



Citrix Workspace

Contents

Citrix Workspace — Überblick	3
Was ist neu	6
Was ist neu in der Workspace-Plattform	7
Neue Features in der Workspace-Benutzeroberfläche	15
Was ist neu beim Global App Configuration Service	33
Erste Schritte mit Citrix Workspace	39
Vorbereitung auf Citrix Workspace	43
Neue Workspace-Benutzeroberfläche	50
Aktivitätsmanager	61
Bereitstellen von DaaS und Virtual Apps and Desktops mit Citrix Workspace	66
Zugriff auf Workspaces konfigurieren	69
Benutzerdefinierte Domäne konfigurieren	79
Sichere Workspaces	100
Services in Workspaces integrieren	110
Citrix Workspace-App konfigurieren	112
Einstellungen für Cloudstores konfigurieren	120
Einstellungen für On-Premises-Stores konfigurieren	123
Kanalkonfiguration testen	127
Verwalten der Workspace-Benutzeroberfläche	131
Anpassen der Darstellung von Workspaces	136
Workspace-Interaktionen anpassen	143
Anpassen von Sicherheits- und Datenschutzrichtlinien	154
DaaS in Citrix Workspace optimieren	165

On-premises bereitgestellte virtuelle Apps und Desktops in Workspaces aggregieren	166
Optimieren der Konnektivität zu Workspaces mit einer direkten Workloadverbindung	178
Servicekontinuität	188
Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS)	216

Citrix Workspace —Überblick

November 27, 2023

Citrix Workspace ist eine digitale Workspace-Lösung, die überall und auf jedem Gerät einen sicheren und einheitlichen Zugriff auf Apps, Desktops und Inhalte (Ressourcen) ermöglicht. Ressourcen können Citrix DaaS, Inhalts-Apps, lokale und mobile Apps, SaaS- und Web-Apps sowie Browser-Apps sein.

Funktionsweise von Citrix Workspace

Durch Aggregation und Integration von [Citrix Cloud Services](#) ermöglicht Citrix Workspace einen einheitlichen Zugriff auf alle Ressourcen, die Endbenutzern (Abonnenten) an einem [Ressourcenstandort](#) zur Verfügung stehen. Endbenutzer von Citrix Workspace heißen Abonnenten, da Sie für diese Mitarbeiter Dienste “abonnieren”, die sie dann über ihren Workspace nutzen können.

Einen Überblick über die in Citrix Workspace verfügbaren Dienste finden Sie unter [Zugriff auf cloudgehostete Dienste über Citrix Workspace](#).

Abonnenten sehen in der Citrix Workspace-Benutzeroberfläche eine vollständige, einheitliche Ansicht jeder Ressource, die Sie ihnen über diese Dienste zur Verfügung stellen. Weitere Informationen zur Verwendung der Benutzeroberfläche von Citrix Workspace durch Abonnenten finden Sie unter [Verwalten der Workspace-Benutzeroberfläche](#).

Abonnenten greifen auf die Dienste, die Sie unter **Workspacekonfiguration** konfigurieren und aktivieren, entweder per Browser über die Workspace-URL zu oder in der [Citrix Workspace-App](#) (die Citrix Receiver ersetzt). Weitere Informationen zum Benutzerzugriff auf Workspace finden Sie unter [Zugriff auf Workspace](#).

Abonnenten authentifizieren sich bei ihrem Workspace über den primären Identitätsanbieter, den Sie unter **Identitäts- und Zugriffsverwaltung** konfigurieren und dann unter **Workspacekonfiguration** aktivieren. Der Abonnent ist danach automatisch für jeden in der Cloud gehosteten Dienst, der für Citrix Workspace erworben wurde, authentifiziert. Dies erhöht die Sicherheit und verbessert die Benutzerfreundlichkeit. Weitere Informationen zum Konfigurieren der Workspaceauthentifizierung finden Sie unter [Sichere Workspaces](#).

Erste Schritte

Das Einrichten von Citrix Workspace erfolgt über die **Citrix Cloud-Konsole**. Dort gibt es den Administratorbildschirm **Identitäts- und Zugriffsverwaltung** und die Citrix Workspace-Verwaltungsschnittstelle **Workspacekonfiguration**. Die ersten Schritte in Citrix Workspace umfassen die folgenden Aufgaben.

1. Stellen Sie sicher, dass Sie die Voraussetzungen zur Implementierung von Citrix Workspace in der **Citrix Cloud-Konsole** erfüllen, wo Sie:
 - das Onboarding bei Cloud-basierten Diensten durchführen.
 - Ihr Bereitstellungsteam zusammenstellen.
 - Ihre Infrastruktur und Ressourcen konfigurieren.
2. Definieren Sie Identitätsanbieter und Konten in der **Identitäts- und Zugriffsverwaltung** für:
 - Citrix Cloud-Administratoren.
 - Citrix Workspace-Abonnenten.
3. Konfigurieren Sie Ihre Workspaces in der **Workspacekonfiguration**. Dies umfasst auch Folgendes:
 - Externer und interner Zugriff.
 - Integration der in der Citrix Cloud-Konsole konfigurierten Dienste in Ihre Workspaces.
 - Anpassen der Workspace-Darstellung und der Benutzeroberfläche für Abonnenten, nachdem sie angemeldet sind.

Neben diesen Grundeinstellungen stehen Ihnen weitere Sicherheits-, Datenschutz- und Optimierungsoptionen zur Auswahl. Die gebräuchlichsten Optionen sind:

- Konfigurieren von Single Sign-On (SSO) für DaaS in Citrix Workspace mithilfe von [Citrix FAS \(Verbundauthentifizierungsdienst\)](#). FAS wird normalerweise verwendet, wenn Sie eine Verbundauthentifizierungsmethode wie Okta oder Azure Active Directory nutzen.

Eine Übersicht über die Aufgaben und die Informationen, die Sie während der Bereitstellung benötigen, finden Sie unter [Erste Schritte mit Citrix Workspace](#). Jeder Schritt führt Sie durch die Citrix Cloud-Konsole und erläutert Aufgaben wie das Konfigurieren des Identitätsanbieters und das Aktivieren von Diensten. Die Anleitung bietet außerdem schnellen Zugriff auf die technischen Informationen, die Sie benötigen, wenn Sie Ihr Bereitstellungsteam zusammenstellen und Ihre Infrastruktur und Ressourcen konfigurieren.

Zugriff auf cloudgehostete Dienste über Citrix Workspace

Abonnenten können mit Citrix Workspace auf die Ressourcen zugreifen, die von cloudgehostete Dienste bereitgestellt werden. Bestehende Citrix Cloud-Kunden können zum vollständigen digitalen Workspace wechseln, indem sie diese Dienste in die Citrix Workspace-Lösung überführen.

In diesem Abschnitt werden die wichtigsten in der cloudgehostete Dienste beschrieben, die (abhängig von Ihren Ansprüchen) für Citrix Workspace aktiviert werden können. Informationen zum Konfigurieren und Aktivieren des Zugriffs auf Ihre erworbenen Dienste finden Sie unter [Erste Schritte mit Citrix Workspace](#). Eine vollständige Beschreibung jeder einzelnen Citrix Workspace-Edition und der enthaltenen Features finden Sie in der [Citrix Workspace-Feature-Matrix](#).

Citrix DaaS

Citrix Workspace ist der cloudbasierte Mehrmandanten-Zugriffspunkt für Citrix DaaS. Befolgen Sie zum Einrichten von Citrix DaaS die unter [Citrix DaaS](#) beschriebenen Schritte.

Für Kunden mit on-premises bereitgestelltem Virtual Apps and Desktops gibt es mehrere Optionen für den Zugriff auf Ressourcen über Citrix Workspace. Welche Option Sie wählen, hängt davon ab, ob Sie eine vollständige Migration in die Cloud oder eine Hybridlösung wünschen und ob Sie einen externen Zugriff zulassen möchten. Weitere Informationen zu diesen Optionen finden Sie unter [Bereitstellen von DaaS mit Citrix Workspace](#).

Mehr Sicherheit für SaaS- und Web-Apps durch Citrix Secure Private Access

Der Dienst **Citrix Secure Private Access** (ehemals **Secure Workspace Access** und **Access Control Service**) bietet Single Sign-On (SSO) für Web- und SaaS-Apps, die in Workspace integriert sind. Sie können hiermit außerdem Zugriffsrechte verwalten und Richtlinien für Zugriffsebenen auf unternehmenseigene Web-Apps festlegen, die auf den Anmeldeinformationen von Abonnenten basieren.

Weitere Informationen zu den Vorteilen von **Citrix Secure Private Access** finden Sie unter [Tech Brief: Secure Private Access](#).

Citrix Gateway Service

Citrix Gateway Service (ehemals **NetScaler Gateway Service**) bildet zusammen mit **Citrix Secure Private Access** eine vollständig in der Cloud gehostete Umgebung, die von Citrix verwaltet wird.

Citrix Gateway liefert eine einheitliche Erfahrung für SaaS-Apps und Virtual Apps and Desktops. Der Dienst ermöglicht externe Verbindungen zu Workspaces, basierend auf einer detaillierten Richtlinieninfrastruktur.

Richten Sie [Citrix Gateway](#) ein, testen Sie die Workspace-URL und geben Sie sie für Ihre Abonnenten frei, um ihnen einen Remotezugriff zu ermöglichen. Weitere Informationen zum Konfigurieren von SaaS-Anwendungen im Citrix Gateway Service finden Sie unter [Support for Software as a Service Apps](#).

Citrix Remote Browser Isolation

Durch Integration von **Citrix Remote Browser Isolation** in Ihre Workspaces isolieren Sie das Web-browsing und schützen damit das Unternehmensnetzwerk vor browserbasierten Angriffen. Wenn Abonnenten zur Workspace-URL navigieren, werden ihre veröffentlichten Browser angezeigt, neben den übrigen Apps und Desktops, die in anderen Citrix Cloud-Diensten konfiguriert sind.

Um Abonnenten Zugriff auf einen isolierten Remotebrowser zu gewähren, richten Sie [Remote Browser Isolation](#) ein, testen die Workspace-URL und geben sie dann für Abonnenten frei.

Citrix Endpoint Management

Mit **Citrix Endpoint Management** können Sie Geräte- und App-Richtlinien mit hoher Sicherheit für Identität, Geräte, Apps, Daten und Netzwerke verwalten. Die Integration in Citrix Workspace unterscheidet sich für neue und bestehende Kunden. Weitere Informationen zur Integration von Endpoint Management in Citrix Workspace finden Sie unter [Integration in die Citrix Workspace-Benutzeroberfläche](#).

Citrix Analytics

Citrix Analytics sammelt Daten und liefert Analysen zu all Ihren Citrix Workspace-Abonnenten. Je nach den Ansprüchen, die Sie besitzen, stehen verschiedene Citrix Analytics-Funktionen zur Verfügung. Dies sind **Citrix Analytics für Sicherheit**, **Citrix Analytics für Leistung** und **Analytics für Nutzung**. Weitere Informationen zu diesen Diensten finden Sie unter [Citrix Analytics](#).

Was ist neu

November 27, 2023

Citrix möchte Citrix Workspace-Kunden neue Features und Updates unverzüglich zur Verfügung zu stellen. Erstreleases werden zunächst auf interne Sites von Citrix angewendet und danach schrittweise auf Kundenumgebungen.

Informationen zum Servicelevelziel im Hinblick auf Cloudskalierung und Serviceverfügbarkeit finden Sie unter [Servicelevelziele](#) für Citrix Cloud. Informationen zu Serviceunterbrechungen und geplanten Wartungsmaßnahmen finden Sie im [Dienstzustandsdashboard](#).

Was ist neu in Citrix Workspace

Bleiben Sie über die neuesten Verbesserungen und Updates in Citrix Workspace auf dem Laufenden, um das volle Potenzial unserer Technologie auszuschöpfen. Maximieren Sie die Produktivität Ihrer Benutzer und steigern Sie die Qualität ihrer Interaktionen, indem Sie zeitnahe Updates von Citrix Workspace integrieren.

- [Was ist neu in der Workspace-Plattform](#)
- [Was ist neu in der Workspace-Benutzeroberfläche](#)

- [Neue Features beim Global App Configuration Service](#)

Citrix Workspace-App auf verschiedenen Plattformen

Über die folgenden Links erfahren Sie mehr über neue Features und Verbesserungen in der **Citrix Workspace-App** für Ihre bevorzugten Plattformen.

- [Android](#)
- [ChromeOS](#)
- [HTML5](#)
- [iOS](#)
- [Linux](#)
- [Mac](#)
- [Microsoft Teams](#)
- [Windows](#)
- [Windows Store](#)

Informieren Sie sich auch über neue Features in [Citrix Enterprise Browser](#).

Was ist neu in der Workspace-Plattform

November 27, 2023

Citrix möchte Citrix Workspace-Kunden neue Features und Updates unverzüglich zur Verfügung zu stellen. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern.

Der Prozess ist für Sie transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Durch diese schrittweise Bereitstellung von Updates werden Produktqualität und Verfügbarkeit maximiert.

Informationen zum Servicelevelziel im Hinblick auf Cloudskalierung und Serviceverfügbarkeit finden Sie unter [Servicelevelziele](#) für Citrix Cloud. Informationen zu Serviceunterbrechungen und geplanten Wartungsmaßnahmen finden Sie im [Dienstzustandsdashboard](#).

November 2023

Benutzerdefinierte Domäne konfigurieren —Allgemeine Verfügbarkeit

Das Feature "Benutzerdefinierte Domäne" ist jetzt allgemein verfügbar. Sie können eine benutzerdefinierte Domäne für Ihren Workspace konfigurieren, um eine Domäne Ihrer Wahl für den

Zugriff auf Ihren Citrix Workspace-Store zu verwenden. Sie können dann diese Domäne anstelle der zugewiesenen cloud.com-Domäne für den Zugriff über einen Webbrowser oder über Citrix Workspace-Anwendungen verwenden. Weitere Informationen finden Sie unter [Benutzerdefinierte Domäne konfigurieren](#).

Aug 2023

Eigenes TLS-Zertifikat für eine benutzerdefinierte Domäne hinzufügen (Preview)

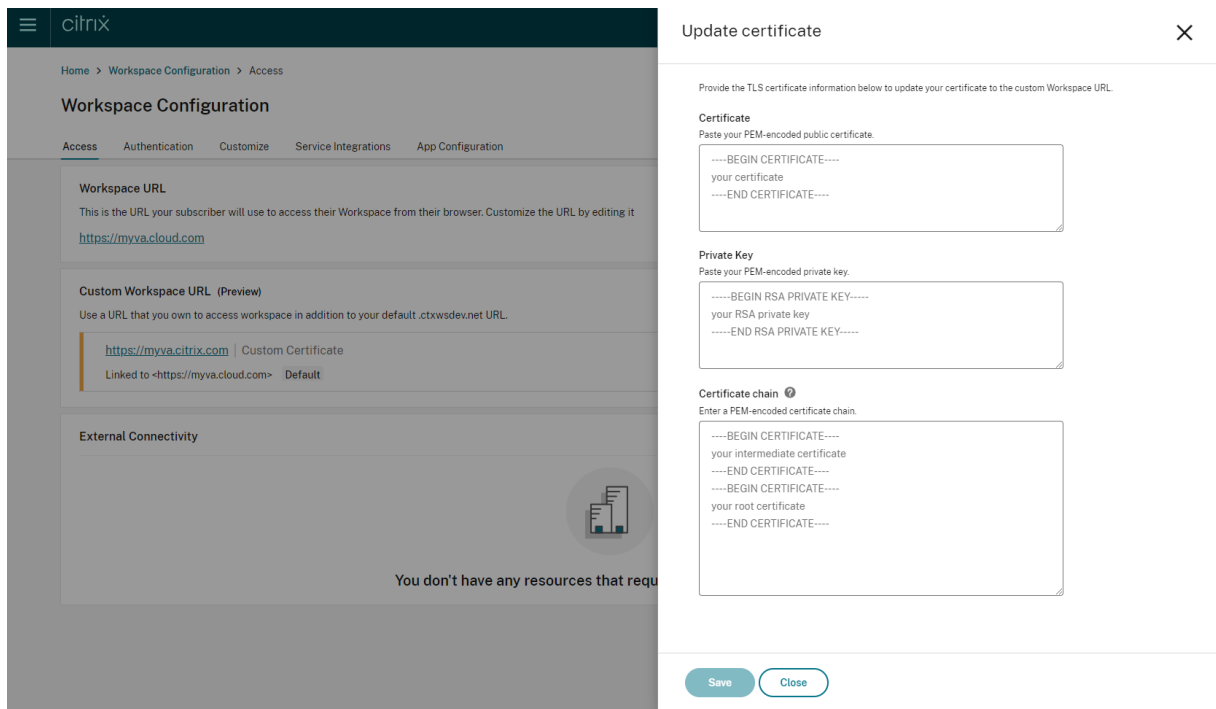
Sie können jetzt Ihr eigenes TLS-Zertifikat zur Authentifizierung hochladen, wenn Sie eine benutzerdefinierte Workspace-URL konfigurieren. Stellen Sie vor dem Hochladen eines Zertifikats sicher, dass das Zertifikat die folgenden Bedingungen erfüllt.

- Es muss PEM-codiert sein.
- Es muss mindestens für die nächsten 30 Tage gültig bleiben.
- Es darf ausschließlich für benutzerdefinierte Workspace-URLs verwendet werden. Platzhalterzertifikate sind nicht zulässig.
- Der allgemeine Name des Zertifikats muss mit der benutzerdefinierten Domäne übereinstimmen.
- SANs auf dem Zertifikat müssen für die benutzerdefinierte Domain sein. Zusätzliche SANs sind nicht zulässig.
- Die Gültigkeitsdauer des Zertifikats darf 10 Jahre nicht überschreiten.

Zum Hinzufügen Ihres Zertifikats gehen Sie zur Seite **URL angeben** und wählen Sie unter “Voreinstellung für die TLS-Zertifikatverwaltung auswählen” die Option **Eigenes Zertifikat hinzufügen**.

The screenshot shows the Citrix Workspace Configuration interface. On the left, the 'Workspace Configuration' sidebar is visible, with 'Access' selected. The main content area shows the 'Add your own domain' dialog box. The dialog has a progress bar with four steps: 1. Overview, 2. Provide a URL, 3. Configure your DNS, and 4. Provision your domain. The 'Provide a URL' step is active. It contains a text input field for the URL, a dropdown for the domain, and a text input for the TLD. Below this is a checkbox for 'Confirm that you or your company own the URL provided.' Underneath is a section for 'Select TLS certificate management preference' with two radio buttons: 'Citrix-managed' (selected) and 'Add your own certificate' (highlighted with a red box). A blue information box below the radio buttons states: 'Verify your custom domain URL and certificate management preferences are correct before proceeding. Changing this information requires deleting and starting over.' At the bottom of the dialog are 'Back', 'Next', and 'Close' buttons, along with a note: 'Domain starts provisioning when you click Next. This may take up to 24 hours.'

Anschließend können Sie Ihr Zertifikat auf der Seite **Eigenes Zertifikat hinzufügen** hinzufügen.



Weitere Informationen finden Sie unter [Benutzerdefinierte Domäne hinzufügen](#).

Hinweis: Sie können Feedback zu diesem Preview-Feature mit dem **Podio-Formular** geben.

Mai 2023

Benutzerdefinierte Domäne konfigurieren (Preview). Sie können eine benutzerdefinierte Domäne für Ihren Workspace konfigurieren, um eine Domäne Ihrer Wahl für den Zugriff auf Ihren Citrix Workspace-Store zu verwenden. Sie können dann diese Domäne anstelle der zugewiesenen cloud.com-Domäne für den Zugriff über einen Webbrowser oder über Citrix Workspace-Anwendungen verwenden. Weitere Informationen finden Sie unter [Benutzerdefinierte Domäne konfigurieren \(Preview\)](#).

März 2023

Zusätzliche Einstellungen für Timeout bei Inaktivität: Sie können jetzt zusätzliche Einstellungen für den Timeout bei Inaktivität für Desktop-Benutzer und mobile Benutzer der Workspace-App erstellen. Weitere Informationen finden Sie unter [Sicherheits- und Datenschutzrichtlinien anpassen](#).

Dezember 2022

Zusätzliche Konfigurationsoption beim Senden benutzerdefinierter Benachrichtigungen: Sie können jetzt beim **Senden benutzerdefinierter Benachrichtigungen** die Platzierung auf der Seite entweder auf oben oder unten einstellen. Weitere Informationen finden Sie unter [Sicherheits- und Datenschutzrichtlinien anpassen](#).

Unterstützung für traditionelles Chinesisch. Citrix Workspace ist jetzt in traditionellem Chinesisch verfügbar.

Oktober 2022

Unterstützung für Koreanisch: Citrix Workspace ist jetzt auf Koreanisch verfügbar.

Unterstützung der Anpassung von Citrix Workspace-App-Einstellungen. Administratoren können jetzt die Einstellungen der Citrix Workspace-App für iOS, Android, HTML5, Mac und Windows mit dem Global App Configuration Service konfigurieren.

August 2022

Verbesserungen beim Start von Workspace. Wenn Benutzer den Workspace über das Internet oder einen Browser starten, wird eine Benachrichtigung mit dem Startstatus ausgelöst. Benutzer, die versuchen den Browser zu schließen, während ein Start ausgeführt wird, werden zur Bestätigung aufgefordert und darüber informiert, dass ein Sitzungsstart ausgeführt wird. Weitere Informationen finden Sie unter [Erste Schritte mit Citrix Workspace](#).

Juni 2022

Unterstützung für Servicekontinuität mit Safari. Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen. Weitere Informationen finden Sie unter [Servicekontinuität im Browser](#).

May 2022

Neue Konfigurationsoption für Verbundidentitätsanbieter: Aktivieren oder deaktivieren Sie Ihren Verbundidentitätsanbieter, damit die Abonnenten bei der Anmeldung bei Workspace zur Authentifizierung aufgefordert werden. Weitere Informationen finden Sie unter [Anpassen von Workspace-Interaktionen](#).

Neuauthentifizierungszeitraum für die Workspace-App allgemein verfügbar: Bei Konfiguration eines Neuauthentifizierungszeitraums können Abonnenten bei Workspace angemeldet bleiben

und müssen sich nicht bei jedem Zugriff auf ihren Workspace anmelden. Bei der Anmeldung über die Workspace-App stimmen die Abonnenten zu, angemeldet zu bleiben. Die Abonnenten bleiben während der Neuauthentifizierung angemeldet, vorausgesetzt sie verwenden Apps und Desktops. Weitere Informationen zu diesem Feature finden Sie unter [Einrichten eines Neuauthentifizierungszeitraums für die Citrix Workspace-App](#).

Unterstützung für Servicekontinuität unter iOS: Servicekontinuität wird jetzt für die Citrix Workspace-App für iOS in allgemeiner Verfügbarkeit unterstützt. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Neue Fehlercodes für die Servicekontinuität: Neue Fehlercodes helfen jetzt bei der Behandlung fehlgeschlagener Servicekontinuitätsverbindungen. Weitere Informationen finden Sie unter [Servicekontinuität](#).

März 2022

Unterstützung für Servicekontinuität unter Android und iOS: Servicekontinuität wird jetzt für die Citrix Workspace-App für Android (allgemeine Verfügbarkeit) und die Citrix Workspace-App für iOS (Technical Preview) unterstützt. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Februar 2022

Unterstützung für Servicekontinuität mit der Citrix Workspace-App für Android (allgemeine Verfügbarkeit) und Citrix Workspace-App für iOS (Technical Preview): Servicekontinuität ermöglicht es Benutzern, sich auch bei Ausfällen mit virtuellen Apps und Desktops zu verbinden. Servicekontinuität wird jetzt für die Citrix Workspace-App für Android (allgemeine Verfügbarkeit) und die Citrix Workspace-App für iOS (Technical Preview) unterstützt. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Benutzerdefinierte Ankündigung senden und Benutzerdefinierte Anmeldeleiste: Zwei neue Features sind jetzt für alle Kunden verfügbar. Mit diesen Features können Workspace-Administratoren ihr eigenes permanentes Banner nach der Anmeldung und eine benutzerdefinierte Nachricht oder Lizenzvereinbarung vor der Anmeldung in der Citrix Workspace-App anzeigen. Weitere Informationen finden Sie unter [Anpassen von Sicherheits- und Datenschutzrichtlinien](#).

Dezember 2021

Entfernen des geteilten Standardanmeldebildschirms für Mitarbeiter und Kunden, die Citrix Content Collaboration verwenden: Mit Citrix Workspace können Sie jetzt einen einheitlichen Anmeldeworkflow für Kunden- und Mitarbeiterbenutzer aktivieren. Weitere Informationen finden Sie unter [Erstellen eines einheitlichen Workflows zur Benutzeranmeldung](#).

Unterstützung für Servicekontinuität im Browser (Citrix Workspace-App für Mac): Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen. Dieses Feature wird jetzt auf Geräten mit der Citrix Workspace-App für Mac unterstützt. Weitere Informationen finden Sie unter [Servicekontinuität](#).

November 2021

Richtliniengesteuerte Designs: Unter **Workspacekonfiguration** können Sie Workspace-Designs erstellen, priorisieren und verschiedenen Benutzergruppen zuteilen. Weitere Informationen finden Sie unter [Anpassen der Darstellung von Workspaces](#).

Oktober 2021

Sprachunterstützung für elektronische Signaturen: Das Feature für elektronische Signaturen unterstützt jetzt neben Deutsch, Französisch, Spanisch, Japanisch, Niederländisch und vereinfachtes Chinesisch auch Italienisch und Portugiesisch (Brasilien). Weitere Informationen finden Sie unter [Unterstützung mehrerer Sprachen für RightSignature](#).

FAS-Unterstützung für mehrere Ressourcenstandorte (allgemein verfügbar): Citrix Workspace unterstützt jetzt Single Sign-On für virtuelle Apps und Desktops über mehrere Ressourcenstandorte. Darüber hinaus können FAS-Server an einem Ressourcenstandort als primäre oder sekundäre Failoverserver für FAS-Server an anderen Ressourcenstandorten festgelegt werden. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

September 2021

Citrix Workspace-App für HTML5 in Citrix Workspace eingeführt: Die Citrix Workspace-App für HTML5 bietet Citrix Workspace in Browsern ohne Installation auf dem Gerät. Weitere Informationen zur Citrix Workspace-App für HTML5 einschließlich neuer Features finden Sie in der [zugehörigen Dokumentation](#).

Unterstützung für Servicekontinuität im Browser (allgemein verfügbar): Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen. Dieses Feature steht für Google Chrome und Microsoft Edge auf Windows-Geräten zur Verfügung. Weitere Informationen finden Sie unter [Servicekontinuität im Browser](#).

Juli 2021

Richtlinie für benutzerdefinierte Abonnentenlizenzvereinbarungen: Sie können eine benutzerdefinierte Nutzungsvereinbarungsrichtlinie anzeigen, die Abonnenten vor der Anmeldung beim Workspace lesen und akzeptieren müssen. Weitere Informationen zu diesem Feature finden Sie unter [Konfigurieren einer Anmelderichtlinie](#).

Neuauthentifizierungszeitraum für die Workspace-App (Preview): Bei Konfiguration eines Neuauthentifizierungszeitraums können Abonnenten bei Workspace angemeldet bleiben und müssen sich nicht bei jedem Zugriff auf ihren Workspace anmelden. Bei der Anmeldung über die Workspace-App stimmen die Abonnenten zu, angemeldet zu bleiben. Die Abonnenten bleiben während der Neuauthentifizierung angemeldet, vorausgesetzt sie verwenden Apps und Desktops. Weitere Informationen zu diesem Previewfeature finden Sie unter [Einrichten eines Neuauthentifizierungszeitraums für die Citrix Workspace-App](#).

Konfiguration eines Netzwerkspeicherorts über Citrix Cloud: Sie können Netzwerkspeicherorte jetzt nicht nur mit dem PowerShell-Skript von Citrix, sondern auch über die Citrix Cloud-Verwaltungskonsole konfigurieren. Weitere Informationen zu diesem Feature finden Sie unter [Optimieren der Konnektivität zu Workspaces mit einer direkten Workloadverbindung](#).

Juni 2021

FAS-Unterstützung für mehrere Ressourcenstandorte (Preview): Citrix Workspace unterstützt jetzt Single Sign-On für virtuelle Apps und Desktops über mehrere Ressourcenstandorte. FAS-Server an einem Ressourcenstandort können als primäre oder sekundäre Failoverserver für FAS-Server an anderen Ressourcenstandorten festgelegt werden. Weitere Informationen zu diesem Previewfeature finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Unterstützung für Servicekontinuität im Browser (Technical Preview): Citrix Workspace Web-Erweiterungen bieten Servicekontinuität für Benutzer, die über einen Browser auf ihre Apps und Desktops zugreifen. Dieser Technical Preview steht für Google Chrome und Microsoft Edge auf Windows-Geräten zur Verfügung. Weitere Informationen finden Sie unter [Servicekontinuität im Browser](#).

Servicekontinuität (allgemeine Verfügbarkeit): Servicekontinuität ermöglicht es Benutzern, sich auch bei Ausfällen in Citrix Cloud-Komponenten oder öffentlichen und privaten Clouds mit virtuellen Apps und Desktops zu verbinden. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Citrix RightSignature-App verfügbar: Nutzen Sie die Citrix App, eine Lösung für elektronische Signaturen, die mit Workspace Premium und Premium Plus angeboten wird, um über Citrix Workspace E-Signaturen für Dokumente auf einem beliebigen Gerät anzufordern. Weitere Informationen finden Sie unter [Konfigurieren der Citrix RightSignature-App](#).

Mai 2021

Benutzerdefinierte Designs (Technical Preview): Das Anpassen der Workspace-Darstellung für Abonnenten umfasst jetzt die Einrichtung benutzerdefinierter Designs und deren Zuweisung zu verschiedenen Benutzergruppen. Sie können Designs erstellen, anpassen und priorisieren, damit Abonnenten in den Benutzergruppen bei der Anmeldung das korrekte Workspace-Design angezeigt wird. Weitere Informationen finden Sie unter [Anpassen der Darstellung von Workspaces](#).

Sprachunterstützung für elektronische Signaturen: Das Feature für elektronische Signaturen bietet jetzt Unterstützung für Deutsch, Französisch, Spanisch, Japanisch, Niederländisch und vereinfachtes Chinesisch. Weitere Informationen finden Sie unter [Unterstützung mehrerer Sprachen für RightSignature](#).

Februar 2021

Änderungen von Kontokennwörtern: Abonnenten können ihr Domänenkennwort in Citrix Workspace ändern. Administratoren können Abonnenten auch Anleitungen geben, mit deren Hilfe sie gültige komplexe Kennwörter gemäß der Kennwortrichtlinie ihres Unternehmens erstellen können. Weitere Informationen finden Sie unter [Änderung des Kontokennworts durch Abonnenten](#).

Dezember 2020

Servicekontinuität als Technical Preview: Servicekontinuität ermöglicht es Benutzern, sich auch bei Ausfällen in Citrix Cloud-Komponenten oder öffentlichen und privaten Clouds mit Citrix DaaS zu verbinden. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Oktober 2020

FedRAMP Ready: Bei Bereitstellung in Citrix Cloud Government ist Citrix Workspace ist FedRAMP Ready FedRAMP ist ein Programm zur Förderung von Sicherheitsstandards für Cloudservices, die von US-Behörden genutzt werden. US-Behörden, die bei Clouddiensten FedRAMP Ready vorschreiben, können jetzt DaaS mit Citrix Workspace und Citrix DaaS Services bereitstellen. Weitere Informationen finden Sie unter [Citrix Cloud Government](#).

Mai 2020

Anleitung zum Einstieg in Citrix Workspace: Citrix Workspace bietet jetzt eine schrittweise Anleitung, mit der Sie Workspaces schnell für Ihre Endbenutzer bereitstellen können. Die Anleitung

führt Sie durch die Citrix Cloud-Konsole, wo Sie einen Identitätsanbieter konfigurieren, Administratoren hinzufügen und Workspace-Authentifizierung und Dienste aktivieren können. Eine Übersicht über alle Aufgaben und Schnellzugriff auf benötigte Anweisungen finden Sie unter [Erste Schritte mit Citrix Workspace](#).

Dezember 2019

Netzwerkpositionsdienst: Sie können jetzt sicherstellen, dass Benutzer, die Apps und Desktops in Workspace im Unternehmensnetzwerk starten, direkt an ihre VDAs weitergeleitet werden. Durch das Umgehen des Gateways werden DaaS-Sitzungen beschleunigt. Informationen und Installationshinweise zu diesem Dienst finden Sie unter [Optimieren der Konnektivität zu Workspaces mit dem Netzwerkpositionsdienst](#).

Verbesserungen für Zuletzt verwendete Apps und Favoriten-Apps: Zuletzt verwendete Apps und Favoriten-Apps werden zuerst in Workspace geladen, sodass Benutzer häufig verwendete Apps und Desktops sofort starten können.

Neue Features in der Workspace-Benutzeroberfläche

November 27, 2023

In den folgenden Abschnitten werden die neuen Features der Workspace-Benutzeroberfläche in aktuellen und früheren Releases aufgeführt.

Hinweis:

- Weitere Informationen finden Sie unter [Neue Workspace-Benutzeroberfläche](#).
- Weitere Informationen zum Aktivitätsmanager finden Sie unter [Aktivitätsmanager](#).

Was ist neu in 23.46

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Bekannte Probleme

Es gibt keine neuen bekannten Probleme.

Frühere Releases

Dieser Abschnitt enthält Informationen zu neuen Features und behobenen Problemen in den früheren Versionen, die wir unterstützen.

23.45

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Behobene Probleme

- Die Google-Suchindexierung wurde aus Citrix Web entfernt, um zu verhindern, dass interne URLs in den Suchergebnissen von Google erscheinen. Wenn Ihre URLs jedoch bereits von Google indexiert wurden, müssen Sie Maßnahmen ergreifen, um sie zu entfernen. Weitere Informationen finden Sie unter [Remove a page hosted on your site from Google](#).

23.44

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.

23.43

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.

23.42

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.

23.41

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

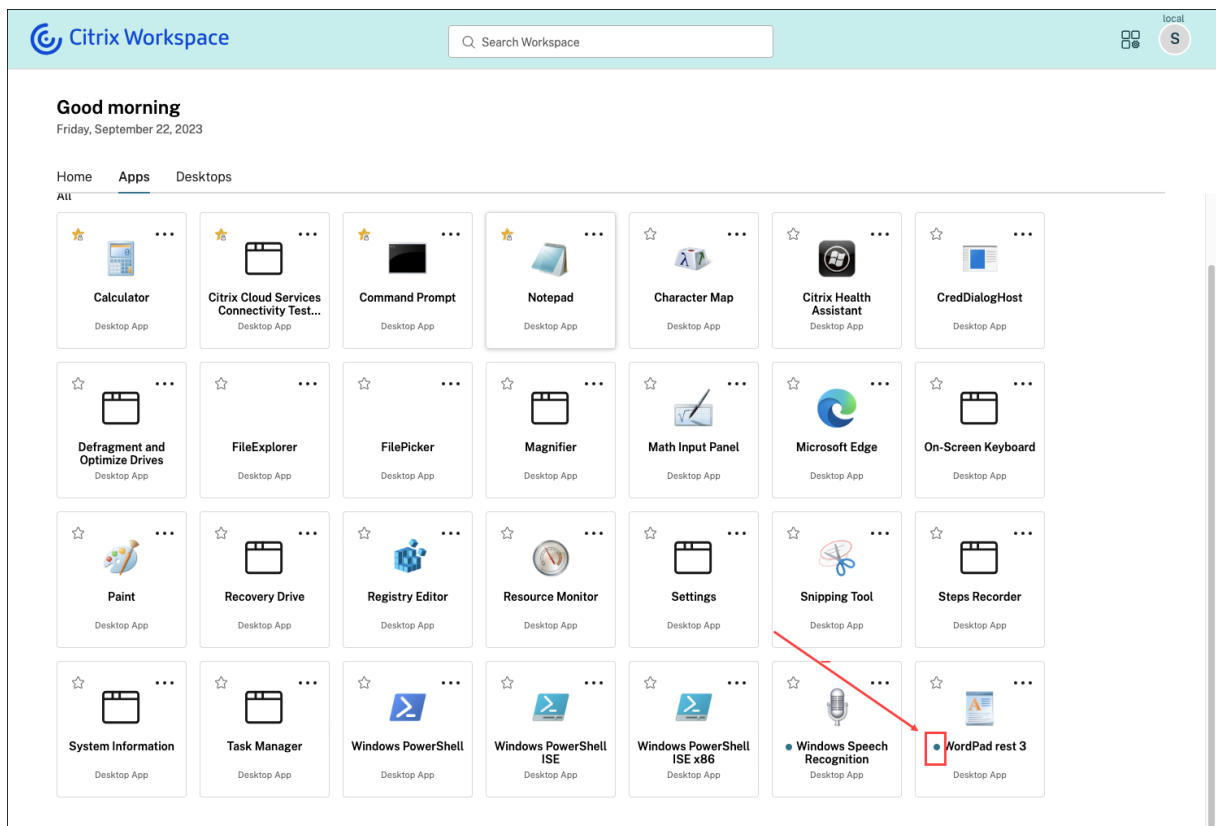
Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.40

Was ist neu

Optimiertes Erkennen neuer Apps Endbenutzer können neu hinzugefügte Apps jetzt leichter erkennen und verwenden. Wenn ein Administrator einem Endbenutzer eine neue App bereitstellt, wird die App im Workspace des Endbenutzers hervorgehoben und erstmalig mit grünem Punkt auf der App-Kachel angezeigt.



Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.39

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.

23.38

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.

23.37

Was ist neu

Neue Workspace-Benutzeroberfläche —allgemeine Verfügbarkeit Die neue Workspace-Benutzeroberfläche ist jetzt allgemein verfügbar. Sie bietet eine neue und übersichtlichere Benutzeroberfläche mit neuen Funktionen und modernem Design. Die Verbesserungen der Benutzeroberfläche gelten für Web, Desktops und Mobilgeräte. Administratoren können es für die Endbenutzer über **Workspace-Konfiguration > Anpassen > Features** aktivieren. Weitere Informationen finden Sie unter [Neue Workspace-Benutzeroberfläche](#).

Hinweis:

Standardmäßig ist der neue UI-Schalter für die nächsten sechs Monate deaktiviert, sofern er nicht von einem Administrator aktiviert wird. Nach sechs Monaten wird die neue Benutzeroberfläche standardmäßig für alle Benutzer aktiviert und die derzeitige Benutzeroberfläche läuft aus. Administratoren müssen innerhalb der nächsten sechs Monate auf die neue Benutzeroberfläche umstellen.

Aktivitätsmanager —allgemeine Verfügbarkeit Der Aktivitätsmanager ist jetzt in der neuen Benutzeroberfläche für Cloud allgemein verfügbar. Der Aktivitätsmanager ist ein einfaches und leistungsstarkes Feature, mit dem die Benutzer ihre Ressourcen effektiv verwalten können. Er steigert die Produktivität, indem er schnelle Aktionen an aktiven und nicht verbundenen Apps und Desktops von jedem Gerät aus ermöglicht. Administratoren können das Feature für die Endbenutzer über **Workspace-Konfiguration > Anpassen > Features > Aktivitätsmanager** aktivieren. Weitere Informationen finden Sie unter [Aktivitätsmanager aktivieren](#).

Nach der Aktivierung werden aktive und getrennte Apps und Desktops im Aktivitätsmanager-Bereich angezeigt. Die Endbenutzer können auf das Menü (...) klicken, um schnelle Aktionen auszuführen.

Die folgenden Aktionen können an aktiven Apps und Desktops ausgeführt werden.

- **Verbindung trennen:** Die Remotesitzung wird getrennt, die Apps und Desktops sind jedoch weiter im Hintergrund aktiv.
- **Abmelden:** Zur Abmeldung von der aktuellen Sitzung. Alle Apps in den Sitzungen werden geschlossen, und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren:** Schließt die getrennten Desktops.
- **Beenden erzwingen:** Schaltet den Desktop bei einem technischen Problem aus.

- **Neu starten:** Führt den Desktop herunter und startet ihn neu.

Der Aktivitätsmanager ermöglicht auch die Interaktion mit nicht verbundenen Apps und Desktops. Stellen Sie sicher, dass Sie ein Upgrade auf die neueste DDC-Version (115) durchgeführt haben. Weitere Informationen finden Sie unter [Getrennte Apps und Desktops](#).

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

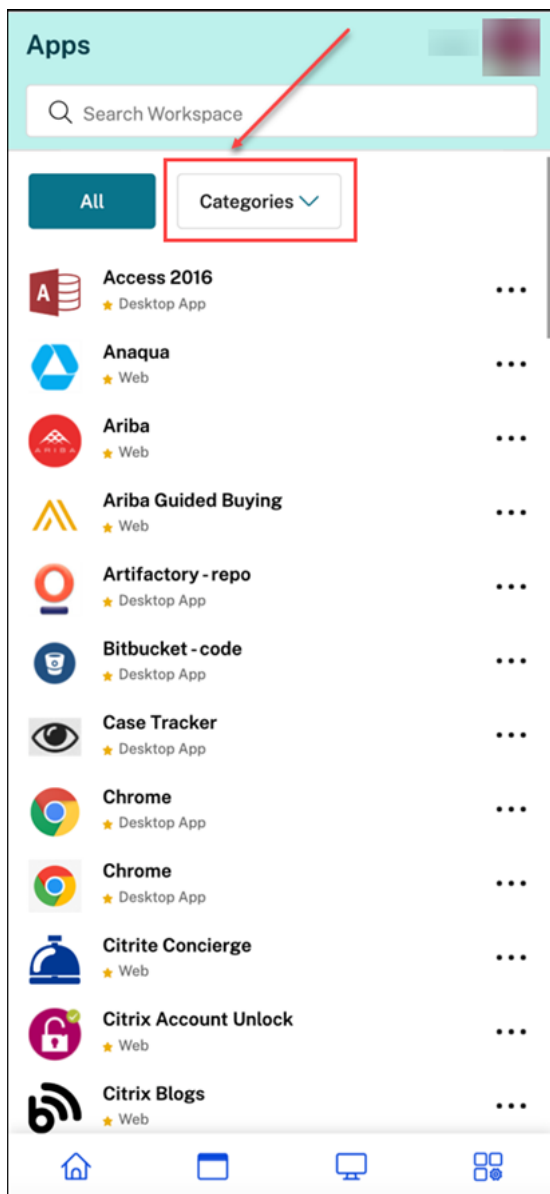
Bekannte Probleme

- Im Aktivitätsmanager werden aktive Sitzungen in allen Stores angezeigt, in denen der Benutzer angemeldet ist.
- Operationen wie Abmelden, Trennen usw. werden für Anwendungen, für die App Protection-Richtlinien aktiviert sind, nicht unterstützt.

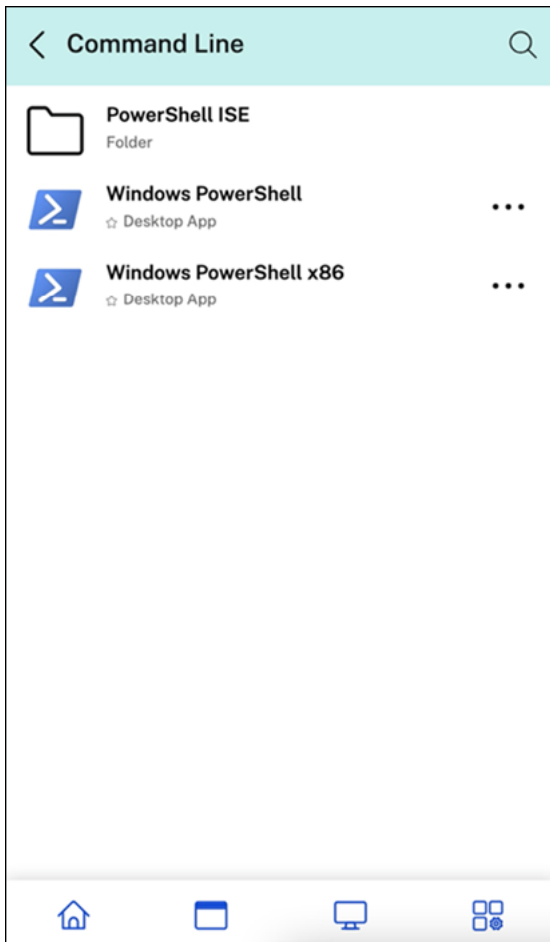
23.36

Was ist neu

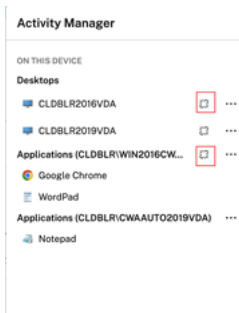
Unterkategorien für Anwendungen auf mobilen Plattformen anzeigen Die Endbenutzer können Apps jetzt auf Android- und iOS-Geräten für den einfachen Zugriff und ein angenehmes App-Browsing in Kategorien und Unterkategorien unterteilt anzeigen. Um Kategorien anzuzeigen, gehen Sie zur Apps-Registerkarte und klicken Sie auf das Dropdownmenü "Kategorien".



Wählen Sie die Kategorie aus. Eine Liste der verfügbaren Unterkategorien und Anwendungen wird gemäß der vom Administrator vorgenommenen Konfiguration angezeigt. Unterkategorien werden als Ordner angezeigt, die je nach Konfiguration durch den Administrator weitere Unterordner oder Anwendungen enthalten können. Weitere Informationen finden Sie unter [Ordnerpfad hinzufügen](#).

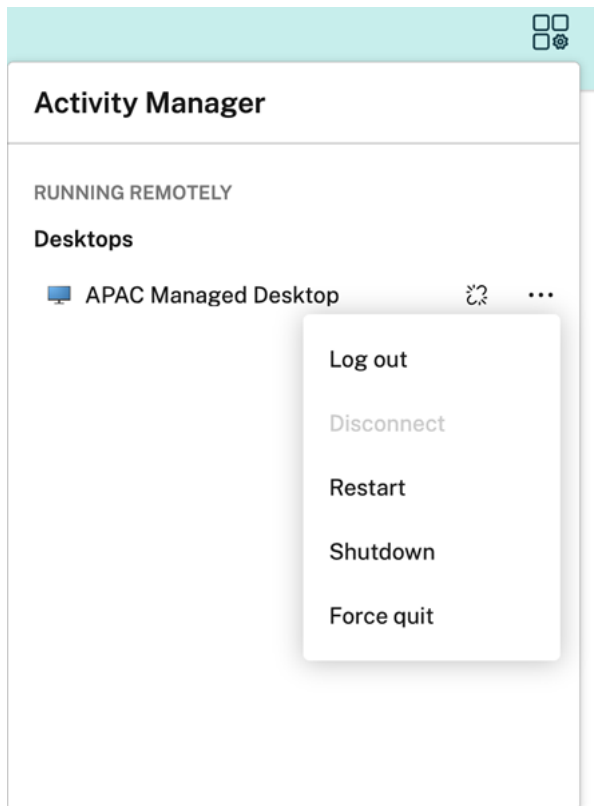


Getrennte Sitzungen im Aktivitätsmanager von jedem Gerät aus verwalten Mit dem Aktivitätsmanager können Endbenutzer jetzt Apps und Desktops, die im getrennten Modus ausgeführt werden, lokal oder remote anzeigen und Aktionen darauf ausführen. Sitzungen können von Mobil- oder Desktop-Geräten aus verwaltet werden, sodass Endbenutzer auch unterwegs Aktionen ausführen können. Das Ausführen von Aktionen an getrennten Sitzungen (z. B. Abmelden oder Herunterfahren) verbessert die Ressourcennutzung und reduziert den Energieverbrauch.



- Getrennte Apps und Desktops werden im Aktivitätsmanagerbereich angezeigt und sind mit einem Symbol einer getrennten Verbindung gekennzeichnet.

- Getrennte Apps sind nach zugehöriger Sitzung gruppiert, die Sitzungen sind mit einem Symbol einer getrennten Verbindung gekennzeichnet



Die Endbenutzer können an ihren getrennten Desktops die folgenden Aktionen über das Menü ausführen:

- **Abmelden:** zum Abmelden von dem getrennten Desktop. Alle Apps in der Sitzung werden geschlossen und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren:** zum Schließen der getrennten Desktops.
- **Ausschalten:** zum Ausschalten der getrennten Desktops im Falle eines technischen Problems.
- **Neu starten:** zum Herunterfahren und erneuten Starten des getrennten Desktops.

Weitere Informationen finden Sie unter [Getrennte Apps und Desktops im Aktivitätsmanager](#).

Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.35

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.

