie die neueste Citrix Workspace-App für iOS, die den neuesten Fix enthält.

Protokolle sammeln

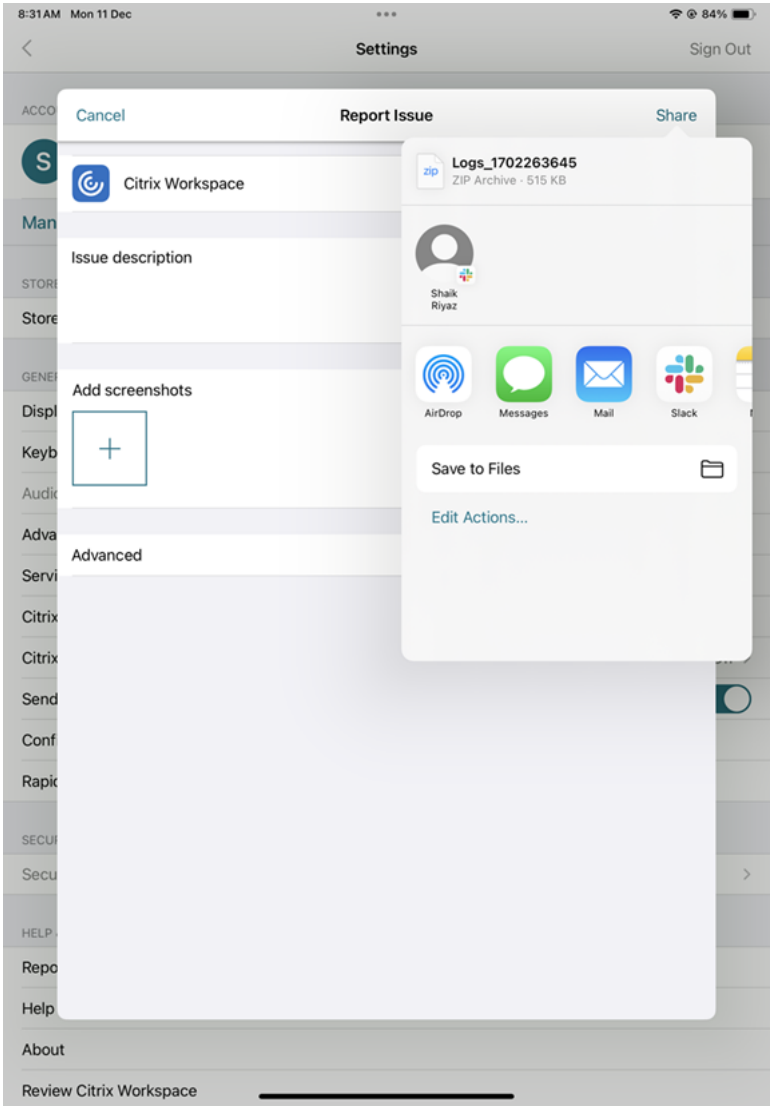
1. Öffnen Sie Ihre Citrix Workspace-App und navigieren Sie zu **Einstellungen**.
2. Wählen Sie unter **Hilfe und Support** die Option **Problem melden** aus.



3. Reproduzieren Sie Ihr Problem.
4. Wählen Sie auf der Seite “Protokollebene auswählen”die Option **Ausführlich** aus.



5. Wählen Sie auf der Seite **Speicherort für Protokoll wählen** die Option **Konsole und Datei** aus.
6. Geben Sie die Zip-Datei für Citrix frei.



So fordern Sie Verbesserungen an

Sie können Ihre Verbesserungsanfragen einreichen, indem Sie dieses Formular ausfüllen.

So greifen Sie auf Technical Preview-Features zu

Sie können Technical Preview-Features mit einem Podio-Formular anfordern, das für jedes Feature einzigartig ist. Dieses Formular finden Sie im Anhang zur Ankündigung des Technical Preview in der Produktdokumentation.

So geben Sie Feedback zu EAR

Um Feedback zur EAR-Version zu geben, tippen Sie hier.