23.34

Was ist neu

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Behobene Probleme

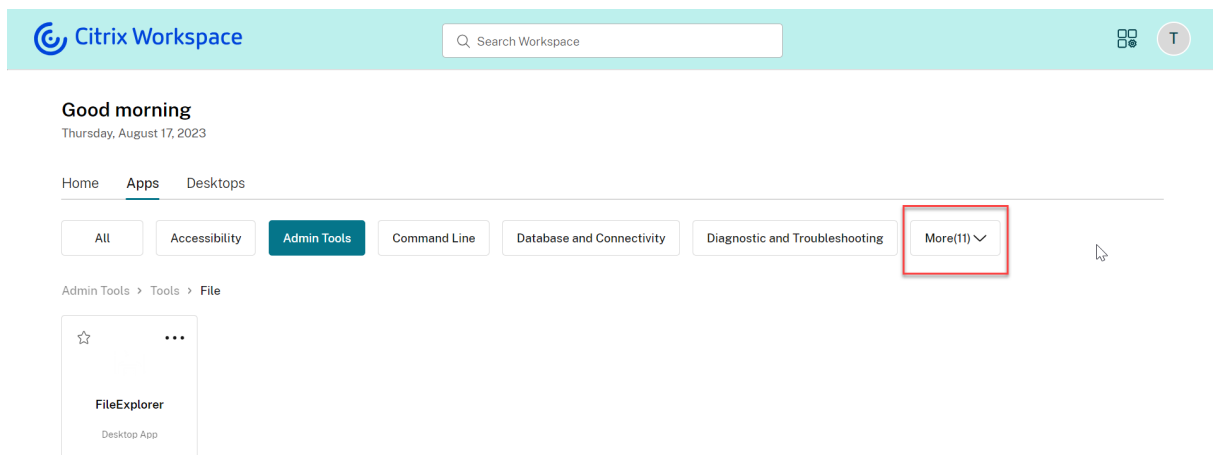
In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.33

Was ist neu

Verbesserte Benutzererfahrung mit App-Kategorisierung Endbenutzer können ihre Anwendungen im Workspace in Kategorien und Unterkategorien unterteilt anzeigen. Wenn die Kategorisierung mehr als zwei Ebenen umfasst, werden die Anwendungen in einer Ordnerstruktur angeordnet. Die Breadcrumbspur ist für die Benutzer sichtbar.

Wenn die Anzahl der von den Administratoren erstellten Hauptkategorien den Platz auf dem Bildschirm eines Benutzers überschreitet, werden die Kategorien anhand der Bildschirmgröße dynamisch in die Dropdownliste **Mehr** verschoben.



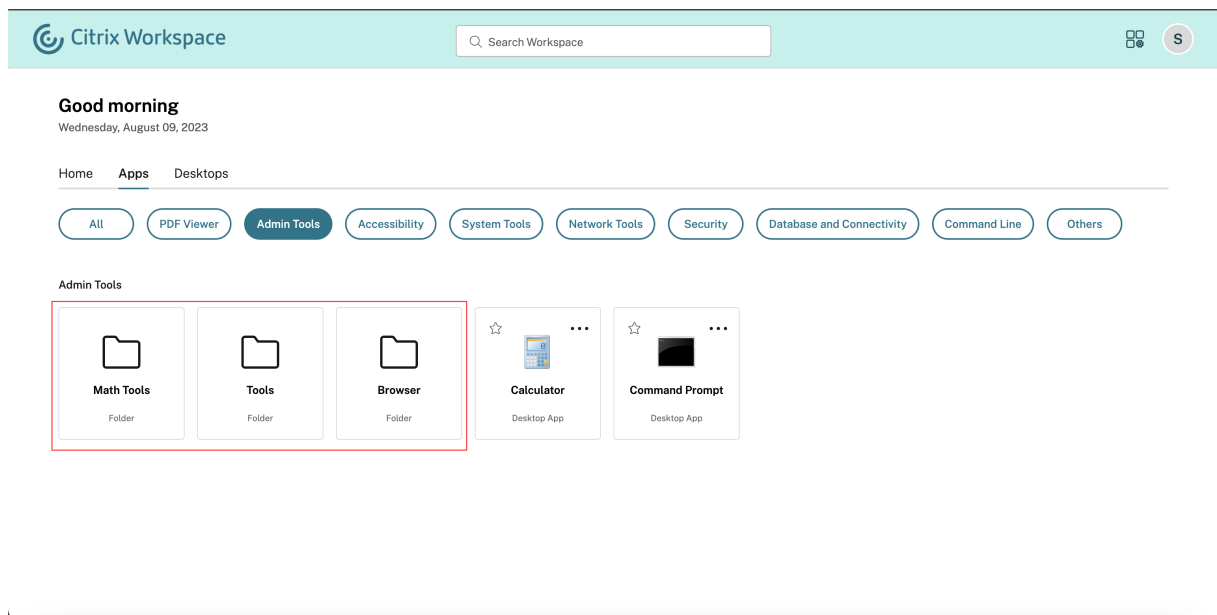
Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.32

Was ist neu

App-Kategorisierung für einfachen Zugriff Administratoren können Apps in Kategorien und Unterkategorien bereitstellen, um den Endbenutzern ein angenehmes App-Browsing zu gestatten. Ab der zweiten Kategorisierungsebene wird eine Ordnerstruktur angezeigt. Die Strukturierung auf mehreren Ebenen sorgt für eine übersichtliche Anzeige und trägt zur Steigerung der allgemeinen Benutzerzufriedenheit bei. Weitere Informationen zum Erstellen von Ordnern und Unterordnern finden Sie unter [Bereitstellungsgruppen erstellen](#).



Behobene Probleme

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

23.31

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.

23.30

Was ist neu

Aktivitätsmanager verwalten Als Administrator können Sie jetzt den Aktivitätsmanager für die Endbenutzer aktivieren oder deaktivieren. Je nach Ihren Unternehmensrichtlinien können Sie das

Feature für alle oder für ausgewählte Benutzer und Benutzergruppen aktivieren. Wenn der Aktivitätsmanager aktiviert ist, können die Endbenutzer damit ihre aktiven Apps und Desktops anzeigen und mit ihnen interagieren. Weitere Informationen finden Sie unter [Aktivitätsmanager](#).

Hinweis:

Dieses Feature wird nur für virtuelle Apps und Desktops unterstützt. Es gilt nicht für Web- und SaaS-Anwendungen.

Aktivitätsmanager aktivieren:

1. Gehen Sie in der Administratorkonsole zu **Workspacekonfiguration > Anpassen > Funktionen**.
2. Aktivieren Sie im Bereich “Aktivitätsmanager” den Ein-/Ausschalter, um den Aktivitätsmanager zu aktivieren.
3. Anschließend können Sie die Zugriffsberechtigungen wie folgt anpassen.
 - Um den Aktivitätsmanager für alle Endbenutzer zu aktivieren, wählen Sie **Für alle aktivieren**.

New Activity Manager

Enabled

Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone

Enable for selected users and user groups

Save **Preview**

- Um den Aktivitätsmanager für ausgewählte Benutzer und Benutzergruppen zu aktivieren, wählen Sie **Für ausgewählte Benutzer und Benutzergruppen aktivieren**. Sie können dann das Verzeichnis auswählen, zu dem die Benutzer oder Benutzergruppen gehören. Anschließend können Sie die relevanten Benutzer und Benutzergruppen anzeigen.

New Activity Manager

Enabled

Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone

Enable for selected users and user groups

Assign Users and Groups

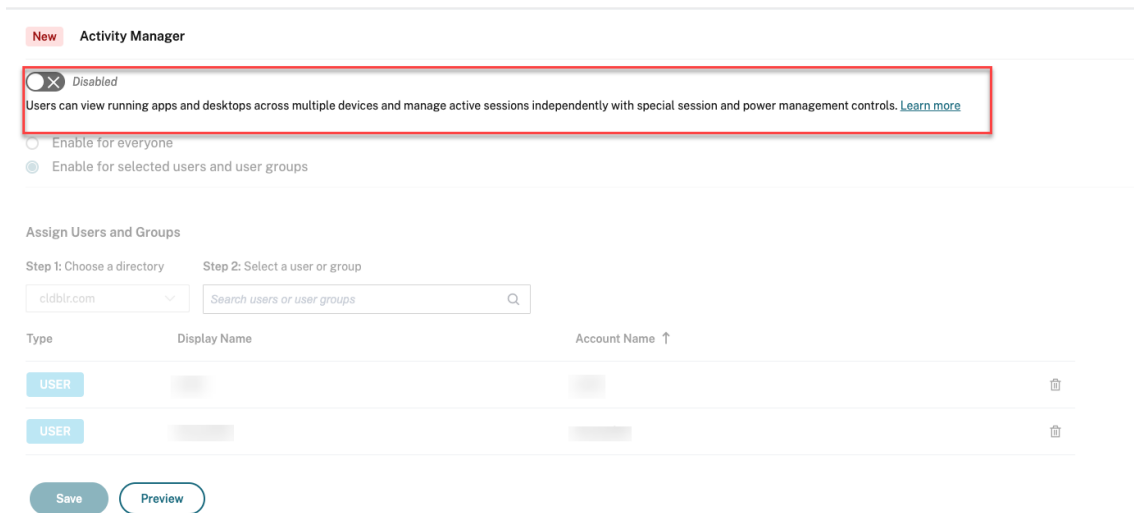
Step 1: Choose a directory Step 2: Select a user or group

cldblr.com Search users or user groups

Type	Display Name	Account Name ↑
USER		
USER		

Save **Preview**

- Um den Aktivitätsmanager für alle Benutzer zu deaktivieren, deaktivieren Sie den Ein-/Ausschalter.



4. Klicken Sie auf **Speichern**.

Behobene Probleme

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

23.29

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.

23.28

Was ist neu

Ankündigung der Einstellung von Internet Explorer Version 23.26 der Citrix Workspace-Benutzeroberfläche ist bis zur letzten Woche des Jahres 2023 im Internet Explorer verfügbar. Citrix unterstützt nach Version 23.26 keine neuen Features, Bugfixes oder Sicherheitspatches. Darüber hinaus erhalten Administratoren eine Benachrichtigung zum Upgrade auf die unterstützten Browser und das unterstützte LTSR (LTSR 2203 oder höher).

Behobene Probleme

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

23.27

Was ist neu

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

Behobene Probleme

- Mit diesem Fix wurden die Fehlergrenzen und die Fehlerbehandlung auf Komponentenebene implementiert. [WSUI-7423]
- Das Offlinebanner wird minimiert, wenn Sie auf das Ellipsensymbol klicken. [WSUI-7797]

23.26

Was ist neu

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

Behobene Probleme

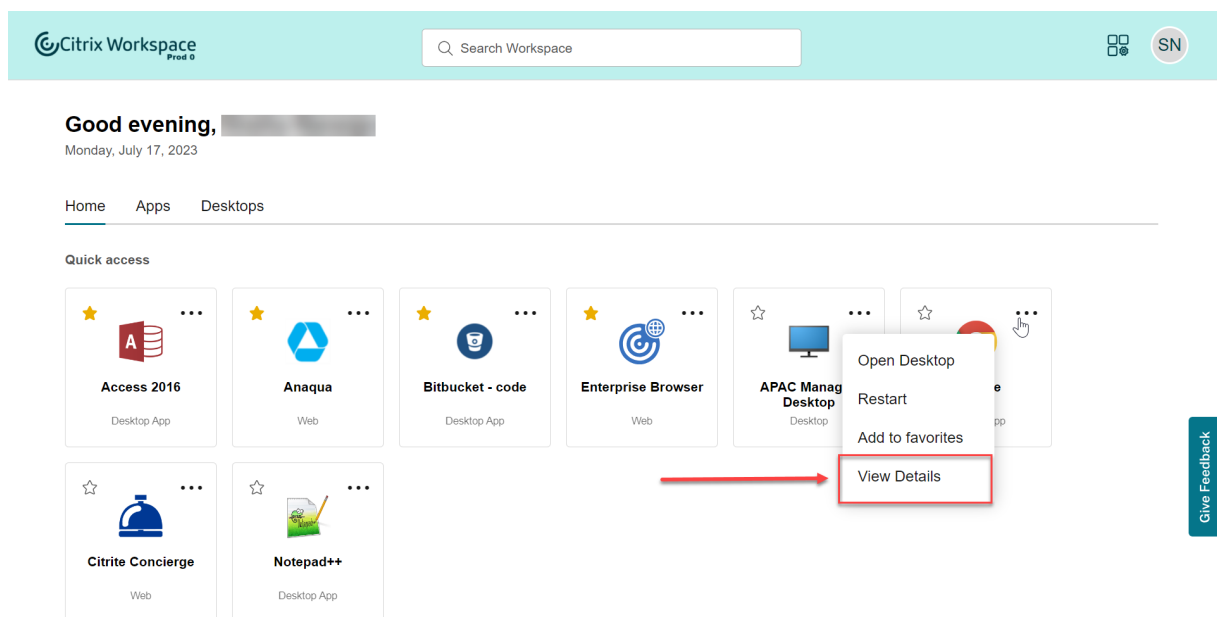
In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

23.25

Was ist neu

Anzeige der Beschreibung der Apps und Desktops Die Endbenutzer können jetzt von Administratoren bereitgestellte Beschreibungen für Apps und Desktops anzeigen. Die Beschreibungen informieren über den Zweck von Apps oder Desktops. Sie sind besonders nützlich, wenn es mehrere Apps mit demselben Namen gibt, die sich aber in der Konfiguration, dem Ort, der Umgebung usw. unterscheiden.

Um die Beschreibung einer App oder eines Desktops anzuzeigen, klicken Sie auf der entsprechenden Kachel auf die Auslassungspunkte und dann auf **Details anzeigen**.



Behobene Probleme

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

23.24

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.

23.23

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.

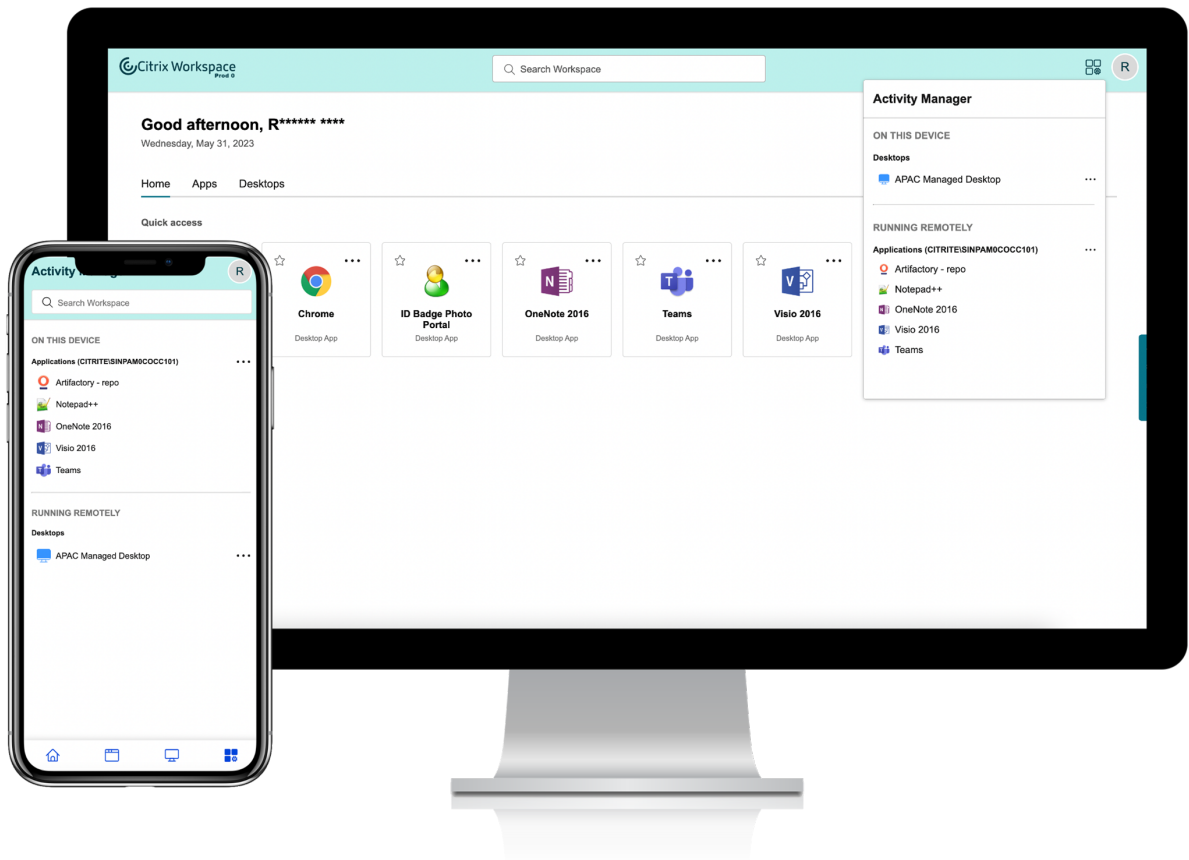
23.22

Was ist neu

Jetzt neu: Aktivitätsmanager Sie können jetzt aktive Apps und Desktops geräteübergreifend über ein einziges Fenster in der Workspace-Benutzeroberfläche verwalten und schnelle Aktionen dafür ausführen. Alle aktiven Apps und Desktops sind in der Sitzung gruppiert, die Sie gerade verwenden.

Das Aktivitätsmanagersymbol wird in der Workspace-Benutzeroberfläche links neben dem Profilsymbol angezeigt. Wenn Sie auf das Symbol klicken, wird Folgendes angezeigt:

- Unter **Auf diesem Gerät** eine Liste der Apps und Desktops, die auf dem aktuell genutzten Gerät gestartet wurden.
- Unter **Remote ausgeführt** eine Liste der Apps und Desktops, die auf anderen Geräten aktiv sind.



Weitere Informationen finden Sie unter [Aktivitätsmanager](#).

Hinweis:

Wenn das Aktivitätsmanager-Symbol nicht deutlich angezeigt wird, können Sie evtl. die Einstellungen unter **Bannertext und Symbolfarbe** ändern. Das Symbol ist möglicherweise nicht aufgrund eines geringen Kontrasts zwischen dem Banner und dem Symbol undeutlich. Weitere Informationen finden Sie unter [Benutzerdefinierte Designs konfigurieren](#).

Bekannte Probleme

- Wenn eine Sitzung unterbrochen wird, können Benutzer sich nicht von ihr abmelden. Getrennte Sitzungen werden im Aktivitätsmanager-Bereich nicht angezeigt.
- In der Citrix Workspace-App für Mac werden in der Liste der aktiven Apps und Desktops, im Aktivitätsmanager aktive Sitzungen aus allen Stores angezeigt.

23.15

Was ist neu

Neue Workspace-Benutzeroberfläche Die Citrix Workspace-App bietet eine neue und übersichtlichere Benutzeroberfläche mit neuen Funktionen und modernem Design. Die Verbesserungen der Benutzeroberfläche gelten für Web, Desktops und Mobilgeräte.

Verbesserte Benutzererfahrung für Erstbenutzer Wenn Sie die heruntergeladene Citrix Workspace-App oder Citrix zum ersten Mal über einen Browser starten, wird ein Bildschirm mit einer Liste relevanter Apps angezeigt. Diese Apps werden vom Administrator festgelegt und können von Ihnen mit einem einzigen Klick als Favoriten hinzugefügt werden.

Verbessertes Sucherlebnis Mit der verbesserten **Suchfunktion** erhalten Sie schnellere Ergebnisse in den Suchmaschinen. Die **Suchoption** ermöglicht eine schnelle und intuitive Suche direkt in der Workspace-App.

Administratorbezogene Aufgaben

Als Administrator können Sie die Benutzererfahrung der Workspace-App für Ihre Abonnenten anpassen. Weitere Informationen finden Sie in den folgenden Abschnitten.

- [Neue Workspace-Benutzererfahrung aktivieren](#)
- [Homebildschirm für Benutzer aktivieren oder deaktivieren](#)

Was ist neu beim Global App Configuration Service

November 27, 2023

In den folgenden Abschnitten werden die neuen Features in aktuellen und früheren Versionen des Global App Configuration Service aufgeführt.

30 Oct 2023

Einstellungen für On-Premises-Stores konfigurieren

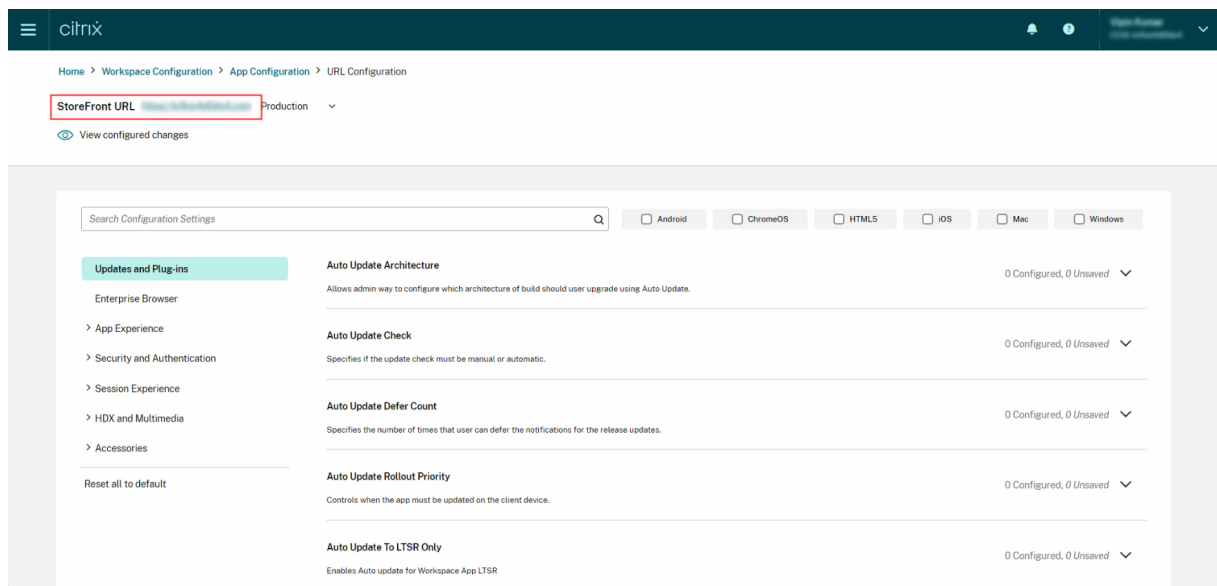
Sie können jetzt die Benutzeroberfläche des Global App Configuration Service verwenden, um Einstellungen für On-Premises-Stores zu konfigurieren. Melden Sie sich dafür bei Ihrem Citrix Cloud-Konto

an und navigieren Sie zu **Workspacekonfiguration > App-Konfiguration**.

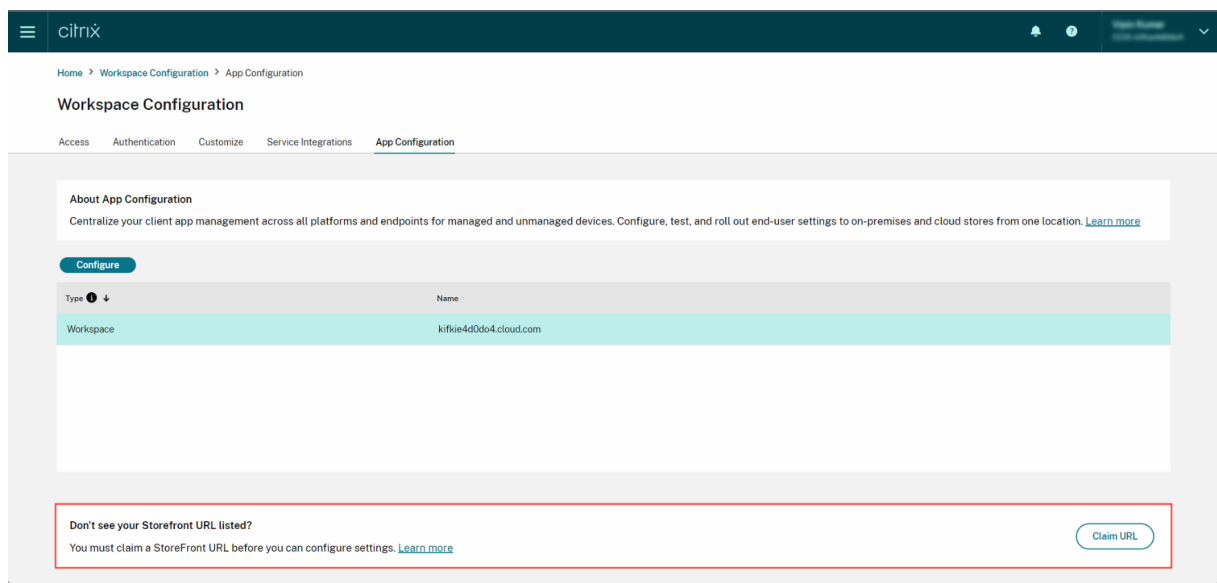
Hinweis:

Wenn Sie noch kein Citrix Cloud-Konto haben, wählen Sie zunächst die Seite zum [Citrix Onboarding](#), um ein Konto zu erstellen.

Stellen Sie sicher, dass Sie Ihre StoreFront-URL beansprucht haben, bevor Sie fortfahren. Wenn die URL beansprucht wurde, wird der folgende Bildschirm angezeigt und Sie können die Einstellungen für Ihren On-Premises-Store konfigurieren.



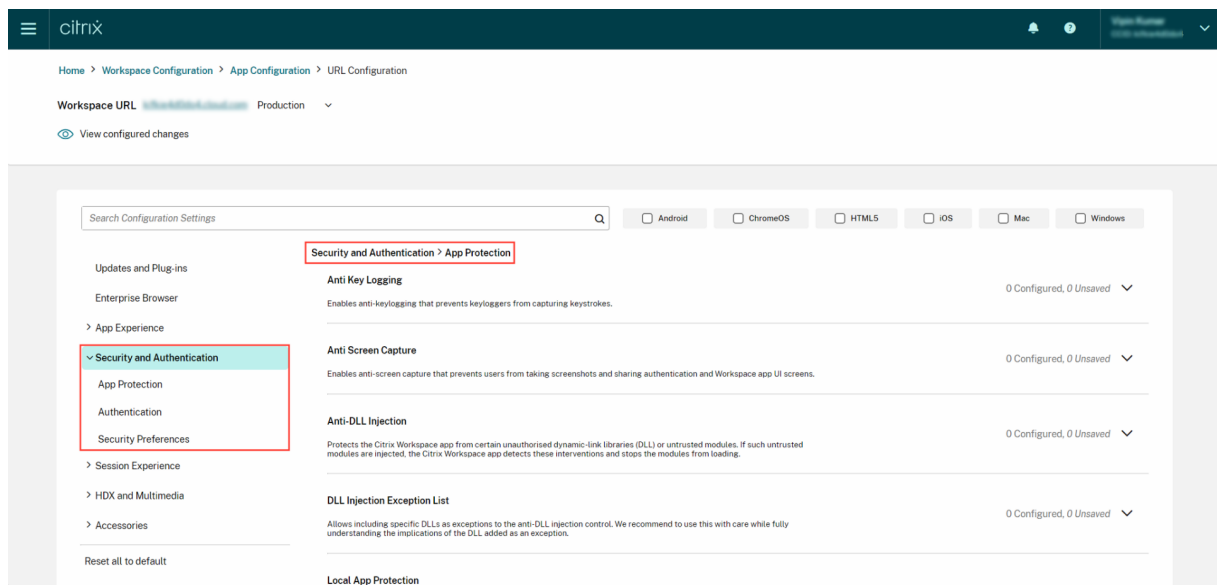
Wenn Sie Ihre URL noch nicht beansprucht haben, wird Ihnen der folgende Bildschirm angezeigt. Klicken Sie im Abschnitt **Einstellungen für On-Premises-Speicher konfigurieren** auf **Start**, um Ihre URL abzurufen. Weitere Informationen finden Sie unter [Erste Schritte](#).



28 Sep 2023

Vereinfachte Kategorisierung von Einstellungen zur leichteren Navigation

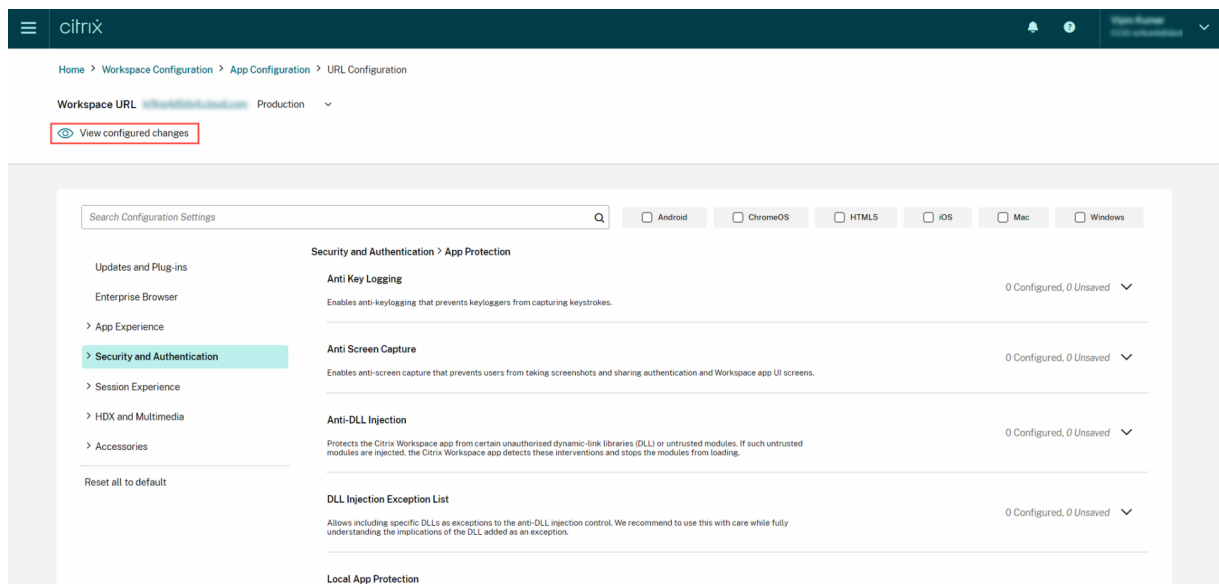
Die Benutzeroberfläche des Global App Configuration Service wurde verbessert und zeigt Einstellungen jetzt in benutzerfreundlichen Kategorien an. Einstellungen wurden anhand von Workflows und Themen der Endbenutzer kategorisiert und umfassen sieben Hauptordner und mehrere Unterordner. Diese übersichtliche Organisation erleichtert Administratoren die Navigation in mehr als 300 Einstellungen.



28 Jul 2023

Zusammenfassung der konfigurierten Einstellungen anzeigen

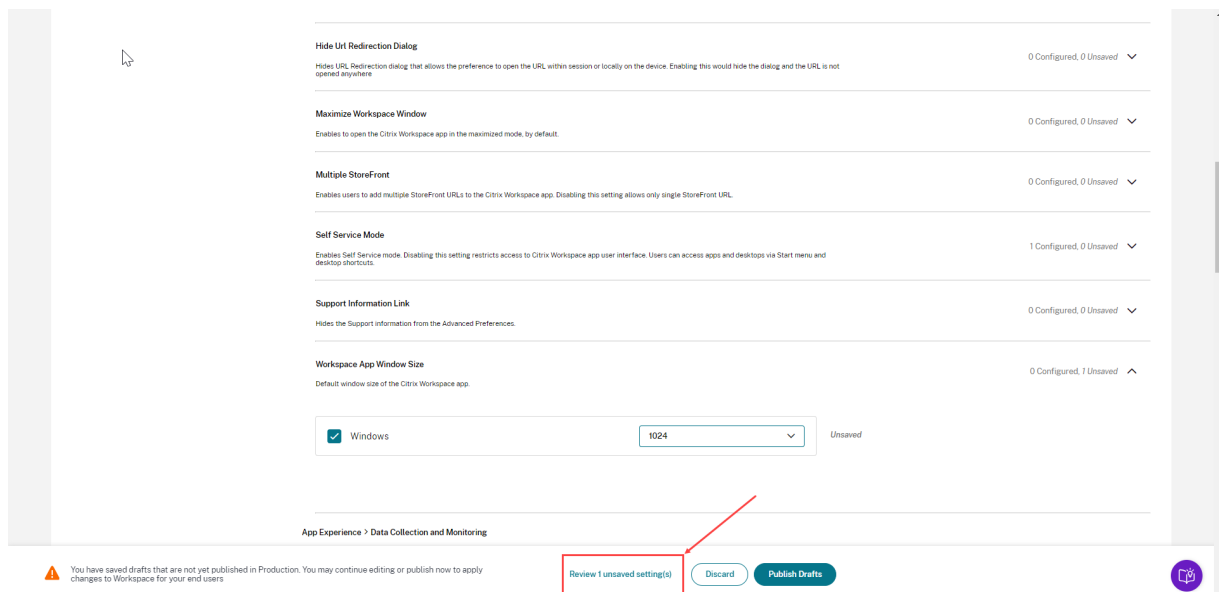
Administratoren können eine Zusammenfassung der aktuellen Konfiguration anzeigen, indem sie auf die Schaltfläche **Konfigurierte Einstellungen anzeigen** klicken. Dadurch entfällt die Notwendigkeit, jede Einstellung einzeln zu erweitern und zu überprüfen. Eine konsolidierte Liste aller konfigurierten Einstellungen ermöglicht es Administratoren, eine umfassende Überprüfung der aktuellen Konfiguration durchzuführen und die Auswirkungen auf die Benutzer abzuschätzen.



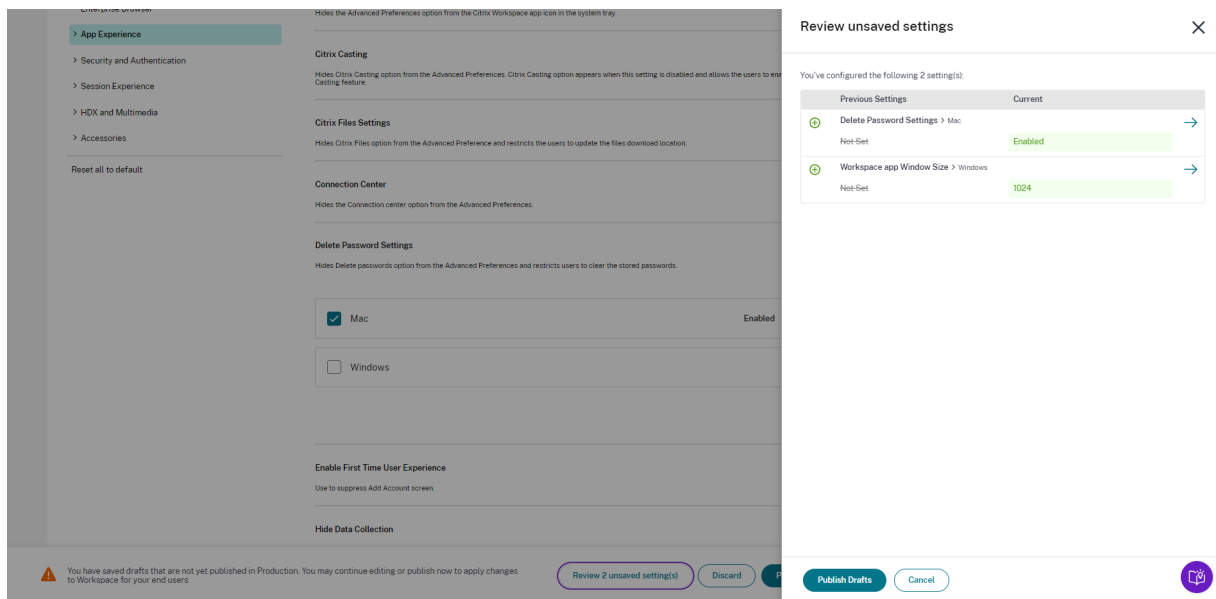
07 Jun 2023

Nicht gespeicherte Änderungen überprüfen

Mit dieser Verbesserung können Administratoren eine abschließende Überprüfung ihrer nicht gespeicherten Änderungen durchführen, bevor sie eine Konfiguration veröffentlichen. Die Anzahl der nicht gespeicherten Einstellungen wird auf der Benutzeroberfläche angezeigt. Administratoren können auf diese Liste zugreifen, indem sie auf die Option **Nicht gespeicherte Änderungen überprüfen** klicken. Auf diese Weise können Administratoren gezielt Änderungen vornehmen und die Datengenauigkeit aufrechterhalten.



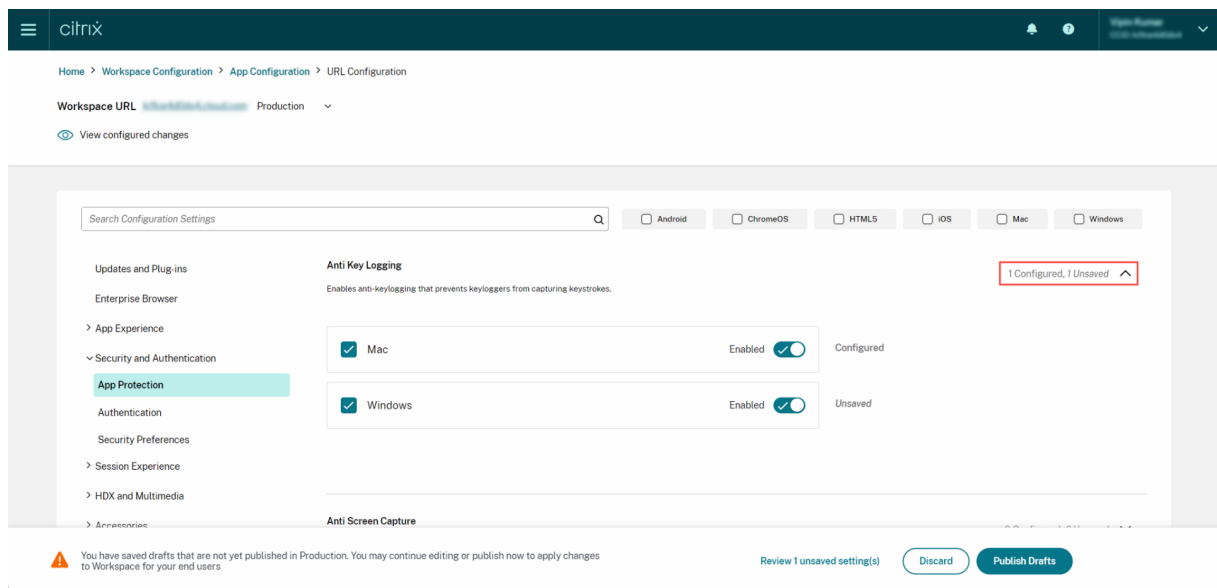
Administratoren können auch zu einer nicht gespeicherten Einstellung navigieren, indem sie auf den Pfeil klicken.



Verbesserte Benutzeroberfläche

Administratoren können jetzt den Status jeder Einstellung anzeigen, ohne diese zu erweitern. Die folgenden Tags werden jetzt angezeigt, damit sie bei jedem Schritt gute Entscheidungen treffen können.

- **Konfiguriert:** Zeigt die Anzahl der Plattformen (Client-OS) an, für die die Einstellung bereits konfiguriert wurde.
- **Nicht gespeichert:** Zeigt die Anzahl der Einstellungen an, die konfiguriert, aber noch nicht gespeichert wurden



May 23, 2023

Verbesserte Suchfunktion

Mit dieser Erweiterung wurde das Sucherlebnis verbessert, um ein robustes und nahtloses Erlebnis zu bieten. Administratoren können sich jetzt problemlos beim Cloud-Portal anmelden und die erforderlichen Einstellungen auf der App-Konfigurationsseite finden. Sie können die folgenden Suchmethoden verwenden.

- **Suche anhand der Beschreibung der Einstellung**

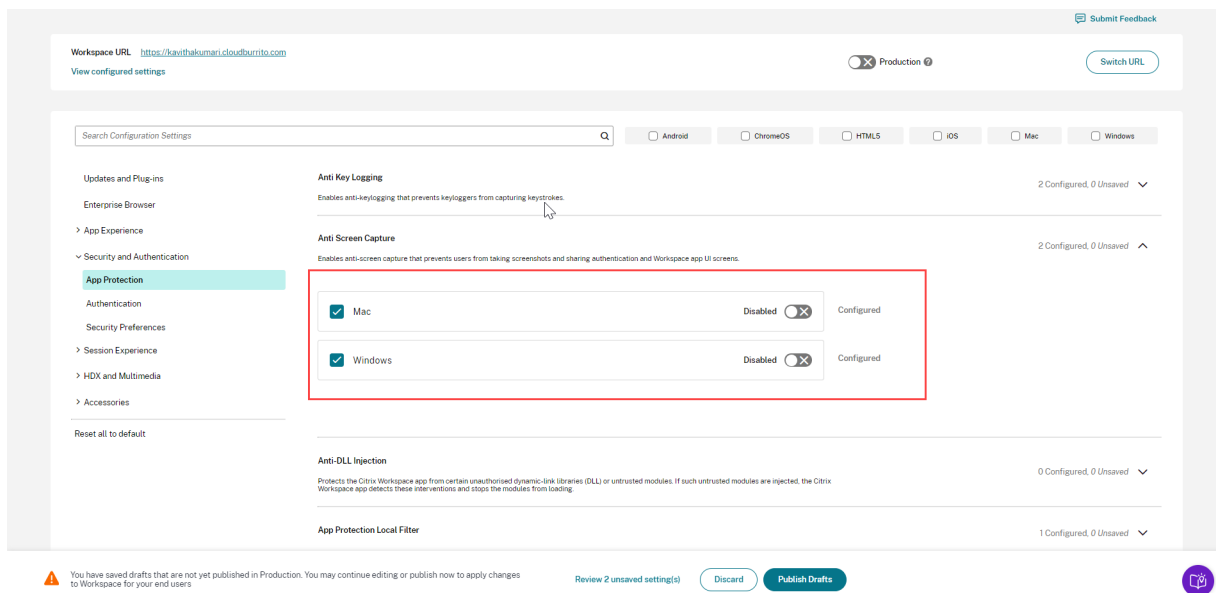
Administratoren können Einstellungen anhand von Schlüsselwörtern aus der Beschreibung der Einstellung suchen. Dies ermöglicht eine flexiblere Suche unter Verwendung relevanter, mit der gewünschten Einstellung verknüpfter Begriffe.

- **Suche anhand des API-Einstellungsnamens**

Administratoren haben die Möglichkeit, nach Einstellungen zu suchen, indem sie den API-Einstellungsnamen eingeben. Diese Methode ermöglicht eine gezieltere Suche, sodass Benutzer schnell die benötigte Einstellung finden.

Relevante Plattformen für jede Einstellung anzeigen

Jede Einstellung zeigt jetzt nur die Plattformen an, für die sie relevant und anwendbar ist. Diese intelligente Filterung stellt sicher, dass die Benutzern eine knappe Liste der relevanten Optionen sehen, die keine unnötigen Einträge enthält.



Erste Schritte mit Citrix Workspace

October 12, 2023

In diesem Artikel werden die Hauptschritte zum Einrichten von Citrix Workspace und zugehörigen Komponenten beschrieben. Eine Zusammenfassung der beteiligten Phasen finden Sie unter [Überblick über den Workflow](#).

Es gibt andere Möglichkeiten des Umstiegs auf die komplette Citrix Workspace-Erfahrung. Die gebräuchlichsten sind folgende:

- Bereitstellen von Citrix Virtual Apps and Desktops über Citrix Workspaces.
 - Wenn Sie über Workspace auf Ressourcen in Ihrer On-Premises-Bereitstellung von Virtual Apps and Desktops zugreifen möchten, konsultieren Sie [Siteaggregation für Hybridlösungen](#).
 - Wenn Sie in die Cloud migrieren möchten, lesen Sie [Vollständige Migration in die Cloud](#).

Überblick über den Workflow

Wenn Sie Citrix Workspace als Neukunde einrichten, gibt es fünf Hauptphasen:

1. [Vorbereiten für Citrix Workspace in Citrix Cloud](#)
2. [Konfigurieren von Zugriff und Authentifizierung für die Abonnenten](#)
3. [Integration von Services in Workspaces](#)

4. [Anpassen von Workspaces](#) an unternehmensspezifische Einstellungen (Logos, Sicherheitsrichtlinien...)
5. [Rollout von Citrix Workspace an die Abonnenten](#)

Das [Success Center](#) bietet zusätzliche lösungsbasierte Orientierungshilfe.

Phase 1: Vorbereiten für Citrix Workspace in Citrix Cloud

Bevor Sie Citrix Workspace konfigurieren, müssen Sie sich bei Citrix Cloud anmelden und sicherstellen, dass Sie die technischen Anforderungen für den Einstieg in Citrix Workspace erfüllen.

Bestehende Citrix Cloud-Kunden mit über die **Identitäts- und Zugriffsverwaltung** hinzugefügten Administratoren können zu [Phase 2: Konfigurieren von Zugriff und Authentifizierung für die Abonnenten](#) springen.

Schritte der Phase 1:

1. Anmeldung bei [Citrix Cloud](#)
2. Hinzufügen von Administratoren mit einer [Citrix Identität](#)
3. Einrichten der Infrastruktur durch:
 - Ressourcenstandorte erstellen
 - Bereitstellen von Cloud Connectors

Die Konfiguration von Citrix Identity umfasst ein zeitbasiertes Einmalkennwort (TOTP). Zusätzlich zu Citrix Identity können Sie die Azure AD-Authentifizierung konfigurieren. Weitere Informationen zum Hinzufügen von Administratoren und zum Konfigurieren der Authentifizierung für Administratoren finden Sie unter [Administratoren](#) in der Citrix Cloud-Produktdokumentation.

Phase 2: Konfigurieren von Zugriff und Authentifizierung für die Abonnenten

Phase 2 umfasst die Konfiguration der Zugriffssteuerung (Workspace-URL und externe Konnektivität) in der **Workspacekonfiguration**.

Sie konfigurieren außerdem mindestens einen Identitätsanbieter in der **Identitäts- und Zugriffsverwaltung** und aktivieren einen davon in der **Workspacekonfiguration** als Primärmethode der Authentifizierung.

Hinweis:

Es gibt zwei Möglichkeiten, auf Citrix Workspace zuzugreifen. Eine Option ist die nativ installierte [Citrix Workspace-App](#), die Citrix Receiver ersetzt und einen einfachen und sicheren Zugriff auf Citrix Cloud Services und Workspaces bietet. Die andere Möglichkeit, auf Citrix Workspace zuzugreifen, ist über einen Browser mit der [Workspace-URL](#). Die Workspace-URL ist standardmäßig

aktiviert, normalerweise im Format: <https://yourcompanyname.cloud.com>.

Weitere Informationen finden Sie unter [Workspace-Zugriff](#).

Konfigurieren des Workspace-Zugriffs

Sie konfigurieren die Zugriffssteuerung in **Workspacekonfiguration > Zugriff**. Dazu gehören normalerweise die folgenden Aufgaben:

- Konfigurieren und Aktivieren der [Workspace-URL](#)
- Konfigurieren der externen Konnektivität mit [Citrix Gateway](#)

Darüber hinaus empfiehlt Citrix, dass Sie die [Citrix Workspace-App](#) installieren und die Abonnenten zu deren Verwendung auffordern, um eine konsistente Benutzererfahrung der Workspaces zu gewährleisten.

Konfigurieren der Abonnentenauthentifizierung für Workspaces

Das Definieren der Art und Weise, wie sich Abonnenten für die Anmeldung bei ihren Workspaces authentifizieren, erfolgt in zwei Schritten:

1. Konfigurieren von Identitätsanbietern in der **Identitäts- und Zugriffsverwaltung**
2. Auswählen einer der Authentifizierungsmethoden, die von den im ersten Schritt konfigurierten Identitätsanbietern bereitgestellt werden, unter **Workspace-Konfiguration > Authentifizierung**

Wenn Sie einen Verbundidentitätsanbieter verwenden, können Sie Single Sign-On (SSO) für DaaS auch mit dem [Citrix Verbundauthentifizierungsdienst \(FAS\)](#) aktivieren.

Weitere Informationen zum Konfigurieren der Abonnentenauthentifizierung für Workspaces finden Sie unter [Sichere Workspaces](#).

Phase 3: Integration von Services in Workspaces

Die Integration Ihrer Services in Workspaces ist ein weiterer zweiteiliger Prozess:

1. Konfigurieren der erworbenen Services in Citrix Cloud. Eine Liste der Services finden Sie unter [Citrix Cloud Services](#).
2. Aktivieren des Zugriffs auf Ihre konfigurierten Services in **Workspacekonfiguration > Serviceintegrationen**. Weitere Informationen zur Serviceintegration finden Sie unter [Aktivieren und Deaktivieren von Services](#).

Phase 4: Anpassen von Workspaces

In der **Workspacekonfiguration** können Sie die Workspace-Benutzeroberfläche für einzelne Abonnenten und gemäß spezieller Unternehmensanforderungen anpassen. Dies erfolgt durch:

- Anpassen des Erscheinungsbilds von Workspaces, einschließlich Logos und benutzerdefinierter Designs. Anweisungen zum Anpassen des Workspace-Erscheinungsbilds finden Sie unter [Anpassen der Darstellung von Workspaces](#).
- Auswahl von Interaktionsoptionen, z. B. das Erstellen von **Favoriten** durch Abonnenten und der automatische Start von Desktops. Anweisungen zum Anpassen der Interaktion von Abonnenten mit ihrem Workspace finden Sie unter [Anpassen von Workspace-Interaktionen](#).
- Anpassen von Datenschutz- und Sicherheitsrichtlinien für Workspaces durch Festlegen eines Timeouts, Erstellen einer Anmelderichtlinie und Zulassen einer Kennwortänderung durch Abonnenten direkt im Workspace. Anweisungen zum Anpassen der Datenschutz- und Sicherheitsrichtlinien für Workspace finden Sie unter [Anpassen von Sicherheits- und Datenschutzrichtlinien](#).

Phase 5: Rollout von Citrix Workspace an die Abonnenten

Citrix empfiehlt, dass Sie die Integrität von Workspaces mit betrieblichen Abnahmeprüfungen verifizieren und sich mit dem [Success Center](#) in Verbindung setzen, um das Onboarding von Abonnenten zu planen. Hauptschritte in dieser Phase:

1. Testen der Workspaces

- Vergewissern Sie sich, dass Sie sich über den Browser und bei der Citrix Workspace-App anmelden können.
- Starten und verwenden Sie alle verfügbaren Apps und Desktops.
- Vergewissern Sie sich, dass Sie auf Ordner und Dateien zugreifen können.
- Vergewissern Sie sich, dass in Benachrichtigungen die erwarteten Aktionen und Aktivitäten angezeigt werden.
- Falls aktiviert, vergewissern Sie sich, dass Sie auf Endpunktresourcen auf Mobilgeräten zugreifen können.

2. Onboarding von Abonnenten

- Informieren Sie die Abonnenten über die Citrix Workspace-Features.
- Teilen Sie die [Workspace-URL](#).
- Leiten Sie die Benutzer zur Installation der [Citrix Workspace-App](#) an.

Weitere Informationen zum Testen von Workspaces und zum Onboarding von Workspace-Abonnenten finden Sie unter [Citrix Workspace end-user adoption resources](#).

Vorbereitung auf Citrix Workspace

November 27, 2023

In diesem Artikel werden die Anforderungen und administrativen Schritte beschrieben, die Sie beim Vorbereiten der Implementierung von Citrix Workspace unterstützen. Die Schritte zur Vorbereitung auf Citrix Workspace umfassen Folgendes:

1. Sicherstellen, dass Sie die [Anforderungen an System und Konnektivität](#) für Citrix Cloud erfüllen.
2. [Planen der Bereitstellung und des Rollouts](#) von Citrix Workspace.
3. [Registrierung oder Anmeldung bei Citrix Cloud](#).
4. [Hinzufügen von Administratoren](#) zu Citrix Cloud und Citrix Workspace.
5. [Überprüfen Ihrer Ansprüche](#) auf Dienste in der Cloud.
6. [Einrichten der erforderlichen Infrastruktur](#) für Citrix Workspace.

Das [Success Center](#) ist eine wichtige Ergänzung dieser Produktdokumentation. Success Center-Artikel bieten eine breite lösungsbasierte Perspektive sowie dienstspezifische Details.

Die Produktdokumentation zu [Citrix Cloud](#) bietet IT-Managern und Entwicklern detaillierte Hinweise, welche Voraussetzungen und Aktivitäten zur Vorbereitung auf Citrix Workspace in Citrix Cloud erforderlich sind.

Anforderungen an System und Konnektivität

Citrix Cloud ist die Konsole, über die Sie Ihre Dienstansprüche anzeigen und verwalten und auf die **Workspacekonfiguration** zugreifen.

Wenn Sie bereits für Citrix Cloud eingerichtet sind, können Sie mit den unter [Planen der Bereitstellung und des Rollouts](#) beschriebenen Schritten fortfahren.

Für Citrix Cloud ist die folgende Konfiguration erforderlich:

- Eine Active Directory-Domäne zum Verwalten der Abonnentenauthentifizierung für Workspaces.
- Mindestens zwei Citrix Cloud Connectors pro Ressourcenstandort.
- Eine dedizierte Maschine für jeden Cloud Connector.
- Physische oder virtuelle Maschinen, die in Ihre Domäne eingebunden sind, um Workloads und andere Komponenten auszuführen.

Sie benötigen mindestens zwei physische oder virtuelle Maschinen, da Sie auf der Hostmaschine für einen Citrix Cloud Connector keine anderen Komponenten installieren können.

Informationen zu den Anforderungen für Cloud Connectors finden Sie unter [Technische Daten zu Citrix Cloud Connector](#). Informationen zur Installation von Cloud Connectors finden Sie unter [Cloud Connector-Installation](#).

Darüber hinaus müssen die folgenden Adressen für den Einsatz von Citrix Workspace erreichbar sein:

- https://*.cloud.com
- https://*.citrixdata.com

Eine vollständige Liste der für Citrix Cloud-Services erforderlichen kontaktierbaren Adressen finden Sie unter [Servicekonnektivitätsanforderungen](#).

Bereitstellung und Rollout planen

Citrix empfiehlt, einen Support- und Verwaltungsplan für Citrix Workspace zu erstellen. Verwenden Sie den [Plan im Success Center](#), um Ziele festzulegen, Anwendungsfälle zu definieren, Risiken zu identifizieren und eine Implementierungsstrategie zu erstellen, die folgende Schritte umfasst:

- Festlegen von Geschäftszielen, hinzuzufügenden Diensten und Anforderungen an Benutzergruppen.
- Identifizieren der technischen Anforderungen zum [Einrichten der Infrastruktur](#) für Citrix Workspace.
- Aufbau Ihres Workspace-Teams. Weisen Sie Ihren Bereitstellungsteams Aufgaben zu und fügen Sie Ihrem Citrix Cloud-Konto [Administratoren](#) mit Zugriff auf die **Workspacekonfiguration** hinzu.
- Planen der Zusammenarbeit mit Prozessinhabern und Abonnenten.
 - Vorbereiten einer Änderungsstrategie und eines Kommunikationsplans.
 - Entwicklung von Schulungs- und Verstärkungsprogrammen.
 - Durchführen von Auswirkungs- und Stakeholderanalysen.

Weitere Informationen zur Planung Ihrer Workspace-Bereitstellung und des Rollouts finden Sie im Success Center unter [Success Readiness Checklist](#).

Registrierung oder Anmeldung bei Citrix Cloud

Bei Registrierung als Neukunde befolgen Sie die Anweisungen unter [Registrierung bei Citrix Cloud](#).

Wenn für Ihre Organisation bereits ein Administratorkonto erstellt wurde, muss der Hauptadministrator Sie zum Firmenkonto hinzufügen. Weitere Informationen finden Sie unter [Hinzufügen von Administratoren](#).

Wenn Sie bereits ein Konto haben, melden Sie sich bei Citrix Cloud mit Ihren Anmeldeinformationen für citrix.com, My Citrix oder Citrix Cloud an.

Weitere Informationen zum Registrieren oder Anmelden bei Citrix Cloud finden Sie im [Kickoff Guide von Citrix Cloud Services](#).

Administratoren hinzufügen

Das erste Administratorkonto wird beim ersten Onboarding von Citrix Cloud erstellt. Der erste Administrator kann dann weitere Administratoren zu Citrix Cloud einladen. Die neuen Administratoren können vorhandene Citrix-Anmeldeinformationen verwenden oder ein neues Konto einrichten.

Administratoren einladen

Administratoren werden Ihrem Citrix Cloud-Konto über **Identitäts- und Zugriffsverwaltung** im Menü auf der linken Seite der Citrix Cloud-Konsole hinzugefügt. Geben Sie die E-Mail-Adresse des hinzuzufügenden Administrators ein, um ihm eine Einladung mit Anmeldeanweisungen zu senden.

Wenn Sie Ihrem Citrix Cloud-Konto Administratoren hinzufügen, definieren Sie die für die Rolle der Administratoren in Ihrem Unternehmen geeigneten Administratorberechtigungen. Administratoren mit **Vollzugriff** haben standardmäßig Zugriff auf die **Workspacekonfiguration**. Administratoren mit **benutzerdefiniertem Zugriff** haben nur Zugriff auf die von Ihnen ausgewählten Funktionen und Dienste. Sie können die Zugriffsberechtigungen der von Ihnen eingeladenen Administratoren ändern.

Weitere Informationen zum Hinzufügen (und Entfernen) von Administratoren finden Sie unter [Administratoren](#).

Administratorauthentifizierung einrichten

Citrix Cloud verwendet standardmäßig den Citrix Identitätsanbieter zur Verwaltung Ihres Citrix Cloud-Kontos. Der Citrix Identitätsanbieter authentifiziert nur Citrix Cloud-Administratoren. Abonnenten müssen sich bei einem der unter [Sichere Arbeitsbereiche](#) aufgeführten Identitätsanbieter authentifizieren.

Jeder Administrator in Ihrem Citrix Cloud-Konto muss außerdem die Multifaktorauthentifizierung einrichten.

Bei der Registrierung wird eine Authentifizierungs-App heruntergeladen und installiert, die dem [TOTP-Standard](#) (Time-Based One-Time Password, zeitbasiertes Einmalkennwort) entspricht, z. B. Citrix SSO. Zur problemlosen Registrierung empfiehlt Citrix, [Citrix SSO](#) herunterzuladen und zu installieren, bevor Sie die folgenden Schritte ausführen.

1. Melden Sie sich bei Ihrem Citrix Cloud-Konto an.

2. Wählen Sie Ihren Namen und wählen Sie im Dropdownmenü **Mein Profil**.
3. Wählen Sie unter **Anmeldesicherheit** die Option **Authentifikator-App einrichten**, um per E-Mail den für Schritt 4 erforderlichen Verifizierungscode zu erhalten.
4. Geben Sie nach Aufforderung diesen Verifizierungscode ein, den Sie in der E-Mail von Citrix erhalten haben, und Ihr Kontokennwort und wählen Sie **Verifizieren**.
5. Scannen Sie den QR-Code oder geben Sie den Schlüssel in eine Authentifizierungs-App ein, die dem TOTP-Standard (Time-Based One-Time Password, zeitbasiertes Einmalkennwort) entspricht, z. B. Citrix SSO.
6. Um zu bestätigen, dass die Multifaktorauthentifizierung korrekt eingerichtet wurde, geben Sie den 6-stelligen Code aus der Authentifizierungs-App ein und wählen dann **Verifizieren**.
7. Wählen Sie **Wiederherstellungstelefon hinzufügen** und geben Sie eine Telefonnummer ein, damit der Citrix Support Sie bei Abfragen zur Multifaktorauthentifizierung erreichen kann, um Ihre Identität zu prüfen.
8. Wählen Sie **Backupcodes generieren**, um eine Liste mit Einmalcodes zu erstellen, die verwendet werden können, wenn Sie den Zugriff auf Ihre Authenticator-App verlieren.
9. Wählen Sie **Codes herunterladen** und bewahren Sie die Textdatei mit Ihren Backupcodes an einem sicheren und zugänglichen Ort auf.
10. Aktivieren Sie das Kontrollkästchen und wählen Sie **Fertig stellen**.

Anweisungen zum Einrichten der Multifaktorauthentifizierung finden Sie auch im [Knowledge Center](#) und in der Citrix Cloud-Produktdokumentation unter [Multifaktorauthentifizierung einrichten](#).

Optional können Sie auch Azure Active Directory (AD) für Administratoren einrichten. Weitere Informationen zu den Identitätsanbietern, die für Citrix Cloud-Administratoren und Workspace-Abonnenten verfügbar sind, finden Sie unter [Identitätsanbieter](#).

Bearbeiten von Administratorberechtigungen

Konfigurieren des benutzerdefinierten Zugriffs auf **Workspacekonfiguration**:

1. Wählen Sie im **Citrix Cloud**-Menü **Identitäts- und Zugriffsverwaltung** und dann **Administratoren**.
2. Suchen Sie den gewünschten Administrator, wählen Sie die Auslassungspunkte und dann **Zugriff bearbeiten**.

← Identity and Access Management

Authentication **Administrators** API Access Domains Recovery

Add administrators from... ▼ Bulk Actions ▼

<input type="checkbox"/>	Administrator↓	Full Name	Status	Access	Identity Provider
<input type="checkbox"/>	[Redacted]	[Redacted]	Active	Full	Citrix Cloud ⋮
<input type="checkbox"/>	[Redacted]	[Redacted]	Active	Full	Citrix Cloud ⋮
<input type="checkbox"/>	[Redacted]	[Redacted]	Active	Full	Citrix Cloud ⋮

Copy Email Address
Delete Administrator
Edit Access

3. Stellen Sie sicher, dass **Benutzerdefinierter Zugriff** aktiviert ist.
4. Um nur den Zugriff auf die **Workspacekonfiguration** zu aktivieren, wählen Sie unter **Allgemeine Verwaltung** die Option **Workspacekonfiguration**.

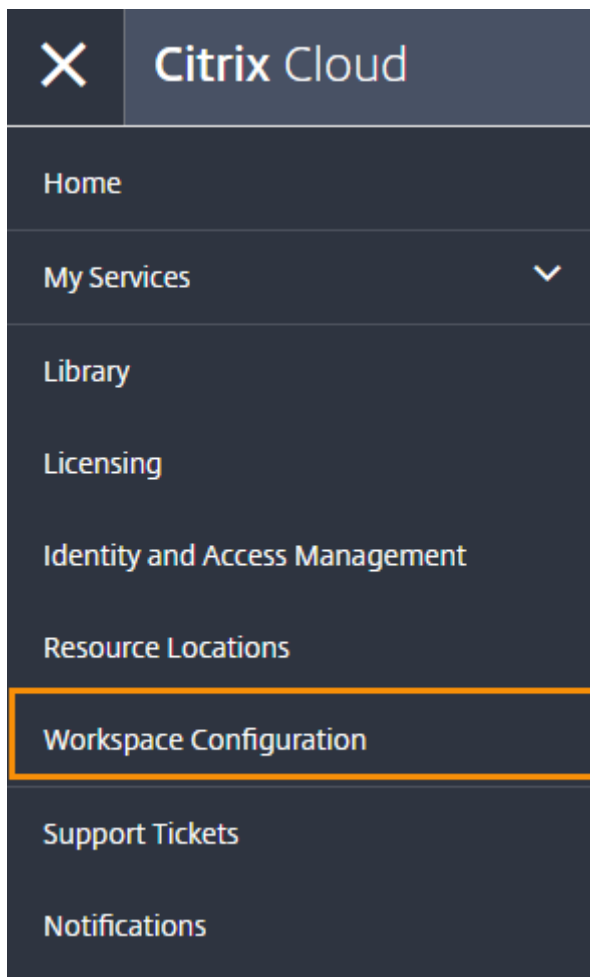
Full access
Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.

Custom access
Switching to custom access will remove management access to certain services.
Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.
[Select all](#) | [Deselect All](#)

General Management

- Domains
- Library
- Notifications
- Resource Location
- Workspace Configuration

Nach dem Aktivieren des Zugriffs können Administratoren sich bei Citrix Cloud anmelden und im **Citrix Cloud**-Menü die Option **Workspacekonfiguration** wählen.



Hinweis:

In Citrix Virtual Apps Essentials ist **Workspacekonfiguration** erst nach dem Erstellen des ersten Katalogs im Citrix Cloud-Menü verfügbar.

Ansprüche überprüfen

Sobald Sie bei Citrix Cloud angemeldet sind, können Sie Ihre Ansprüche –also die von Ihnen erworbenen Citrix Produkte und Dienste –verwalten. Citrix Produkte und Dienste werden in einem Kartenlayout im Citrix Cloud-Dashboard angezeigt. Für Produkte und Dienstleistungen, die Sie gekauft und abonniert haben, wird eine Schaltfläche **Verwalten** angezeigt.

Um einen neuen Dienst zu testen, können Sie im entsprechenden Feld im Citrix Cloud-Dashboard die Option **Testversion anfordern** oder **Demo anfordern** auswählen. Weitere Informationen zu Testversionen finden Sie unter [Citrix Cloud Service - Testversionen](#).

Wenn Sie einen neuen Dienst kaufen möchten, können Sie eine Testversion in einen Produktionsservice umwandeln, ohne eine Neukonfiguration vorzunehmen oder ein neues Konto zu erstellen.

Um einen Dienst zu kaufen, notieren Sie sich Ihre Organisations-ID (rechts oben in der Citrix Cloud-Konsole) und gehen Sie zu <https://www.citrix.com/product/citrix-cloud>.

Infrastruktur einrichten

Zum Einrichten der für Citrix Workspace erforderlichen Infrastruktur müssen Sie Ihre Ressourcen mit Citrix Cloud verbinden. Hierfür sind folgende Schritte erforderlich:

- Connectors in Ihrer Umgebung bereitstellen.
- Ressourcenstandorte erstellen.

Ressourcenstandorte enthalten die Ressourcen zum Bereitstellen von Cloud Services für Ihre Abonnenten. Sie verwalten diese Ressourcen über die Citrix Cloud-Konsole. Ressourcenstandorte enthalten unterschiedliche Ressourcen, je nachdem, welche Dienste Sie verwenden.

Um einen Ressourcenstandort zu erstellen, müssen Sie mindestens zwei Cloud Connectors in Ihrer Domäne installieren.

Citrix Cloud Connector ist eine Komponente, die einen Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten bereitstellt. Der Kanal stellt über den Standard-HTTPS-Port (443) und das TCP-Protokoll Verbindungen zur Cloud her. Es werden keine eingehenden Verbindungen akzeptiert.

Weitere Informationen finden Sie unter [Citrix Cloud Connector](#).

Hinweis:

Workspace unterstützt keine Verbindungen von Legacyclients, die Verbindungen mit Ressourcen unter Einsatz einer PNAgent-URL herstellen. Wenn Ihre Umgebung solche Legacyclients enthält, müssen Sie StoreFront on-premises bereitstellen und die Legacyunterstützung aktivieren. Zum Schützen solcher Clientverbindungen verwenden Sie Citrix Gateway on-premises statt des Citrix Gateway-Service.

Nächstes Thema: Workspace erstellen

Nachdem die Vorbereitung für Citrix Workspace abgeschlossen ist, folgen die nächsten Schritte:

- [Konfigurieren des Zugriffs auf Workspaces](#), einschließlich der Workspace-URL und externer Verbindungen.
- Konfigurieren der Workspace-Authentifizierung, mit Anweisungen unter [Sichere Workspaces](#).
- [Integration von Services in Workspaces](#)
- Anpassen der Workspace-Benutzeroberfläche:

- [Anpassen der Darstellung von Workspaces.](#)
- [Anpassen von Workspace-Interaktionen.](#)
- [Sicherheits- und Datenschutzrichtlinien anpassen.](#)

Neue Workspace-Benutzeroberfläche

November 27, 2023

Die neue Workspace-Benutzeroberfläche ist übersichtlicher, vereinfacht den Zugriff auf wichtige Funktionen und ermöglicht eine präzisere Nutzung der Workspace-App je nach Bedarf.

In diesem Artikel werden die wichtigsten Features vorgestellt, die Abonnenten nach der Anmeldung im Workspace sehen, und es wird zusammengefasst, wie Benutzer auf Workspaces zugreifen und mit ihnen interagieren können.

Hinweis:

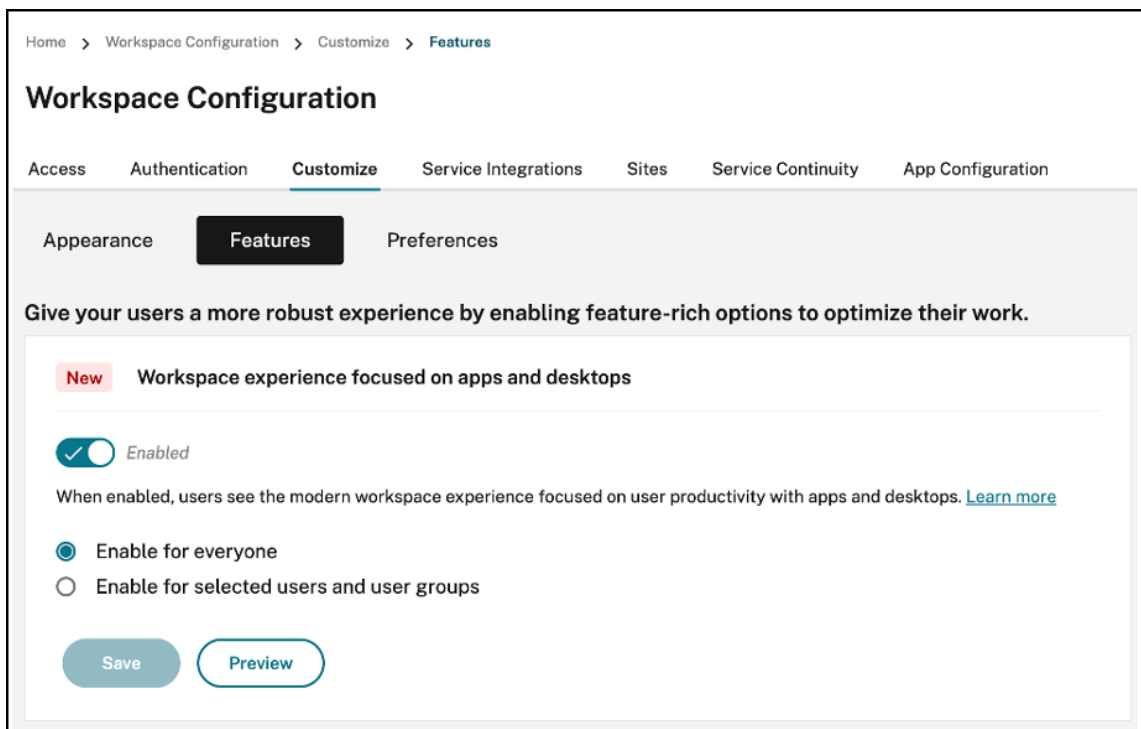
Die neue Benutzeroberfläche wird von allen LTSR-Versionen der Citrix Workspace-App unterstützt. Sie ist auch mit allen Webbrowsern kompatibel bis auf Internet Explorer (hierfür ist die Citrix Workspace-Benutzeroberfläche auf Version 23.26 festgelegt).

Neue Workspace-Benutzererfahrung aktivieren

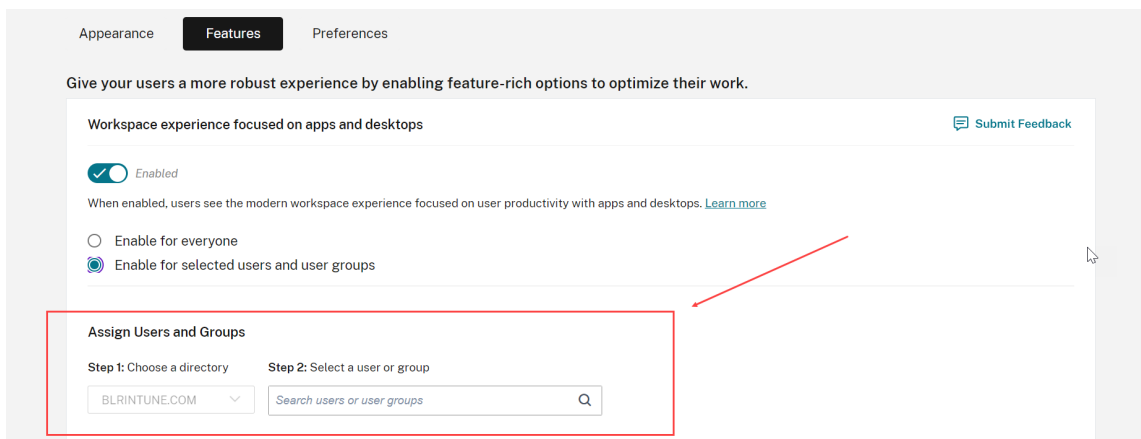
Sie können die neue Workspace-Benutzeroberfläche für bestehende Benutzer aktivieren. Wenn diese Option aktiviert ist, können Benutzer im modernen Workspace noch produktiver mit Apps und Desktops arbeiten.

Führen Sie folgende Schritte aus, um die neue Benutzeroberfläche zu aktivieren:

1. Gehen Sie in der Administratorkonsole zu **Workspacekonfiguration > Anpassen > Funktionen**.
2. Aktivieren Sie den Schalter unter **Workspace-Erfahrung mit Fokus auf Apps und Desktops**. In der Standardeinstellung ist der Schalter ausgeschaltet und das Feature ist deaktiviert. Sie können dieses Feature für alle Benutzer oder für ausgewählte Benutzer aktivieren.



- To enable the new UI for all end users, select **Enable for everyone**.
- To enable the new UI for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



3. Klicken Sie auf **Speichern**.
4. Starten Sie die Workspace-App neu.

Hinweis:

Es kann fünf Minuten dauern, bis die aktualisierte Benutzeroberfläche angezeigt wird. Möglicher-

weise wird Benutzern vorübergehend eine ältere Version der Benutzeroberfläche angezeigt. Wenn die Benutzeroberfläche in einem Browser geöffnet ist, müssen Benutzer die Seite eventuell aktualisieren.

Themen, Symbole und Schriftarten

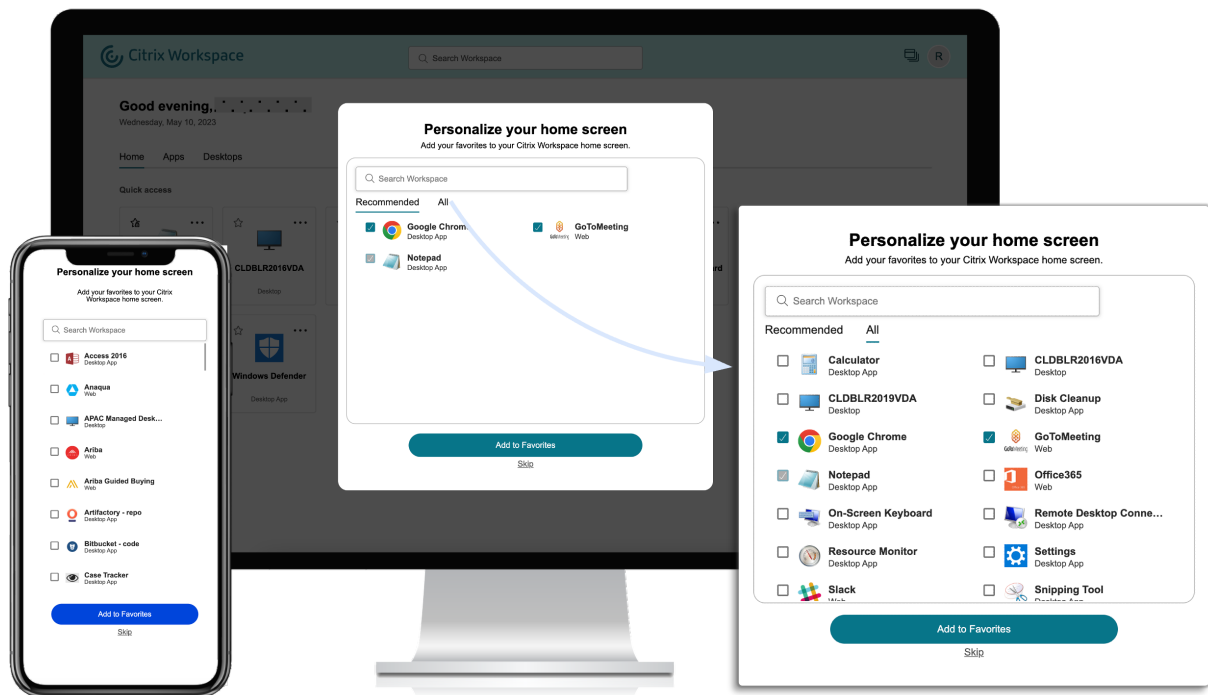
Die neuen Farbdesigns bieten einen verbesserten Kontrast und eine einheitliche Farbpalette. Die Schriftart wird für die Benutzeroberfläche in allen unterstützten Betriebssystemen verwendet. Neue Symbole sind in Form und Farbe leichter zu unterscheiden, was für eine bessere Lesbarkeit und visuelle Klarheit sorgt.

Benutzererfahrung für Erstbenutzer der Workspace-App

Beim Zugriff auf die neue Benutzeroberfläche können Erstbenutzer in einem Pop-upfenster mehrere Apps als Favoriten markieren.

Die Benutzererfahrung für Erstbenutzer wird aktiviert, wenn Sie mehr als 20 Apps haben und keine davon zu den Favoriten hinzugefügt ist. Die Benutzererfahrung wird auf allen Browsern und nativen Clients (Mac, Windows, Linux und ChromeOS) und auf Mobilgeräten (iOS und Android) unterstützt. Sie wird Ihnen beim ersten Anmelden angezeigt.

Empfohlene oder vorgegebene Apps werden im Erstbenutzer-Bildschirm auf der Registerkarte **Empfohlen** angezeigt, wie vom Administrator in der DaaS-Konsole für Citrix Virtual Apps and Desktops und in der Secure Private Access-Konsole für Web- und SaaS-Apps festgelegt. Vorgegebene Apps sind standardmäßig ausgewählt und das Häkchen ist deaktiviert. **Empfohlene** Apps sind automatisch definierte Favoriten-Apps sind standardmäßig ausgewählt, und das Kontrollkästchen ist für Benutzer aktiviert. Sie können auch andere Apps zum Abonnieren auswählen oder sie auf allen Registerkarten als Favorit festlegen. Alle ausgewählten Apps werden automatisch zu den Favoriten hinzugefügt und auf der Homepage angezeigt.



Bei fünf oder weniger Apps wird in der Citrix Workspace-App für Windows eine Desktopverknüpfung zum Schnellzugriff angezeigt.

Alle angezeigten Apps werden für Benutzer abonniert, und es werden die entsprechenden Desktopverknüpfungen erstellt.

Einschränkungen

- Da der *Benutzerpersonalisierungsdienst* bislang nicht erkennt, ob es sich beim Benutzer um einen Erstbenutzer handelt, erscheint der **Personalisierungsbildschirm** einmal pro Gerät und Browser sowie jedes Mal im Inkognito-Modus, wenn Benutzer keinen Favoriten festlegen.
- Wenn der Administrator das Tag für vorgegebene oder empfohlene Apps aus den Apps entfernt, haben Apps unter **Favoriten** keine Auswirkung.
- Wenn ein Endbenutzer keine Apps unter **Favoriten** hinzugefügt hat, wird der **Personalisierungsbildschirm** bei jedem Öffnen der Workspace-App angezeigt.

Um dies zu vermeiden führen Sie folgende Schritte aus:

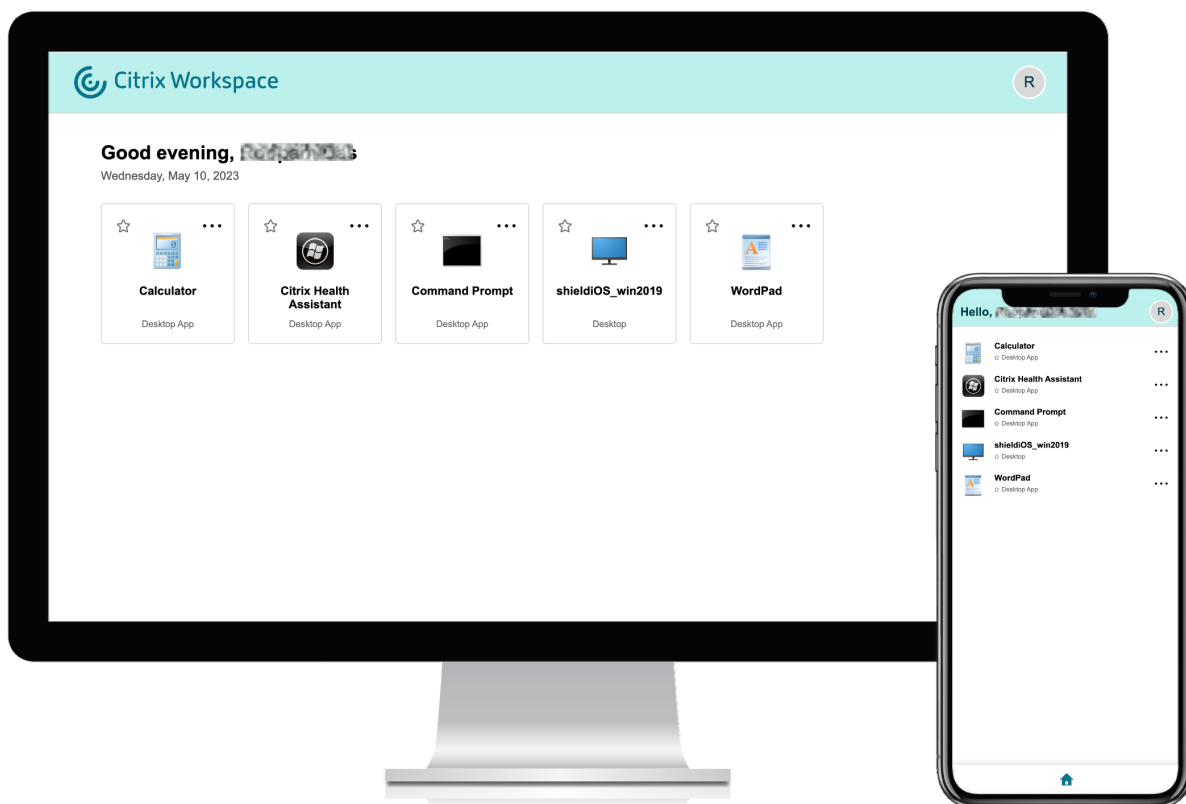
- End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.
- Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage > Full Configuration >**

Applications). This prevents the Personalization screen from appearing for all the end-users. For more information, see [Customize workspace interactions](#).

Verbesserung von Optik und Layout des Workspace

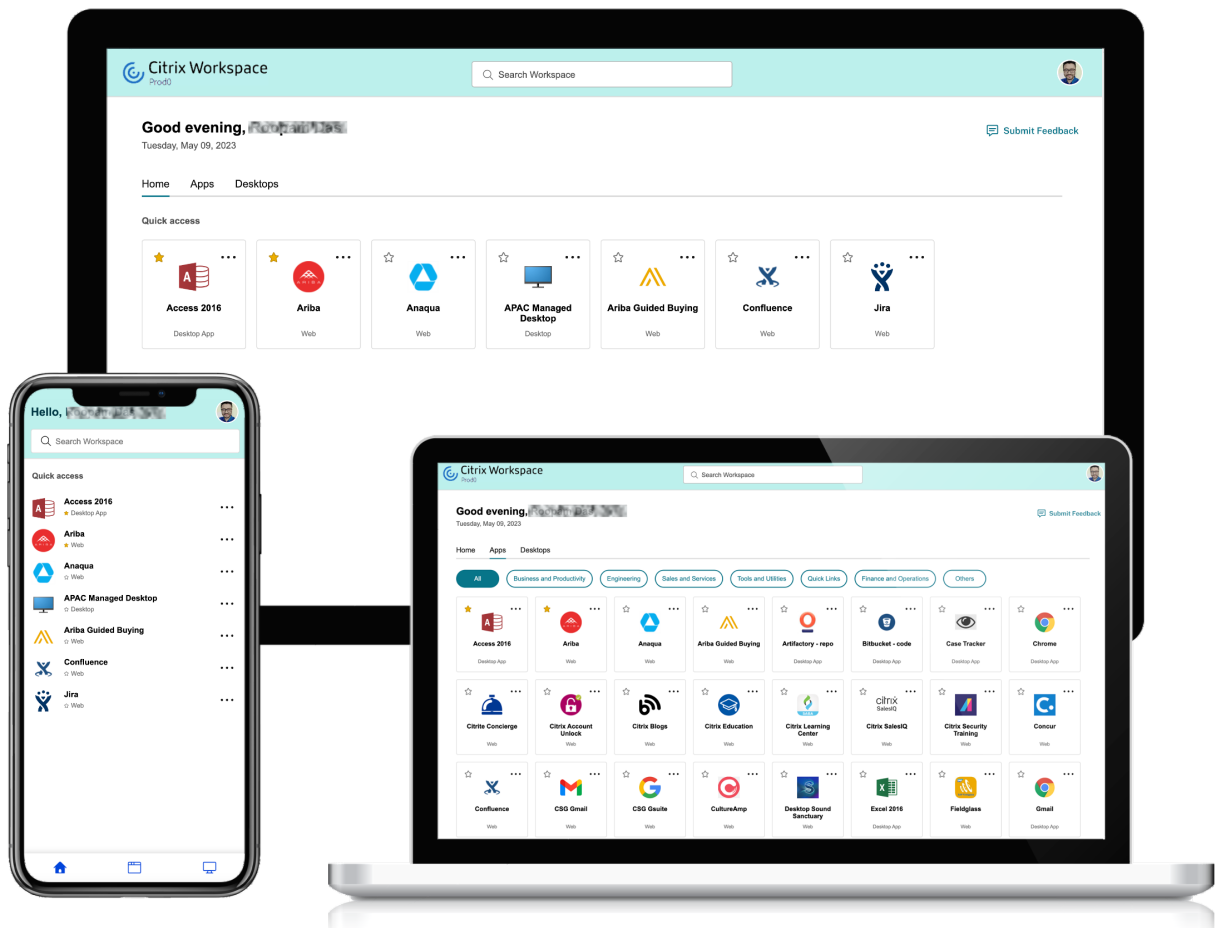
Die neue Benutzererfahrung legt den Fokus auf eine intuitive und anwenderfreundliche Nutzung. Ihre Apps und Favoriten für virtuelle Desktops sind oben auf der Benutzeroberfläche angeordnet, um die Anwendung zu vereinfachen. Citrix besitzt auch eine neue Homepage, um besser durch regelmäßig verwendete Apps und Desktops zu navigieren.

Wenn Sie weniger als 20 Apps verwenden, wird eine vereinfachte Ansicht ohne Registerkarten oder Kategorien angezeigt. Alle Apps und Desktops befinden sich auf derselben Seite. Auf diesem Bildschirm werden zuerst Ihre Favoriten angezeigt, gefolgt von allen übrigen Apps in alphabetischer Reihenfolge. Alle Apps haben ein Sternsymbol, mit dem Sie die App als Favorit markieren oder die Auswahl aufheben können. Die Anzeige der vereinfachten Ansicht der Workspace-App hängt davon ab, wie viele Apps Sie verwenden. Die Apps werden nicht von Administratoren festgelegt.



Wenn Sie mehr als 20 Apps verwenden, wird nach der Anmeldung die Homepage geöffnet. Auf diesem Bildschirm werden zuerst alle Favoriten-Apps angezeigt, gefolgt von den zuletzt verwendeten Apps

(maximal fünf Apps). Die Sternsymbole für die **vorgegebenen** Apps sind gesperrt. Sie können die Apps nicht aus den Favoriten entfernen. Wenn der Administrator die Homepage nicht aktiviert hat, wird stattdessen der **Apps**-Bildschirm angezeigt. Auf diesem Bildschirm werden zuerst Ihre Favoriten angezeigt, gefolgt von allen übrigen Apps in alphabetischer Reihenfolge. Wenn der Administrator Kategorien erstellt und ihnen Apps zugewiesen hat, werden die einzelnen Kategorien angezeigt. Sie können dann die gewünschte App-Kategorie auswählen.



Kategorisierung von Apps

Endbenutzer können ihre Anwendungen im Workspace in Kategorien und Unterkategorien unterteilt anzeigen. Die Unterkategorien werden in einer Ordnerstruktur angezeigt. Die Strukturierung auf mehreren Ebenen sorgt für eine übersichtliche Anzeige und trägt zur Steigerung der allgemeinen Benutzerzufriedenheit bei.

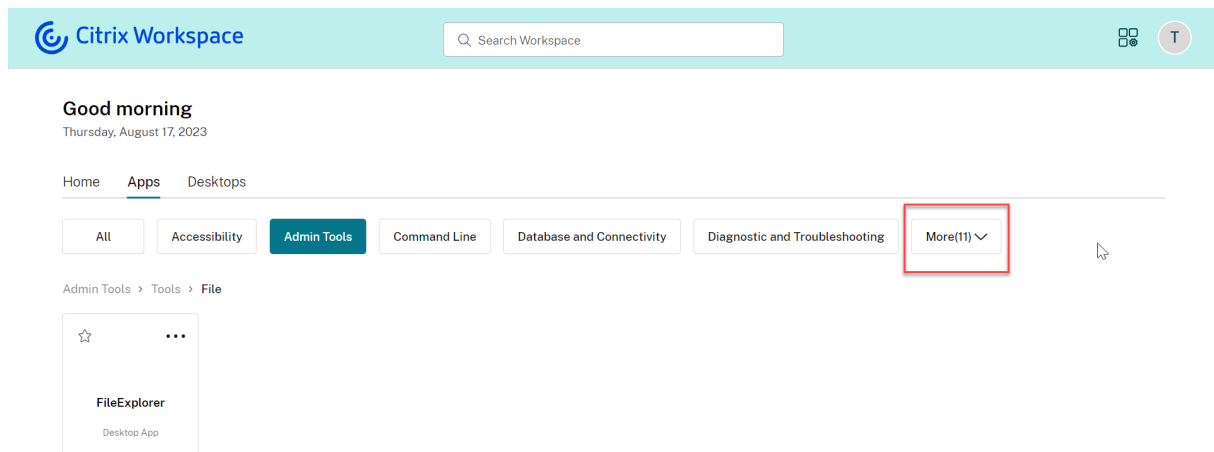
Hinweis:

Damit Apps in einer Ordnerstruktur angezeigt werden, müssen Administratoren einen Ordnerp-

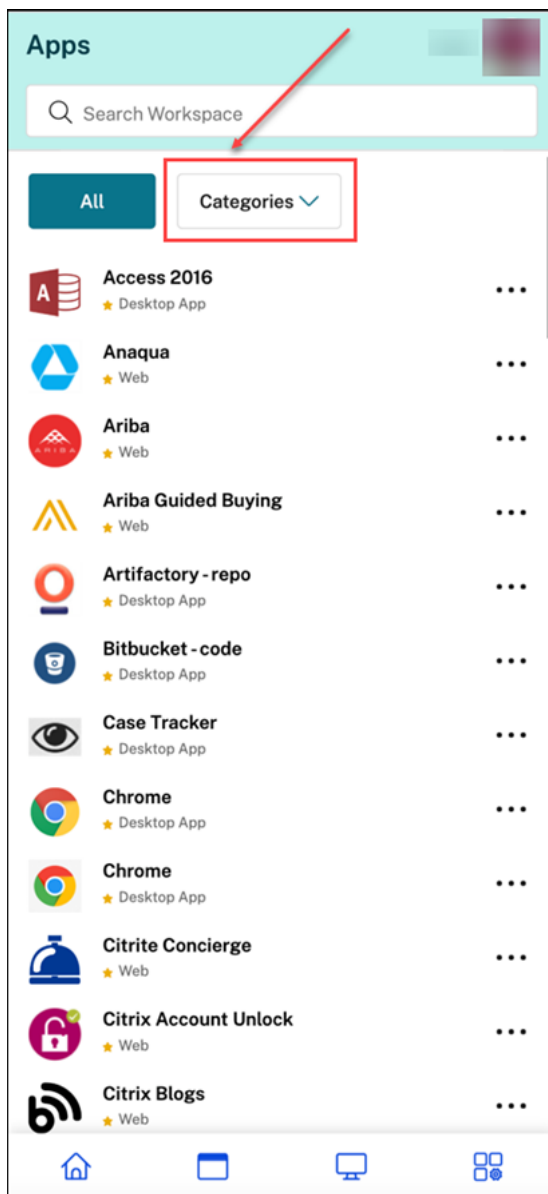
fad hinzufügen. Weitere Informationen finden Sie unter Ordnerpfad hinzufügen.

Wenn die Anzahl der von den Administratoren erstellten Hauptkategorien den Platz auf dem Bildschirm eines Benutzers überschreitet, werden die Kategorien anhand der Bildschirmgröße dynamisch in die Dropdownliste **Mehr** verschoben.

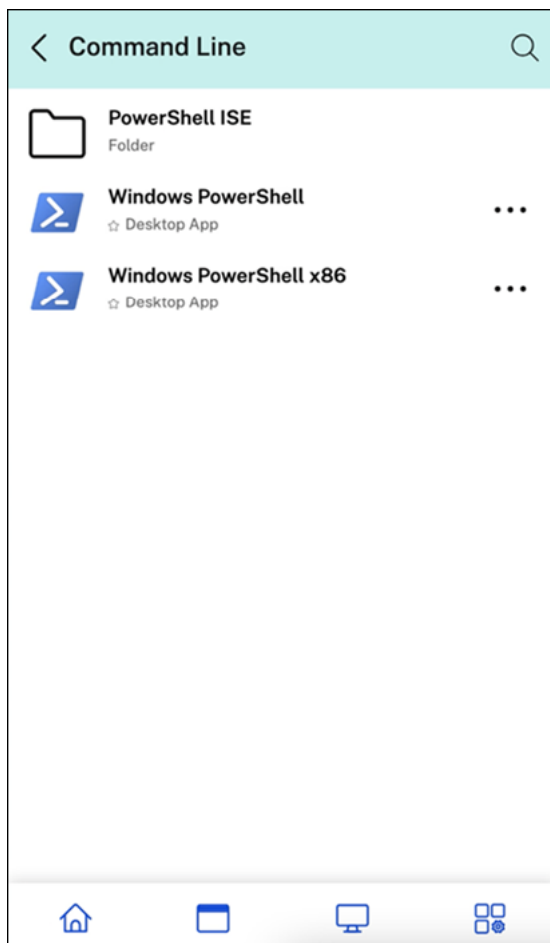
Die Navigations-Breadcrumbs werden ebenfalls angezeigt.



Gehen Sie auf einer mobilen Plattform zur Apps-Registerkarte und klicken Sie auf das Dropdownmenü **Kategorien**, um eine Liste der verfügbaren Kategorien anzuzeigen. Unterkategorien werden als Ordner angezeigt, die je nach Konfiguration durch den Administrator weitere Unterordner oder Anwendungen enthalten können.



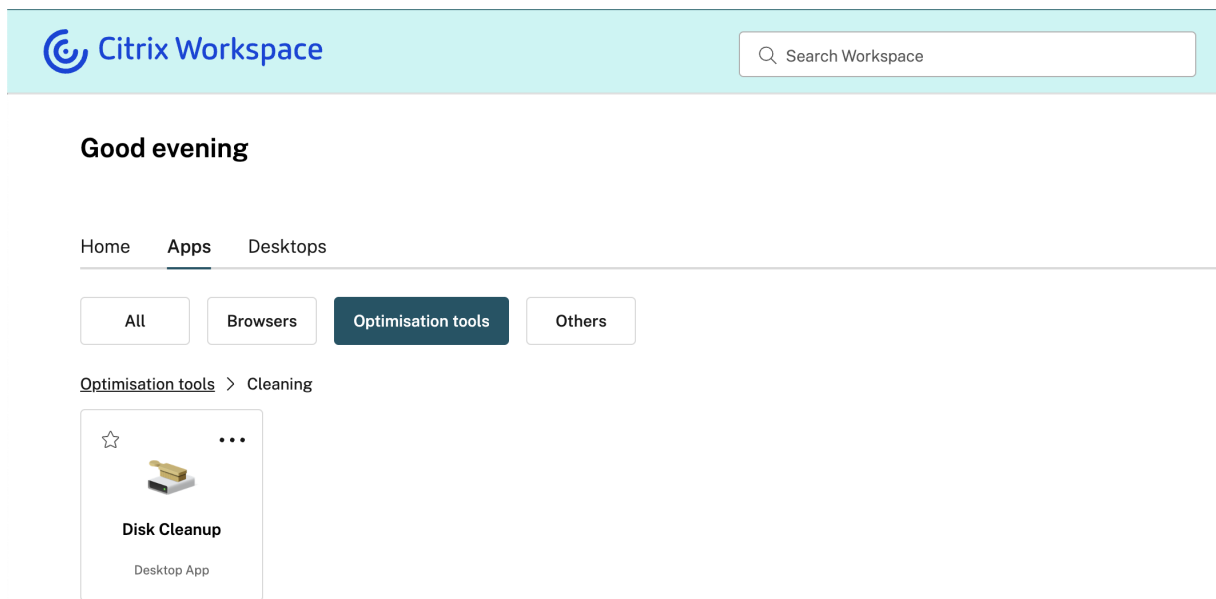
Wählen Sie die Kategorie aus. Eine Liste der verfügbaren Unterkategorien und Anwendungen wird gemäß der vom Administrator vorgenommenen Konfiguration angezeigt.



Ordnerpfad hinzufügen

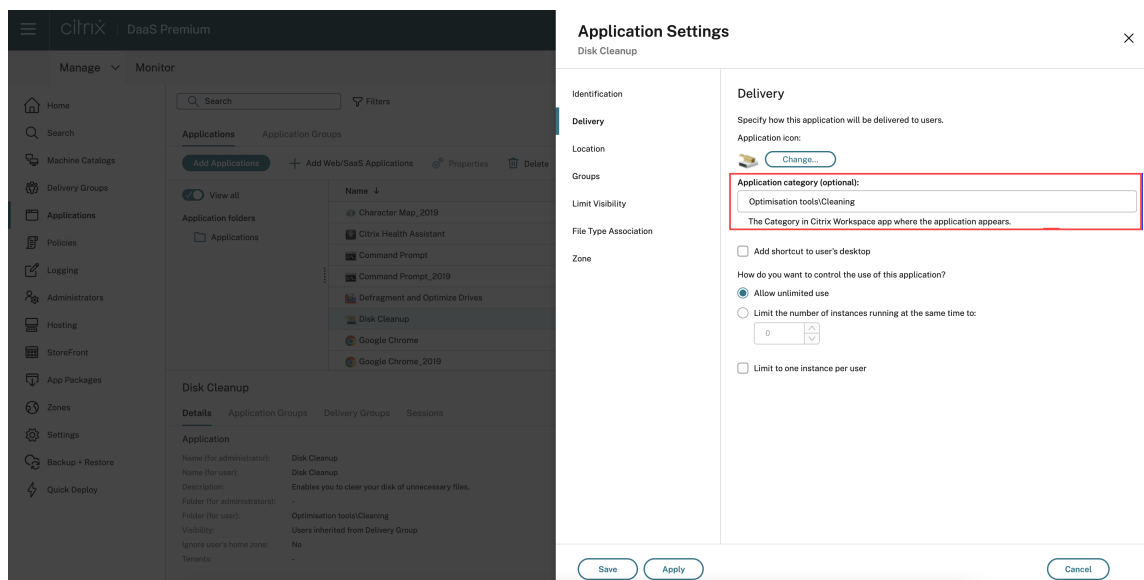
Der Ordnerpfad hilft Ihnen beim Definieren der Kategorien, unter denen eine App angezeigt wird. Er stellt die Ordnerstruktur dar, die Endbenutzern auf dem Bildschirm angezeigt wird.