Häufig auftretende Probleme und Tipps zur Problembehebung

Getrennte Sitzungen

Benutzer können eine Citrix Workspace-App für iOS-Sitzung wie folgt trennen (kein Abmelden):

- Beim Anzeigen einer veröffentlichten App oder einem veröffentlichten Desktop in einer Sitzung:
  - Tippen Sie auf den Pfeil oben auf dem Bildschirm, um das Dropdownmenü in der Sitzung anzuzeigen.
  - Tippen Sie auf die Schaltfläche **Home**, um zum Launchpad zurückzukehren.
  - Achten Sie auf den weißen Schatten unter dem Symbol einer der veröffentlichten Apps, die noch in einer aktiven Sitzung sind; tippen Sie auf das Symbol.
  - Tippen Sie auf "Trennen".
- Schließen der Citrix Workspace-App für iOS:
  - Tippen Sie zweimal auf die Schaltfläche **Home** des Geräts.
  - Suchen Sie die Citrix Workspace-App für iOS im iOS App Switcher.
  - Tippen Sie im angezeigten Dialogfeld auf "Trennen".
- Drücken Sie die Home-Taste auf dem Mobilgerät.
- Tippen Sie auf "Home"oder "Wechseln"im Dropdownmenü der App.

Die Sitzung bleibt im getrennten Zustand. Benutzer können sich mit dieser Sitzung später wieder verbinden. Administratoren können verifizieren, dass getrennte Sitzungen nach einem bestimmten Zeitraum als inaktiv angezeigt werden.

Um die App im inaktiven Modus anzuzeigen, konfigurieren Sie ein Sitzungstimeout für die ICA-TCP-Verbindung in der Konfiguration des Remotedesktop-Sitzungsserverhosts (früher "Terminaldienstekonfiguration"genannt).

Weitere Informationen zur Konfiguration von Remotedesktopdiensten (früher "Terminaldienste" genannt) finden Sie in der Produktdokumentation für Microsoft Windows Server.

Abgelaufene Kennwörter

Die Citrix Workspace-App für iOS unterstützt das benutzerseitige Ändern abgelaufener Kennwörter. Benutzer werden zur Eingabe der benötigten Informationen aufgefordert.

Geräte mit Jailbreak

Benutzer können die Sicherheit der Bereitstellung kompromittieren, wenn sie Verbindungen mit iOS-Geräten mit Jailbreak herstellen. Geräte mit Jailbreak wurden von ihren Besitzern modifiziert, wodurch meistens bestimmte Sicherheitsfunktionen umgangen werden.

Wenn die Citrix Workspace-App für iOS ein iOS-Gerät mit Jailbreak erkennt, wird der Benutzer mit einer angezeigten Warnung darauf hingewiesen.

Zur weiteren Sicherung der Umgebung können Sie StoreFront oder das Webinterface so konfigurieren, dass Geräte mit erkanntem Jailbreak keine Apps ausführen können.

Anforderungen

- Citrix Receiver für iOS 6.1 oder höher
- StoreFront 3.0 oder Webinterface 5.4 oder höher
- Zugriff auf StoreFront oder das Webinterface mit einem Administratorkonto

Verhindern, dass Geräte mit erkanntem Jailbreak Apps ausführen

1. Melden Sie sich am StoreFront- oder Webinterface-Server als ein Benutzer mit Administratorrechten an.
2. Suchen Sie die Datei **`default`**`.ica`, die in einem der folgenden Verzeichnisse gespeichert ist:
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\conf` (Microsoft Internetinformationsdienste)
    - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\App\\_Data` (Microsoft Internetinformationsdienste)
    - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. Fügen Sie unter dem Abschnitt **[Application]** Folgendes hinzu: **AllowJailBrokenDevices=OFF**
4. Speichern Sie die Datei und starten Sie den StoreFront- oder Webinterface-Server neu.

Nach dem Neustart des StoreFront-Servers können Benutzer, denen die Warnung zu Geräten mit Jailbreak angezeigt wird, keine Apps vom StoreFront- oder Webinterface-Server starten.

Zulassen, dass Geräte mit erkanntem Jailbreak Apps ausführen Wenn Sie AllowJailBrokenDevices nicht einstellen, wird die Warnmeldung standardmäßig den Benutzern von Geräten mit Jailbreak angezeigt; die Benutzer können die Anwendungen jedoch starten.