Angenommen, Sie haben eine App, deren Ordner als **Optimisation tools/Cleaning** definiert ist. Zum Zugriff auf diese App müssen Endbenutzer "Optimisation tools > Cleaning" aufrufen, wobei "Optimisation tools" eine Kategorie und "Cleaning" die zugehörige Unterkategorie ist.



Ordnerpfad für eine Anwendung definieren:

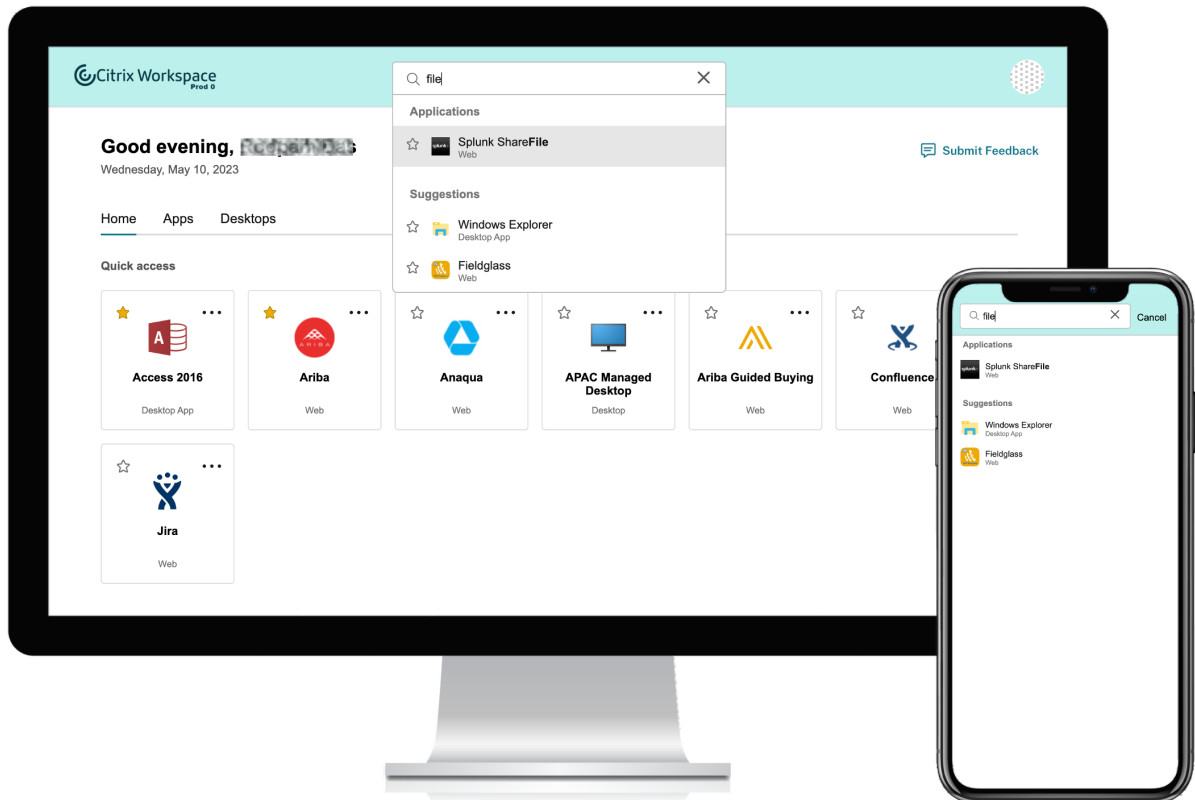
1. Navigieren Sie in der Admin-Cloud-Konsole zu **Citrix DaaS**.
2. Gehen Sie zu **Anwendungen** und suchen Sie die App.
3. Klicken Sie mit der rechten Maustaste auf die App und wählen Sie **Eigenschaften**.
4. Definieren Sie im Feld **Anwendungskategorie** den Ordnerpfad.



5. Klicken Sie auf **Speichern**.

Verbesserte Suchfunktion

Mit der verbesserten **Suchfunktion** erhalten Sie schnellere Ergebnisse in den Suchmaschinen. Die **Suchoption** wird in der Symbolleiste angezeigt und ermöglicht eine schnelle und intuitive Suche direkt in der Workspace-App.



Es gibt folgende Verbesserungen:

- Standardsuche zeigt die fünf zuletzt verwendeten Apps oder Desktops an
- Suche besitzt eine aktivierte Rechtschreibprüfung und zeigt automatisch vervollständigte Ergebnisse an
- Suchergebnisse enthalten Apps in virtuellen Sitzungen, basierend auf kürzlich aufgerufenen Apps, sowie Web- und SaaS-Apps
- Suche nach vom Administrator erstellten Kategorien durchführen
- **Favoriten** erscheinen in Suchergebnissen zuerst

Aktivitätsmanager

October 12, 2023

Der Aktivitätsmanager ist ein einfaches und leistungsstarkes Feature in Citrix Workspace, mit dem Benutzer ihre Ressourcen effektiv verwalten können. Er steigert die Produktivität, indem er schnelle Aktionen an aktiven Apps und Desktops von jedem Gerät aus ermöglicht. Die Benutzer können nahtlos mit ihren Sitzungen interagieren und nicht mehr benötigte Sitzungen beenden oder trennen, wodurch Ressourcen freigesetzt und die Leistung stets optimiert wird.

Im Aktivitätsmanager wird eine konsolidierte Liste der auf dem aktuellen Gerät und auf allen Remotegeräten mit aktiven Sitzungen aktiven Apps und Desktops angezeigt. Die Benutzer können diese Liste anzeigen, indem sie auf das Aktivitätsmanagersymbol klicken (neben dem Profilsymbol auf dem Desktop, auf Mobilgeräten am unteren Bildschirmrand).

Hinweis:

Wenn das Aktivitätsmanager-Symbol in einem dunkleren Banner nicht zu sehen ist, können Sie evtl. die Einstellungen unter **Bannertext und Symbolfarbe** ändern. Das Symbol ist möglicherweise nicht aufgrund eines geringen Kontrasts zwischen dem Banner und dem Symbol undeutlich. Weitere Informationen finden Sie unter [Benutzerdefinierte Designs konfigurieren](#).

Aktivitätsmanager aktivieren

Als Administrator können Sie jetzt den Aktivitätsmanager für die Endbenutzer aktivieren oder deaktivieren. Je nach Ihren Unternehmensrichtlinien können Sie das Feature für alle oder für ausgewählte Benutzer und Benutzergruppen aktivieren.

Hinweis:

Der Aktivitätsmanager kann nur für die neue Benutzeroberfläche aktiviert werden. Weitere Informationen finden Sie unter [Neue Workspace-Benutzererfahrung aktivieren](#).

Aktivitätsmanager aktivieren:

1. Gehen Sie in der Administratorkonsole zu **Workspacekonfiguration > Anpassen > Funktionen**.
2. Aktivieren Sie im Bereich "Aktivitätsmanager" den Ein-/Ausschalter, um den Aktivitätsmanager zu aktivieren.
3. Anschließend können Sie die Zugriffsberechtigungen wie folgt anpassen.
 - Um den Aktivitätsmanager für alle Endbenutzer zu aktivieren, wählen Sie **Für alle aktivieren**.

New Activity Manager

Enabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Save **Preview**

- Um den Aktivitätsmanager für ausgewählte Benutzer und Benutzergruppen zu aktivieren, wählen Sie **Für ausgewählte Benutzer und Benutzergruppen aktivieren**. Sie können dann das Verzeichnis auswählen, zu dem die Benutzer oder Benutzergruppen gehören. Anschließend können Sie die relevanten Benutzer und Benutzergruppen anzeigen.

New Activity Manager

Enabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory Step 2: Select a user or group

cidblr.com Search users or user groups

Type	Display Name	Account Name ↑	
USER			🗑️
USER			🗑️

Save **Preview**

- Um den Aktivitätsmanager für alle Benutzer zu deaktivieren, deaktivieren Sie den Ein-/Ausschalter.

New Activity Manager

Disabled
Users can view running apps and desktops across multiple devices and manage active sessions independently with special session and power management controls. [Learn more](#)

Enable for everyone
 Enable for selected users and user groups

Assign Users and Groups

Step 1: Choose a directory Step 2: Select a user or group

cidblr.com Search users or user groups

Type	Display Name	Account Name ↑	
USER			🗑️
USER			🗑️

Save **Preview**

4. Klicken Sie auf **Speichern**.

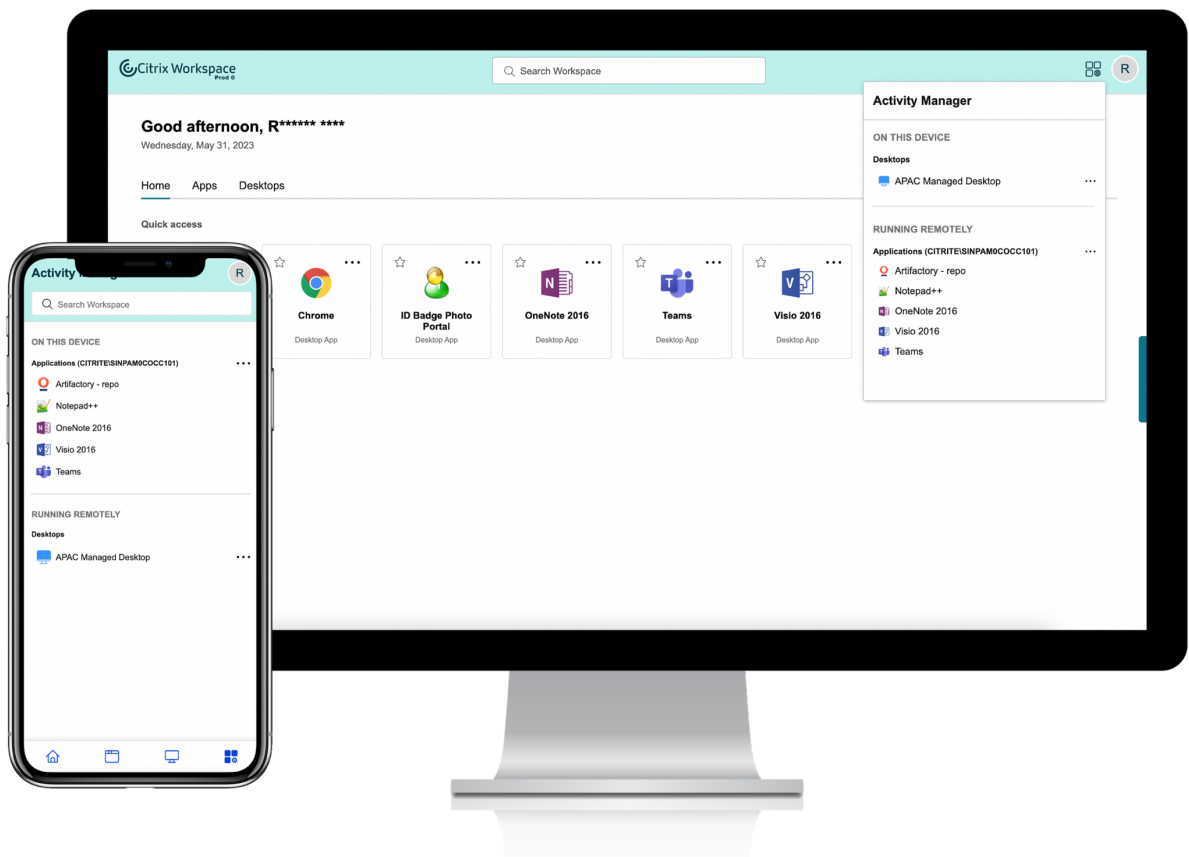
Hinweis:

Dieses Feature wird nur für virtuelle Apps und Desktops unterstützt. Es gilt nicht für Web- und SaaS-Anwendungen.

Aktivitätsmanager verwenden

Aktive Apps und Desktops werden im Aktivitätsmanager wie folgt gruppiert.

- Unter **Auf diesem Gerät** wird die Liste der Apps und Desktops angezeigt, die auf dem aktuell genutzten Gerät aktiv sind.
- Unter **Remote ausgeführt** wird die Liste der Apps und Desktops angezeigt, die auf anderen Geräten aktiv sind.

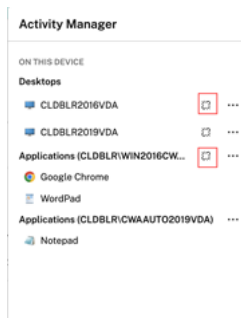


Die Benutzer können die folgenden Aktionen an einer App oder an einem Desktop ausführen, indem sie auf die zugehörige Menüschaltfläche (...) klicken.

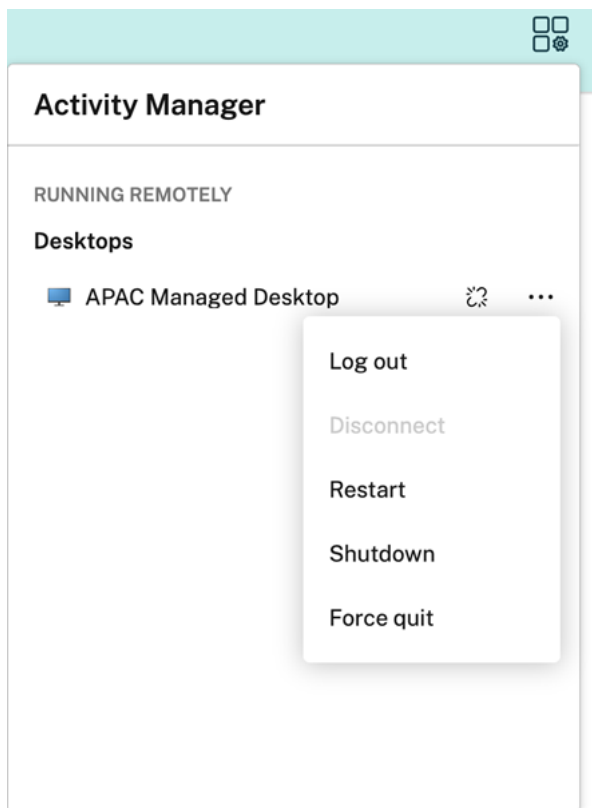
- **Verbindung trennen:** Die Remotesitzung wird getrennt, die Apps und Desktops sind jedoch weiter im Hintergrund aktiv.
- **Abmelden:** Zur Abmeldung von der aktuellen Sitzung. Alle Apps in den Sitzungen werden geschlossen, und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren:** Schließt die getrennten Desktops.
- **Beenden erzwingen:** Schaltet den Desktop bei einem technischen Problem aus.
- **Neu starten:** Fährt den Desktop herunter und startet ihn neu.

Getrennte Apps und Desktops

Mit dem Aktivitätsmanager können Endbenutzer jetzt Apps und Desktops, die im getrennten Modus ausgeführt werden, lokal oder remote anzeigen und Aktionen darauf ausführen. Sitzungen können von Mobil- oder Desktop-Geräten aus verwaltet werden, sodass Endbenutzer auch unterwegs Aktionen ausführen können. Das Ausführen von Aktionen an getrennten Sitzungen (z. B. Abmelden oder Herunterfahren) verbessert die Ressourcennutzung und reduziert den Energieverbrauch.



- Getrennte Apps und Desktops werden im Aktivitätsmanagerbereich angezeigt und sind mit einem Symbol einer getrennten Verbindung gekennzeichnet.
- Getrennte Apps sind nach zugehöriger Sitzung gruppiert, die Sitzungen sind mit einem Symbol einer getrennten Verbindung gekennzeichnet



Die Endbenutzer können an ihren getrennten Desktops die folgenden Aktionen über das Menü ausführen:

- **Abmelden:** zum Abmelden von dem getrennten Desktop. Alle Apps in der Sitzung werden geschlossen und alle nicht gespeicherten Dateien gehen verloren.
- **Herunterfahren:** zum Schließen der getrennten Desktops.
- **Ausschalten:** zum Ausschalten der getrennten Desktops im Falle eines technischen Problems.
- **Neu starten:** zum Herunterfahren und erneuten Starten des getrennten Desktops.

Bei getrennten Sitzungen bestehen folgende Unterschiede im Aktivitätsmanager.

- Wenn Sie in einem Browser bei Citrix Workspace angemeldet sind und eine lokale Sitzung trennen, wird die Sitzung zunächst unter "Auf diesem Gerät" angezeigt. Sobald Sie den Aktivitätsmanager schließen und erneut öffnen, wird die getrennte Sitzung jedoch unter "Remote ausgeführt" angezeigt.
- Wenn Sie über ein natives Gerät bei der Citrix Workspace-App angemeldet sind und eine lokale Sitzung trennen, verschwindet die Sitzung aus der Liste. Sobald Sie den Aktivitätsmanager schließen und erneut öffnen, wird die getrennte Sitzung jedoch unter "Remote ausgeführt" angezeigt.

Bereitstellen von DaaS und Virtual Apps and Desktops mit Citrix Workspace

October 12, 2023

Citrix Workspace ist ein Mehrmandanten-Cloudservice und ersetzt [StoreFront](#), einen on-premises bereitgestellten Einzelmandanten-App-Store zur Aggregation von Citrix DaaS-Apps und -Desktops. Die Citrix Workspace-Plattform ist die Cloud-Komponente, die die Tools, Dienste und Funktionen bereitstellt, die für den Remotezugriff und für das Erweitern und Anpassen von Aufgaben über Citrix Workspace erforderlich sind.

Sie haben verschiedene Möglichkeiten zur Aggregation von DaaS mit Citrix Workspace. Welche Option Sie wählen, hängt von folgenden Faktoren ab:

- Planen Sie eine vollständige Migration in die Cloud oder eine Hybridlösung?
- Möchten Sie externen Zugriff auf DaaS erlauben?

Vollständige Migration in die Cloud

Wenn Sie Ihre On-Premises-Konfiguration in die Cloud migrieren, können Abonnenten über Workspace auf DaaS zugreifen. Hierfür verschieben Sie Ihre IT-verwaltete Infrastruktur in eine von Citrix verwaltete Umgebung. Eine vollständige Migration in die Cloud bedeutet, dass Sie weniger Komponenten selbst verwalten müssen.

Citrix empfiehlt die Verwendung des [automatisierten Konfigurationstools \(ACT\)](#), das die Migration von einer oder mehreren On-Premises-Sites zu einem Cloudservice vereinfacht. Die wichtigsten Schritte dieses Prozesses sind:

1. Stellen Sie sicher, dass Sie die [Voraussetzungen für die Migration Ihrer Konfiguration](#) erfüllen.
2. Exportieren Sie Ihre On-Premises-Konfiguration. Informationen zu diesem Verfahren finden Sie unter [Exportieren der On-Premises-Konfiguration von Citrix Virtual Apps and Desktops](#).
3. Importieren Sie Ihre Konfiguration in die Cloud. Informationen zu diesem Verfahren finden Sie unter [Importieren der Konfiguration in Citrix DaaS](#).

Weitere Informationen zur automatisierten Konfiguration finden Sie unter [Migrieren in die Cloud](#) und in der [Anleitung in der Tech Zone](#).

Siteaggregation für Hybridlösungen

Sie können mit Ihrer vorhandenen On-Premises-Bereitstellung von Virtual Apps and Desktops zu Citrix Workspace wechseln. Dieser Vorgang wird als Siteaggregation bezeichnet. Dabei wird Ihre IT-verwaltete Infrastruktur durch eine von Citrix verwaltete Infrastruktur ersetzt.

Sie können eine Siteaggregation wählen, um schrittweise zu Workspace zu wechseln oder weil Sie eine Hybridlösung suchen, die nur einige Komponenten in der Cloud hostet. Beim Hybridmodell können Sie Cloudkapazität neben On-Premises-Ressourcen verwalten und Endbenutzern eine einheitliche Erfahrung bieten, ohne vollständig in die Cloud zu wechseln.

Bevor Sie mit der Siteaggregation von StoreFront zu Workspace wechseln, müssen Sie Active Directory (AD) konfigurieren und Cloud Connectors an Ihren Ressourcenstandorten installieren.

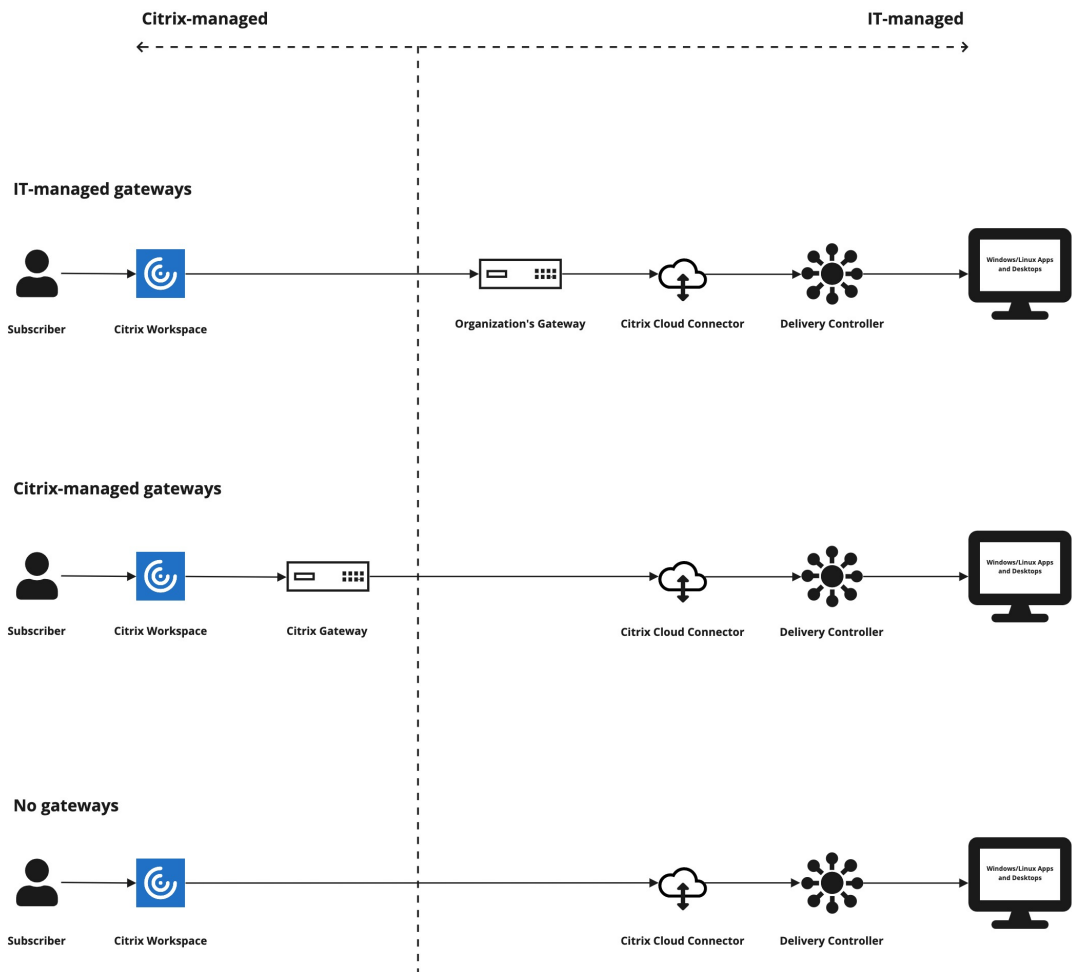
Die Siteaggregation umfasst drei Hauptschritte:

1. **Discovery der Site.** Eine Site umfasst alle Komponenten einer Produktionsbereitstellung. Möglicherweise haben Sie unterschiedliche Sites für einzelne Standorte und Zweigstellen.
2. **Verifizieren der Active Directory-Verbindung.** Abonnenten müssen sich mit AD bei Citrix Workspace authentifizieren. Stellen Sie sicher, dass Abonnenten sich authentifizieren können, indem die AD-Domänen erkannt werden, in denen Ihre Cloud Connectors installiert sind.
3. **Auswahl des Bereitstellungstyps.** Für diesen Schritt gibt es drei Konnektivitätsoptionen:
 - IT-verwaltete Gateways
 - Von Citrix verwaltete Gateways
 - Kein Gateway

Weitere Informationen finden Sie unter [Konnektivitätsoptionen](#).

Konnektivitätsoptionen

Die folgenden drei Optionen bieten Zugriff auf DaaS über Citrix Workspace, angepasst an verschiedene Geschäftsanforderungen.



Konnektivitätsoption

Szenario

Traditionelle (IT-verwaltete) Gateways

Wählen Sie diese Option, um Ihr eigenes Gateway für externe Verbindungen zu DaaS zu verwenden. Auf diese Weise können Sie bereits vorhandene On-Premises-Gateways nutzen.

Von Citrix verwaltete Gateways

Wählen Sie diese Option, um **Citrix Gateway Service** für externe Verbindungen zu virtuellen Apps und Desktops zu verwenden. **Citrix Gateway Service** dient dann als Proxyserver für HDX-Verbindungen zwischen Clients und VDAs.

Konnektivitätsoption

Szenario

Kein Gateway (nur intern)

Wählen Sie diese Option, wenn DaaS von Abonnenten *nur* mithilfe von Clients im Unternehmensnetzwerk gestartet werden soll. Bei dieser Option haben Abonnenten keinen externen Zugriff auf DaaS.

Weitere Informationen zur Siteaggregation und zu den erforderlichen Schritten finden Sie unter [Aggregieren von on-premises bereitgestellten virtuellen Apps und Desktops in Workspaces](#).

Konfigurieren der Resilienz und Optimierung von Workspace

Informationen zur Verbesserung der Effizienz und Verfügbarkeit von DaaS über Citrix Workspace finden Sie unter [Optimierung von DaaS in Citrix Workspace](#). Citrix stellt Anweisungen zu folgenden Themen bereit:

- Optimieren der Konnektivität mit einer direkten Workloadverbindung.
- Sicherstellen der Servicekontinuität während eines Ausfalls zur Gewährleistung der resilienten Offline-Nutzung.
- Konfigurieren von Single Sign-On (SSO) für virtuelle Apps und Desktops mithilfe von Citrix FAS (Verbundauthentifizierungsdienst).

Zugriff auf Workspaces konfigurieren

November 27, 2023

Citrix empfiehlt, die neueste Version der Citrix Workspace-App für den Zugriff auf Workspaces zu verwenden. Die Citrix Workspace-App ersetzt Citrix Receiver. Der Zugriff auf Workspace ist auch über die aktuelle Version von Microsoft Edge, Google Chrome, Mozilla Firefox oder Apple Safari unter Verwendung der Workspace-URL möglich.

Dieser Artikel enthält eine Übersicht über die Schritte zur Konfiguration und Verwendung folgender Elemente:

- [Workspace-URL](#)
- [Citrix Workspace-App \(früher Citrix Receiver\)](#)
- Citrix Gateways oder Citrix Gateway Service für [externe Verbindungen](#)
- Identitätsanbieter für die [Authentifizierung bei Workspaces](#)

Übersicht

Abonnenten können über einen Browser mit der Workspace-URL oder über die auf ihren Geräten installierte Citrix Workspace-App auf Citrix Workspace zugreifen.

Die Workspace-URL ist anpassbar und standardmäßig aktiviert. Anweisungen zum Bearbeiten der Workspace-URL finden Sie unter [Workspace-URL](#) in diesem Artikel.

Die Citrix Workspace-App ersetzt Citrix Receiver als nativ installierte App für den Zugriff auf die Workspace-Benutzeroberfläche (UI). Informationen zur Citrix Workspace-App und zum Umstieg von Citrix Receiver finden Sie in diesem Artikel unter [Citrix Workspace-App \(ehemals Citrix Receiver\)](#).

Remote-Abonnenten erhalten externen Zugriff auf ihre Workspaces, wenn Sie externe Konnektivität mit Citrix Gateway oder Citrix Gateway Service konfigurieren. Informationen zum Aktivieren des Remotezugriffs auf Workspaces finden Sie in diesem Artikel unter [Externe Konnektivität](#).

Alternativ können Sie Citrix Workspace allein für interne Konnektivität verwenden oder StoreFront on-premises hosten. Für interne Konnektivität muss der Endpunkt eine direkte Verbindung mit der IP-Adresse des Virtual Delivery Agent (VDA) herstellen.

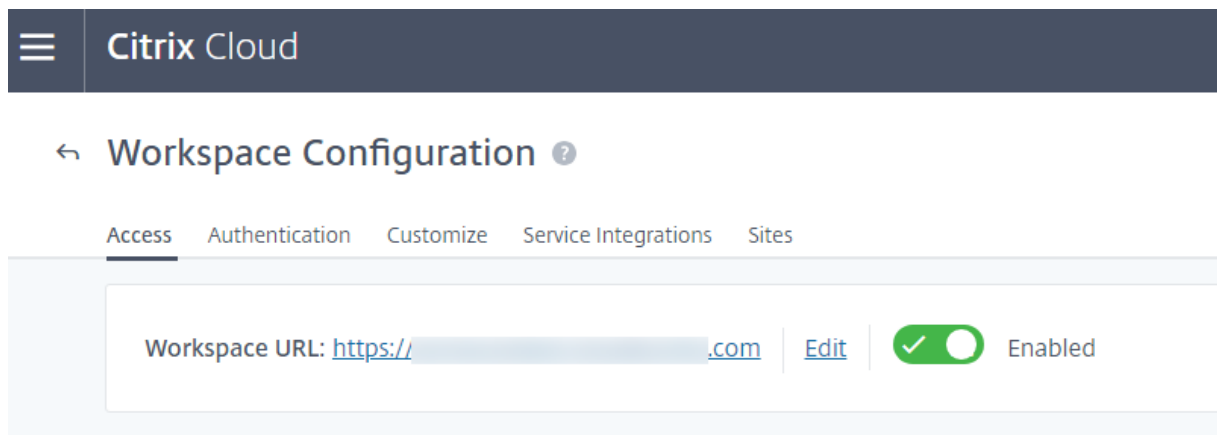
Citrix Workspace unterstützt eine wachsende Liste von Identitätsanbietern, die Sie mit Citrix Cloud verbinden und dann unter **Workspace-Konfiguration** aktivieren, um Abonnenten für ihre Workspaces zu authentifizieren. Informationen zum Konfigurieren der Authentifizierung für Workspace-Abonnenten finden Sie in diesem Artikel unter [Authentifizierung bei Workspaces](#).

Citrix Workspace unterstützt außerdem folgende Authentifizierungsoptionen:

- Token als zweiter Authentifizierungsfaktor zur Anmeldung bei Workspaces über Active Directory. Weitere Informationen zum Einrichten der Multifaktorauthentifizierung für Workspaces finden Sie unter [Zweistufige Authentifizierung](#).
- Citrix Verbundauthentifizierungsdienst (FAS) für Single Sign-On (SSO) für DaaS in Citrix Workspace. Informationen zum Einrichten von SSO mit FAS finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Workspace-URL

Die Workspace-URL ist einsatzbereit und in **Citrix Cloud > Workspace-Konfiguration > Zugriff**, wo Sie sie aktivieren, bearbeiten und deaktivieren können.



Anpassen der Workspace-URL

Der erste Teil der Workspace-URL ist anpassbar. Sie können die URL beispielsweise von `https://example.cloud.com` in `https://newexample.cloud.com` ändern.

Sie können die Workspace-URL nur ändern, wenn sie aktiviert ist. Wenn die URL deaktiviert ist, müssen Sie sie zuerst aktivieren.

Um die Workspace-URL zu aktivieren, gehen Sie zu **Workspace-Konfiguration > Zugriff** und aktivieren Sie die Umschaltfläche. Die erneute Aktivierung der Workspace-URL kann bis zu 10 Minuten dauern.

Der erste Teil der Workspace-URL stellt die Organisation dar, die das Citrix Cloud-Konto verwendet, und muss der [Endbenutzervereinbarung der Cloud Software Group](#) entsprechen. Jeglicher Missbrauch der geistigen Eigentumsrechte von Dritten, einschließlich Marken, kann zum Widerruf und zur Neuzuweisung der URL oder zur Sperrung des Citrix Cloud-Kontos führen.

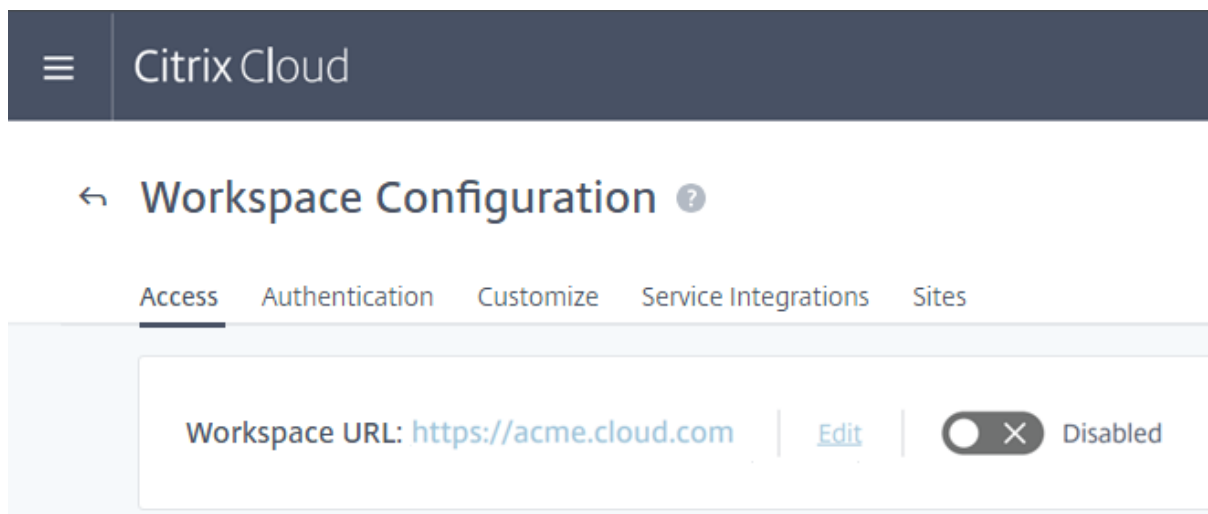
Um die URL anzupassen, gehen Sie zu **Workspace-Konfiguration > Zugriff** und wählen Sie **Bearbeiten**. Für den anpassbaren Teil der URL gilt:

- Er muss zwischen 6 und 63 Zeichen lang sein. Wenn Sie den anpassbaren Teil der URL auf weniger als 6 Zeichen ändern möchten, erstellen Sie ein Ticket in Citrix Cloud.
- Nur Buchstaben und Zahlen sind zulässig.
- Unicode-Zeichen sind nicht zulässig.

Wenn Sie eine URL umbenennen, wird die alte URL sofort entfernt und ist nicht mehr verfügbar. Teilen Sie Abonnenten die neue URL mit und aktualisieren Sie manuell alle lokalen Citrix Workspace-Apps, damit sie die neue URL verwenden.

Deaktivieren der Workspace-URL

Sie können die Workspace-URL deaktivieren, um zu verhindern, dass Benutzer sich über Citrix Workspace authentifizieren. Das ist beispielsweise dann der Fall, wenn Abonnenten für den Zugriff auf Ressourcen eine On-Premises-StoreFront-URL verwenden sollen oder wenn Sie den Zugriff während einer Wartung unterbinden möchten.



Das Deaktivieren der Workspace-URL kann bis zu 10 Minuten dauern.

Das Deaktivieren der Workspace-URL hat folgende Auswirkungen:

- Alle Serviceintegrationen sind deaktiviert. Abonnenten haben keinen Zugriff auf Daten und Anwendungen von Services in Citrix Workspace.
- Sie können die Workspace-URL nicht ändern. Sie müssen die URL erneut aktivieren, bevor Sie sie ändern können.
- Alle, die die URL besuchen, erhalten im Browser eine Meldung, dass der Workspace nicht gefunden werden kann oder dass Ressourcen nicht geladen werden können.

Citrix Workspace-App (ehemals Citrix Receiver)

Wichtig:

Citrix Receiver hat das Ende seines Lebenszyklus erreicht und wird nicht mehr unterstützt. Wenn Sie Citrix Receiver weiterhin verwenden, ist der technische Support auf die in [Lifecycle Milestones Definitions](#) beschriebenen Optionen beschränkt. Informationen zu Lebenszyklus-Meilensteinen für Citrix Receiver nach Plattform finden Sie unter [Lifecycle milestones for Citrix Workspace app and Citrix Receiver](#).

Die Citrix Workspace-App ist eine nativ installierte App für den Zugriff auf Workspaces, die Citrix Receiver ersetzt.

Unterstützte Authentifizierungsmethoden für Citrix Workspace-App

Die folgende Tabelle enthält die von der Citrix Workspace-App unterstützten Authentifizierungsmethoden. Die Tabelle enthält Authentifizierungsmethoden, die für bestimmte Versionen von Citrix Receiver relevant sind, welche von der Citrix Workspace-App ersetzt werden.

Citrix Workspace-App	Active Directory-Authentifizierung	Active Directory plus Token-Authentifizierung	Azure Active Directory-Authentifizierung
Citrix Workspace für Windows	Ja	Ja	Ja (Workspace-App; Receiver 4.9 LTSR CU2 und höher; Receiver 4.11 CR und höher)
Citrix Workspace für Linux	Ja	Ja	Ja (Workspace-App; Receiver 13.8 und höher)
Citrix Workspace für Mac	Ja	Ja	Ja
Citrix Workspace für iOS	Ja	Ja	Ja
Citrix Workspace für Android	Ja	Ja	Ja (Workspace-App; Receiver 3.13 und höher)

Weitere Informationen zu den von der Citrix Workspace-App unterstützten Features nach Plattform finden Sie in der [Citrix Workspace-App-Feature-Matrix](#).

Eine Übersicht über die Unterstützung von TLS und SHA2 mit Citrix Receivern finden Sie unter [CTX23226](#).

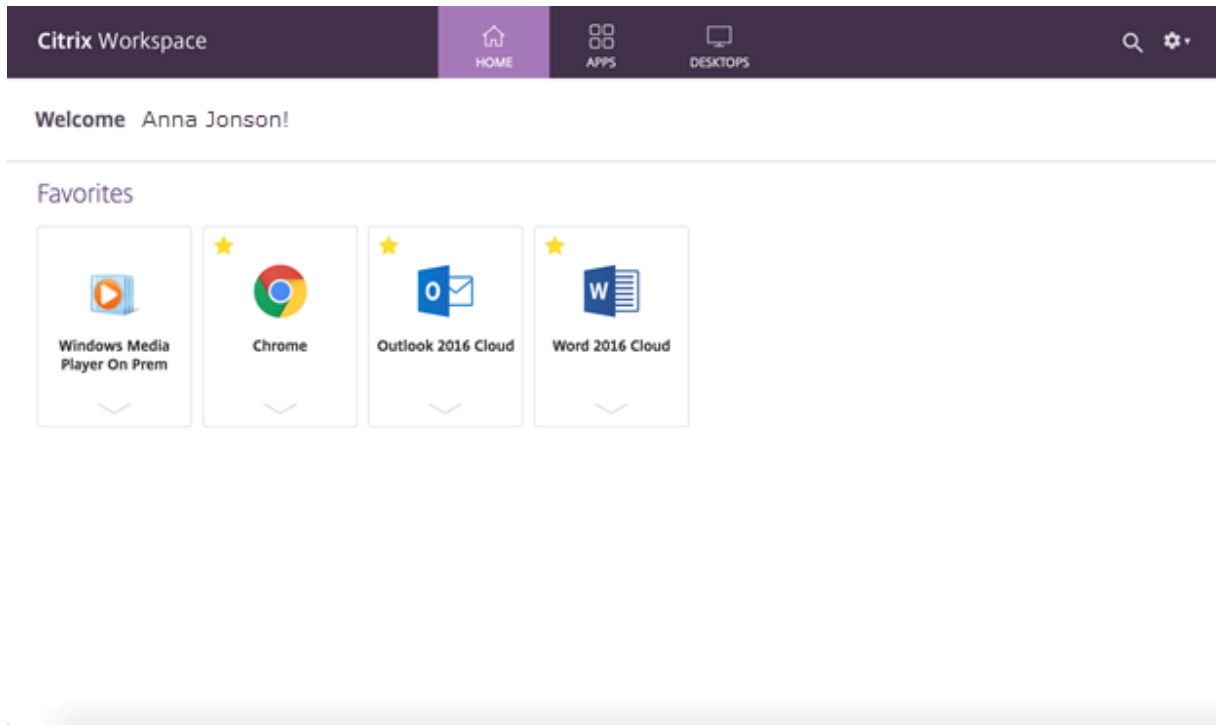
Wechsel von Citrix Receiver zur Citrix Workspace-App

Die Citrix Workspace-App ersetzt und erweitert sämtliche Funktionen von Citrix Receiver.

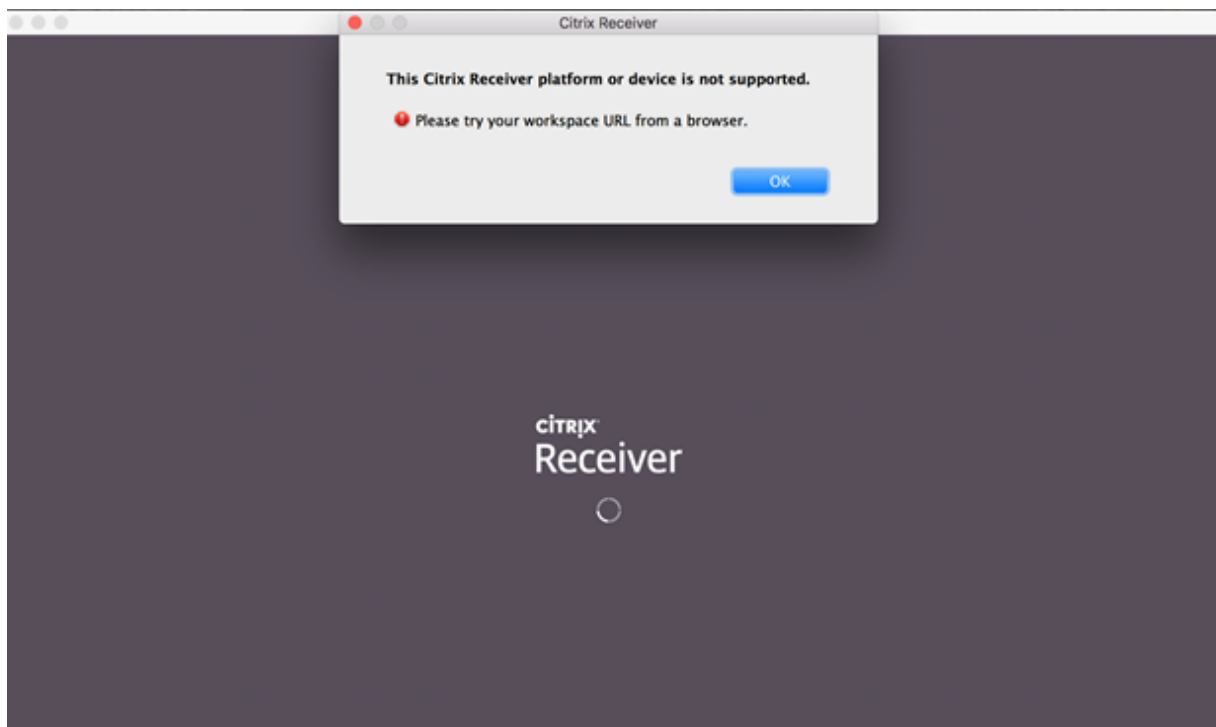
Die Citrix Workspace-App bietet Zugriff für Abonnenten auf SaaS-, Web- und virtuelle Apps per Single Sign-On (SSO). Weitere Informationen zum Single Sign-On für Workspace-Abonnenten finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Dieses Zugriffssteuerungsfeature wird in Citrix Receiver nicht unterstützt. Wenn daher dieselben Services und die Zugriffssteuerung aktiviert sind, sehen Citrix Receiver-Benutzer weiterhin die violette Be-

nutzeroberfläche, jedoch ohne Web- und SaaS-Apps. Darüber hinaus wird die Registerkarte **Dateien** in Citrix Receiver nicht unterstützt und Abonnenten können auf diese Weise nicht darauf zugreifen.



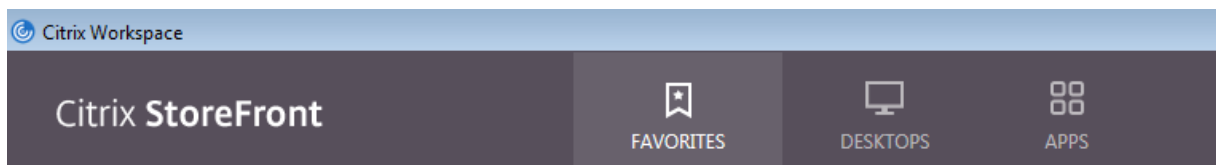
Auch Azure Active Directory (AAD) ist nicht mit Citrix Receiver kompatibel. Wenn Abonnenten versuchen, mit Citrix Receiver auf einen Workspace zuzugreifen, während AAD als Authentifizierungsmethode aktiviert ist, wird eine Meldung angezeigt, dass das Gerät nicht unterstützt wird. Nach dem Upgrade auf die Citrix Workspace-App können sie auf ihren Workspace zugreifen.



Für Kunden, die auf die Citrix Workspace-App aktualisieren (oder einen Webbrowser verwenden), wird die neue Benutzeroberfläche angezeigt. Weitere Informationen zur Verwendung der Benutzeroberfläche finden Sie unter [Verwalten der Workspace-Benutzeroberfläche](#).

Abgesehen von der neuen Benutzeroberfläche ermöglicht die Citrix Workspace-App Abonnenten, alle neuen Features zu verwenden, die Sie aktiviert haben. Die Abonnenten können über Citrix Gateway Service auf die Registerkarte **Dateien** zugreifen, DaaS anzeigen und auf Web- und SaaS-Apps zugreifen.

Wenn Sie eine StoreFront-On-Premises-Bereitstellung haben, wird beim Upgrade von Citrix Receiver auf die Citrix Workspace-App nur das Symbol zum Öffnen der Citrix Workspace-App geändert.



Hinweis:

Für [Citrix Cloud Government](#)-Benutzer wird weiterhin eine lila Benutzeroberfläche angezeigt, wenn sie die Citrix Workspace-App verwenden oder über einen Webbrowser auf Workspace zugreifen.

Externe Konnektivität

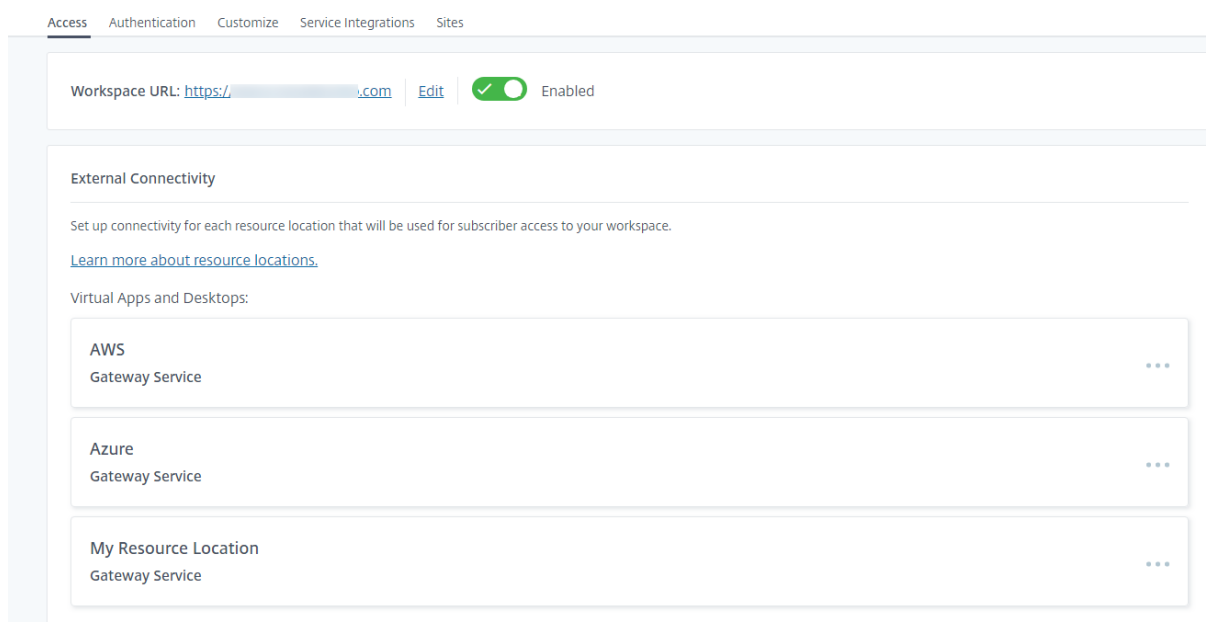
Bieten Sie Remote-Abonnenten sicheren Zugriff, indem Sie den Ressourcenstandorten Citrix Gateways oder den Citrix Gateway-Service hinzufügen.

Citrix unterstützt die folgenden Optionen für externe Konnektivität:

- Citrix hostet Citrix Gateway und Citrix ADC.
- Sie hosten Citrix Gateway und Citrix ADC on-premises.

Sie können Citrix Gateways über **Workspacekonfiguration > Zugriff > Externe Konnektivität** oder über **Citrix Cloud > Ressourcenstandorte** hinzufügen.

← Workspace Configuration ⓘ



Hinweis:

Der Abschnitt "Externe Konnektivität" unter **Workspacekonfiguration > Zugriff** ist in Citrix Virtual Apps Essentials nicht verfügbar. Der Citrix Virtual Apps Essentials Service verwendet den Citrix Gateway Service, für den keine zusätzliche Konfiguration erforderlich ist.

Authentifizierung bei Workspaces

Die Konfiguration der Workspaceauthentifizierung für Abonnenten erfolgt in zwei Schritten:

1. Definieren Sie einen oder mehrere Identitätsanbieter in **Identitäts- und Zugriffsverwaltung**. Anweisungen finden Sie unter [Identitäts- und Zugriffsverwaltung](#).

2. Wählen Sie unter **Workspacekonfiguration** einen der von Ihnen konfigurierten Identitätsanbieter als Authentifizierungsmethode aus, mit der Abonnenten sich bei ihren Workspaces anmelden. Anweisungen finden Sie unter [Auswählen und Ändern von Authentifizierungsmethoden](#).

Wenn Sie unter **Identitäts- und Zugriffsverwaltung** mehrere Identitätsanbieter konfigurieren, haben Sie unter **Workspacekonfiguration** mehr Auswahlmöglichkeiten, wie Abonnenten sich bei ihren Workspaces anmelden können.

Unterstützte Identitätsanbieter für die Authentifizierung von Abonnenten

Die Abonnenten können sich mit einer der folgenden Methoden bei ihren Workspaces authentifizieren:

- [Active Directory](#)
- [Active Directory plus Token](#)
- [Azure Active Directory](#)
- [Citrix Gateway](#)
- [Okta](#)
- [SAML 2.0](#)
- [Google](#)

Weitere Informationen zu unterstützten Methoden der Abonnentenauthentifizierung für Workspaces finden Sie unter [Sichere Workspaces](#).

Active Directory (AD) erfordert mindestens zwei Citrix Cloud Connectors in der on-premises bereitgestellten AD-Domäne. Informationen zum Citrix Cloud Connector finden Sie unter [Citrix Cloud Connector](#).

AD plus Token ist der standardmäßige Identitätsanbieter zur Authentifizierung von Abonnenten bei Workspaces. Abonnenten generieren Token als zweiten Authentifizierungsfaktor mit jeder App, die dem Standard [Zeitbasiertes Einmalkennwort \(TOTP\)](#) entspricht, z. B. Citrix SSO. Informationen zum Einrichten der tokenbasierten zweistufigen Authentifizierung finden Sie unter [Zweistufige Authentifizierung](#).

Ändern von Identitätsanbietern

Unter **Workspacekonfiguration** wählen Sie einen Identitätsanbieter als primäre Authentifizierungsmethode für Citrix Workspace aus. Der von Ihnen gewählte Identitätsanbieter muss zuerst unter **Identitäts- und Zugriffsverwaltung** konfiguriert werden. Wenn Sie den Identitätsanbieter unter **Workspacekonfiguration** ändern, hat dies keine Auswirkung auf die Identitätsanbieter, die von Ihnen unter **Identitäts- und Zugriffsverwaltung** konfiguriert wurden.

Das Konfigurieren von Identitätsanbietern unter **Identitäts- und Zugriffsverwaltung** ändert nicht die primäre Authentifizierungsmethode für die Anmeldung bei Citrix Workspace. Um die primäre Authentifizierungsmethode für die Anmeldung bei Citrix Workspace zu *ändern*, sind folgende Schritte erforderlich:

1. Konfigurieren Sie den neuen Identitätsanbieter unter **Identitäts- und Zugriffsverwaltung**.
2. Ändern Sie den Identitätsanbieter unter **Workspacekonfiguration**.

Sie können Ihre primäre Authentifizierungsmethode für Citrix Workspace konfigurieren und ändern, ohne Ihre Produktionsumgebung zu beeinträchtigen. Um den neuen Identitätsanbieter zu testen, können Sie entweder eine Citrix Cloud-Testorganisation erstellen oder unter **Workspacekonfiguration** einen Zeitplan festlegen, um die Authentifizierungsmethode zu ändern, wenn Abonnenten ihre Workspaces nicht verwenden.

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

Mit Single Sign-On (SSO) für sekundäre Ressourcen bietet Citrix Workspace Abonnenten nach der Anmeldung am Workspace ein nahtloses Benutzererlebnis. Im Verbund mit Citrix Gateway stellt Citrix Secure Private Access den Single Sign-On für SaaS- und Web-Apps als integrierten Bestandteil von Citrix Workspace bereit.

Neben den SSO-Funktionen können Sie mit Citrix Secure Private Access erweiterte Sicherheitsrichtlinien festlegen, einen kontextbezogenen Zugriff konfigurieren und Analysedaten sammeln. Weitere Informationen zu Citrix Secure Private Access finden Sie unter [Citrix Secure Private Access](#).

Single Sign-On (SSO) für DaaS

Neben SaaS- und Web-Apps bieten Active Directory (AD) sowie AD plus Token Single Sign-On für DaaS-Apps und -Desktops, nachdem Abonnenten sich am Workspace angemeldet haben.

Wenn Sie einen anderen Identitätsanbieter für die Anfangsauthentifizierung des Abonnenten bei Citrix Workspace auswählen, können Sie auch den Citrix Verbundauthentifizierungsdienst (FAS) installieren und konfigurieren. Mit FAS geben Abonnenten ihre Anmeldeinformationen nur einmal ein, um auf DaaS zuzugreifen, genau wie bei SaaS- und Web-Apps.

FAS wird normalerweise verwendet, wenn Sie einen der folgenden Identitätsanbieter für die Workspaceauthentifizierung verwenden:

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

Hinweis:

Je nach Konfiguration von Citrix Gateway ist FAS möglicherweise nicht erforderlich, um Single Sign-On für DaaS zu nutzen. Weitere Informationen zum Konfigurieren von Citrix Gateway finden Sie unter [Create an OAuth IdP policy on the on-premises Citrix Gateway](#).

Weitere Informationen zu FAS finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Weitere Informationen

- [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#)
- [Referenzarchitektur: Übersicht über die Architekturen des Verbundauthentifizierungsdiensts](#)
- [Tech Insight: Federated Authentication Service](#)

Benutzerdefinierte Domäne konfigurieren

November 27, 2023

Wenn Sie eine benutzerdefinierte Domäne für Ihren Workspace konfigurieren, können Sie eine Domäne Ihrer Wahl für den Zugriff auf Ihren Citrix Workspace-Store verwenden. Sie können dann diese Domäne anstelle der zugewiesenen cloud.com-Domäne für den Zugriff über einen Webbrowser oder über Citrix Workspace-Anwendungen verwenden.

Eine benutzerdefinierte Domäne kann nicht für andere Citrix Workspace-Kunden freigegeben werden. Jede benutzerdefinierte Domäne kann nur von diesem Kunden verwendet werden. Wählen Sie stets eine benutzerdefinierte Domäne, die Sie keinem anderen Kunden zuweisen möchten, es sei denn, Sie sind bereit, die benutzerdefinierte Domäne später zu entfernen.

Das Deaktivieren der Workspace-URL in Citrix Cloud deaktiviert nicht den Zugriff auf Citrix Workspace über die benutzerdefinierte Domäne. Um bei einer benutzerdefinierten Domäne den Zugriff auf Citrix Workspace zu deaktivieren, müssen Sie auch die benutzerdefinierte Domäne deaktivieren.

Unterstützte Szenarios

Szenarios	Unterstützt	Nicht unterstützt
Identitätsanbieter	AD (+Token), Azure AD, Citrix Gateway, Okta und SAML	Google
Ressourcentypen	Virtual Apps and Desktops	SaaS-Apps
Zugriffsmethoden	Browser (ohne Internet Explorer), Citrix Workspace-App für Windows, Mac, Linux und iOS-Apps	-
Verwendung	Workspace	Cloud Connector und Cloudadministratorkonsole

Unterschiede zur aktuellen benutzerdefinierten Workspace-URL

Wenn Sie bereits eine benutzerdefinierte Workspace-URL für Ihren Kunden aktiviert haben, wird Ihnen die folgende Ansicht angezeigt.

Sie können diese URL vorerst verwenden und mit den Schritten in diesem Dokument fortfahren, um eine andere benutzerdefinierte Workspace-URL zu integrieren. Diese Funktion ist zukünftig nicht mehr verfügbar.

Wenn Sie dieselbe URL verwenden möchten, entfernen Sie zunächst die vorherige benutzerdefinierte Workspace-URL und alle DNS-Einträge.

Voraussetzungen

- Sie können entweder eine neu registrierte Domäne oder eine bestehende Domäne wählen. Die Domäne muss im Format mit Unterdomäne (your.company.com) vorliegen. Die Verwendung einer Stammdomäne (company.com) wird von Citrix nicht unterstützt.
- Citrix empfiehlt, eine dedizierte Domäne als benutzerdefinierte Domäne für den Zugriff auf Citrix Workspace verwenden. Dann können Sie dies bei Bedarf problemlos ändern.
- Benutzerdefinierte Domänen dürfen keine Marken von Citrix enthalten. Eine Liste aller Citrix-Marken finden Sie [hier](#).
- Die von Ihnen gewählte Domäne muss im öffentlichen DNS konfiguriert sein. Alle CNAME-Datensatznamen und -werte in Ihrer Domänenkonfiguration müssen für Citrix auflösbar sein.

Hinweis:

Konfigurationen mit privatem DNS werden nicht unterstützt.

- Die Länge des Domännennamens darf 64 Zeichen nicht überschreiten.

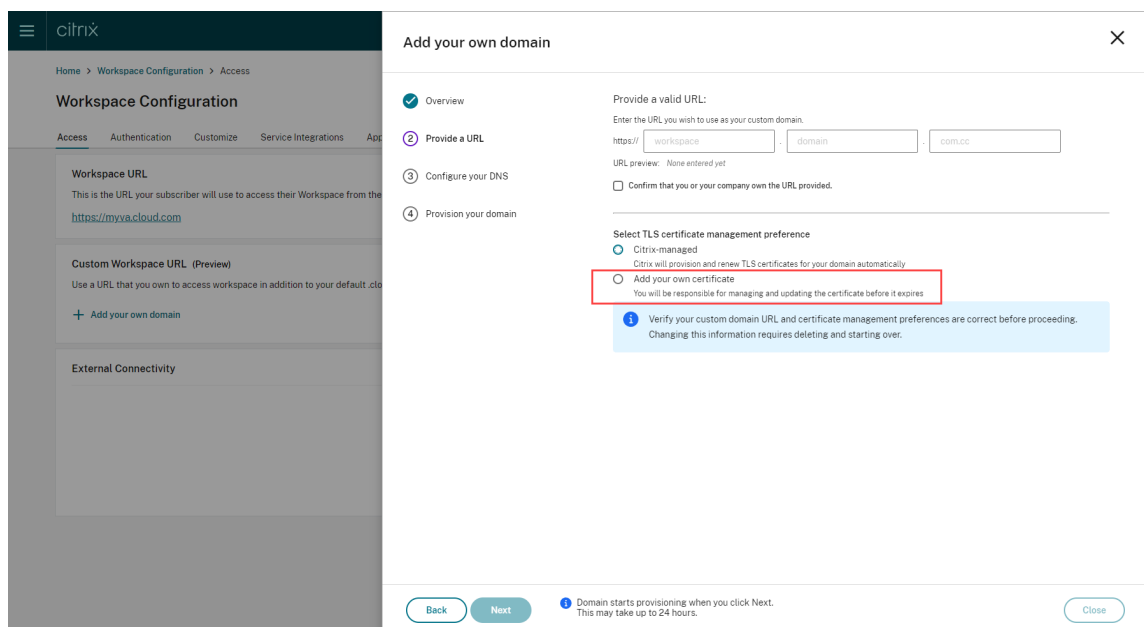
Benutzerdefinierte Domäne konfigurieren

Sobald eine benutzerdefinierte Domäne eingerichtet ist, können Sie die URL oder den Zertifikattyp nicht mehr ändern. Sie können sie nur löschen. Stellen Sie sicher, dass die gewählte Domäne nicht bereits in DNS konfiguriert ist. Entfernen Sie alle vorhandenen **CNAME**-Datensätze, bevor Sie versuchen, Ihre benutzerdefinierte Domain zu konfigurieren.

Wenn Sie mit SAML eine Verbindung zu Ihrem Identitätsanbieter herstellen, müssen Sie einen zusätzlichen Schritt zur SAML-Konfiguration ausführen. Weitere Informationen finden Sie unter [SAML](#).

Benutzerdefinierte Domäne hinzufügen

1. Melden Sie sich bei Citrix Cloud an unter <https://citrix.cloud.com>.
2. Wählen Sie im Citrix Cloud-Menü zunächst **Workspacekonfiguration** und dann **Zugriff**.
3. Wählen Sie auf der Registerkarte **Zugriff** unter **Benutzerdefinierte Workspace-URL** die Option **Fügen Sie Ihre eigene Domäne hinzu**.



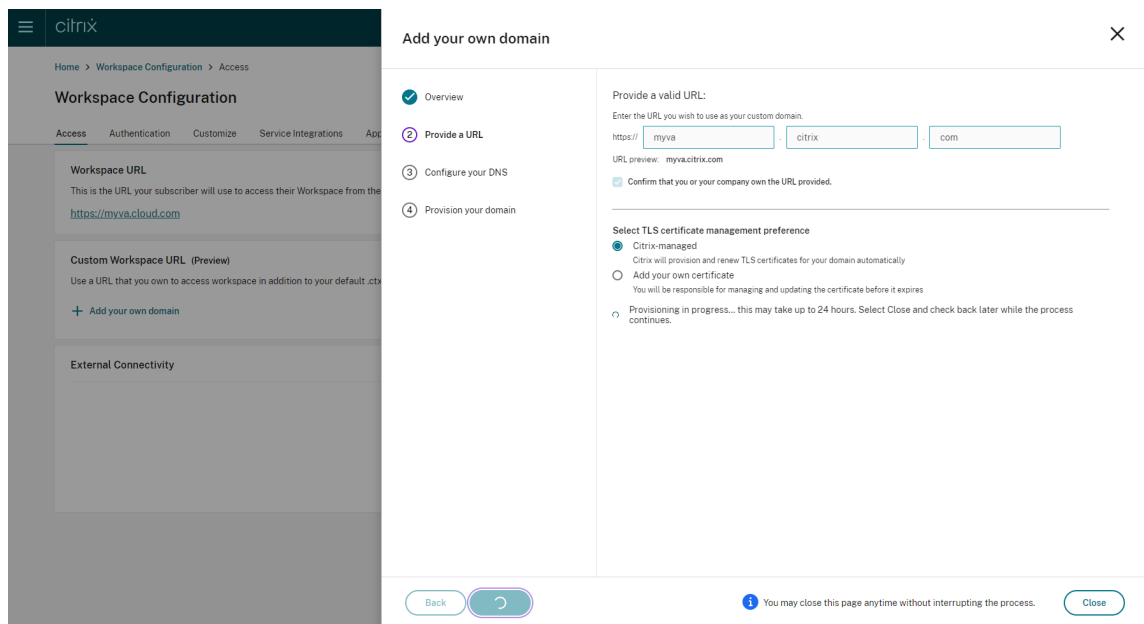
4. Lesen Sie die Informationen auf der Seite **Übersicht** und wählen Sie **Weiter**.

5. Geben Sie Ihre gewählte Domäne auf der Seite **URL angeben** ein. Aktivieren Sie **Bestätigen Sie, dass Sie oder Ihr Unternehmen Eigentümer der angegebenen URL sind**, um zu bestätigen, dass Ihnen die Domäne gehört, und wählen Sie die gewünschte TLS-Zertifikatsverwaltung. Citrix empfiehlt die Option mit Verwaltung, da die Zertifikatsverlängerungen für Sie erledigt werden. Weitere Informationen finden Sie unter **Verlängertes Zertifikat bereitstellen**. Klicken Sie auf **Weiter**.

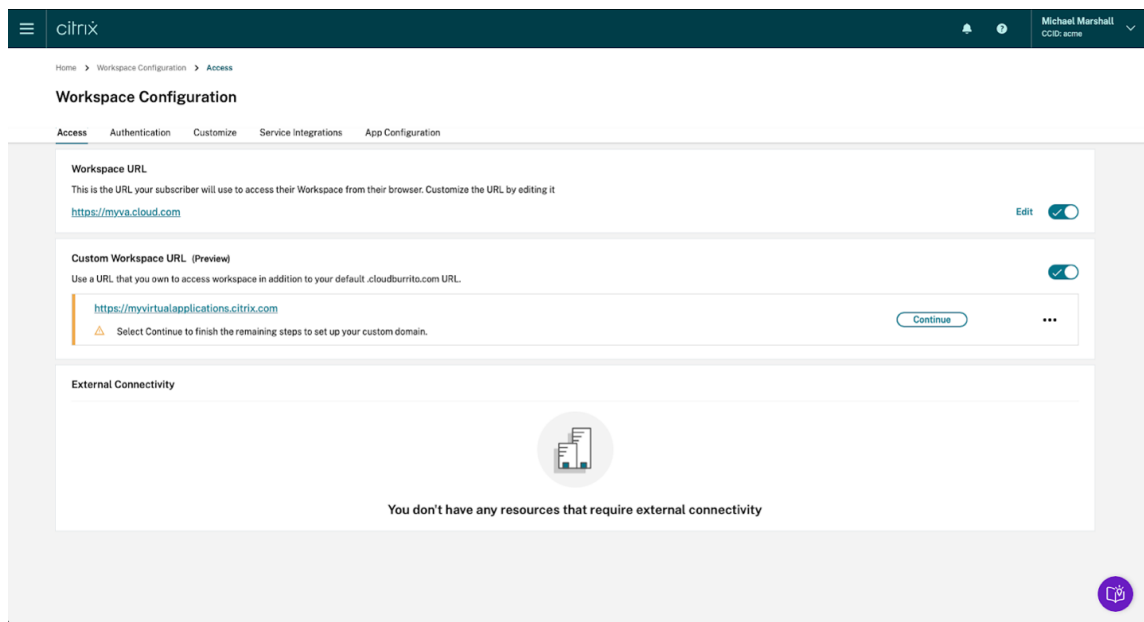
Wenn auf dieser Seite Warnungen angezeigt werden, beheben Sie zuerst das hervorgehobene Problem, bevor Sie fortfahren.

Wenn Sie ein eigenes Zertifikat bereitstellen, müssen Sie einen zusätzlichen Schritt ausführen.

Die Provisioning der von Ihnen ausgewählten Domäne kann etwas dauern. Sie können die Seite während des Provisionings offen lassen oder schließen.



6. Wenn beim Provisioning die Seite **URL angeben** geöffnet ist, wird automatisch die Seite **DNS konfigurieren** geöffnet. Wenn Sie die Seite geschlossen haben, klicken Sie auf der Registerkarte **Zugriff** für Ihre benutzerdefinierte Domäne auf **Weiter**.

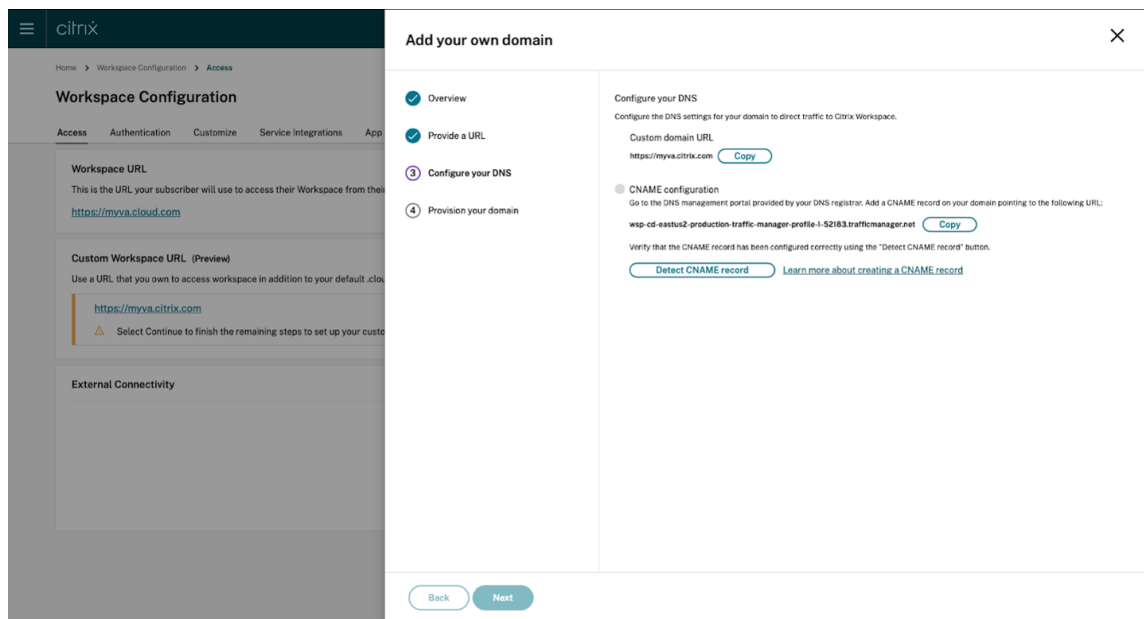


7. Führen Sie diesen Schritt im Verwaltungsportal durch, das vom DNS-Registral bereitgestellt wird. Fügen Sie Ihrer gewählten benutzerdefinierten Domäne einen **CNAME**-Eintrag hinzu, der auf den Ihnen zugewiesenen Azure Traffic Manager verweist.

Kopieren Sie die Adresse des Traffic Managers von der Seite **DNS konfigurieren**. Die Adresse im Beispiel lautet:

wsp-cd-eastus2-production-traffic-manager-profile-1-52183.trafficmanager.net

Wenn Sie im DNS CAA-Einträge (Certificate Authority Authorization) konfiguriert haben, fügen Sie einen Eintrag hinzu, mit dem *Let's Encrypt* Zertifikate für Ihre Domäne generieren kann. *Let's Encrypt* ist die Zertifizierungsstelle (ZS), mit der Citrix ein Zertifikat für Ihre benutzerdefinierte Domäne generiert. Der Wert für den CAA-Eintrag muss wie folgt lauten: *0 issue "letsencrypt.org"*

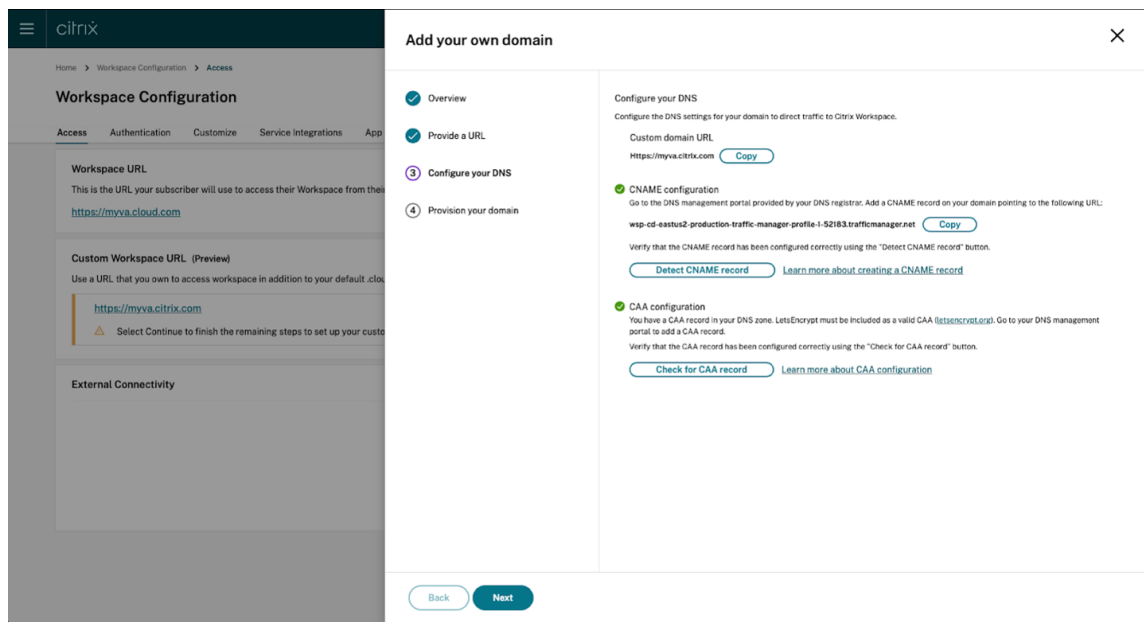


8. Nachdem Sie den CNAME-Eintrag beim DNS-Anbieter konfiguriert haben, wählen Sie **CNAME-Eintrag erkennen**, um Ihre DNS-Konfiguration zu überprüfen. Wenn der CNAME-Eintrag korrekt konfiguriert wurde, erscheint neben dem Abschnitt **CNAME-Konfiguration** ein grünes Häkchen.

Wenn auf dieser Seite Warnungen angezeigt werden, beheben Sie zuerst das hervorgehobene Problem, bevor Sie fortfahren.

Wenn Sie beim DNS-Anbieter CAA-Einträge konfiguriert haben, wird eine separate **CAA-Konfiguration** angezeigt. Wählen Sie **Auf CAA-Eintrag prüfen**, um Ihre DNS-Konfiguration zu überprüfen. Bei korrekter CAA-Datensatzkonfiguration wird neben dem Abschnitt **CAA-Konfiguration** ein grünes Häkchen angezeigt.

Wenn Ihre DNS-Konfiguration verifiziert ist, klicken Sie auf **Weiter**.

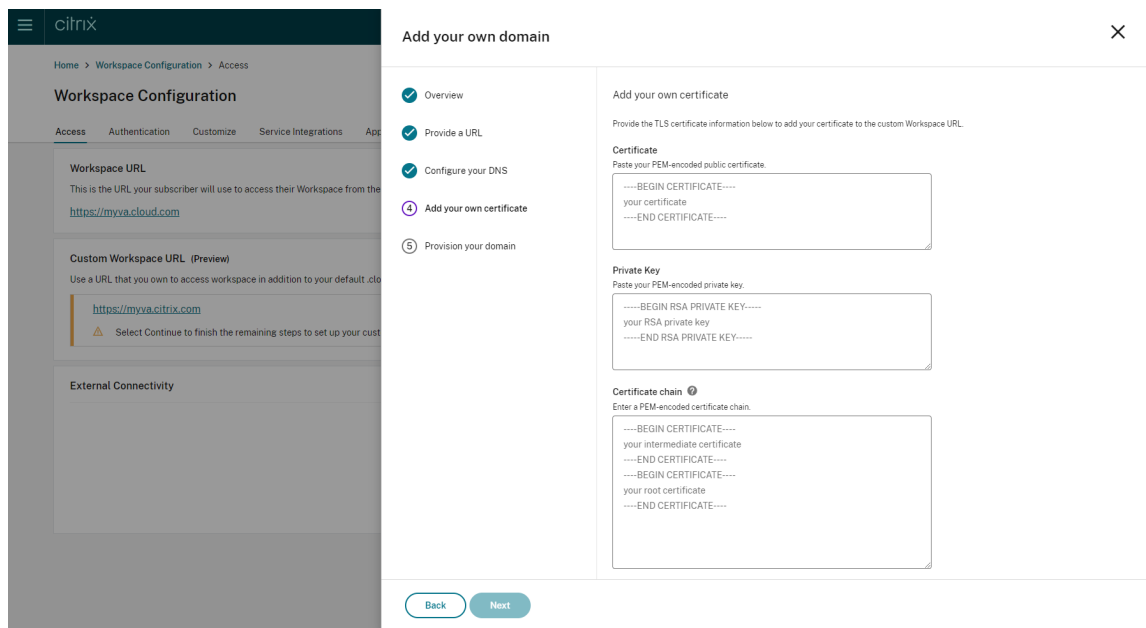


9. **Dieser Schritt ist optional.** Wenn Sie Ihr eigenes Zertifikat hinzufügen möchten, geben Sie die erforderlichen Informationen auf der Seite **Eigenes Zertifikat hinzufügen** ein.

Wenn auf dieser Seite Warnungen angezeigt werden, beheben Sie zuerst das hervorgehobene Problem, bevor Sie fortfahren.

Stellen Sie sicher, dass das Zertifikat die folgenden Bedingungen erfüllt.

- Es muss PEM-codiert sein.
- Es muss mindestens für die nächsten 30 Tage gültig bleiben.
- Es darf ausschließlich für benutzerdefinierte Workspace-URLs verwendet werden. Platzhalterzertifikate sind nicht zulässig.
- Der allgemeine Name des Zertifikats muss mit der benutzerdefinierten Domäne übereinstimmen.
- SANs auf dem Zertifikat müssen für die benutzerdefinierte Domain sein. Zusätzliche SANs sind nicht zulässig.
- Die Gültigkeitsdauer des Zertifikats darf 10 Jahre nicht überschreiten.



Hinweis:

Citrix empfiehlt, dass Sie ein Zertifikat mit einer sicheren kryptographischen Hashfunktion (SHA 256 oder höher) verwenden. Sie sind für die Verlängerung des Zertifikats verantwortlich. Wenn Ihr Zertifikat abgelaufen ist oder bald abläuft, konsultieren Sie den Abschnitt "Verlängertes Zertifikat bereitstellen".

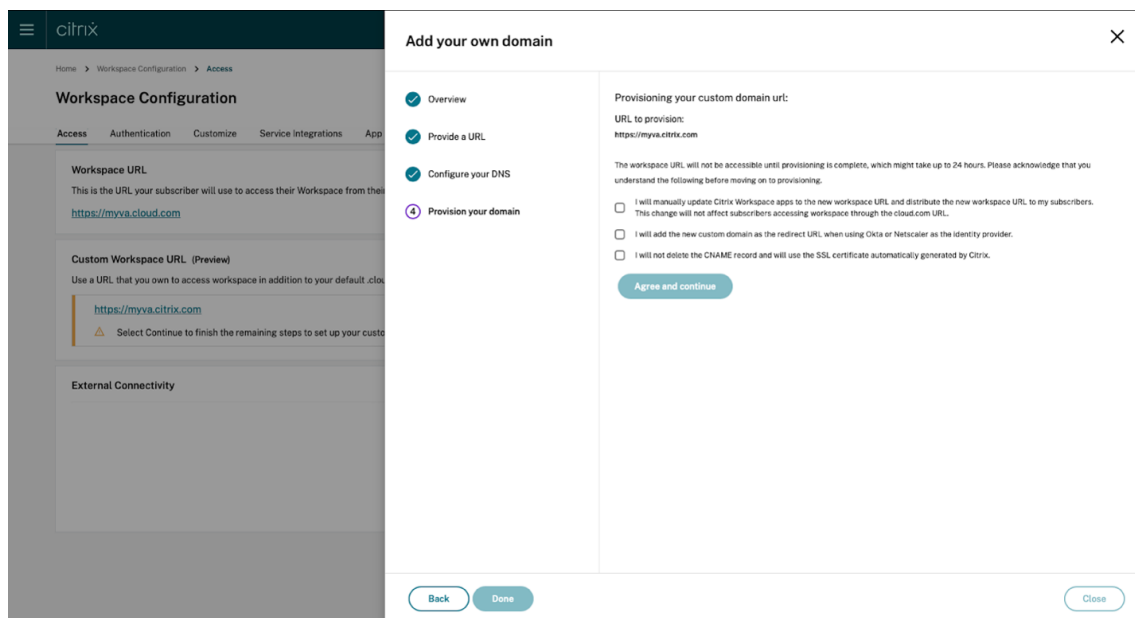
- Dieser Schritt ist optional.** Wenn Sie SAML als Identitätsanbieter verwenden, geben Sie die entsprechende Konfiguration an. Geben Sie die erforderlichen Daten auf der Seite **Für SAML konfigurieren** ein.

Verwenden Sie die folgenden Details, wenn Sie die Anwendung im Identitätsanbieter konfigurieren:

Eigenschaft	Value
Zielgruppe	<code>https://saml.cloud.com</code>
Empfänger	<code>https://<your custom domain>/saml/acs</code>
ACS-URL-Validator	<code>https://<your custom domain>/saml/acs</code>
ACS-Verbraucher-URL	<code>https://<your custom domain>/saml/acs</code>
Single-Logout-URL	<code>https://<your custom domain>/saml/logout/callback</code>

11. Lesen Sie die Informationen auf der Seite **Provisioning Ihrer Domäne durchführen** und bestätigen Sie die Anweisungen. Wenn Sie bereit sind fortzufahren, wählen Sie **Zustimmen und fortfahren**.

Dieser letzte Provisioningschritt kann einige Zeit in Anspruch nehmen. Sie können bei geöffneter Seite warten, bis der Vorgang abgeschlossen ist, oder die Seite schließen.



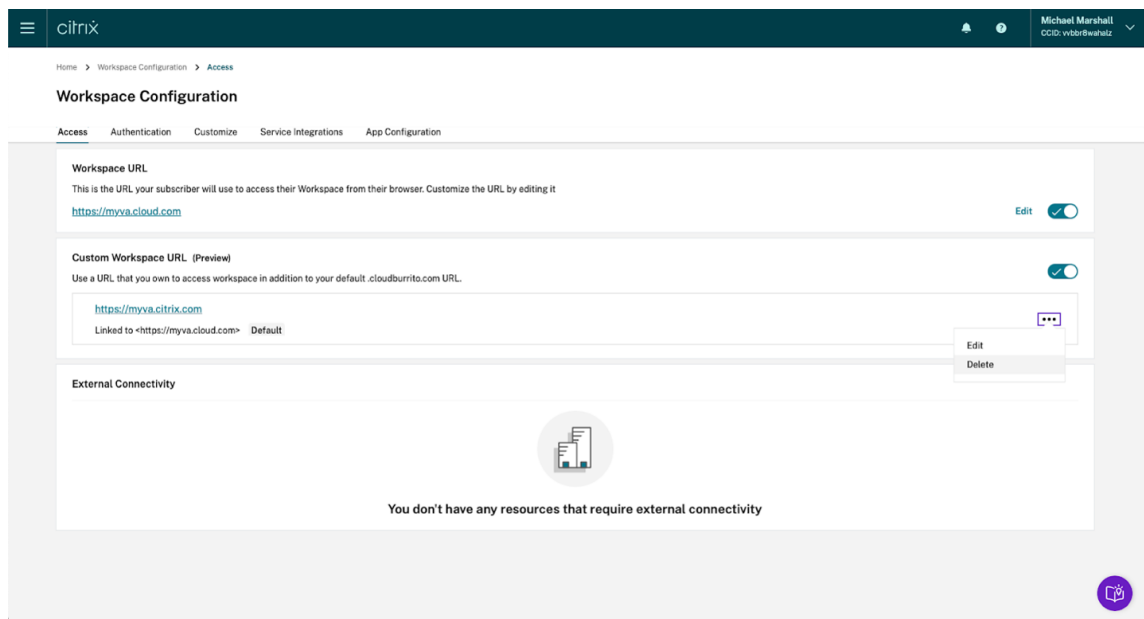
Benutzerdefinierte Domäne löschen

Wenn Sie eine benutzerdefinierte Domäne vom Kunden löschen, können Sie nicht mehr über eine benutzerdefinierte Domäne auf Citrix Workspace zugreifen. Nach dem Löschen der benutzerdefinierten Domäne können Sie nur über die cloud.com-Adresse auf Citrix Workspace zugreifen.

Wenn Sie eine benutzerdefinierte Domäne löschen, müssen Sie sicherstellen, dass der CNAME-Eintrag vom DNS-Anbieter entfernt wurde.

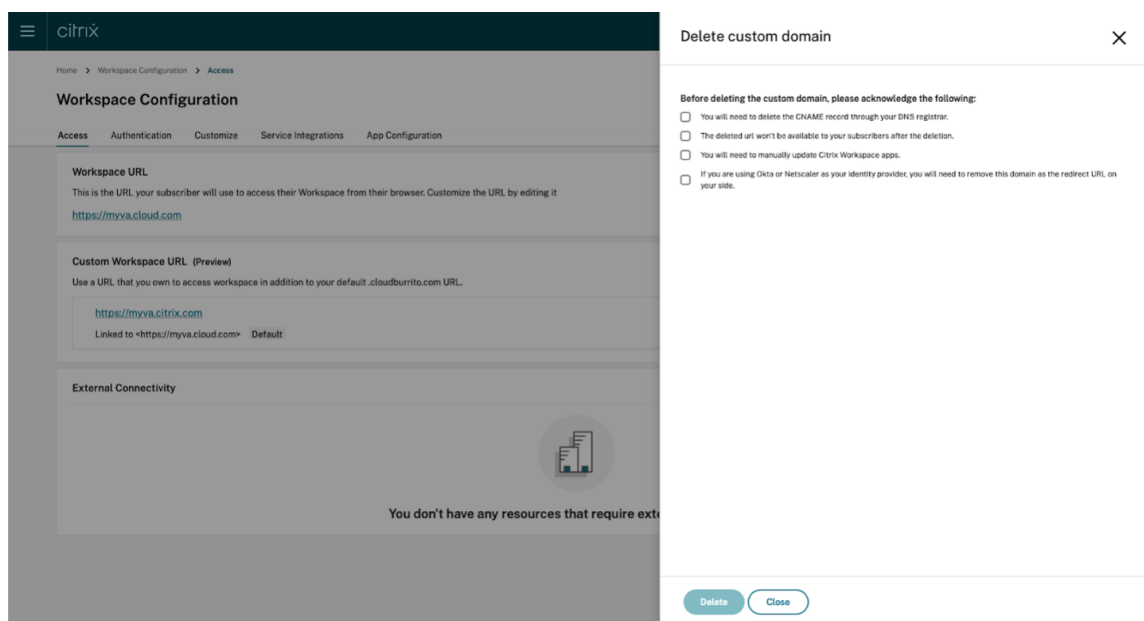
Schritte zum Löschen einer benutzerdefinierten Domäne:

1. Melden Sie sich bei Citrix Cloud an unter <https://citrix.cloud.com>.
2. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Zugriff**.
3. Erweitern Sie das Kontextmenü (...) für die benutzerdefinierte Domäne auf der Registerkarte **Zugriff** und wählen Sie **Löschen**.



4. Lesen Sie die Informationen auf der Seite **Benutzerdefinierte Domäne löschen**, und bestätigen Sie die vorliegenden Anweisungen. Wenn Sie bereit sind, wählen Sie **Löschen**.

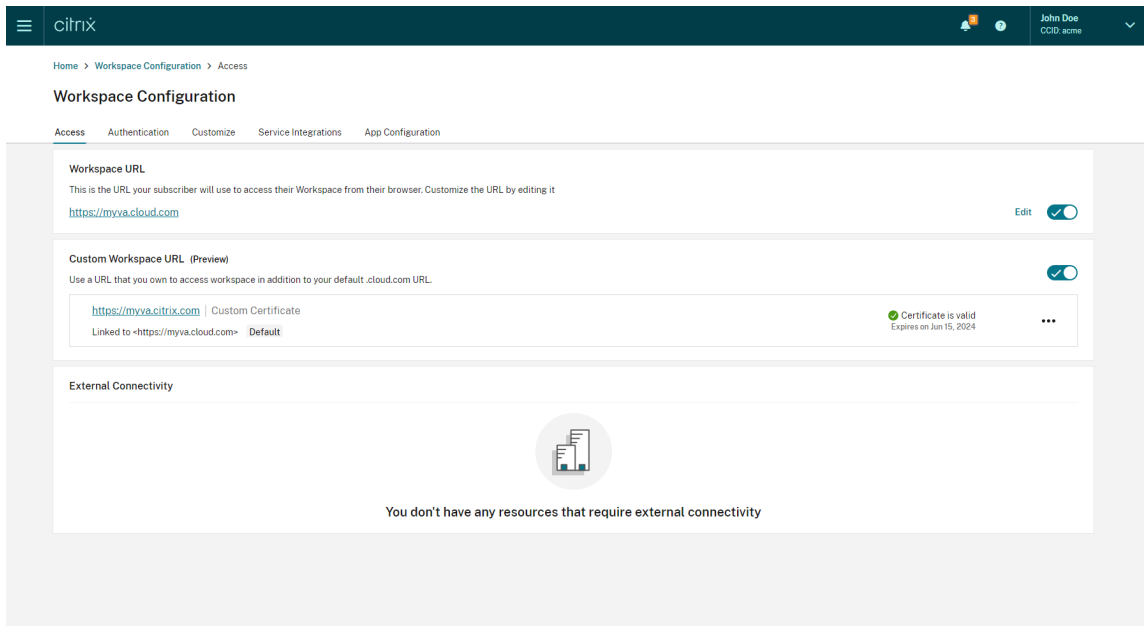
Das Löschen einer benutzerdefinierten Domäne nimmt einige Zeit in Anspruch. Sie können bei geöffneter Seite warten, bis der Vorgang abgeschlossen ist, oder die Seite schließen.



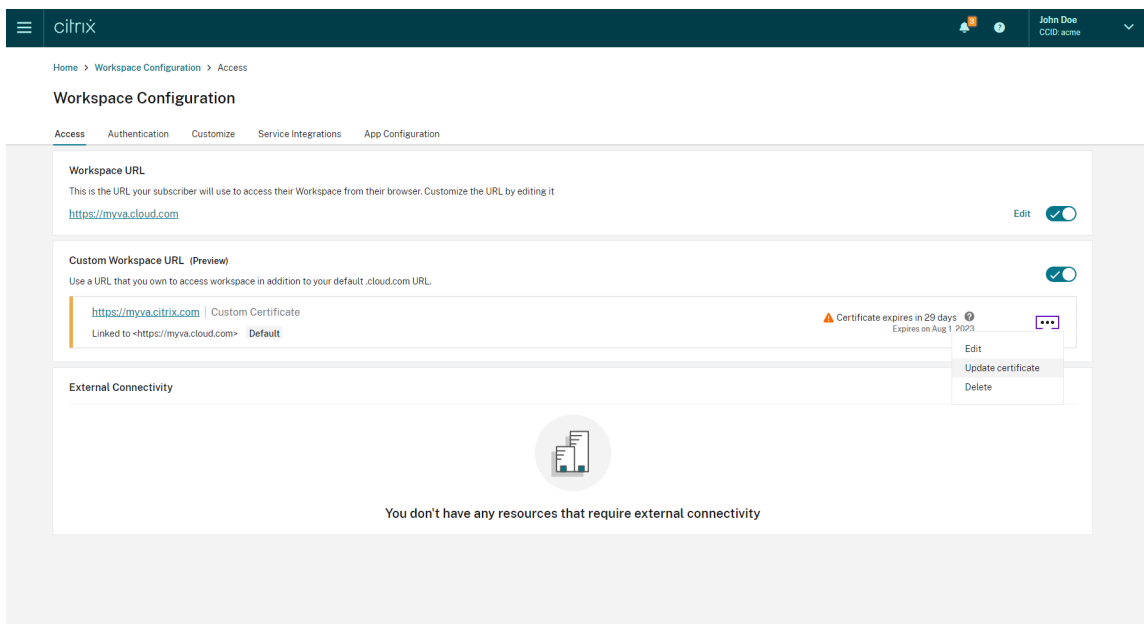
Verlängertes Zertifikat bereitstellen

1. Melden Sie sich bei [Citrix Cloud](#) an.
2. Wählen Sie im Citrix Cloud-Menü **Workspacekonfiguration > Zugriff**.

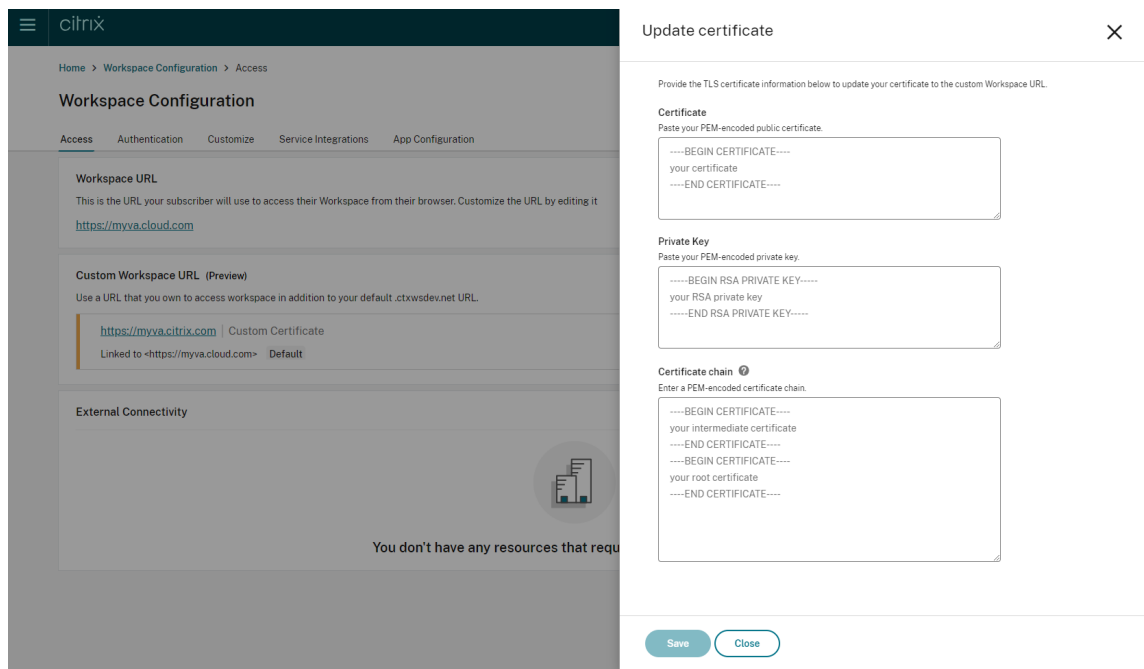
3. Das Ablaufdatum des Zertifikats wird neben der benutzerdefinierten Domäne angezeigt, der es zugewiesen ist.



Wenn Ihr Zertifikat in 30 Tagen oder weniger abläuft, wird für die benutzerdefinierte Domäne eine Warnung angezeigt.



4. Erweitern Sie das Kontextmenü (...) für die benutzerdefinierte Domäne auf der Registerkarte **Zugriff**. Wählen Sie **Zertifikat aktualisieren**.



5. Geben Sie die erforderlichen Informationen auf der Seite **Zertifikat aktualisieren** ein und klicken Sie auf **Speichern**.

Wenn auf dieser Seite Warnungen angezeigt werden, beheben Sie zuerst das hervorgehobene Problem, bevor Sie fortfahren.

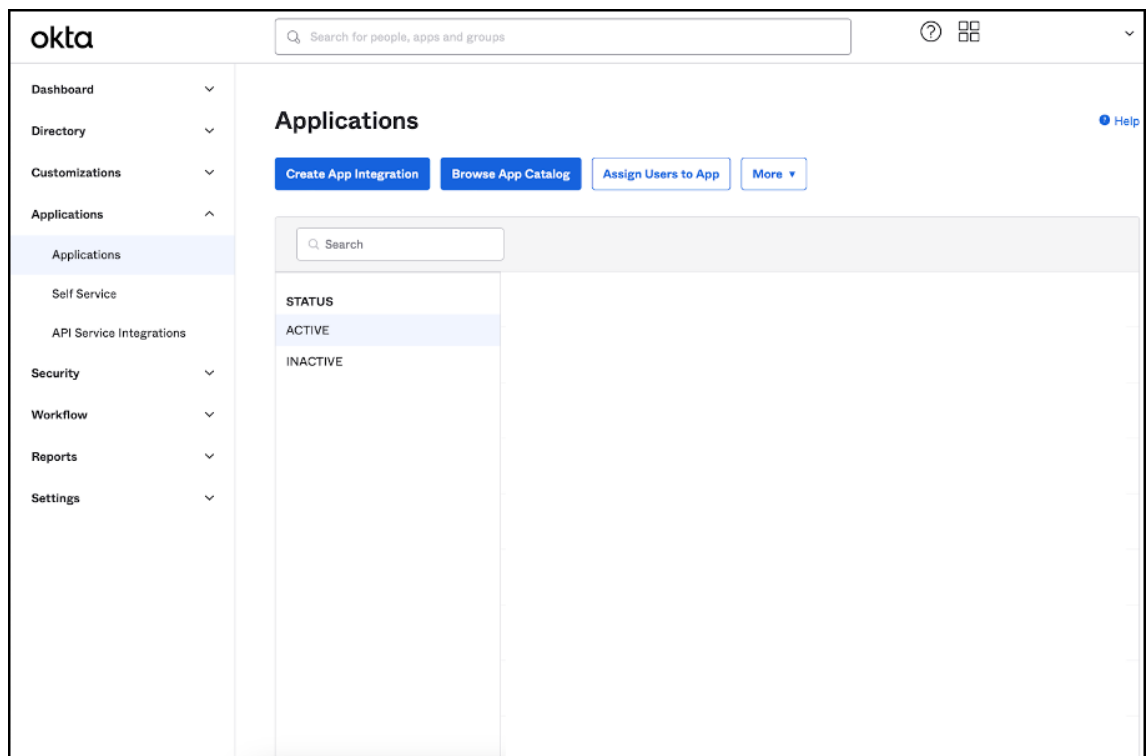
Das Zertifikat muss dieselben Anforderungen erfüllen wie bei der Erstellung der benutzerdefinierten Domäne (siehe [Benutzerdefinierte Domäne hinzufügen](#)).