So lassen Sie ausdrücklich zu, dass Benutzer Anwendungen auf Geräten mit Jailbreak ausführen können:

1. Melden Sie sich am StoreFront- oder Webinterface-Server als ein Benutzer mit Administratorrechten an.
2. Suchen Sie die Datei default.ica, die in einem der folgenden Verzeichnisse gespeichert ist:
   - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\conf` (Microsoft Internetinformationsdienste)
   - `C:\\inetpub\\wwwroot\\Citrix\\*storename*\\App\\_Data` (Microsoft Internetinformationsdienste)
   - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. Fügen Sie unter dem Abschnitt **[Application]** Folgendes hinzu: **AllowJailBrokenDevices=ON**
4. Speichern Sie die Datei und starten Sie den StoreFront- oder Webinterface-Server neu.

Wenn Sie AllowJailBrokenDevices auf ON setzen, wird den Benutzern die Warnung zur Verwendung eines Geräts mit Jailbreak angezeigt, sie können jedoch Anwendungen über StoreFront- oder das Webinterface ausführen.

Verlust der HDX-Audioqualität

Von Citrix Virtual Apps and Desktops und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) kann die Qualität von HDX-Audio zur Citrix Workspace-App für iOS reduziert sein. Das Problem tritt auf, wenn Sie Audio und Video gleichzeitig verwenden.

Das Problem tritt auf, wenn die Citrix Virtual Apps and Desktops- und Citrix DaaS-HDX-Richtlinien die Audiodatenmenge zusammen mit den Videodaten nicht handhaben können.

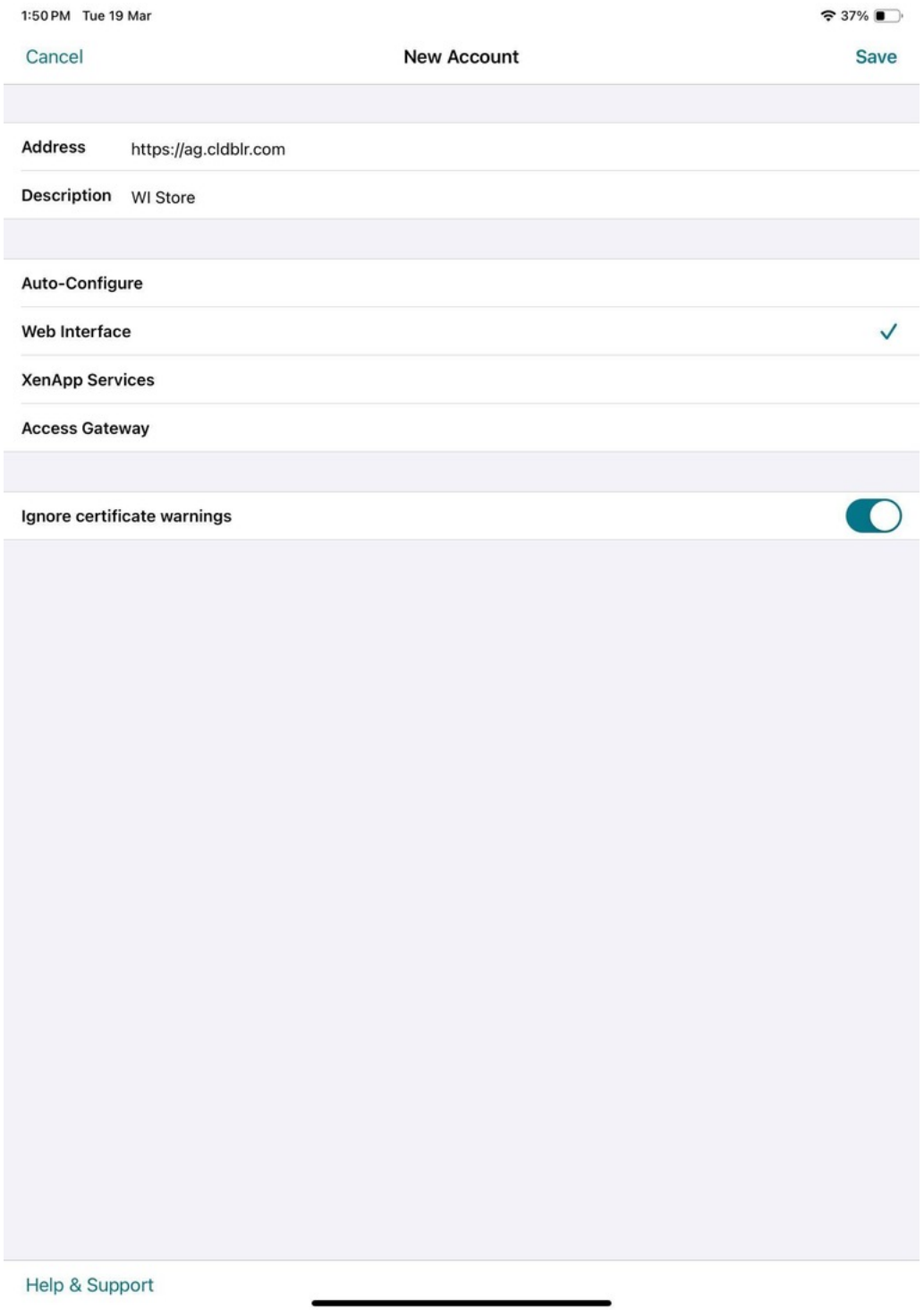
Empfehlungen zum Erstellen von Richtlinien für eine verbesserte Audioqualität finden Sie im Knowledge Center-Artikel CTX123543.