Konfiguration Ihres Identitätsanbieters

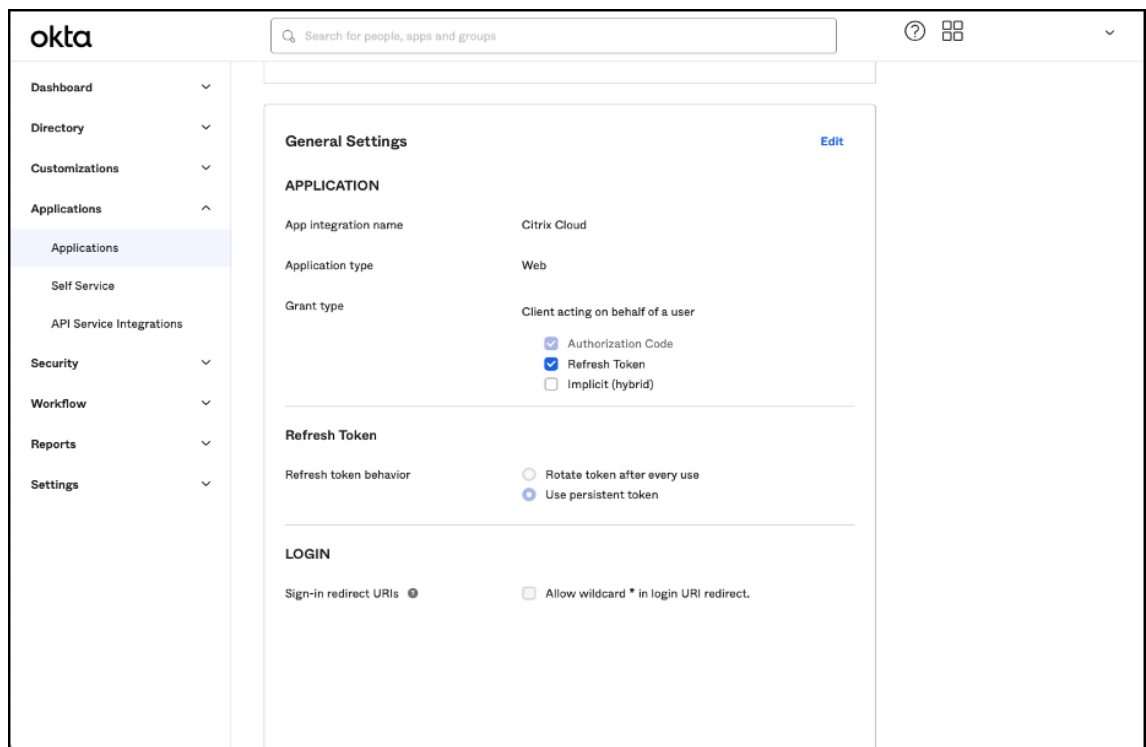
Okta konfigurieren

Führen Sie die folgenden Schritte aus, wenn Sie Okta als Identitätsanbieter für den Zugriff auf Citrix Workspace verwenden.

1. Melden Sie sich beim Administratorportal für Ihre Okta-Instanz an. Diese Instanz enthält die Anwendung, die von Citrix Cloud verwendet wird.
2. Erweitern Sie **Applications** und wählen Sie **Applications** im Menü.



3. Öffnen Sie die mit Citrix Cloud verknüpfte Anwendung.
4. Wählen Sie im Abschnitt **General Settings** die Option **Edit**.



5. Fügen Sie unter **General Settings** im Abschnitt **LOGIN** einen neuen Wert für **Sign-in redirect**

URIs hinzu. Fügen Sie den neuen Wert zusätzlich hinzu, ohne vorhandene Werte zu ersetzen. Der neue Wert muss das folgende Format haben: <https://your.company.com/core/login-okta>

- Fügen Sie in demselben Abschnitt einen neuen Wert für **Sign-out redirect URIs** hinzu. Fügen Sie den neuen Wert zusätzlich hinzu, ohne vorhandene Werte zu ersetzen. Der neue Wert muss das folgende Format haben: <https://your.company.com>

The screenshot shows the Okta application configuration interface. The left sidebar contains navigation options: Dashboard, Directory, Customizations, Applications, Self Service, API Service Integrations, Security, Workflow, Reports, and Settings. The main content area is titled 'Web' and includes the following sections:

- Application type:** Web
- Grant type:** Client acting on behalf of a user. Options: Authorization Code (checked), Refresh Token (checked), Implicit (hybrid) (unchecked).
- Refresh Token:** Refresh token behavior. Options: Rotate token after every use (unchecked), Use persistent token (checked).
- LOGIN:**
 - Sign-in redirect URIs:** Allow wildcard * in login URI redirect. (unchecked). Existing URIs: <https://accounts.cloud.com/core/login-okta> and <https://myva.citrix.com/core/login-okta>. A '+ Add URI' button is present.
 - Sign-out redirect URIs:** Existing URI: <https://myva.citrix.com>. A '+ Add URI' button is present.
 - Login initiated by:** App Only (selected in a dropdown menu).
 - Initiate login URI:** <https://accounts.cloud.com/core/login-okta>.

At the bottom right, there are 'Save' and 'Cancel' buttons.

- Klicken Sie zum Speichern der neuen Konfiguration auf **Speichern**.

Konfiguration von OAuth-Richtlinien und -Profilen

Wichtig

Die bestehende OAuth-Richtlinie und das OAuth-Profil, die Citrix Cloud mit Citrix Gateway oder dem Hochverfügbarkeitspaar für adaptive Authentifizierung verknüpft, dürfen nur bei Verlust der OAuth-Anmeldeinformationen aktualisiert werden. Wenn Sie diese Richtlinie ändern, kann dadurch die Verbindung zwischen Citrix Cloud und Workspaces unterbrochen werden. Dies kann Ihre Fähigkeit beeinträchtigen, sich bei Workspaces anzumelden.

Citrix Gateway konfigurieren

Der Citrix Cloud-Administrator hat Zugriff auf den unverschlüsselten geheimen Clientschlüssel. Diese Anmeldeinformationen werden von Citrix Cloud beim Verknüpfen mit Citrix Gateway unter **Identitäts- und Zugriffsverwaltung > Authentifizierung** bereitgestellt. OAuth-Profil und OAuth-Richtlinie wurden beim Herstellen der Verbindung manuell vom Citrix-Administrator auf dem Citrix Gateway erstellt.

Sie benötigen die Client-ID und den unverschlüsselten geheimen Clientschlüssel, die beim Verbinden mit Citrix Gateway bereitgestellt wurden. Diese Anmeldeinformationen werden von Citrix Cloud bereitgestellt und sind sicher gespeichert.

Der unverschlüsselte geheime Schlüssel wird benötigt, um über die Citrix ADC-Schnittstelle oder die Befehlszeilenschnittstelle (CLI) eine OAuth-Richtlinie und ein OAuth-Profil zu erstellen.

Dies ist ein Beispiel für die Benutzeroberfläche, wenn Client-ID und geheimer Schlüssel dem Citrix-Administrator zur Verfügung gestellt werden. Wenn der Citrix-Administrator die Anmeldeinformationen nicht beim Verbindungsprozess speichert, kann er keine Kopie des unverschlüsselten geheimen Schlüssels abrufen, nachdem die Verbindung zum Citrix Gateway hergestellt ist.

Create a connection with Citrix Gateway

Copy the Client ID and Secret and Redirect URL

Go to your On-Premises Citrix Gateway and input your ID, Secret, and URL to establish the connection. [Learn more](#)

When configuration is completed, test your Gateway connection to enable this identity provider.

Client ID: 3dc ecbd

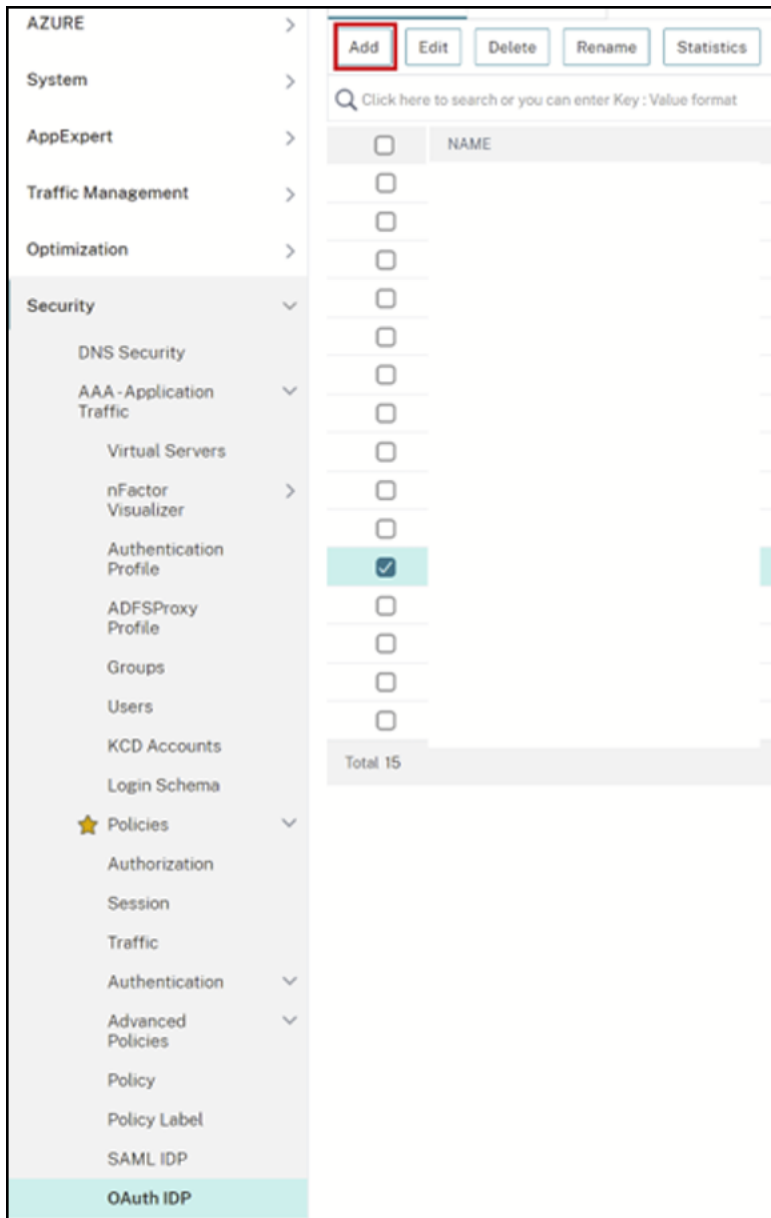
Secret: zGr rag==

Redirect URL: https://accounts.cloud .com
/core/login-cip

You will not have access to the client ID and secret later. You will have to generate a new pair if you lose track of the original. [Download](#) the key to save your ID and secret.

Verwendung von Citrix Cloud Führen Sie folgende Schritte aus, um mit der Citrix Gateway-Schnittstelle ein zusätzliches OAuth-Profil samt OAuth-Richtlinie hinzuzufügen:

1. Wählen Sie im Menü **Sicherheit > AAA —Anwendungsverkehr > OAuth IdP**. Wählen Sie die vorhandene OAuth-Richtlinie aus und klicken Sie auf **Hinzufügen**



2. Ändern Sie nach Aufforderung den Namen der neuen OAuth-Richtlinie. Er muss sich von der vorhandenen Richtlinie unterscheiden, die Sie im vorherigen Schritt ausgewählt haben. Citrix empfiehlt, *custom-url* zum Namen hinzuzufügen.

← Create Authentication OAuth IDP Policy

Name*
GatewayGateway-OAuthPol ⓘ

Action*
Add Edit

Log Action
Add Edit

Undefined-Result Action

Expression *
Select Select Select
true

3. Erstellen Sie in der Citrix Gateway-GUI Ihr vorhandenes OAuth-Profil.
4. Klicken Sie in demselben GUI-Menü neben **Aktion** auf **Hinzufügen**.

Create Authentication OAuth IDP Profile

Name*
 ⓘ

Client ID*
 ⓘ

Client Secret*
 ⓘ

Redirect URL*
 ⓘ

Issuer Name
 ⓘ

Audience
 ⓘ

Skew Time (mins)

Default Authentication Group

Relying Party Metadata URL

Refresh Interval

Encrypt Token ⓘ

Signature Service

Attributes

Send Password ⓘ

5. Binden Sie in der Citrix Gateway-GUI die neue OAuth-Richtlinie in den vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver ein.
6. Gehen Sie zu **Sicherheit > Virtuelle Server > Bearbeiten**.

PRIORITY	POLICY NAME	EXPRESSION	ACTION	GOTO EXPRESSION
10	OAuth	true	OAuthProfile	NEXT
20	~OAuth	true	OAuthProfile	NEXT

Verwendung der Befehlszeilenschnittstelle (CLI)

Wichtig

Wenn keine gespeicherte Kopie der OAuth-Anmeldeinformationen vorliegt, müssen Sie Ihr Citrix Gateway trennen und erneut verbinden und Ihr bestehendes OAuth-Profil mit neuen OAuth-Anmeldeinformationen aktualisieren, die von der Identitäts- und Zugriffsverwaltung von Citrix Cloud bereitgestellt werden. Aktualisieren Sie Ihr bestehendes OAuth-Profil nur dann mit neuen Anmeldeinformationen, wenn die alten Anmeldeinformationen nicht wiederhergestellt werden können. Dies wird nur dann empfohlen, wenn Sie keine andere Wahl haben.

1. Verwenden Sie ein SSH-Tool wie PuTTY, um sich mit Ihrer Citrix Gateway-Instanz zu verbinden.
2. Erstellen Sie OAuthProfile und OAuthPolicy. Fügen Sie OAuthIDPProfile Authentifizierung hinzu.

```
"CustomDomain-OAuthProfile"-clientID "<clientID>"-clientSecret "<unencrypted client secret>"-redirectURL "https://hostname.domain.com/core/login-cip"-audience "<clientID>"-sendPassword ON
add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule true -action "CustomDomain-OAuthProfile"
```

3. Binden Sie die OAuthPolicy in den zugehörigen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit weniger Priorität als die bestehende Richtlinie ein. Diese Instanz geht davon aus, dass die bestehende Richtlinie eine Priorität von 10 hat. Für die neue Richtlinie wird daher eine Priorität von 20 verwendet. Binden Sie den virtuellen Authentifizierungsserver ein.

```
"CitrixGatewayAAAvServer"-policy "CustomDomain-OAuthPol"-priority 20
```

Adaptive Authentifizierung konfigurieren

Wichtig

Das verschlüsselte Geheimnis und die Verschlüsselungsparameter für das OAuth-Profil unterscheiden sich auf den primären und sekundären Hochverfügbarkeitsgateways für die Adaptive Authentifizierung. Stellen Sie sicher, dass Sie das verschlüsselte Geheimnis vom primären Hochverfügbarkeitsgateway empfangen, und führen Sie diese Befehle auch auf dem primären HA-Gateway aus.

Der Citrix Cloud-Administrator hat keinen Zugriff auf den unverschlüsselten geheimen Clientschlüssel. OAuth-Richtlinie und OAuth-Profil werden beim Provisioning vom Citrix-Dienst "Adaptive Authentifizierung" erstellt. Es ist notwendig, beim Erstellen der OAuth-Profile das verschlüsselte Geheimnis und die CLI-Befehle aus der Datei ns.conf zu verwenden. Dies kann nicht mit der Citrix ADC-Benutzeroberfläche durchgeführt werden. Binden Sie die neue OAuthPolicy in den bestehenden virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver ein. Verwenden Sie dabei eine höhere Prioritätszahl als für die bestehende Richtlinie, die mit dem Server verbunden ist. Beachten Sie, dass niedrigere Prioritätszahlen zuerst ausgewertet werden. Legen Sie für die bestehende Richtlinie eine Priorität von 10 und für die neue Richtlinie eine Priorität von 20 fest, damit sie in der richtigen Reihenfolge ausgewertet werden.

1. Stellen Sie mithilfe eines SSH-Tools wie PuTTY eine Verbindung zum primären Knoten der Adaptiven Authentifizierung her.

```
show ha node
```

```
Done
> show ha node
1) Node ID: 0
   IP: 192.168.0.4 (adaptive-auth-1)
   Node State: UP
   Master State: Secondary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: SUCCESS
   Propagation: ENABLED
   Enabled Interfaces : 0/1
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : None
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
   Sync Status Strict Mode: DISABLED
   Hello Interval: 200 msec
   Dead Interval: 3 secs
   Node in this Master State for: 9:0:15:41 (days:hrs:min:sec)
2) Node ID: 1
   IP: 192.168.0.7
   Node State: UP
   Master State: Primary
   Fail-Safe Mode: OFF
   INC State: ENABLED
   Sync State: ENABLED
   Propagation: ENABLED
   Enabled Interfaces : 0/1
   Disabled Interfaces : None
   HA MON ON Interfaces : None
   HA HEARTBEAT OFF Interfaces : None
   Interfaces on which heartbeats are not seen : None
   Interfaces causing Partial Failure: None
   SSL Card Status: NOT PRESENT
Done
```

2. Suchen Sie in der ausgeführten Konfiguration des primären Hochverfügbarkeitsgateways nach

der Zeile, die Ihr vorhandenes OAuth-Profil enthält.

```
sh runn | grep oauth
```

3. Kopieren Sie die Ausgabe aus der Citrix ADC-Befehlszeilenschnittstelle (CLI), einschließlich aller Verschlüsselungsparameter.

```
> sh runn | grep oauth
add authentication OAuthIDPProfile AAAuthAutoConfig oAuthIdpProf -clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret od20
514a222303d -encrypted -encryptmethod ENCMTHD_3 -kek -suffix 2023_04_
9_09_12_25 -redirectURL "https://accounts.cloudburst.com/core/login-cip" -audience b1656835-20d1-4f6b-addd-1a531fd253f6 -sendPassword ON
```

4. Ändern Sie die im vorherigen Schritt kopierte Zeile, und erstellen Sie damit einen neuen CLI-Befehl, mit dem Sie ein OAuth-Profil mit der verschlüsselten Version der Client-ID erstellen können. Dazu müssen alle Verschlüsselungsparameter enthalten sein.

- Ändern Sie den Namen des OAuth-Profiles in *CustomDomain-OAuthProfile*.
- Aktualisieren Sie die `-redirectURL` auf <https://hostname.domain.com/core/login-cip>.

Hier sehen Sie ein Beispiel, nachdem beide Aktualisierungen vorgenommen wurden:

```
add authentication OAuthIDPProfile "CustomDomain-OAuthProfile"-
clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret <long
encrypted client Secret> -encrypted -encryptmethod ENCMTHD_3
-kek -suffix 2023_04_19_09_12_25 -redirectURL "https://hostname
.domain.com/core/login-cip" -audience b1656835-20d1-4f6b-add-1
a531fd253f6 -sendPassword ON

add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule
true -action "CustomDomain-OAuthProfile"
```

5. Binden Sie die OAuthPolicy in den zugehörigen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit weniger Priorität als die bestehende Richtlinie ein. Der Name des virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsservers für alle Bereitstellungen der Adaptiven Authorisierung ist *auth_vs*. Diese Instanz geht davon aus, dass die bestehende Richtlinie eine Priorität von 10 hat. Für die neue Richtlinie wird daher eine Priorität von 20 verwendet.

```
bind authentication vserver "auth_vs"-policy "CustomDomain-
OAuthPol"-priority 20
```

Bekannte Einschränkungen

Dies sind einige bekannte Einschränkungen der Lösung mit benutzerdefinierter Domäne:

Workspace-Plattform

- Es wird derzeit nur eine einzige benutzerdefinierte Domäne pro Kunde unterstützt.

- Eine benutzerdefinierte Domäne kann nur mit der standardmäßigen Workspace-URL verknüpft werden. Andere Workspace-URLs, die über das Mehrfach-URL-Feature hinzugefügt wurden, können keine benutzerdefinierte Domäne haben. Das Mehrfach-URL-Feature ist derzeit in der “Private Tech Preview”-Phase und möglicherweise nicht für alle Kunden verfügbar.
- Wenn Sie in der vorherigen Lösung eine benutzerdefinierte Domäne konfiguriert haben und SAML oder AzureAD zur Authentifizierung des Citrix Workspace-Zugriffs verwenden, müssen Sie in der neuen Lösung **zuerst** die **bestehende benutzerdefinierte Domäne löschen**, bevor Sie eine benutzerdefinierte Domäne konfigurieren können.

SAML

Die SAML-Unterstützung ist auf einen der folgenden Anwendungsfälle beschränkt:

- SAML kann ausschließlich für cloud.com-Domänen verwendet werden. In dieser Instanz würde die SAML-Verwendung den Zugriff auf Citrix Workspace und den Citrix Cloud-Administratorzugriff abdecken.
- SAML kann ausschließlich für eine benutzerdefinierte Domäne verwendet werden.

Citrix Workspace-App für Windows

- Das Feature wird nicht in Version 2305 und 2307 der Citrix Workspace-App für Windows unterstützt. Führen Sie ein Update auf die neueste unterstützte Version aus.

Sichere Workspaces

October 12, 2023

Als Administrator können Sie festlegen, ob Abonnenten sich bei ihrem Workspace mit einer der folgenden Authentifizierungsmethoden authentifizieren müssen:

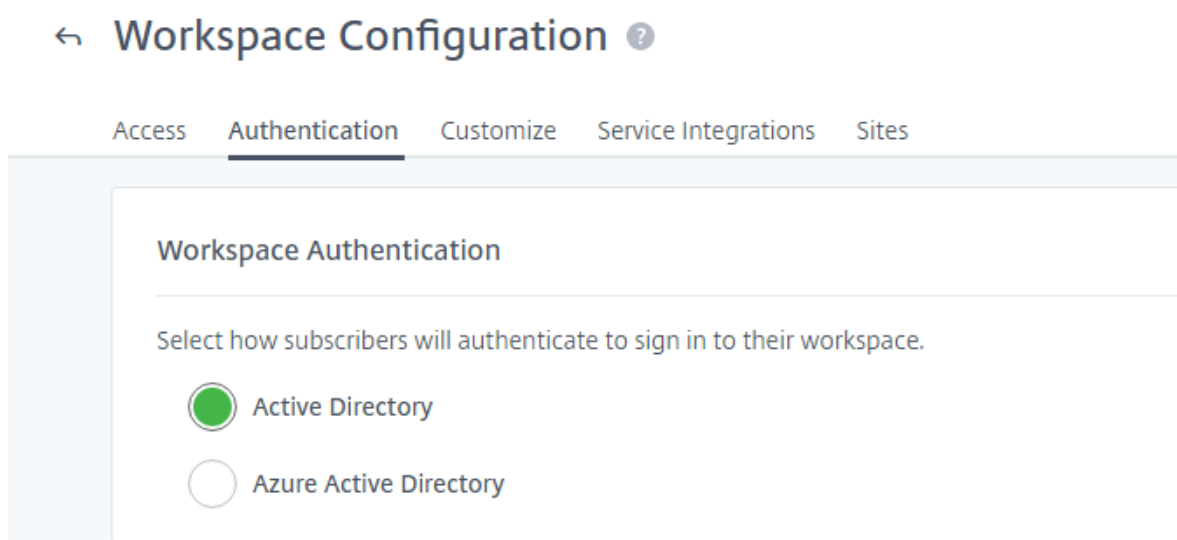
- Active Directory (AD)
- Active Directory plus Token
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

Diese Authentifizierungsoptionen sind für jeden Citrix Cloud Service verfügbar. Weitere Informationen finden Sie unter [Tech Brief: Workspaceidentität](#).

Citrix Workspace unterstützt außerdem den Citrix Verbundauthentifizierungsdienst (FAS) für das Single Sign-On bei Citrix DaaS. Durch SSO mit FAS müssen sich Abonnenten nicht mehr bei DaaS authentifizieren, wenn sie sich mit einer Verbundauthentifizierungsmethode bei ihren Workspaces angemeldet haben. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Wählen bzw. Ändern der Authentifizierungsmethode

Wenn Sie Ihre Identitätsanbieter konfiguriert haben, können Sie unter **Workspacekonfiguration > Authentifizierung > Workspaceauthentifizierung** wählen bzw. ändern, wie Abonnenten sich bei ihrem Workspace authentifizieren.



Wichtig:

Das Ändern der Authentifizierungsmodi kann bis zu fünf Minuten dauern und führt während dieser Zeit zu einem Ausfall für Ihre Abonnenten. Citrix empfiehlt, Änderungen auf Zeiträume mit geringer Nutzung zu beschränken. Wenn Abonnenten bei Citrix Workspace über einen Browser oder die Citrix Workspace-App angemeldet sind, weisen Sie sie an, den Browser oder die App zu schließen. Nach etwa fünf Minuten können sie sich mit der neuen Authentifizierungsmethode neu anmelden.

Active Directory (AD)

Standardmäßig verwendet Citrix Cloud für die Authentifizierung von Abonnenten bei Workspaces Active Directory (AD).

Die Verwendung von AD erfordert mindestens zwei Citrix Cloud Connectors in der On-Premises-AD-Domäne. Weitere Informationen zur Installation des Cloud Connectors finden Sie unter [Cloud Connector-Installation](#).

Active Directory (AD) plus Token

Für erhöhte Sicherheit unterstützt Citrix Workspace für die AD-Anmeldung ein zeitbasiertes Token als zweiten Authentifizierungsfaktor.

Bei jeder Anmeldung fordert Workspace die Abonnenten auf, ein Token aus einer Authentifizierungs-App auf ihrem registrierten Gerät einzugeben. Vor der Anmeldung müssen die Abonnenten ihr Gerät mit einer Authentifizierungs-App registrieren, die den Vorgaben des TOTP-Standards (zeitbasierte Einmalkennwörter) entspricht, z. B. Citrix SSO. Derzeit können Abonnenten jeweils nur ein Gerät registrieren.

Weitere Informationen finden Sie unter [Tech Insight: Authentifizierung - TOTP](#) und [Tech Insight: Authentifizierung - Push](#).

Anforderungen für AD plus Token

Für die Authentifizierung per Active Directory plus Token gelten die folgenden Anforderungen:

- Eine Verbindung zwischen Active Directory und Citrix Cloud mit mindestens zwei installierten Cloud Connectors in Ihrer On-Premises-Umgebung. Anforderungen und Anweisungen finden Sie unter [Verbinden von Active Directory mit Citrix Cloud](#).
- Auf der Seite **Identitäts- und Zugriffsverwaltung** muss die Option **Active Directory + Token** aktiviert sein. Informationen finden Sie unter [Aktivieren der Authentifizierung über Active Directory plus Token](#).
- Die Abonnenten haben Zugriff auf E-Mail, um Geräte zu registrieren.
- Ein Gerät, auf das die Authentifizierungs-App heruntergeladen werden kann.

Erstmalige Registrierung

Geräte können mit dem unter [Registrieren von Geräten für die zweistufige Authentifizierung](#) beschriebenen Verfahren erneut registriert werden.

Beim ersten Anmelden bei Workspace folgen Abonnenten den Anweisungen zum Herunterladen der Citrix SSO-App. Die Citrix SSO-App generiert alle 30 Sekunden ein eindeutiges Einmalkennwort auf einem registrierten Gerät.

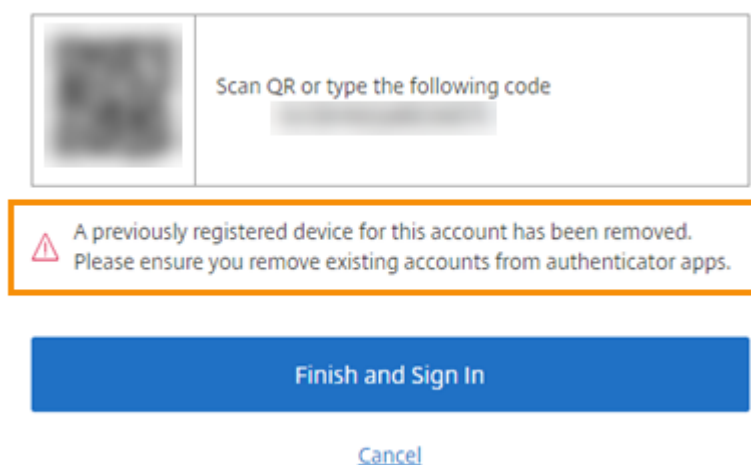
Wichtig:

Während der Geräteregistrierung erhalten Abonnenten eine E-Mail mit temporärem Verifizierungscode. Dieser temporäre Code wird nur zur Registrierung des Abonentengeräts verwendet. Die Verwendung des Codes als Token für die Anmeldung mit zweistufiger Authentifizierung in Citrix Workspace wird nicht unterstützt. Nur Verifizierungscodes, die von einer Authentifikator-App auf einem registrierten Gerät generiert werden, sind unterstützte Token für die zweistufige Authentifizierung.

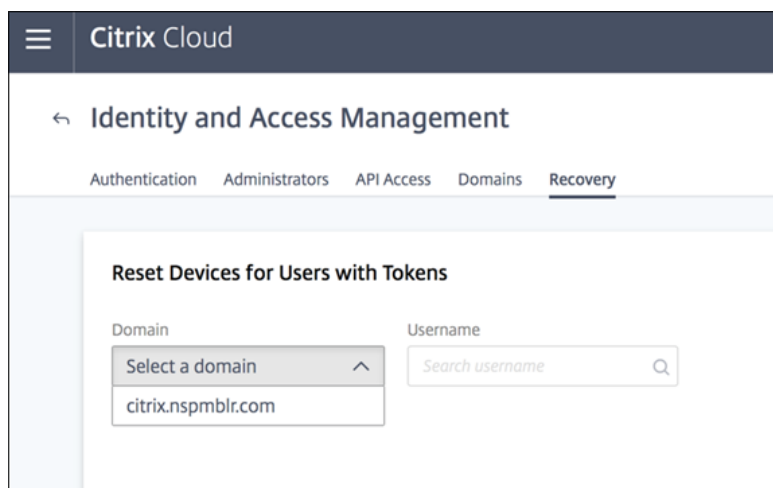
Erneute Registrierung von Geräten

Hat ein Abonnent sein registriertes Gerät nicht mehr oder muss er es erneut registrieren (z. B. nachdem Inhalte vom Gerät gelöscht wurden), gibt es in Workspace folgende Optionen:

- Das Gerät kann mit dem unter [Registrieren von Geräten für die zweistufige Authentifizierung](#) beschriebenen Verfahren erneut registriert werden. Da Abonnenten jeweils nur ein Gerät registrieren können, wird die bestehende Geräteregistrierung durch das Registrieren eines neuen Geräts bzw. das erneute Registrieren eines bestehenden Geräts entfernt.



- Administratoren können Abonnenten anhand von deren Active Directory-Namen suchen und ihr Gerät zurücksetzen. Gehen Sie dazu zu **Identitäts- und Zugriffsverwaltung > Wiederherstellung**. Bei der nächsten Anmeldung bei Workspace muss der Abonnent die Schritte zur erstmaligen Registrierung ausführen.



Azure Active Directory

Um Abonnenten mit Azure Active Directory (AD) bei Workspaces zu authentifizieren, muss Folgendes vorliegen:

- Azure AD mit einem Benutzer, der über globale Administratorrechte verfügt. Weitere Informationen über die Azure AD-Anwendungen und -Berechtigungen, die Citrix Cloud verwendet, finden Sie unter [Azure Active Directory-Berechtigungen für Citrix Cloud](#).
- Ein Citrix Cloud Connector, der in der On-Premises-Domäne von AD installiert ist. Die Maschine muss außerdem in die Domäne eingebunden sein, die mit Azure AD synchronisiert ist.
- VDA Version 7.15.2000 LTSR CU VDA oder aktuelles Release 7.18 VDA oder höher.
- Eine Verbindung zwischen Azure AD und Citrix Cloud. Weitere Informationen finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).

Wenn Sie Ihr Active Directory mit Azure AD synchronisieren, müssen die UPN- und SID-Einträge in der Synchronisierung enthalten sein. Wenn diese Einträge nicht synchronisiert werden, schlagen bestimmte Workflows in Citrix Workspace fehl.

Warnung:

- Wenn Sie Azure AD verwenden, nehmen Sie nicht die Registrierungsänderung vor, die in [CTX225819](#) beschrieben wird. Wenn Sie diese Änderung vornehmen, können Sitzungsstartfehler für Azure AD-Benutzer auftreten.
- Das Hinzufügen einer Gruppe als Mitglied einer anderen Gruppe (Verschachtelung) wird unterstützt, wenn die Funktion `DSAuthAzureAdNestedGroups` aktiviert ist. Sie können `DSAuthAzureAdNestedGroups` aktivieren, indem Sie eine Anfrage an den Citrix Support senden.

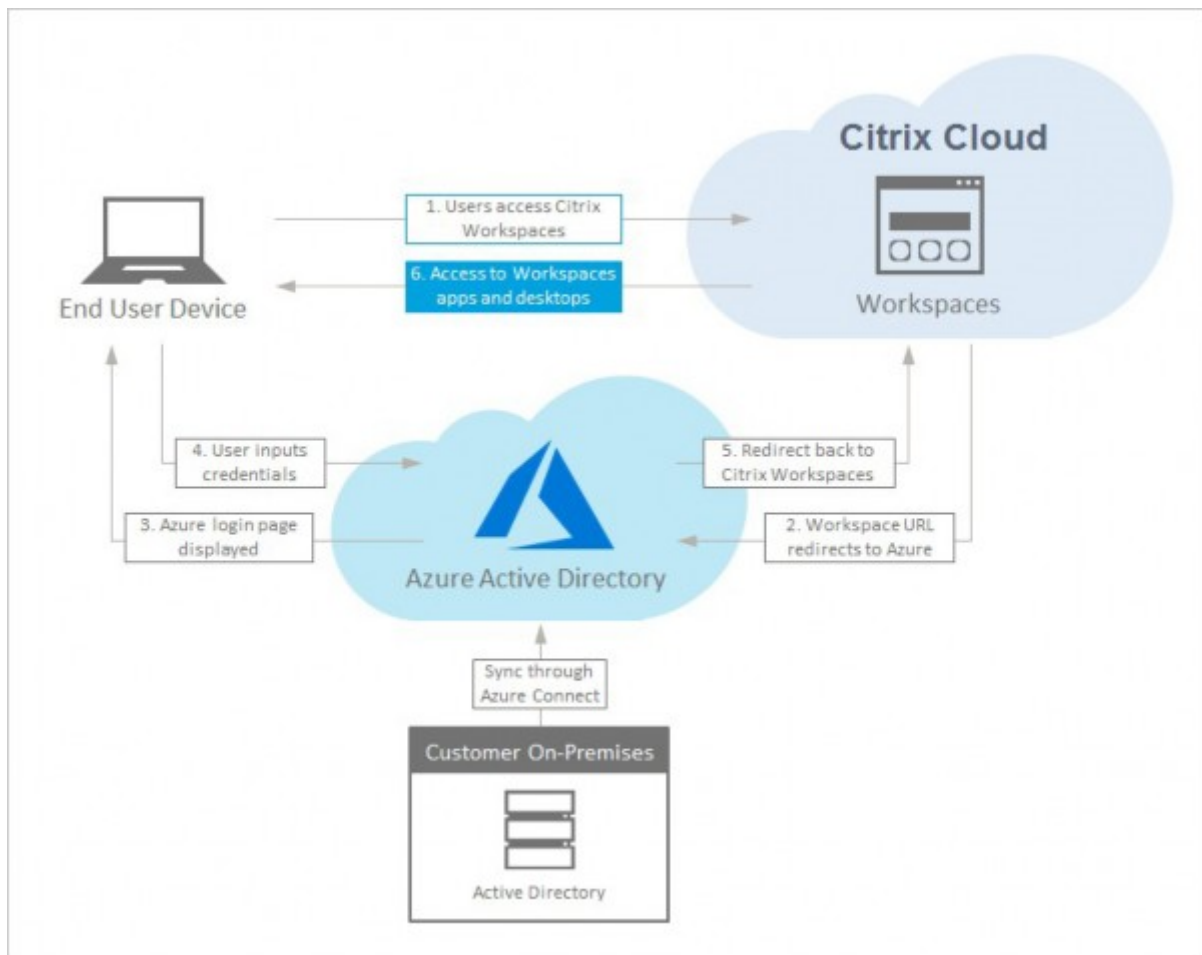
Nach dem Aktivieren der Azure AD-Authentifizierung:

- **Zusätzliche Sicherheit:** Benutzer müssen sich aus Sicherheitsgründen beim Starten einer App oder eines Desktops erneut anmelden. Die Kennwortinformationen werden direkt vom Benutzergerät an den VDA gesendet, der die Sitzung hostet.
- **Anmeldeumgebung:** Die Azure AD-Authentifizierung bietet eine Verbundanmeldung und kein Single Sign-On (SSO). Die Abonnenten melden sich über eine Azure-Anmeldeseite an und müssen sich möglicherweise erneut authentifizieren, wenn sie Citrix DaaS öffnen.

Für SSO aktivieren Sie den Citrix Verbundauthentifizierungsdienst in Citrix Cloud. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Sie können die Anmeldeoberfläche für Azure AD anpassen. Informationen hierzu finden Sie in der [Dokumentation von Microsoft](#). Alle Anmeldeanpassungen (das Logo), die in der Workspacekonfiguration vorgenommen werden, wirken sich nicht auf die Anmeldeumgebung in Azure AD aus.

Die folgende Abbildung verdeutlicht die Schrittfolge bei der Authentifizierung in Azure AD:



Citrix Gateway

Citrix Workspace unterstützt die Verwendung eines on-premises Citrix Gateway als Identitätsanbieter, um die Abonnentenauthentifizierung bei Workspaces zu verwalten. Weitere Informationen finden Sie unter [Tech Insight: Authentifizierung –Citrix Gateway](#).

Anforderungen für Citrix Gateway

Für die Authentifizierung mit Citrix Gateway gelten folgende Anforderungen:

- Eine Verbindung zwischen Ihrem Active Directory und Citrix Cloud. Anforderungen und Anweisungen finden Sie unter [Verbinden von Active Directory mit Citrix Cloud](#).
- Abonnenten müssen Active Directory-Benutzer sein, um sich bei ihrem Workspace anzumelden.
- Bei einem Verbund müssen Ihre AD-Benutzer mit dem Verbundanbieter synchronisiert sein. Citrix Cloud benötigt die AD-Benutzerattribute, damit die Benutzer sich anmelden können.
- Ein on-premises Citrix Gateway:
 - Citrix Gateway 12.1 54.13 Advanced Edition oder höher
 - Citrix Gateway 13.0 41.20 Advanced Edition oder höher
- Authentifizierung mit **Citrix Gateway** auf der Seite **Identitäts- und Zugriffsverwaltung** aktiviert. Dadurch werden Client-ID, Geheimnis und Umleitungs-URL generiert, die für die Verbindung zwischen Citrix Cloud und On-Premises-Gateway erforderlich sind.
- Auf dem Gateway wird mit der generierten Client-ID, dem Geheimnis und der Umleitungs-URL eine OAuth-IdP-Authentifizierungsrichtlinie konfiguriert.

Weitere Informationen finden Sie unter [Verbinden eines on-premises Citrix Gateway als Identitätsanbieter mit Citrix Cloud](#).

Citrix Gateway für Abonnenten

Bei aktivierter Authentifizierung mit Citrix Gateway wird der folgende Workflow für Abonnenten ausgeführt:

1. Der Abonnent navigiert im Browser zur Workspace-URL oder startet die Workspace-App.
2. Der Abonnent wird zur Citrix Gateway-Anmeldeseite umgeleitet und mit der im Gateway konfigurierten Methode authentifiziert. Bei der Methode kann es sich um die Multifaktorauthentifizierung, Verbund, Richtlinien für bedingten Zugriff usw. handeln. Sie können die Gateway-Anmeldeseite an das Aussehen der Workspace-Anmeldeseite anpassen. Verwenden Sie hierfür die Schrittfolge unter [CTX258331](#).
3. Nach erfolgter Authentifizierung wird der Workspace des Abonnenten angezeigt.

Google

Citrix Workspace unterstützt die Verwendung von Google als Identitätsanbieter, um die Abonnentenauthentifizierung bei Workspaces zu verwalten.

Anforderungen für Google

- Eine Verbindung zwischen Ihrem On-Premises-Active Directory und Google Cloud.
- Ein Entwicklerkonto mit Zugriff auf die Google Cloud Platform-Konsole. Dieses Konto ist erforderlich, um ein Dienstkonto und einen Schlüssel zu erstellen und die Admin SDK-API zu verwenden.
- Administratorkonto mit Zugriff auf die Google Workspace-Administratorkonsole. Dieses Konto ist für die Konfiguration der domänenweiten Delegation und eines API-Benutzerkontos mit Schreibzugriff erforderlich.
- Eine Verbindung zwischen Ihrer On-Premises-Active Directory-Domäne und Citrix Cloud, wobei auf der Seite **Identitäts- und Zugriffsverwaltung** die Authentifizierungsoption **Google** aktiviert ist. Zum Erstellen dieser Verbindung installieren Sie mindestens zwei Cloud Connectors in Ihrer Ressource.

Weitere Informationen finden Sie unter [Verbinden von Google als Identitätsanbieter mit Citrix Cloud](#).

Abonnenten-Benutzererfahrung mit Google

Bei aktivierter Authentifizierung mit Google wird der folgende Workflow für Abonnenten ausgeführt:

1. Der Abonnent navigiert im Browser zur Workspace-URL oder startet die Workspace-App.
2. Der Abonnent wird zur Google-Anmeldeseite umgeleitet und mit der in Google Cloud konfigurierten Methode authentifiziert (z. B. Multifaktorauthentifizierung, Richtlinien für bedingten Zugriff usw.).
3. Nach erfolgter Authentifizierung wird der Workspace des Abonnenten angezeigt.

Okta

Citrix Workspace unterstützt die Verwendung von Okta als Identitätsanbieter, um die Abonnentenauthentifizierung bei Workspaces zu verwalten. Weitere Informationen finden Sie unter [Tech Insight: Authentifizierung - Okta](#).

Anforderungen für Okta

Für die Authentifizierung mit Okta gelten folgende Anforderungen:

- Eine Verbindung zwischen Ihrem On-Premises-Active Directory und Ihrer Okta-Organisation.
- Eine Okta-OIDC-Webanwendung, die für die Verwendung mit Citrix Cloud konfiguriert ist. Zum Verbinden von Citrix Cloud mit Ihrer Okta-Organisation müssen Sie die Client-ID und das Clientgeheimnis für diese Anwendung angeben.
- Eine Verbindung zwischen Ihrer On-Premises-Active Directory-Domäne und Citrix Cloud, wobei auf der Seite **Identitäts- und Zugriffsverwaltung** die Authentifizierungsoption **Okta** aktiviert ist.

Weitere Informationen finden Sie unter [Verbinden von Okta als Identitätsanbieter mit Citrix Cloud](#).

Abonnenten-Benutzererfahrung mit Okta

Bei aktivierter Authentifizierung mit Okta wird der folgende Workflow für Abonnenten ausgeführt:

1. Der Abonnent navigiert im Browser zur Workspace-URL oder startet die Workspace-App.
2. Der Abonnent wird zur Okta-Anmeldeseite umgeleitet und mit der in Okta konfigurierten Methode authentifiziert (z. B. Multifaktorauthentifizierung, Richtlinien für bedingten Zugriff usw.).
3. Nach erfolgreicher Authentifizierung wird der Workspace des Abonnenten angezeigt.

Die Okta-Authentifizierung bietet eine Verbundanmeldung und kein Single Sign-On. Die Abonnenten melden sich bei ihrem Workspace über eine Okta-Anmeldeseite an und müssen sich möglicherweise erneut authentifizieren, wenn sie Citrix DaaS öffnen. Für SSO aktivieren Sie den Citrix Verbundauthentifizierungsdienst in Citrix Cloud. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

SAML 2.0

Citrix Workspace unterstützt die Verwendung von SAML 2.0, um die Abonnentenauthentifizierung bei Workspaces zu verwalten. Sie können den SAML-Anbieter Ihrer Wahl verwenden, sofern er SAML 2.0 unterstützt.

Anforderungen für SAML 2.0

Für die SAML-Authentifizierung gelten die folgenden Anforderungen:

- SAML-Anbieter, der SAML 2.0 unterstützt.
- On-Premises-Active Directory-Domäne.

- Zwei Cloud Connectors, an einem Ressourcenstandort bereitgestellt und mit Ihrer On-Premises-AD-Domäne verbunden.
- AD-Integration mit Ihrem SAML-Anbieter.

Weitere Informationen zur Konfiguration der SAML-Authentifizierung für Workspaces finden Sie unter [Verbinden von SAML als Identitätsanbieter mit Citrix Cloud](#).

Abonnenten-Benutzererfahrung mit SAML 2.0

1. Der Abonnent navigiert im Browser zur Workspace-URL oder startet die Citrix Workspace-App.
2. Der Abonnent wird auf die Anmeldeseite des SAML-Identitätsanbieters für seine Organisation weitergeleitet. Der Abonnent authentifiziert sich mit dem für den SAML-Identitätsanbieter konfigurierten Mechanismus, z. B. mehrstufiger Authentifizierung oder Richtlinien für bedingten Zugriff.
3. Nach erfolgter Authentifizierung wird der Workspace des Abonnenten angezeigt.

Citrix Verbundauthentifizierungsdienst (FAS)

Citrix Workspace unterstützt den Citrix Verbundauthentifizierungsdienst (FAS) für das Single Sign-On bei Citrix DaaS. Ohne FAS werden solche Abonnenten mehrfach aufgefordert, ihre Anmeldeinformationen einzugeben, um auf DaaS zuzugreifen.

Weitere Informationen finden Sie unter [Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Oberfläche für die Abmeldung von Abonnenten

Verwenden Sie **Einstellungen > Abmelden**, um die Abmeldung von Workspace und Azure AD durchzuführen. Wenn Abonnenten den Browser schließen, statt die **Abmeldeoption** zu verwenden, bleiben sie möglicherweise bei Azure AD angemeldet.

Wichtig:

Wenn im Citrix Workspace ein Timeout aufgrund von Inaktivität im Browser auftritt, bleiben Abonnenten in Azure AD angemeldet. Dadurch wird verhindert, dass ein Citrix Workspace-Timeout andere Azure AD-Anwendungen zum Schließen zwingt.

Weitere Informationen

- [Tech Brief: Workspace Single Sign-On](#)
- [Tech Insights –Citrix Workspace](#)
- [Proof of Concept –Citrix Workspace](#)

Services in Workspaces integrieren

November 27, 2023

In diesem Artikel werden die Schritte zum Hinzufügen von Diensten zu Citrix Workspace beschrieben. Dies ist ein zweistufiger Vorgang:

1. Konfigurieren Sie einzelne Dienste in Citrix Cloud. Unter [Citrix Cloud Services](#) finden Sie eine Liste der Citrix Cloud-Dienste sowie Links zu Anweisungen für jeden Dienst.
2. Aktivieren (und deaktivieren) Sie den Zugriff auf Ihre konfigurierten Dienste in **Workspacekonfiguration > Serviceintegrationen**.

Konfigurieren von Diensten

Ihre erworbenen Dienste werden im Citrix Cloud-Dashboard im Kartenlayout angezeigt. Zu jedem erworbenen Dienst gibt es eine Schaltfläche **Verwalten**.

Konfigurieren von erworbenen Diensten:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie in der Kachel des Dienstes, den Sie konfigurieren möchten, die Option **Verwalten**.
3. Befolgen Sie die Anweisungen zum Einrichten dieses Dienstes.

Eine kurze Beschreibung der in der Cloud gehosteten Dienste finden Sie unter [Zugriff auf cloudgehostete Dienste über Citrix Workspace](#).

Um einen neuen Dienst auszuprobieren, können Sie eine Testversion oder Demo anfordern. Weitere Informationen zu Testversionen finden Sie unter [Citrix Cloud Service - Testversionen](#).

Aktivieren von Diensten

Nachdem Sie Ihre Dienste konfiguriert haben, können Sie sie in Citrix Workspace integrieren.

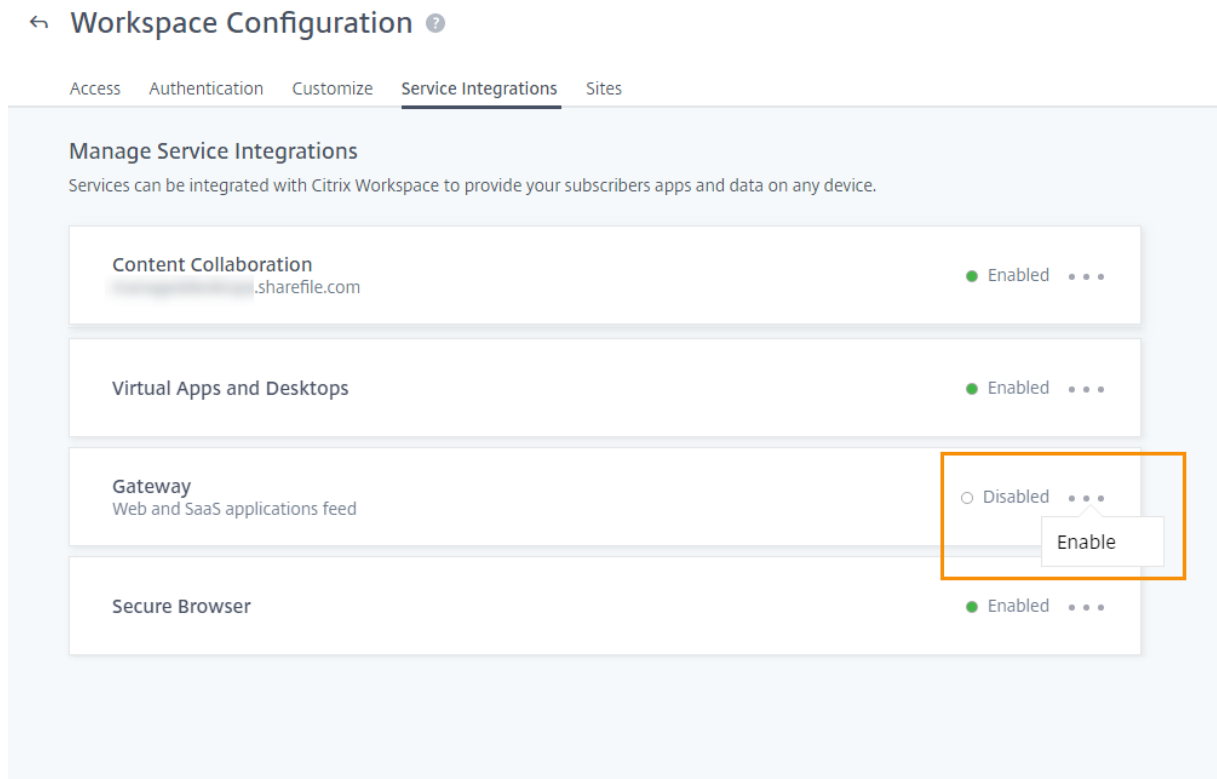
DaaS und **Remote Browser Isolation** sind nach dem Abonnieren standardmäßig aktiviert. Alle anderen neuen Dienste, die von Ihrer Organisation abonniert werden, sind standardmäßig deaktiviert.

Hinweis:

Citrix App Essentials Service und **Citrix DaaS** werden in **Workspacekonfiguration** auf der Registerkarte **Serviceintegrationen** als "Citrix DaaS" angezeigt.

Aktivieren der Workspaceintegration für einen Dienst:

1. Navigieren Sie zu **Workspacekonfiguration > Serviceintegrationen**.
2. Klicken Sie neben dem Dienst auf die Auslassungspunkte (...) und wählen Sie **Aktivieren**.



Aktivieren von Diensten

Durch die Deaktivierung der Workspaceintegration wird der Zugriff von Abonnenten auf diesen Service blockiert. Die Workspace-URL wird dadurch nicht deaktiviert. Abonnenten können jedoch nicht mehr auf Daten und Anwendungen von diesem Dienst in Citrix Workspace zugreifen.

Deaktivieren der Workspaceintegration für einen Service

1. Navigieren Sie zu **Workspacekonfiguration > Serviceintegrationen**.
2. Wählen Sie die Schaltfläche mit den Auslassungspunkten neben dem Dienst und anschließend **Deaktivieren**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Bestätigen**. Abonnenten können dann nicht auf Daten oder Anwendungen des Dienstes zugreifen.



Subscribers will no longer have access to data and applications from this service in Citrix Workspace

Are you sure you want to disable workspace integration for Virtual Apps and Desktops?

Cancel

Confirm

Citrix Workspace-App konfigurieren

November 27, 2023

Sie können die Citrix Workspace-App mit dem Global App Configuration Service (GACS) konfigurieren. Damit können Sie die App-Einstellungen für Endbenutzer auf verwalteten und nicht verwalteten Geräten verwalten.

Die Einstellungen können mit einer der folgenden Methoden sowohl für Cloud-Umgebungen (Citrix Workspace) als auch für On-Premises-Umgebungen (Citrix StoreFront) konfiguriert werden:

- Global App Configuration Service-Benutzeroberfläche (UI):
 - [Einstellungen für Cloudstores konfigurieren](#)
 - [Einstellungen für On-Premises-Stores konfigurieren](#)
- API – Informationen zum Konfigurieren von Einstellungen mithilfe von APIs finden Sie unter [Citrix Developer](#).

Dieser Dienst wird unter Windows, Mac, Android, iOS, HTML5 und ChromeOS unterstützt.

Hauptvorteile

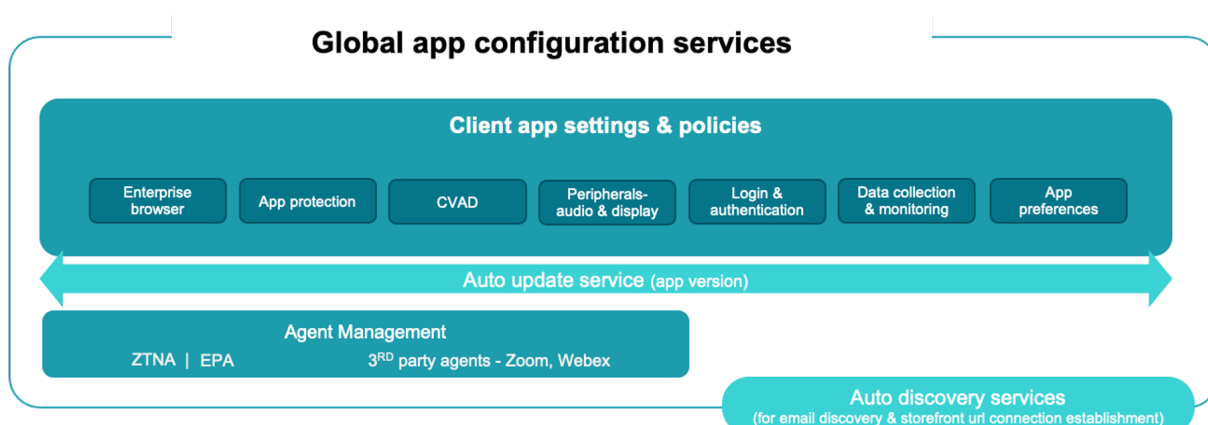
Mit dem Global App Configuration Service können Sie über eine zentrale Oberfläche folgende Aufgaben erledigen:

- Einstellungen für verwaltete und nicht verwaltete (BYOD) Geräte konfigurieren
- Einstellungen für mehrere Stores konfigurieren
- Client-App-Agents (z. B. Endpoint Analysis, ZTNA) und Drittanbieter-Agents (z. B. Zoom, Webex) aktualisieren und verwalten
- Citrix Workspace-App für Endbenutzer automatisch aktualisieren und verwalten
- Konfiguration vor dem Rollout an die Endbenutzer testen

Funktionsweise des Global App Configuration Service

Der Global App Configuration Service ist eine Citrix IP-Lösung, mit der die Einstellungen von Client-Apps konfiguriert und verwaltet werden. Er bietet unter Einsatz der folgenden Dienste und Einstellungen eine reibungslose Erfahrung für die Endbenutzer.

- **Autodiscoveryservice:** Ordnet Domänen Store-URLs zu, sodass die Endbenutzer sich mit ihrer E-Mail-Adresse anmelden können. Endbenutzer müssen ihre Store-URLs nicht bei der Anmeldung angeben.
- **Automatischer Updatedienst und Agentverwaltung:** Aktualisiert die Citrix Workspace-App automatisch auf die angegebene Version für Ihre Endbenutzer. Sie können flexibel verschiedene App-Versionen für verschiedene Plattformen konfigurieren.
- **Einstellungen und Richtlinien für Client-Apps:** Alle Endbenutzereinstellungen in der Citrix Workspace-App können zentral konfiguriert und festgelegt werden. Dies umfasst Einstellungen zu Anmeldung, Sicherheit, Authentifizierungsoptionen und virtueller App sowie Desktop-Einstellungen.



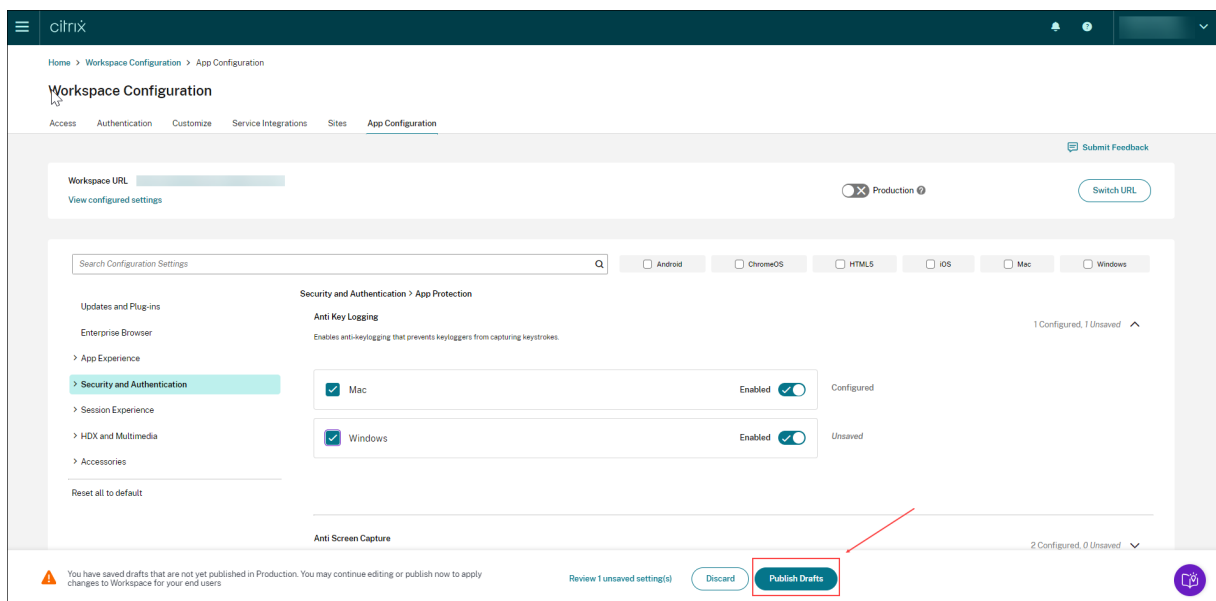
Voraussetzungen

Stellen Sie vor dem Konfigurieren der App-Einstellungen sicher, dass die Version der Citrix Workspace-App den angegebenen Versionen entspricht oder höher ist. Weitere Informationen finden Sie in der folgenden Tabelle.

Citrix Workspace-App-Plattform	Unterstützte Mindestversion
Windows	Aktuelles Release –2106, LTSR - 2203.1
Mac	2203.1
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

Verwendung von Global App Configuration Service

Um Einstellungen zu konfigurieren, melden Sie sich im [Citrix Cloud-Portal](#) an und gehen Sie zu **Workspacekonfiguration > App-Konfiguration**. Ändern Sie die App-Einstellungen gemäß den Richtlinien Ihrer Organisation. Sie können dann auf **Entwürfe veröffentlichen** klicken, um die Einstellungen zu veröffentlichen.

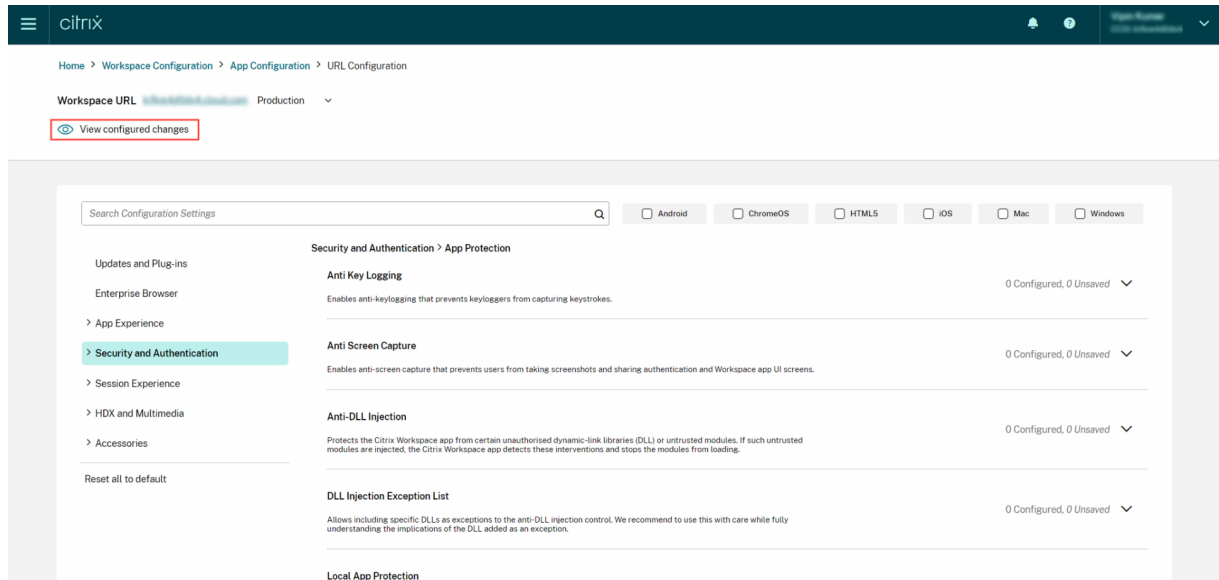


Die Benutzeroberfläche bietet außerdem die folgenden Optionen für eine vereinfachte Benutzererfahrung.

Zusammenfassung der konfigurierten Einstellungen anzeigen

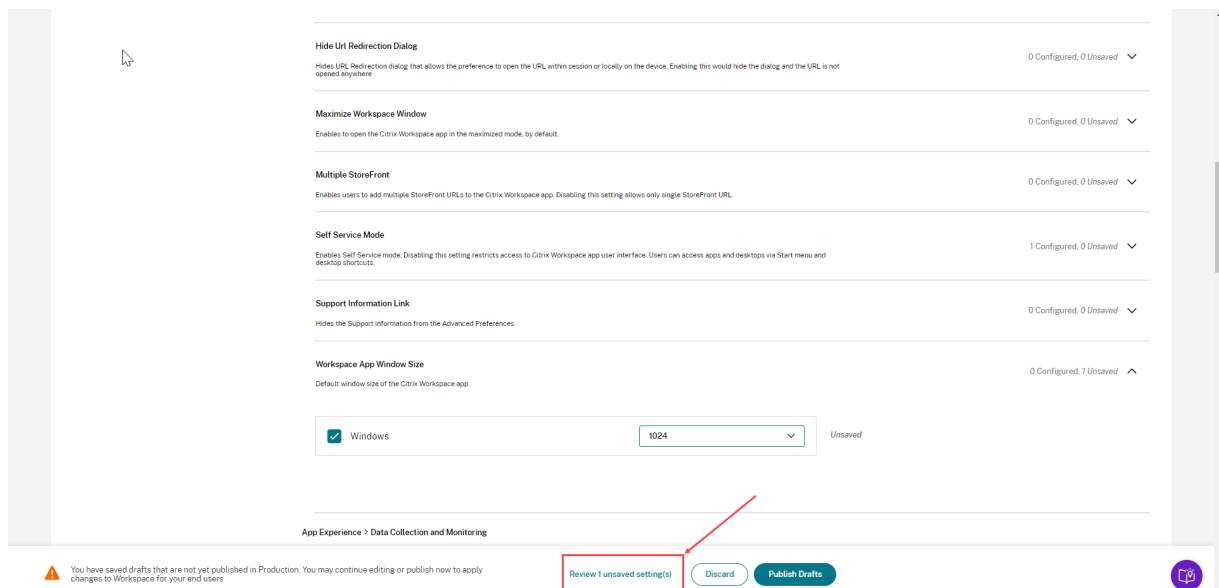
Sie können eine Zusammenfassung der aktuellen Konfiguration anzeigen, indem Sie auf die Schaltfläche **Konfigurierte Einstellungen anzeigen** klicken. Sie müssen dann nicht jede Einstellung

einzelnen erweitern und überprüfen. Eine konsolidierte Liste aller konfigurierten Einstellungen ermöglicht es Ihnen, eine umfassende Überprüfung der aktuellen Konfiguration durchzuführen und die Auswirkungen auf die Benutzer abzuschätzen.

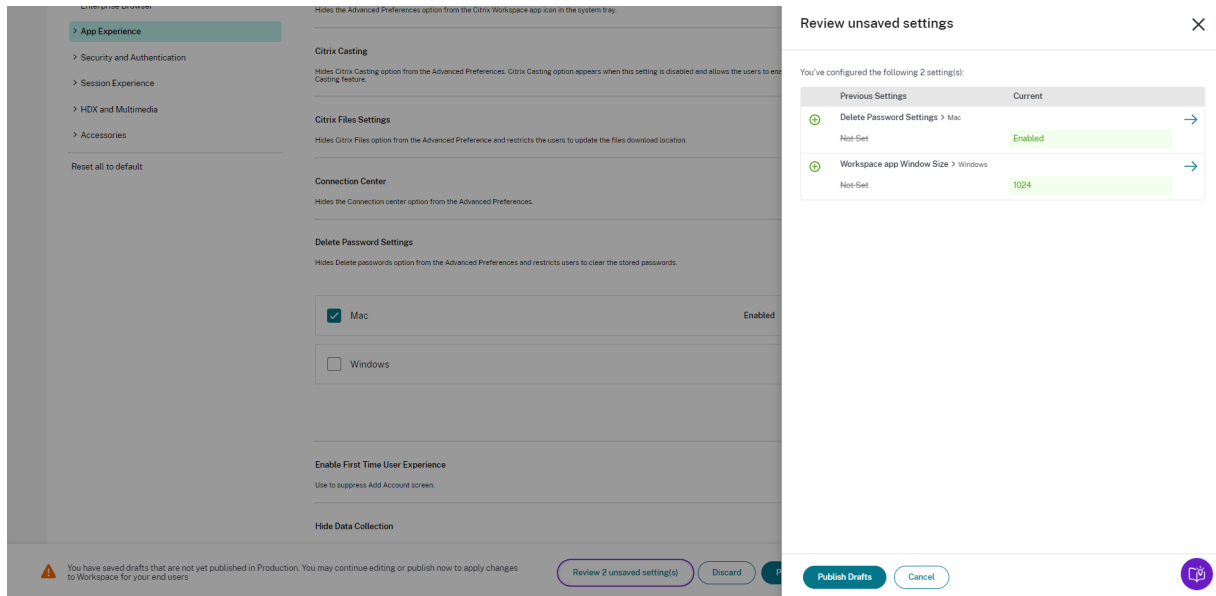


Nicht gespeicherte Änderungen überprüfen

Führen Sie eine abschließende Überprüfung Ihrer nicht gespeicherten Änderungen durch, bevor Sie die Konfiguration veröffentlichen. Die Anzahl der nicht gespeicherten Einstellungen wird auf der Benutzeroberfläche angezeigt. Sie können auf diese Liste zugreifen, indem Sie auf die Option **Nicht gespeicherte Änderungen überprüfen** klicken. Auf diese Weise können Sie gezielt Änderungen vornehmen und die Datengenauigkeit aufrechterhalten.



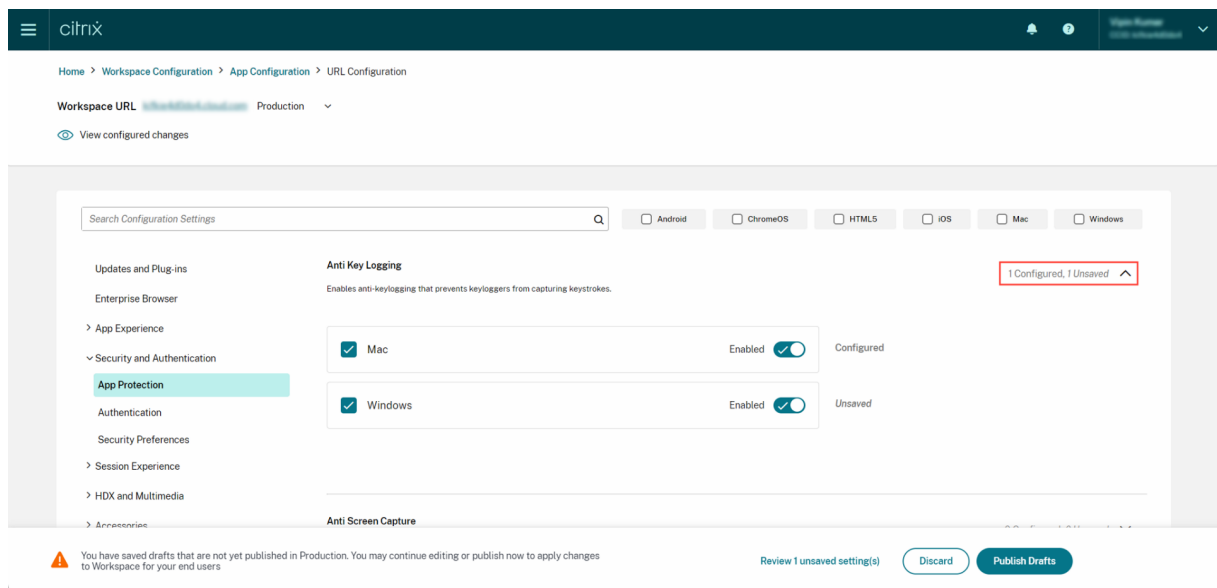
Sie können auch zu einer nicht gespeicherten Einstellung navigieren, indem Sie auf den Pfeil klicken.



Verbesserte Benutzeroberfläche

Sehen Sie sich den Status jeder Einstellung an, ohne sie zu erweitern. Die folgenden Tags werden jetzt angezeigt, damit Sie bei jedem Schritt gezielt Entscheidungen treffen können.

- **Konfiguriert:** Zeigt die Anzahl der Plattformen (Client-OS) an, für die die Einstellung bereits konfiguriert wurde.
- **Nicht gespeichert:** Zeigt die Anzahl der Einstellungen an, die konfiguriert, aber noch nicht gespeichert wurden



Verbesserte Suchoption

Das Sucherlebnis wurde verbessert, um ein robustes und nahtloses Erlebnis zu bieten. Administratoren können sich jetzt problemlos beim Cloud-Portal anmelden und die erforderlichen Einstellungen auf der App-Konfigurationsseite finden. Sie können die folgenden Suchmethoden verwenden.

- **Suche anhand der Beschreibung der Einstellung**

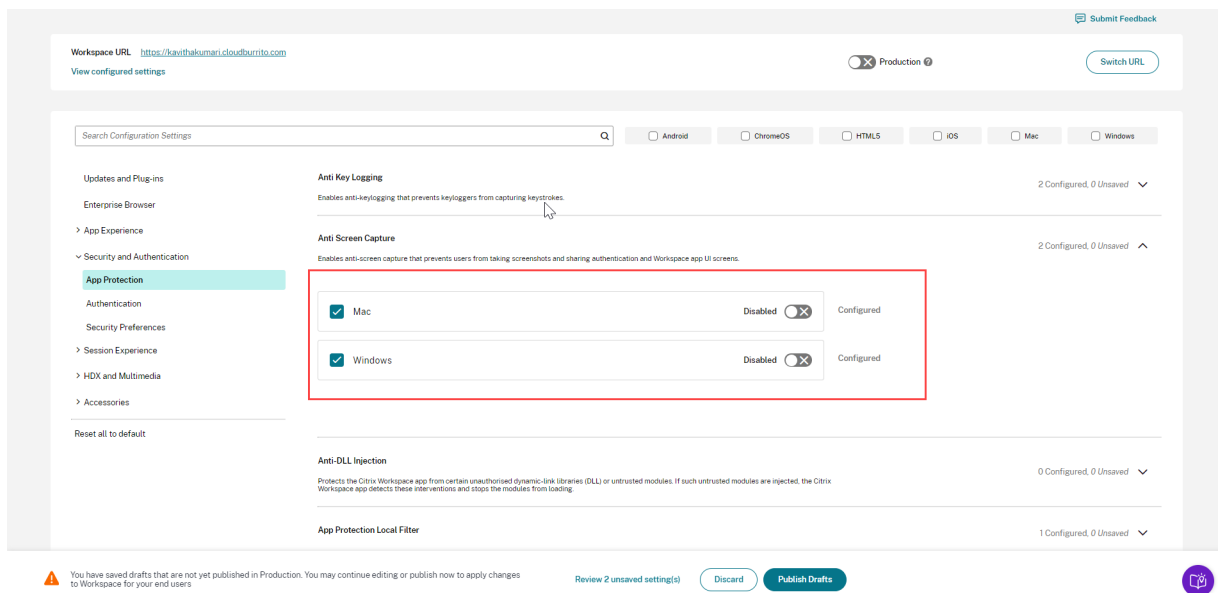
Sie können Einstellungen anhand von Schlüsselwörtern aus der Beschreibung der Einstellung suchen. Dies ermöglicht eine flexiblere Suche anhand relevanter Begriffe, die mit der gewünschten Einstellung verknüpft sind.

- **Suche anhand des API-Einstellungsnamens**

Sie können nach Einstellungen suchen, indem Sie den Namen der API-Einstellung eingeben. Diese Methode ermöglicht eine gezieltere Suche, sodass Benutzer schnell die benötigte Einstellung finden.

Relevante Plattformen für jede Einstellung anzeigen

Jede Einstellung zeigt jetzt nur die Plattformen an, für die sie relevant und anwendbar ist. Dieser Ansatz stellt sicher, dass Benutzer eine angepasste Liste der zutreffenden Optionen sehen.



Häufigkeit des Abrufs aktualisierter Einstellungen

Wenn die Konfiguration veröffentlicht ist, kann es einige Stunden dauern, bis die Einstellungen auf der Clientseite aktualisiert werden.

- Innerhalb der Sitzung werden die Einstellungen wie folgt aktualisiert.

Plattform	Maximaler Zeitdauer der Aktualisierung der Einstellungen
Citrix Workspace-App für Windows	Bis zu 6 Stunden
Citrix Workspace-App für macOS	Bis zu 6 Stunden
Citrix Workspace-App für HTML5	Bis zu 3 Stunden
Citrix Workspace-App für ChromeOS	Bis zu 3 Stunden
Citrix Workspace-App für iOS	Bis zu 6 Stunden
Citrix Workspace-App für Android	Bis zu 6 Stunden

- Unter Windows und macOS können die Einstellungen sofort aktualisiert werden, wenn die Endbenutzer ihre Citrix Workspace-App beenden und neu starten.
- Wenn ein Endbenutzer seiner Citrix Workspace-App einen Store hinzufügt, werden die Einstellungen für diesen Store automatisch aktualisiert.

Rangfolge für die Anwendung der Einstellungen

Neben dem Global App Configuration Service können plattformspezifische Tools (wie GPO für Windows), zur Konfiguration von Endbenutzereinstellungen verwendet werden.

Im Falle eines Konflikts zwischen den über den Global App Configuration Service konfigurierten Einstellungen und denjenigen, die über andere Tools konfiguriert wurde, gilt folgende Priorität für die Einstellungen.

Plattform	Storetyp	Anwendungspriorität
Citrix Workspace-App für Windows	StoreFront und Cloud	Gruppenrichtlinienobjekt (GPO) > Global App Configuration Service > Registrierung
Citrix Workspace-App für Mac	StoreFront und Cloud	MDM > Global App Configuration Service > UserDefaults
Citrix Workspace-App für HTML5	StoreFront	Global App Configuration Service > Configuration.js
	Cloud	Global App Configuration Service
Citrix Workspace-App für ChromeOS	StoreFront	Google-Admin-Richtlinie > Global App Configuration Service > Configuration.js
	Cloud	Google-Admin-Richtlinie > Global App Configuration Service
Citrix Workspace-App für iOS	StoreFront und Cloud	Global App Configuration Service
Citrix Workspace-App für Android	StoreFront und Cloud	Global App Configuration Service

Einschränkungen

- Der Global App Configuration Service wird für Linux nicht unterstützt.
- Unter Windows und Mac können Sie nicht mehr als einen Global App Configuration Service-aktivierten Store hinzufügen.

Weitere Ressourcen

- [Technical Brief on Global App Configuration service](#)
- [FAQs: Global App Configuration service settings and behaviours](#)
- [Webinar-Aufzeichnung: How to use Global App Configuration service](#)
- [Citrix Features Explained: Global App Configuration Service](#)

Einstellungen für Cloudstores konfigurieren

November 27, 2023

Übersicht

Sie können die Einstellung für Cloudstores der Citrix Workspace-App mit dem Global App Configuration Service (GACS) konfigurieren. Damit können Administratoren die Citrix Workspace-App für Endbenutzer auf verwalteten und nicht verwalteten Geräten konfigurieren und verwalten. Dieser Dienst wird unter Windows, Mac, Android, iOS, HTML5 und ChromeOS unterstützt.

Voraussetzung

- Die Adresse <https://discovery.cem.cloud.us> muss kontaktierbar sein. Sie ist für das Funktionieren von E-Mail-basierter Ermittlung und Global App Configuration Service erforderlich.
- Stellen Sie sicher, dass Sie Zugriff auf ein Citrix Cloud-Konto haben. Falls nicht, können Sie ein Konto unter <https://onboarding.cloud.com/> erstellen. Weitere Informationen finden Sie unter [Bei Citrix Cloud registrieren](#).
- Stellen Sie sicher, dass Sie ein Workspace-Abonnement haben.

Erste Schritte

Sie können sich bei Ihrem Citrix Cloud-Konto anmelden und Einstellungen unter **Workspacekonfiguration > App-Konfiguration** konfigurieren.

Überprüfen Sie vor dem Fortfahren, ob Sie über die folgenden Berechtigungen verfügen.

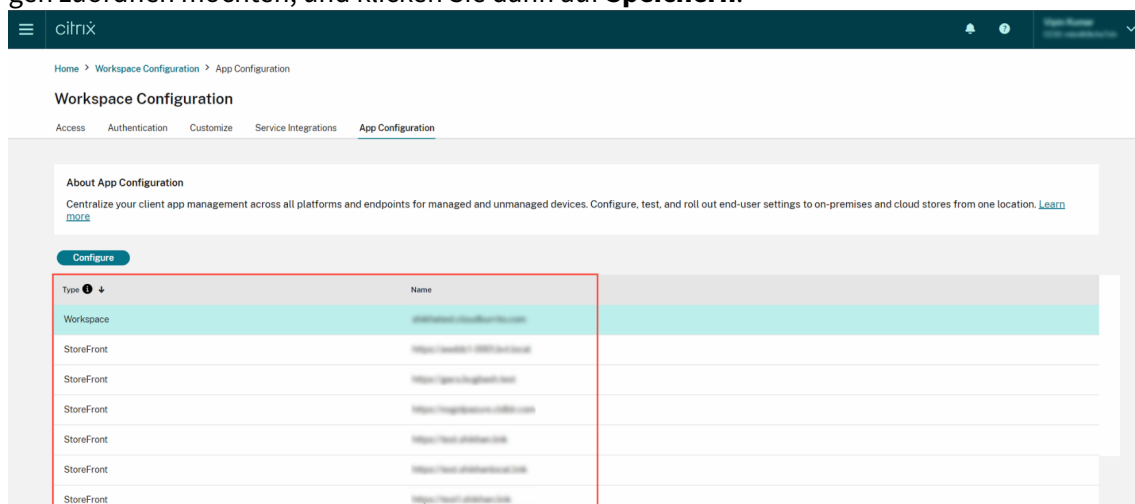
- **Workspace-Abonnement:** Das Workspace-Abonnement ist erforderlich, um eine Workspace-URL zu erstellen. Ohne Abonnement können Sie keine Cloudstores hinzufügen und konfigurieren. Ihnen wird nur die Option zur Konfiguration von On-Premises-Stores angeboten.

- **Workspace-URL:** Wenn Sie ein Workspace-Abonnement haben, aber Ihre URL noch nicht hinzugefügt haben, wird der folgende Bildschirm angezeigt. Sie können unter **Einstellungen für Cloudstores konfigurieren** auf **Start** klicken, um Ihre URL zu erstellen.

Einstellungen konfigurieren

Sie können die Einstellungen für die Citrix Workspace-App über das Citrix Cloud-Portal konfigurieren. Wenn mehrere Stores für Ihr Unternehmen konfiguriert wurden, können Sie jeden separat konfigurieren.

1. Melden Sie sich bei [Citrix Cloud](#) mit Ihren Citrix Cloud-Anmeldeinformationen an.
2. Gehen Sie zu **Workspacekonfiguration > App-Konfiguration**.
3. Klicken Sie auf **URL wechseln**, um den Store auszuwählen, für den Sie Einstellungen konfigurieren möchten.
4. Wählen Sie in der Liste der URLs der konfigurierten Store den Store aus, für den Sie Einstellungen zuordnen möchten, und klicken Sie dann auf **Speichern**.



5. Ändern Sie die Einstellungen für Ihre bevorzugten Plattformen nach Bedarf.
6. Klicken Sie auf **Entwürfe veröffentlichen**, um die Einstellungen zu speichern.

Hinweis:

Es kann einige Stunden dauern, bis die Einstellungen auf den Citrix Workspace-App-Clients aktualisiert werden. Weitere Informationen finden Sie unter [Häufigkeit des Abrufs aktualisierter Einstellungen](#).

E-Mail-basierte Erkennung einrichten

Der Dienst für die E-Mail-basierte Erkennung ermöglicht es Endbenutzern, sich automatisch mit ihrer E-Mail-Adresse anzumelden. Sie müssen keine Store-URLs angeben.

Um diesen Dienst für Cloudspeicher zu aktivieren, müssen Sie die folgenden Schritte ausführen.

1. [Beanspruchen einer Domäne](#)
2. [Zuordnung zwischen Domäne und URL erstellen](#)

Beanspruchen einer Domäne

Domäne beanspruchen:

1. Gehen Sie zu <https://adsui.cloud.com>.
2. Gehen Sie zu **Ansprüche > Domänen > Domäne hinzufügen**.
3. Geben Sie die Domäne ein, die Sie beanspruchen möchten (z. B. ace.example.com).
4. Klicken Sie auf **Bestätigen**.
5. Kopieren Sie das angezeigte DNS-Token.
6. Um einen DNS-TXT-Eintrag zu erstellen, rufen Sie das Dienstanbieterportal auf und fügen Sie das DNS-Token hinzu.
7. Überprüfungsprozess starten:
 - a) Gehen Sie zu **Ansprüche > Domänen**.
 - b) Gehen Sie zu der Domäne, die Sie hinzugefügt haben, und klicken Sie auf die Auslassungspunkte.
 - c) Wählen Sie **Domäne überprüfen**.
 - d) Klicken Sie auf **DNS-Prüfung starten**.

Sobald die Überprüfung abgeschlossen ist, ändert sich der Status Ihrer Domäne von *ausstehend* zu *verifiziert*.

Zuordnung zwischen Domäne und URL erstellen

1. Gehen Sie zu **Ansprüche > Domänen**.
2. Gehen Sie zu der Domäne, die Sie hinzugefügt haben, und klicken Sie auf die Auslassungspunkte.
3. Klicken Sie auf **Weitere Server-URL hinzufügen**.

4. Geben Sie die Store-URL ein, die Sie dieser Domäne zuordnen möchten.
5. Klicken Sie auf **Speichern**.

Einstellungen für On-Premises-Stores konfigurieren

November 27, 2023

Übersicht

Sie können die Einstellungen der Citrix Workspace-App für On-Premises-Stores mit dem Global App Configuration Service (GACS) konfigurieren. Damit können Sie die Citrix Workspace-App für Endbenutzer auf verwalteten und nicht verwalteten Geräten konfigurieren und verwalten. Der Global App Configuration Service wird unter Windows, Mac, Android, iOS, HTML5 und ChromeOS unterstützt.

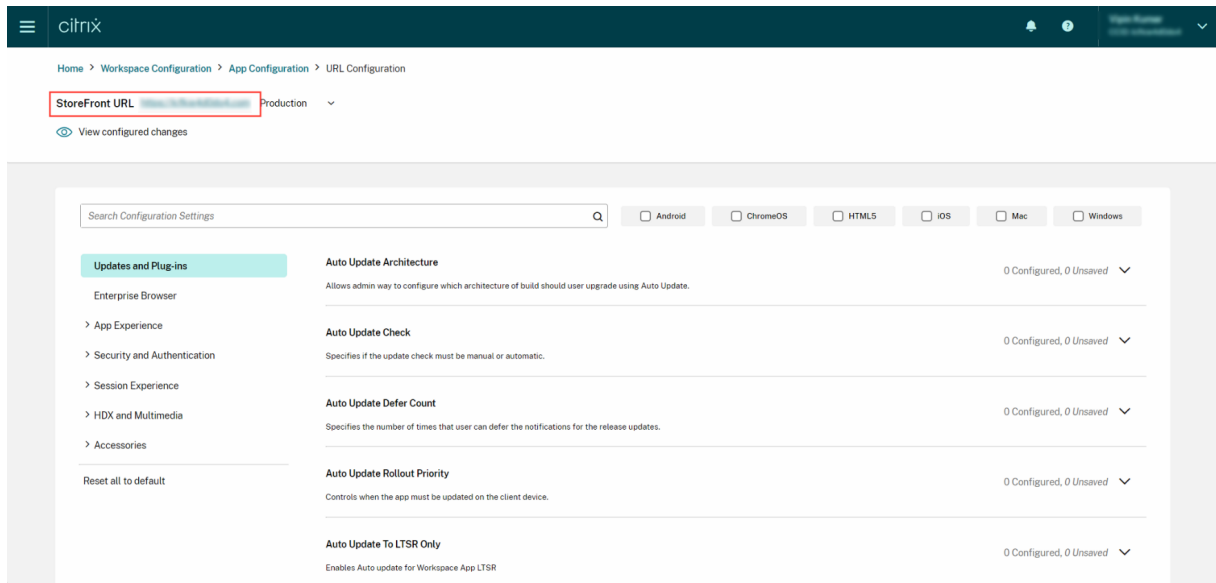
Voraussetzung

- Die Adresse <https://discovery.cem.cloud.us> muss kontaktierbar sein. Sie ist für das Funktionieren von E-Mail-basierter Ermittlung und Global App Configuration Service erforderlich.
- Stellen Sie sicher, dass Sie Zugriff auf ein Citrix Cloud-Konto haben. Wenn Sie noch kein Konto haben, können Sie unter <https://onboarding.cloud.com/> ein Konto erstellen. Weitere Informationen finden Sie unter [Bei Citrix Cloud registrieren](#).
- In einer On-Premises-Umgebung müssen Sie eine URL beanspruchen, bevor Sie die Einstellungen konfigurieren können. Weitere Informationen finden Sie unter [URL beanspruchen](#).

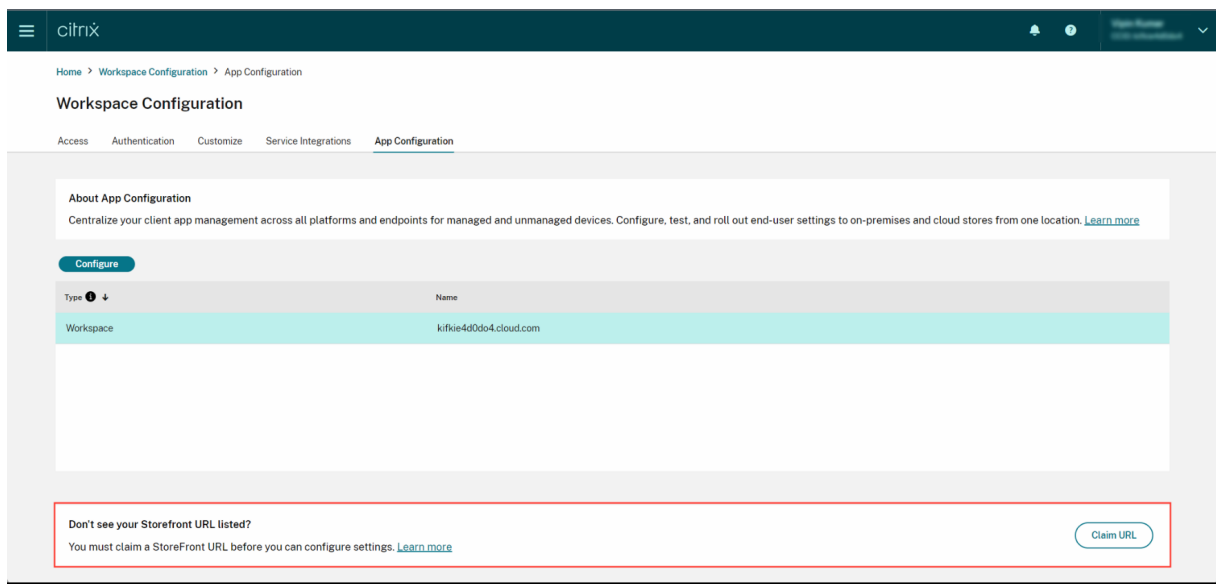
Erste Schritte

Um Einstellungen für einen On-Premises-Store zu konfigurieren, melden Sie sich bei Ihrem Citrix Cloud-Konto an und navigieren zu **Workspacekonfiguration > App-Konfiguration**.

Wenn Sie Ihre StoreFront-URL beansprucht haben, wird Ihnen der folgende Bildschirm angezeigt, wo Sie die Einstellungen konfigurieren können. Weitere Informationen finden Sie unter [Einstellungen konfigurieren](#).



Wenn Sie Ihre StoreFront-URL noch nicht beansprucht haben, werden Sie im folgenden Bildschirm dazu aufgefordert, bevor Sie fortfahren. Weitere Informationen finden Sie unter URL für On-Premises-Stores beanspruchen.



URL für On-Premises-Stores beanspruchen

Sie müssen einen Anspruch auf Ihre URL geltend machen, bevor Sie die Einstellungen für die URL konfigurieren können.

URL beanspruchen:

1. Melden Sie sich bei <https://adsui.cloud.com/url> mit Ihren Citrix Cloud-Anmeldeinformationen an.

2. Gehen Sie zu **Ansprüche > URLs > URL hinzufügen**.
3. Geben Sie die gewünschte URL ein.
4. Klicken Sie auf **Bestätigen**. Das Popupfenster zur Überprüfung wird angezeigt.

Hinweis:

Wenn in der On-Premises-Umgebung kein NetScaler Gateway installiert ist, können Sie den Überprüfungsprozess nicht durchführen (ab Schritt 5). Führen Sie in diesem Fall die Schritte 1 bis 4 oben aus und kontaktieren Sie unser [Support-Team](#), mit der Kunden-ID und URL, die Sie beanspruchen möchten.

5. Wenn in Ihrer On-Premises-Umgebung ein NetScaler Gateway installiert ist, können Sie Ihre URL mithilfe der folgenden Schritte überprüfen.
 - a) **Kopieren** Sie den Token, der im Popupfenster angezeigt wird.
 - b) Erstellen und konfigurieren Sie eine Responder-Aktion und eine Responder-Richtlinie in Ihrem Citrix ADC.
 - c) Binden Sie die Responder-Richtlinien global ein.
 - d) Gehen Sie zu `https://<customergatewayurl>/vpn/CitrixClaims` , um zu überprüfen, ob Ihre Responder-Richtlinie korrekt konfiguriert ist.
 - e) Gehen Sie zurück zu **Ansprüche > URLs** und suchen Sie die URL, die Sie hinzugefügt haben.
 - f) Klicken Sie auf die Auslassungspunkte für die hinzugefügte URL.
 - g) Wählen Sie **URL überprüfen**.
 - h) Klicken Sie auf **Anspruchsprüfung starten**, um den Überprüfungsprozess zu starten.

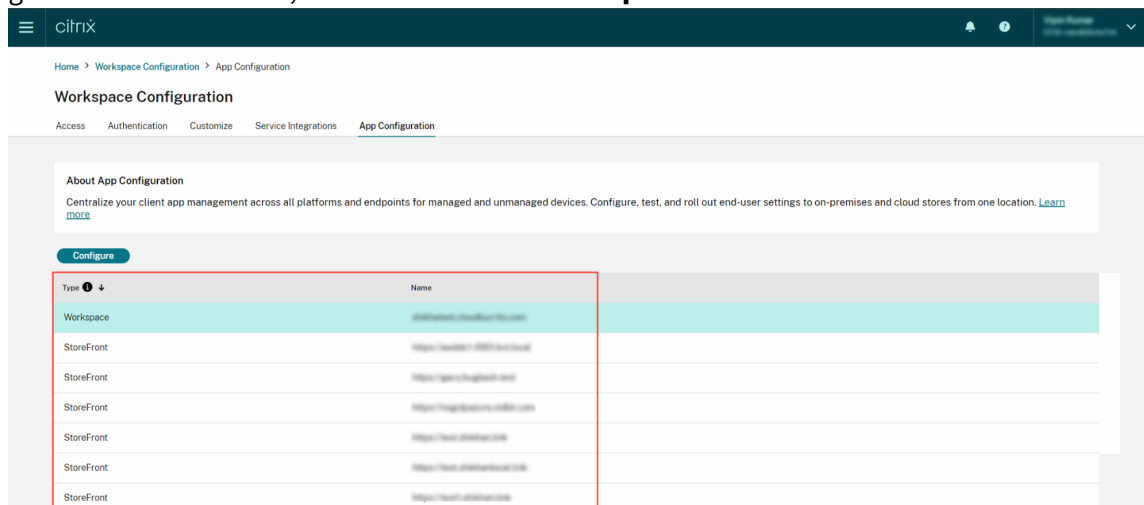
Nach Abschluss der Konfiguration ändert sich der Status Ihrer Domäne von *Ausstehend* in *Verifiziert*.

Einstellungen konfigurieren

Sobald Sie die URL beansprucht haben, können Sie Einstellungen für die Citrix Workspace-App konfigurieren. Wenn mehrere Stores für Ihr Unternehmen konfiguriert wurden, können Sie die Einstellungen für jeden Store separat konfigurieren.

1. Gehen Sie zum [Citrix Cloud-Portal](#) und melden Sie sich mit Ihren Anmeldeinformationen an.
2. Gehen Sie zu **Workspacekonfiguration > App-Konfiguration**.
3. Klicken Sie auf **URL wechseln**, um den Store auszuwählen, für den Sie Einstellungen konfigurieren möchten.

4. Wählen Sie in der Liste der URLs der konfigurierten Store den Store aus, für den Sie Einstellungen zuordnen möchten, und klicken Sie dann auf **Speichern**.



5. Ändern Sie die Einstellungen für Ihre bevorzugten Plattformen nach Bedarf.
6. Klicken Sie auf **Entwürfe veröffentlichen**, um die Einstellungen zu speichern.

Hinweis:

Es kann einige Stunden dauern, bis die Einstellungen auf den Citrix Workspace-App-Clients aktualisiert werden. Weitere Informationen finden Sie unter [Häufigkeit des Abrufs aktualisierter Einstellungen](#).

E-Mail-basierte Ermittlung einrichten

Der Dienst für die E-Mail-basierte Erkennung ermöglicht es Endbenutzern, sich automatisch mit ihrer E-Mail-Adresse anzumelden. Sie müssen keine Store-URLs angeben.

Um diesen Dienst für Cloudspeicher zu aktivieren, müssen Sie die folgenden Schritte ausführen.

1. [Beanspruchen einer Domäne](#)
2. [Zuordnung zwischen Domäne und URL erstellen](#)

Beanspruchen einer Domäne

Domäne beanspruchen:

1. Gehen Sie zu [Autodiscoverydienst](#).
2. Gehen Sie zu **Ansprüche > Domänen > Domäne hinzufügen**.
3. Geben Sie die Domäne ein, die Sie beanspruchen möchten (z. B. ace.example.com).

4. Klicken Sie auf **Bestätigen**.
5. Kopieren Sie den auf dem Bildschirm angezeigten DNS-Token in die Zwischenablage.
6. Um einen DNS-TXT-Eintrag zu erstellen, rufen Sie das Dienstanbieterportal auf und fügen Sie das DNS-Token hinzu.
7. Überprüfungsprozess starten:
 - a) Gehen Sie zu **Ansprüche > Domänen**.
 - b) Gehen Sie zu der Domäne, die Sie hinzugefügt haben, und klicken Sie auf die Auslassungspunkte.
 - c) Wählen Sie **Domäne überprüfen**.
 - d) Klicken Sie auf **DNS-Prüfung starten**.

Sobald die Überprüfung abgeschlossen ist, ändert sich der Status Ihrer Domäne von *ausstehend* zu *verifiziert*.

Hinweis:

Sie können maximal 10 Domänen beanspruchen. Wenn Sie mehr als 10 Domänen beanspruchen möchten, wenden Sie sich an den [Citrix Support](#) und geben Sie Ihre Kunden-ID und URL an.

Zuordnung zwischen Domäne und URL erstellen

1. Gehen Sie zu **Ansprüche > Domänen**.
2. Gehen Sie zu der Domäne, die Sie hinzugefügt haben, und klicken Sie auf die Auslassungspunkte.
3. Klicken Sie auf **Weitere Server-URL hinzufügen**.
4. Geben Sie die Store-URL ein, die Sie dieser Domäne zuordnen möchten, und speichern Sie sie.

Kanalkonfiguration testen

November 27, 2023

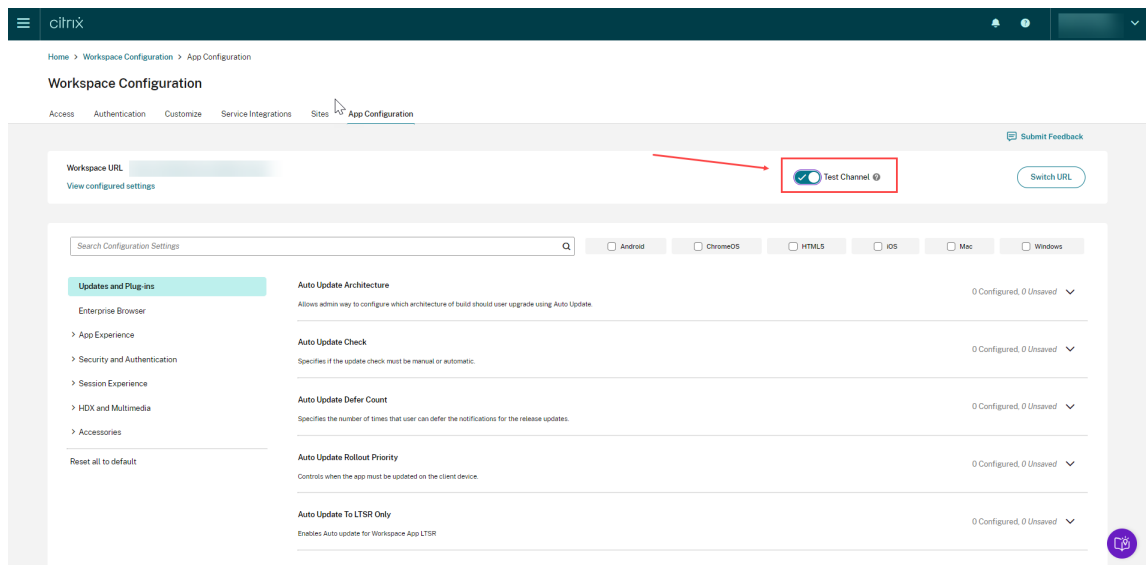
Sie können Ihre Konfiguration testen, bevor Sie sie für die Endbenutzer aktivieren. Damit können Sie Probleme erkennen und lösen, die nach der Bereitstellung auftreten könnten.