Desktop- und App-Sitzungen für ein individuelles Store-Erlebnis konnten nicht gestartet werden

Möglicherweise können Sie Desktop- und App-Sitzungen nicht über die Citrix Workspace-App starten, wenn Sie über ein benutzerdefiniertes Store-Erlebnis verfügen. Die automatische Erkennung des Store-Typs wird nur für E-Mail-Adressen und nicht für Store-URLs unterstützt. Es wird empfohlen, die E-Mail-Adresse oder den Webinterface-Anmeldemodus zu verwenden, wenn Sie einen benutzerdefinierten Store haben. Weitere Informationen finden Sie unter Manuelle Einrichtungund Konfigurieren der e-mail-basierten Kontoermittlung.

Gehen Sie wie folgt vor, um ein Konto manuell über den Webinterface-Anmeldemodus zu konfigurieren:

1. Tippen Sie auf **Konten > Bildschirm “Konten”> Pluszeichen (+)**. Der Bildschirm **Neues Konto** wird angezeigt.
2. Tippen Sie links unten im Bildschirm auf das Symbol links neben **Optionen** und tippen Sie auf **Manuelles Setup**. Andere Felder werden auf dem Bildschirm angezeigt.
3. Geben Sie im Feld **Adresse** die sichere URL der Site oder des Citrix Gateways an (z. B. agee.mycompany.com).
4. Wählen Sie die **Webinterface**-Verbindung aus. In diesem Verbindungsmodus wird eine Citrix Virtual Apps-Website angezeigt, die einem Webbrowser ähnelt. Diese Benutzeroberfläche wird auch Webansicht genannt.



5. Verwenden Sie für die Zertifikatssicherheit die Einstellung im Feld **Zertifikatwarnungen ignorieren** und legen Sie fest, ob eine Verbindung mit dem Server hergestellt wird, selbst wenn das Zertifikat ungültig, selbstsigniert oder abgelaufen ist. Die Standardeinstellung ist AUS.

> **Wichtig:**
>
> Wenn Sie diese Option aktivieren, vergewissern Sie sich, dass Sie eine Verbindung mit dem richtigen Server herstellen. Citrix empfiehlt dringend, dass alle Server ein gültiges Zertifikat haben, um Benutzergeräte vor Onlinesicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt, dass die Zertifikatsicherheit nicht ausgelassen wird.

6. Tippen Sie auf **Speichern**.
7. Geben Sie den Benutzernamen und das Kennwort (oder das Token, wenn Sie die zweistufige Authentifizierung ausgewählt haben) ein und tippen Sie dann auf "Anmelden". Der Citrix Workspace-App für iOS-Bildschirm wird angezeigt, von dem Sie auf die Desktops zugreifen und die Anwendungen hinzufügen und öffnen können.

> **Hinweis:**
>
> Sie müssen die Benutzeranmeldeinformationen für jede Verbindung eingeben, da diese im Webinterface-Anmeldemodus nicht gespeichert werden.

Häufig gestellte Fragen

So verbessern Sie die Videoleistung auf virtuellen Apps und virtuellen Desktops für Geräte mit geringem Stromverbrauch oder Mobilgeräte

Informationen zur Verbesserung und Konfiguration der Videoleistung virtueller Desktops über den Registrierungswert MaxFramesPerSecond oder über HDX-Richtlinien, je nach Version von Citrix Virtual Apps and Desktops, finden Sie im Knowledge Center-Artikel CTX123543.

Ich kann meine Apps oder Desktops nicht sehen, nachdem ich mich bei Citrix Workspace-App angemeldet habe

Wenden Sie sich an den Helpdesk Ihres Unternehmens oder an den Administrator Ihres IT-Supportteams, um weitere Unterstützung zu erhalten.

Wie behebe ich langsame Verbindungen?

Wenn Sie auf eines der folgenden Probleme stoßen, befolgen Sie die im folgenden Abschnitt zur **Problemumgehung** genannten Schritte.

- Langsame Verbindungen zur Citrix Virtual Apps and Desktops-Site

- Fehlende App-Symbole
- Wiederholte Protokolltreiber-Fehlermeldungen

Workaround Deaktivieren Sie die Eigenschaften des Citrix PV Ethernet-Adapters für die Netzwerkschnittstelle auf dem Citrix Virtual Apps-Server, dem Citrix Secure Web Gateway und dem Webinterface-Server.
Folgende Eigenschaften des Citrix PV Ethernet-Adapters sind standardmäßig aktiviert. Sie müssen alle diese Eigenschaften deaktivieren.

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

> **Hinweis:**
>
> Ein Serverneustart ist nicht erforderlich. Dieser Workaround gilt für Windows Server 2003 und 2008 (32 Bit). Dieses Problem wirkt sich nicht auf Windows Server 2008 R2 aus.

Problem mit Zifferntasten und Sonderzeichen beheben

Wenn Zifferntasten oder chinesische IME-Zeichen nicht wie erwartet funktionieren, müssen Sie die Option Unicode-Tastatur deaktivieren.
So deaktivieren Sie die Unicode-Tastatur:

1. Navigieren Sie zu **Einstellungen** > **Tastaturoptionen**.
2. Stellen Sie **Unicode-Tastatur** auf **Aus**.

Citrix Workspace-App für iOS

July 1, 2024

Die Citrix Workspace-App für iOS ist Clientsoftware, die im App Store zum Download verfügbar ist. Hiermit können Sie auf virtuelle Desktops und gehostete Anwendungen, die mit Citrix Virtual Apps and Desktops bereitgestellt werden, zugreifen und diese ausführen.

iOS ist das Betriebssystem für Mobilgeräte von Apple, wie iPads und iPhones. Die Citrix Workspace-App für iOS kann auf Geräten mit dem iOS-Betriebssystem, wie iPhone X, iPad mini und iPad Pro, ausgeführt werden.

Sprachunterstützung

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

Einstellung von Features und Plattformen

Die Ankündigung in diesem Artikel bietet Ihnen frühzeitige Informationen über Plattformen, Citrix Produkte und Features, die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element.

Veraltete Elemente werden nicht sofort entfernt. Citrix setzt den Support in diesem Release fort, aber die Elemente werden in einem zukünftigen Release entfernt.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung des DTLS 1.0-Protokolls	Citrix Workspace-App für iOS Version 24.5.0	-	DTLS 1.2-Protokoll
Unterstützung für die Protokolle TLS 1.0 und TLS 1.1	Citrix Workspace-App für iOS Version 24.4.0	-	Protokoll TLS 1.2 oder TLS 1.3
XenApp-Dienste (auch bekannt als PNAgent)	Citrix Workspace-App für iOS Version 23.7.5	-	Nutzen Sie in der Citrix Workspace-App die Store-URL und nicht die XenApp-Dienste-URL für Verbindungen zu Stores.
iOS-Version 14	Citrix Workspace-App für iOS Version 23.10.0	Ziel: Citrix Workspace-App für iOS 23.12.0	Upgrade auf die neueste verfügbare Version von iOS
iOS-Version 13.x	Citrix Workspace-App für iOS Version 22.9.5	Ziel: Dezember 2022 und Version 22.12.0	Upgrade auf die neueste verfügbare Version von iOS

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
iOS Version 11.x und 12.x	Citrix Workspace-App für iOS Version 21.12.0	Ziel: Aug 2022 und Version 22.8.0	Upgrade auf die neueste verfügbare Version von iOS
iOS-Version 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 kein Upgrade auf die neueste Version (aus dem App Store) der Citrix Workspace-App durchführen.
- Neue Benutzer der Citrix Workspace-App auf veralteten Plattformversionen können nur eine ältere kompatible Version aus dem App Store herunterladen.
- Benutzer mit veralteten Plattformversionen erhalten keine neuen Features oder Sicherheitspatches, die mit jeder neueren Version der Citrix Workspace-App geliefert werden.