Die Testfunktion reduziert die Wahrscheinlichkeit von Störungen oder Fehlern während der Bereitstellung erheblich und erhöht die allgemeine Benutzerzufriedenheit.

Konfiguration testen:

1. Melden Sie sich beim [Cloud-Portal](#) mit Ihren Citrix Cloud-Anmeldeinformationen an.

2. Gehen Sie zu **Workspacekonfiguration > App-Konfiguration**.
3. Stellen Sie den Umschalter auf **Testkanal**. Er ist standardmäßig auf **Produktion** eingestellt.



4. Ändern Sie die Einstellungen für Ihre bevorzugten Plattformen nach Bedarf.
5. Sie können dann auf **Entwürfe veröffentlichen** klicken, um die Einstellungen im Testkanal zu veröffentlichen.

Hinweis:

Der Global App Configuration Service unterstützt nur zwei Kanäle pro Store –Produktion (Standard) und Test.

Kanalunterstützung auf Endbenutzergeräten konfigurieren

Windows

Um die von Administratoren definierte Konfiguration auf einem Windows-Gerät zu testen, müssen die Benutzer folgenden Registrierungsschlüssel erstellen.

```
1 Path- HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
2 Name- AppConfigChannelName
3 Type- REG_SZ
4 Value- testrolloutchannel1
5
6 <!--NeedCopy-->
```

Mac

Um die vom Administrator definierte Konfiguration auf einem Mac-Gerät zu testen, müssen die Benutzer folgende Schritte ausführen.

1. Legen Sie den Namen des Testkanals für den Global App Configuration Service mit folgendem Befehl fest:

```
1 defaults write com.citrix.receiver.nomas GACSCChannelName  
   testrolloutchannel1  
2  
3 <!--NeedCopy-->
```

2. Starten Sie Citrix Workspace Helper mit den folgenden Befehlen neu:

```
1 launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.  
   plist  
2  
3 launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.  
   plist  
4  
5 <!--NeedCopy-->
```

Nach dem Neustart des Geräts wird die Konfiguration für den Testkanal automatisch abgerufen.

iOS

Um die vom Administrator definierte Konfiguration auf einem iOS-Gerät zu testen, gehen Sie wie folgt vor.

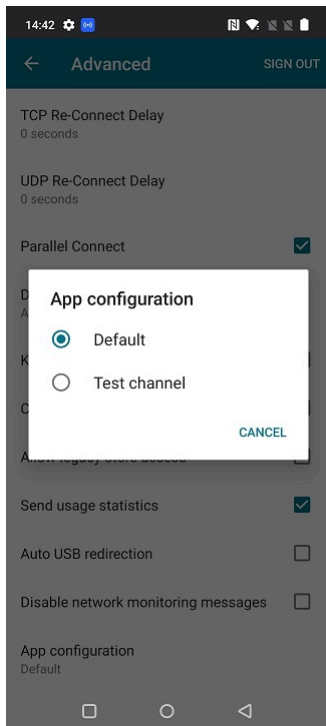
1. Melden Sie sich bei der Citrix Workspace-App an.
2. Gehen Sie zu **Einstellungen** > **Erweitert** > **App-Konfiguration**.
3. Wählen Sie den Testkanal.
4. Sie können jetzt die vom Administrator erstellte Konfiguration testen.



Android

Um die vom Administrator definierte Konfiguration auf einem Android-Gerät zu testen, gehen Sie wie folgt vor.

1. Melden Sie sich bei der Citrix Workspace-App an.
2. Gehen Sie zu **Einstellungen > Erweitert > App-Konfiguration**.
3. Wählen Sie den Testkanal.
4. Sie können jetzt die vom Administrator erstellte Konfiguration testen.



Verwalten der Workspace-Benutzeroberfläche

November 27, 2023

Dieser Artikel bietet einen Überblick darüber, wie Abonnenten auf ihre Workspaces zugreifen und mit ihnen interagieren können. Es werden Optionen zur Verbesserung der Workspace-Benutzeroberfläche und Lösungen für häufig auftretende Probleme erläutert.

Workspace-Zugriff

Abonnenten können auf zweierlei Art auf Citrix Workspace zugreifen:

- Über einen Browser mit der Workspace-URL
- Per Citrix Workspace-App, die auf Abonentengeräten installiert ist

Browserzugriff

Abonnenten müssen die neueste Version von Edge, Chrome, Firefox oder Safari verwenden, wenn sie sich über den Browser anmelden. Benutzer können ihre Workspace-URL eingeben, um auf ihre Workspaces zuzugreifen. Weitere Informationen finden Sie unter [Workspace Browser Compatibility](#).

Die Workspace-URL ist standardmäßig aktiviert, normalerweise im Format <https://yourcompanyname.cloud.com>. Informationen zum Konfigurieren der Workspace-URL finden Sie unter [Workspace-URL](#).

Zugriff per Citrix Workspace-App

Citrix empfiehlt, die neueste Version der Citrix Workspace-App für den Zugriff auf Workspaces zu verwenden.

Die Citrix Workspace-App ist eine nativ installierte App, die Citrix Receiver ersetzt und eine plattformübergreifend konsistente Workspace-Benutzeroberfläche bietet. Die Citrix Workspace-App ist für verschiedene Betriebssysteme verfügbar. Weitere Informationen finden Sie in der Produktdokumentation der [Citrix Workspace-App](#).

Wenn Sie bislang Citrix Receiver verwendet haben, sollten Sie Ihre Benutzer anleiten, ein Upgrade auf die Citrix Workspace-App durchzuführen, um alle Features der Workspace-Benutzeroberfläche nutzen zu können. Weitere Informationen zu den von der Citrix Workspace-App unterstützten Features (sortiert nach Plattform) finden Sie in der [Workspace-App-Feature-Matrix](#).

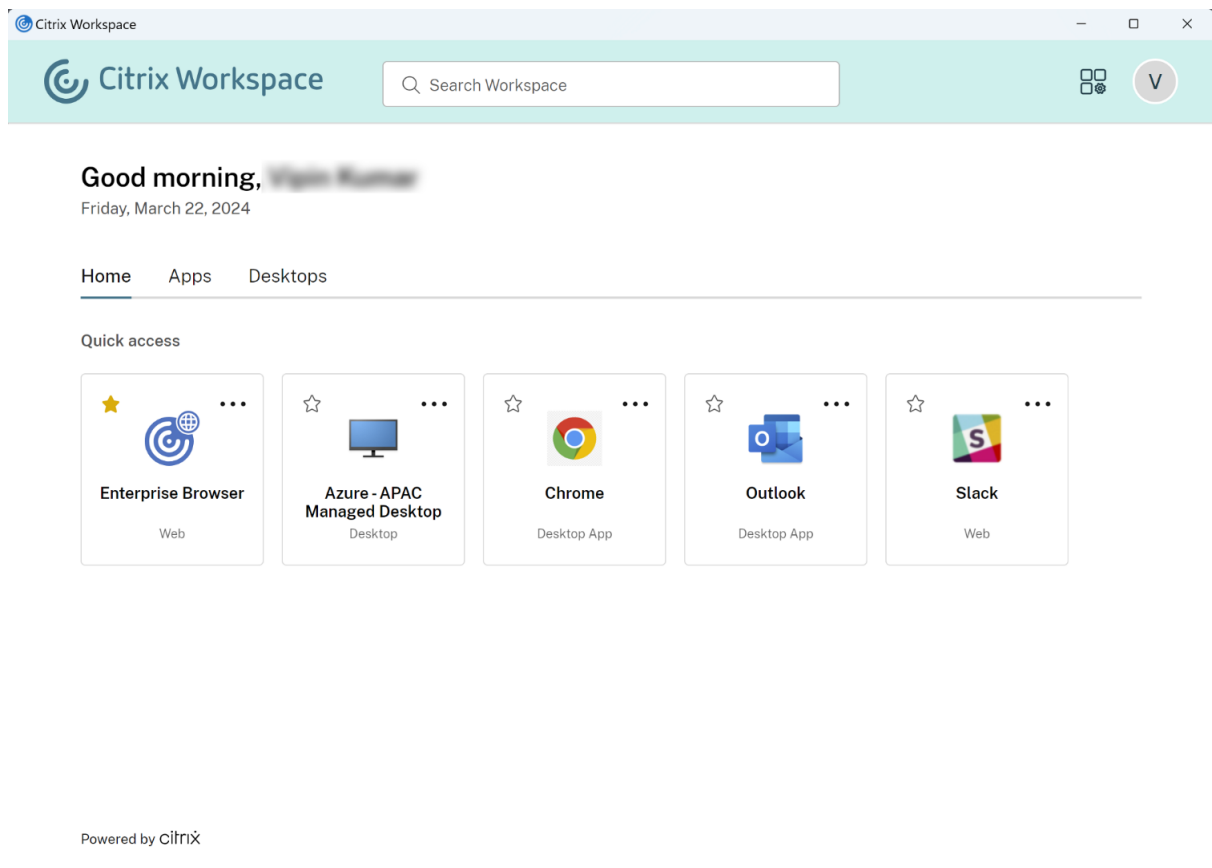
Informationen zur Installation der Citrix Workspace-App finden Sie unter [Download Citrix Workspace app](#).

Bei Geräten, auf denen die Citrix Workspace-App-Software nicht installiert werden kann, ermöglicht die Citrix Workspace-App für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.

Workspace-Benutzeroberfläche und Features

Neue Kunden. Wenn Sie ein neuer Workspace-Kunde sind, erhalten die Abonnenten die neueste Version der Benutzeroberfläche, sobald diese verfügbar ist.

Bestehende Kunden. Wenn Sie eine ältere Version der Citrix Workspace verwendet haben, kann es etwa fünf Minuten dauern, bis die aktualisierte Benutzeroberfläche angezeigt wird. Möglicherweise wird vorübergehend eine ältere Version der Benutzeroberfläche angezeigt.



Die Citrix Workspace-Benutzeroberfläche umfasst die folgenden Features:

Single Sign-On (SSO)

Citrix Workspace bietet eine nahtlose Erfahrung mit Single Sign-On (SSO) für sekundäre Ressourcen, die normalerweise eine zweite Authentifizierung erfordern würden.

Kartenlayout

Apps, Desktops, Dateien, Aktionen und der **Aktivitätsfeed** werden als Karten dargestellt. Ein Pop-upfenster zeigt weitere Details und Aktionen.

Einstellungen

Abonnenten greifen über ein Menü auf **Einstellungen** zu, das angezeigt wird, wenn sie ihr Profilsymbol oben rechts im Workspace auswählen.

Profilsymbol

Abonnenten können ein Bild in ihr Profil hochladen. Wenn kein Profilbild festgelegt ist, wird standardmäßig ein Symbol verwendet, das auf dem Active Directory-Anzeigenamen des Abonnenten basiert.

Suche

Mit dem oben angezeigten Suchtool können alle Ressourcen im Workspace durchsucht werden. Abonnenten können Apps direkt aus den Suchergebnissen heraus öffnen. Für die Suche ist die Eingabe von mindestens drei Zeichen erforderlich.

Ansicht “Zuletzt verwendet” und “Favoriten”

Abonnenten können zwischen der Ansicht **Zuletzt verwendet** und **Favoriten** für ihre Apps, Desktops und Dateien wählen.

Sie können **Favoriten** konfigurieren, um das Feature für Abonnenten in der **Workspacekonfiguration** zu aktivieren oder zu deaktivieren. Weitere Informationen zum Aktivieren und Deaktivieren des Features **Favoriten** in Citrix Workspace finden Sie unter [Zulassen von Favoriten](#).

Zweistufige Authentifizierung (optional)

Bevor Abonnenten die zweistufige Authentifizierung für Citrix Workspace verwenden können, müssen sie ihr Gerät registrieren. Während der Registrierung präsentiert Workspace einen QR-Code, den der Abonnent mit einer Authentifikator-App scannen kann. Die Authentifikator-App muss dem [Standard des zeitbasierten Einmalkennworts \(TOTP\)](#) folgen, z. B. [Citrix SSO](#).

Hinweis:

Für eine reibungslose Registrierung empfiehlt Citrix, [Citrix SSO](#) vorher herunterzuladen und auf dem Gerät zu installieren.

Zur Registrierung für die zweistufige Authentifizierung fordern Sie den Abonnenten auf, folgende Schritte auszuführen:

1. Öffnen Sie einen Browser, navigieren Sie zur Workspace-Anmeldeseite und wählen Sie **Haben Sie kein Token?**.
2. Geben Sie den Benutzernamen im Format `domain\username` oder die Firmen-E-Mail-Adresse ein und wählen Sie **Weiter**. Citrix Cloud sendet dem Abonnenten eine E-Mail mit einem temporären Verifizierungscode.

3. Geben Sie bei entsprechender Aufforderung den Verifizierungscode und das Kennwort Ihres Active Directory-Kontos ein und wählen Sie **Weiter**.

WICHTIG:

Der Verifizierungscode ist ein temporäres Token mit einer Gültigkeitsdauer von 24 Stunden und wird nur zur Registrierung des Geräts des Abonnenten verwendet. Der Abonnent darf den Code nicht verwenden, um sich per zweistufiger Authentifizierung bei seinem Workspace anzumelden.

4. Scannen Sie in der Authentifikator-App den QR-Code oder geben Sie den Verifizierungscode manuell ein.
5. Wählen Sie **Fertigstellen** und **Anmelden**, um die Registrierung abzuschließen.

Nach Abschluss der Registrierung können die Abonnenten zur Citrix Workspace-Anmeldeseite zurückkehren und ihre Active Directory-Anmeldeinformationen zusammen mit dem Token eingeben, der in der Authentifikator-App angezeigt wird.

Nur Verifizierungs-codes, die von einer Authentifikator-App auf einem registrierten Gerät generiert werden, sind unterstützte Token für die zweistufige Authentifizierung. Abonnenten dürfen nicht den während der Registrierung gesendeten temporären E-Mail-Token verwenden.

Anpassen von Workspaces

In der **Workspacekonfiguration** können Sie die Workspace-Benutzeroberfläche für einzelne Abonnenten und gemäß spezieller Unternehmensanforderungen anpassen.

- Wie Sie zielgerichtete Benachrichtigungen im **Aktivitätsfeed** und auf der Karte **Aktionen** von Workspaces konfigurieren, erfahren Sie unter [Anpassen von Workspace-Benachrichtigungen](#).
- Wie Sie die Darstellung von Workspaces anpassen, einschließlich Logos und benutzerdefinierter Designs, erfahren Sie unter [Anpassen der Darstellung von Workspaces](#).
- Wie Sie die Interaktion von Abonnenten mit ihrem Workspace anpassen, damit Abonnenten beispielsweise **Favoriten** erstellen können und Desktops automatisch starten, erfahren Sie unter [Anpassen von Workspace-Interaktionen](#).
- Informationen zum Anpassen der Datenschutz- und Sicherheitsrichtlinien finden Sie unter [Anpassen von Sicherheits- und Datenschutzrichtlinien](#). Die Datenschutz- und Sicherheitsrichtlinien umfassen Einstellungen wie den Timeoutzeitraum, die Anmeldezeitlinie und die Kennwortverwaltung für Endbenutzer.

Problembehandlung

Ab- und erneute Anmeldung nach Wechsel der Authentifizierungsmethode

Wenn Sie die Authentifizierungsmethode ändern, wird Abonnenten, die angemeldet sind, möglicherweise eine Fehlermeldung angezeigt. Abonnenten müssen sich bei Citrix Workspace abmelden, den Browser oder die Citrix Workspace-App schließen und sich nach ca. 5 Minuten wieder anmelden. Abonnenten können sich dann mit der neuen Authentifizierungsmethode anmelden.

Weitere Informationen finden Sie unter [Auswählen und Ändern von Authentifizierungsmethoden](#).

Aktualisieren nach Änderungen an Ihrem Serviceabonnement

Wenn Sie Ihr Serviceabonnement geändert haben, müssen Abonnenten die lokale Citrix Workspace-App möglicherweise manuell aktualisieren. Aktualisieren der Citrix Workspace-App für Windows:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das Symbol für Citrix Workspace und wählen Sie **Erweiterte Einstellungen > Citrix Workspace zurücksetzen**.
2. Öffnen Sie die Citrix Workspace-App für Windows und wählen Sie **Konten > Hinzufügen**.
3. Geben Sie die Workspace-URL ein und wählen Sie **Hinzufügen**.

Sie können die Citrix Workspace-App auch über den Browser aktualisieren. Aktualisieren über den Browser:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das Symbol für Citrix Workspace und wählen Sie **Erweiterte Einstellungen > Citrix Workspace zurücksetzen**.
2. Geben Sie die Workspace-URL in den Browser ein und melden Sie sich an.
3. Laden Sie die Konfigurationsdatei von **Einstellungen > Kontoeinstellungen > Erweitert > Workspacekonfiguration herunterladen** herunter.

Es wird eine Datei mit der Erweiterung **.cr** heruntergeladen, die den Workspace Ihrer lokalen Citrix Workspace-App hinzufügt.

Anpassen der Darstellung von Workspaces

October 12, 2023

Workspace-Benutzeroberfläche anpassen

In diesem Abschnitt wird beschrieben, wie Sie das Erscheinungsbild von Workspaces unter **Konfiguration > Anpassen > Darstellung** anpassen können.

Über Designs können Sie Farben und Logos von Workspaces konfigurieren. Logos müssen die erforderlichen Abmessungen aufweisen, um eine verzerrte Darstellung bzw. das Erscheinen einer Fehlermeldung zu vermeiden.

Logo	Erforderliche Abmessungen	Max. Größe	Unterstützte Formate
Unternehmenslogo bei Anmeldung	480 x 120 Pixel	2 MB	JPEG, JPG oder PNG
Logo nach Anmeldung	340 x 80 Pixel	2 MB	JPEG, JPG oder PNG

Änderungen an der Workspacedarstellung werden sofort wirksam, wenn Sie **Speichern** auswählen.

Anpassen des Standarddesigns

Das Standarddesign umfasst das Anmeldelogo und das Workspace-Logo sowie die Farben, die nach der Anmeldung für Abonnenten angezeigt werden. Sie können eines oder mehrere dieser Elemente ändern.

Workspace Configuration

- Access
- Authentication
- Customize
- Service Integrations
- Sites
- Service Continuity

- Appearance
- Features
- Preferences

Customize how subscribers will see their workspace.

Cancel Update

Default Appearance

Sign-in Appearance

Logo

This logo will appear on the sign-in page.



After Sign-in Appearance

Logo

This logo will appear after sign-in.



Colors

These colors appear in sign-in screens and within the workspace experience.

Banner color:



Accent color:

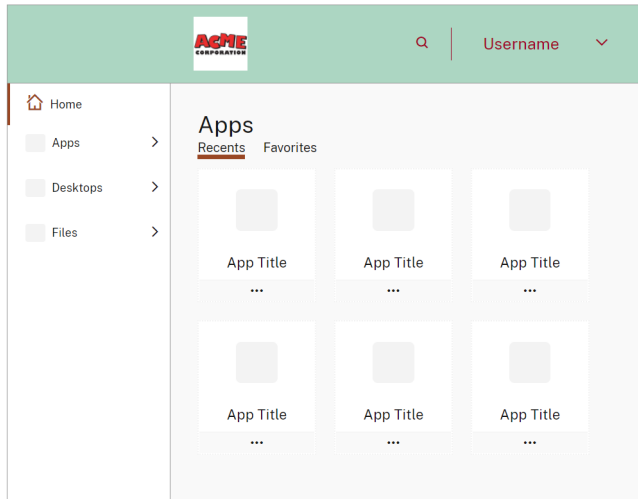


Banner text and icon color:



Preview

This is how your workspace will look:



Reset to Default

Appearance themes

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

+ Add theme



Anpassen des Designs für die Anmeldung

Auf der Anmeldeseite können Sie nur das Logo ersetzen. Der Rest, einschließlich der Farben, ist davon nicht betroffen.



The image shows a login form for Citrix Workspace. At the top center is the Citrix logo, a stylized 'C' composed of three concentric, curved lines. Below the logo is the text 'Citrix Workspace' in a large, dark teal font. Underneath is a 'Username' label followed by a text input field containing the placeholder text 'domain\user or user@domain.com'. Below that is a 'Password' label followed by a text input field containing the placeholder text 'Enter password'. At the bottom of the form is a large, rounded teal button with the text 'Sign In' in white.

Änderungen der Darstellung des Workspaces werden sofort wirksam. Bei lokalen Citrix Receiver-Apps kann es etwa fünf Minuten dauern, bis die aktualisierte Benutzeroberfläche angezeigt wird.

Hinweis:

Änderungen am Anmeldelogo wirken sich nicht auf Benutzer aus, die sich über externe Identitätsanbieter wie Azure AD oder Okta anmelden.

Informationen zum Anpassen der Azure AD-Anmeldeseite finden Sie in der [Microsoft-Dokumentation](#). Informationen zum Anpassen der Okta-Anmeldeseite finden Sie in der [Okta Developer-Dokumentation](#).

Sie können auch die Anmeldeseite für ein on-premises bereitgestelltes Citrix Gateway anpassen, konfiguriert im Citrix ADC-Gerät und nicht in der **Workspacekonfiguration**. Weitere Informationen finden Sie im [Support Knowledge Center-Artikel](#).

Anpassen der Darstellung von Workspaces

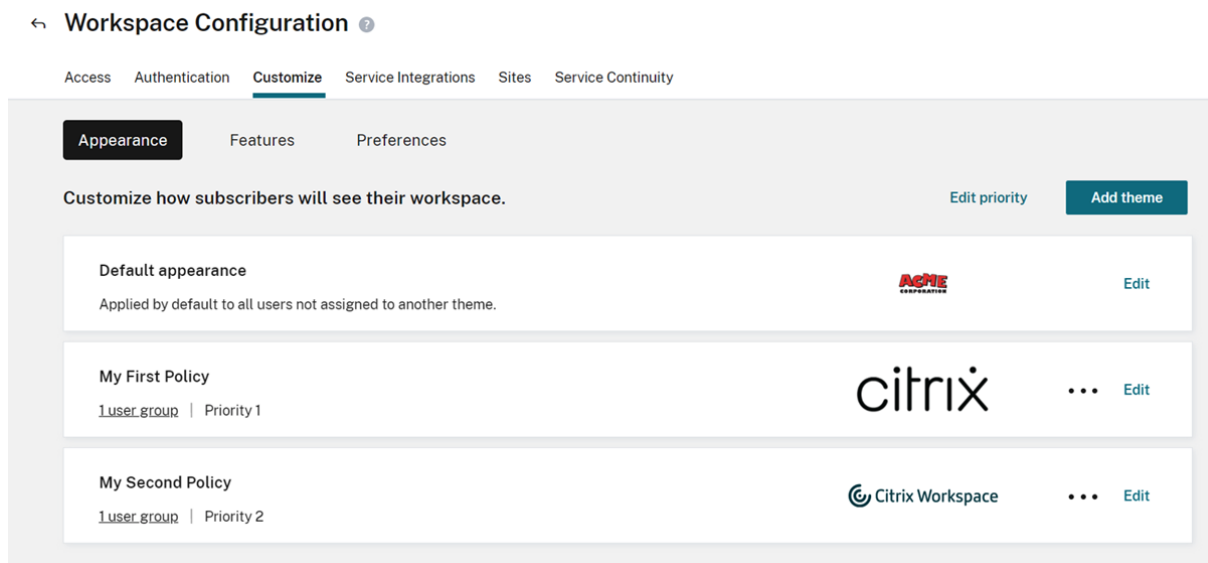
Das Anmeldelogo muss nicht mit dem Logo identisch sein, das oben links im Workspace angezeigt wird, nachdem sich ein Abonnent angemeldet hat. Zusätzlich zum Ersetzen des Workspace-Logos können Sie die Banner-, Akzent-, Text- und Symbolfarben für den Workspace vorgeben.

Erstellen mehrerer benutzerdefinierter Designs

Wichtig:

Dies ist ein **Einzelmandantenfeature**. Citrix Service Provider-Mandanten müssen über eigene Ressourcenstandorte, Cloud Connectors und eine dedizierte Active Directory-Domäne verfügen. Citrix Service Provider-Mandanten, die einen Ressourcenstandort, Cloud Connectors und eine Active Directory-Domäne teilen (Mehrmandantenumgebung), werden derzeit nicht unterstützt.

Sie können mehrere Citrix Workspace-Designs für einzelne Benutzergruppen konfigurieren und priorisieren. Die benutzerdefinierten Designs werden in Form von Karten unter dem Standarddesign aufgeführt. Wenn Sie keine zusätzlichen Designs einrichten, wird das Standarddesign für alle Benutzer angewendet.



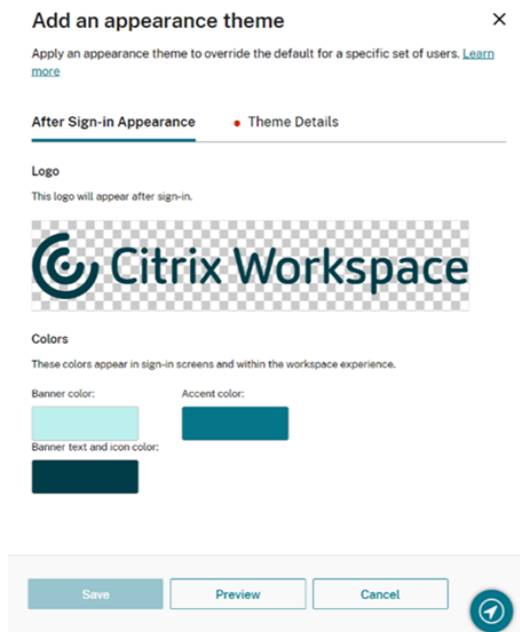
Konfigurieren benutzerdefinierter Designs

Um ein erstes benutzerdefiniertes Design unter dem Standarddesign hinzuzufügen, wählen Sie unten links auf der Karte im Abschnitt **Standarddarstellung** die Option **Design hinzufügen** aus.

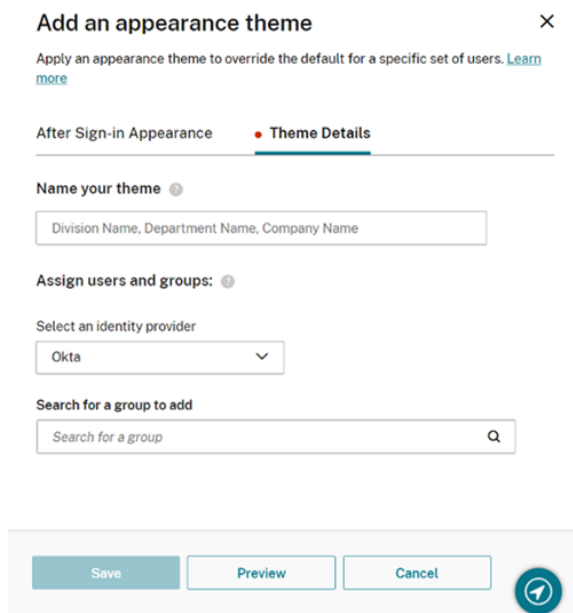
Wenn Sie unter dem Standarddesign bereits ein benutzerdefiniertes Design hinzugefügt haben, wählen Sie oben rechts in der Liste der Designs die Option **Design hinzufügen**.

1. Konfigurieren Sie das benutzerdefinierte Design folgendermaßen:

- a) Laden Sie das **Logo** hoch (optional).
- b) Definieren Sie Banner-, Akzent-, Text- und Symbol**farben** (optional).



2. Wählen Sie **Designdetails** und geben Sie einen aussagekräftigen Namen für das Design ein.



3. Weisen Sie dem Design Benutzergruppen zu:

- a) Wählen Sie einen Identitätsanbieter und die zugehörige Domäne aus, wenn Sie dazu aufgefordert werden.

- b) Suchen Sie die Benutzergruppe, die Sie dem benutzerdefinierten Design hinzufügen möchten.
- c) Wählen Sie das Pluszeichen (+) neben dieser Gruppe.
- d) Wiederholen Sie diesen Vorgang für jede Gruppe, die Sie dem Design hinzufügen möchten.

Add an appearance theme ×

Apply an appearance theme to override the default for a specific set of users. [Learn more](#)

After Sign-in Appearance
Theme Details

Name your theme ⓘ

My First Policy

Assign users and groups: ⓘ

Select an identity provider

Active Directory
▼

Select a domain

domain.com
▼

Search for a group to add

🔍

User groups (1):

Group
🗑️

4. Wählen Sie **Vorschau**, um zu sehen, wie der Workspace für Abonnenten angezeigt wird. Wenn Sie fertig sind, speichern Sie das Design.

Hinweis:

Die **Workspacevorschau** zeigt keine Vorschau, wenn Sie mit der älteren violetten Benutzeroberfläche arbeiten.

5. Wiederholen Sie die Schritte 1 bis 4, um weitere benutzerdefinierte Designs hinzuzufügen.

Priorisierung benutzerdefinierter Designs

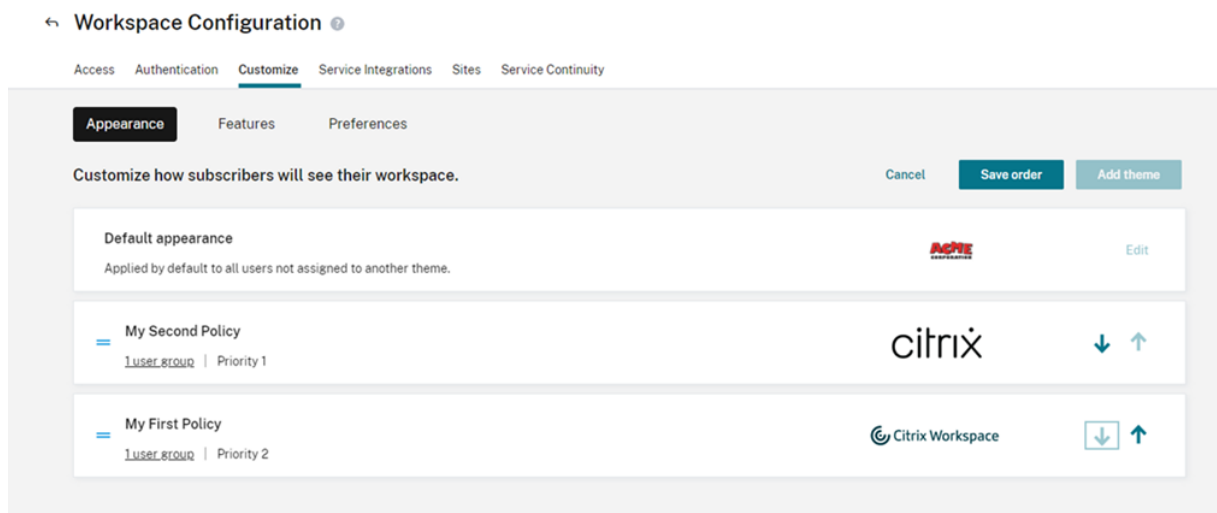
Benutzer können mehreren Benutzergruppen angehören, denen verschiedene Designs zugewiesen wurden. Sie können vorgeben, welches Design dem Abonnenten in diesem Fall angezeigt wird, indem Sie die Priorität der benutzerdefinierten Designs festlegen.

Wichtig

Damit die Priorisierung benutzerdefinierter Designs funktioniert, müssen Sie mindestens zwei benutzerdefinierte Designs unter dem Standarddesign konfigurieren.

1. Wählen Sie oben rechts in der Designliste neben **Design hinzufügen** die Option **Priorität bearbeiten**.

2. Sie können die Priorität von Designs auf zweierlei Art ändern:
 - Verwenden Sie die Pfeile rechts neben den Designs.
 - Ziehen Sie einzelne Designs an dem Ziehpunkt links auf der Karte in der Liste nach oben und unten.
3. Nachdem Sie die Designs umgeordnet haben, wählen Sie **Reihenfolge speichern**.



Workspace-Interaktionen anpassen

November 27, 2023

Sie können anpassen, wie Abonnenten Workspace verwenden. Wählen Sie dazu **Workspacekonfiguration > Anpassen > Einstellungen**.

Wenn Sie die Workspace-Einstellungen, die sich auf die Anmeldeerfahrung auswirken, an die Anforderungen Ihres Unternehmens anpassen möchten, gehen Sie zu [Anpassen von Sicherheits- und Datenschutzrichtlinien](#).

Wenn Sie die Darstellung von Workspace vor und nach der Anmeldung anpassen möchten, gehen Sie zu [Anpassen der Darstellung von Workspaces](#).

Caching zulassen

Die Einstellung **Caching zulassen** verbessert die Leistung für Abonnenten, die über einen Webbrowser auf Citrix Workspace zugreifen. Caching wird unterstützt, wenn mit einem [unterstützten Webbrowser](#) auf Citrix Workspace zugegriffen wird. Bei Verwendung einer lokal installierten Citrix Workspace-App ist das Caching nicht verfügbar.

Wenn Caching aktiviert ist, werden vertrauliche Daten möglicherweise lokal auf den Geräten der Abonnenten gespeichert. Dabei handelt es sich um Dateimetadaten, die mit einem für die authentifizierte Identität des Abonnenten eindeutigen Schlüssel verschlüsselt sind. Die verschlüsselten Daten werden in der Eigenschaft `localStorage` des Webbrowsers auf dem Gerät des Abonnenten gespeichert.

Wenn Sie das Caching deaktivieren, werden die verschlüsselten Daten gelöscht, wenn der Abonnent sich das nächste Mal über den Webbrowser bei Citrix Workspace anmeldet. Außerdem kann der Abonnent diese Daten manuell löschen, indem er die Browsingdaten aus seinem Webbrowser löscht.

Favoriten zulassen

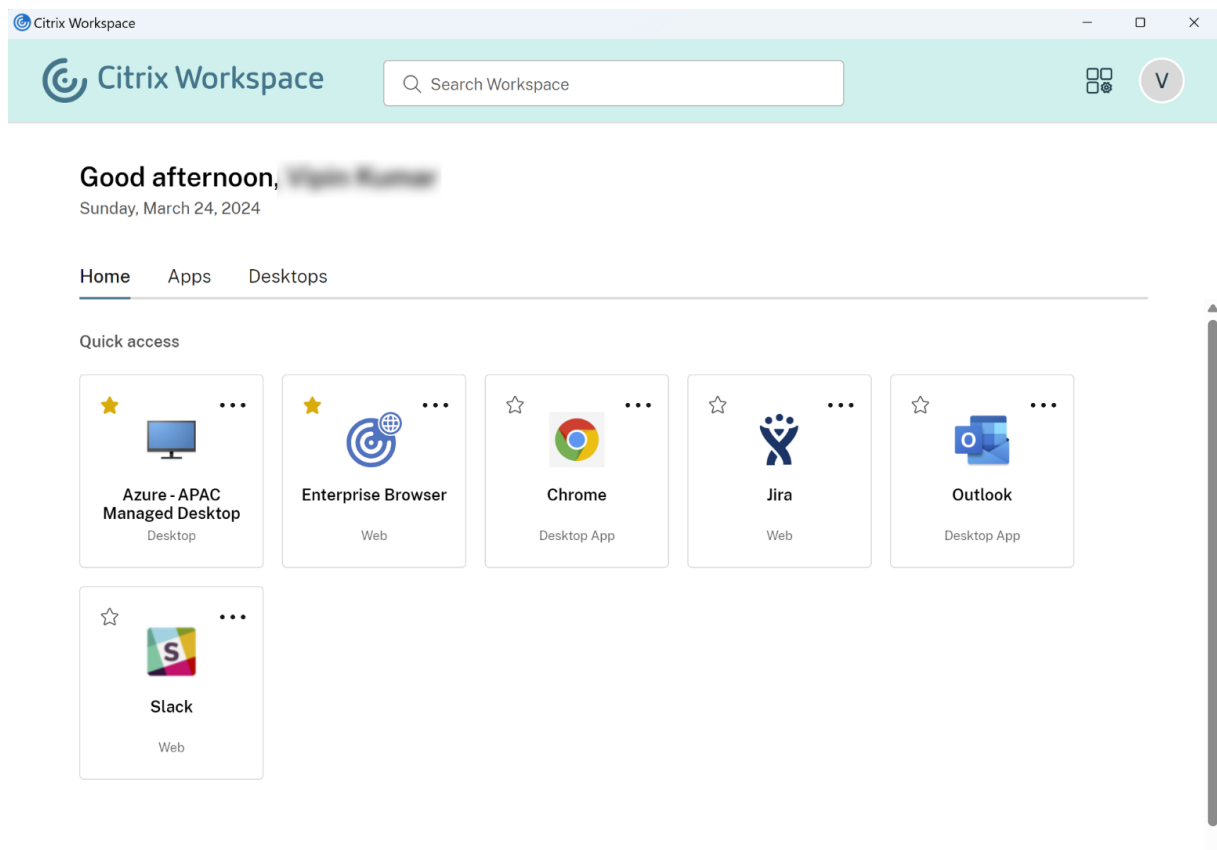
Kunden, die Zugriff auf die **Workspacekonfiguration** und die neue Workspace-Benutzeroberfläche haben, können Abonnenten ermöglichen, Favoriten von App- und Desktopressourcen einzurichten und wieder zu entfernen. Das Feature **Favoriten zulassen** ist standardmäßig aktiviert.

Hinweis:

- Für bestehende Kunden, deren Workspaceabonnement zwischen Dezember 2017 und April 2018 begonnen hat, ist **Favoriten zulassen** standardmäßig **deaktiviert**. Der Administrator entscheidet, wann diese Funktion für die Abonnenten aktiviert wird.

Benutzeroberfläche von “Favoriten zulassen” für Abonnenten

Wenn dies aktiviert ist (Standardeinstellung), können Abonnenten bis zu 250 **Favoriten** über das Sternensymbol oben links in den Karten (nicht obligatorischer) Apps und Desktops hinzufügen. Der Stern von Favoriten wird gelb angezeigt.



Wenn ein Abonnent das Maximum von 250 Favoriten überschreitet, wird der älteste Favorit entfernt, damit die neuesten **Favoriten** erhalten bleiben

Wenn die Option deaktiviert ist, wird auf App- und Desktop-Karten kein Stern angezeigt und auf der Navigationsleiste werden die Untermenüs **Alle Apps** bzw. **Favoriten** für diese Ressourcen nicht angezeigt. Als **Favoriten** markierte Apps und Desktops werden nicht gelöscht und können wiederhergestellt werden, wenn Sie **Favoriten** erneut aktivieren.

Hinweis:

Wenn Ihre Abonnenten keinen Zugriff auf konfigurierte Desktops haben, werden in der Randleiste keine Desktops zur Auswahl angezeigt.

App- und Desktop-Schlüsselwörter

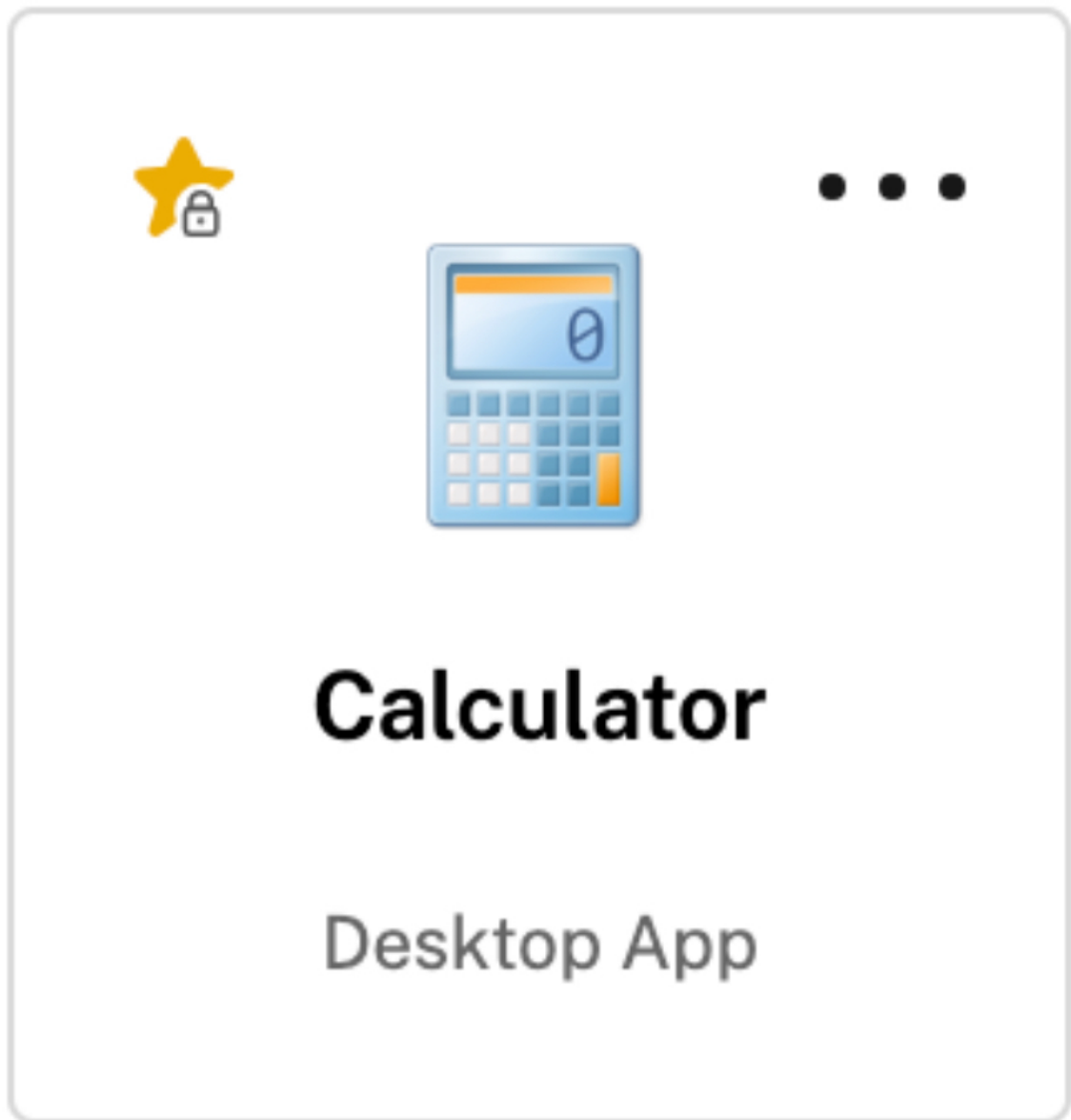
Administratoren können **Favoriten-Apps** für Abonnenten automatisch hinzufügen, indem sie die Einstellungen **KEYWORDS:Auto** und **KEYWORDS:Mandatory** in Citrix DaaS (**Verwalten** > **Vollständige Konfiguration** > **Anwendungen**) verwenden.

The screenshot shows the 'Application Settings' dialog in Citrix Studio. On the left is a 'Studio' sidebar with a list of settings: Identification (highlighted with a blue arrow), Delivery, Location, Groups, Limit Visibility, File Type Association, and Zone. The main area is titled 'Identification' and contains the following fields and text:

- Identify this application.
- Application name (for user):
- Application name (for administrator):
- Description and keywords:

Below the description field, there is explanatory text: "This is the description that will be seen by the user. You can also use this field to enter keywords for StoreFront." followed by a blue link labeled "Learn More". At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Apply".

- **KEYWORDS:Auto.** Die App bzw. der Desktop wird als **Favorit** hinzugefügt. Abonnenten können den **Favoriten** entfernen.
- **KEYWORDS:Mandatory.** Die App bzw. der Desktop wird als **Favorit** hinzugefügt, Abonnenten können den **Favoriten** jedoch nicht entfernen. Für obligatorische Apps und Desktops wird ein Sternsymbol mit Vorhängeschloss angezeigt, das darauf hinweist, dass das Entfernen des Favoriten nicht möglich ist.



Hinweis:

Wenn Sie beide Schlüsselwörter (**Mandatory** und **Auto**) für eine App verwenden, setzt **Mandatory** das Schlüsselwort **Auto** außer Kraft und die bevorzugte App oder der bevorzugte Desktop kann nicht entfernt werden.

Für Abonnenten, die nur Zugriff auf Apps und Desktops mit dem Schlüsselwort **Mandatory** erhalten gilt Folgendes:

- Der Abonnent sieht nur die Seite **Apps** im linken Navigationsbereich von Workspace. Die Seite **Favoriten** wird im linken Bereich nicht angezeigt, da nicht unterschieden wird zwischen Apps, die auf der Seite **Apps** bzw. der Seite **Favoriten** angezeigt werden.

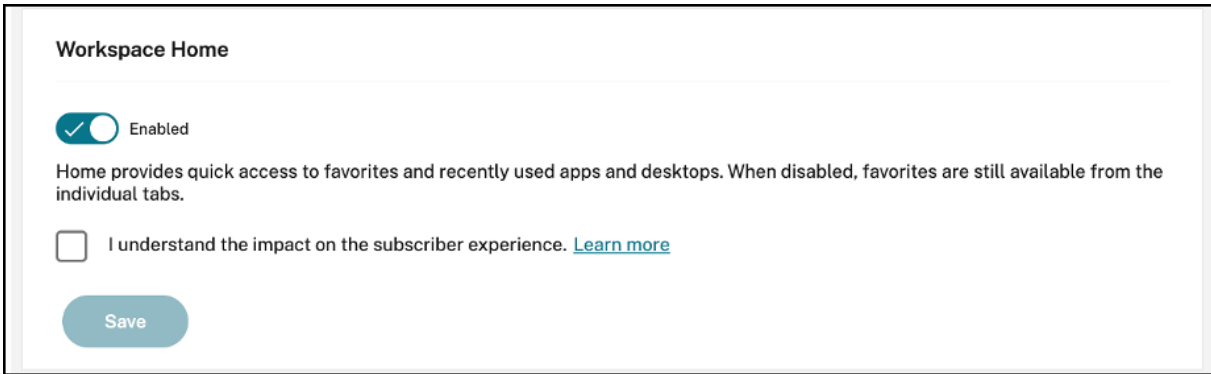
- Der Abonnent sieht keine Registerkarte **Favoriten** auf der Homepage. Es wird nur die Registerkarte **Zuletzt verwendet** angezeigt.

Homebildschirm für Benutzer aktivieren oder deaktivieren (Preview)

Sie können die **Homepage** für Benutzer aktivieren oder deaktivieren, um ihnen die Organisation ihrer Apps zu erleichtern.

Dieses Feature ist verfügbar, wenn Benutzer mehr als 20 Apps auf dem Desktop haben. Bei 20 Apps und weniger wird Benutzern eine Einzelansicht ohne Navigations- und Suchoptionen angezeigt.

Zum Konfigurieren der Einstellungen gehen Sie zu **Workspacekonfiguration > Anpassen > Darstellung**. Wenn der Schalter aktiviert ist, werden Benutzer zur **Homepage** geleitet. Wenn Sie den Schalter deaktivieren, werden Benutzer direkt zur Seite der **App** geleitet. Standardmäßig ist der Schalter eingeschaltet und das Feature ist aktiviert.



Workspace Home

Enabled

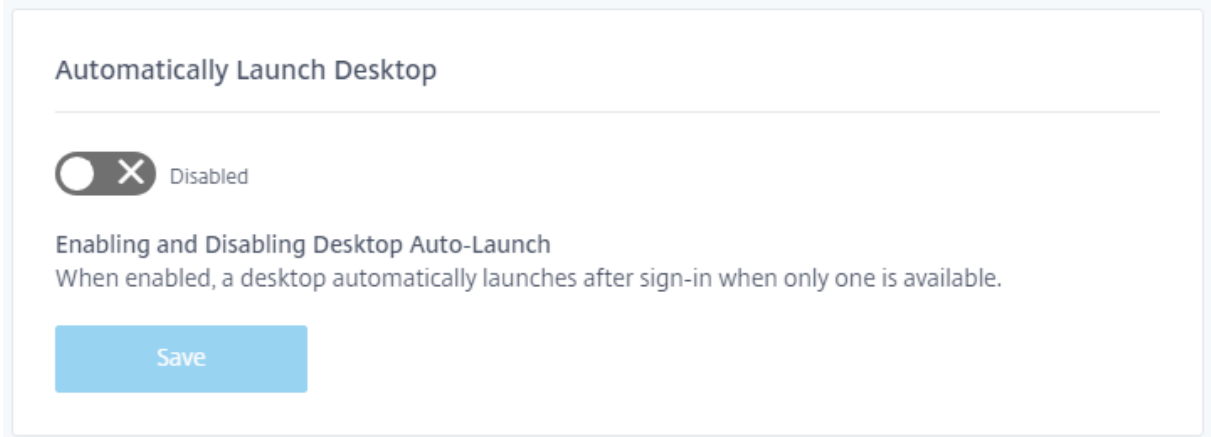
Home provides quick access to favorites and recently used apps and desktops. When disabled, favorites are still available from the individual tabs.

I understand the impact on the subscriber experience. [Learn more](#)

Save

Desktop automatisch starten

Die Option **Desktop automatisch starten** ist für Kunden mit Zugriff auf die **Workspacekonfiguration** und die neue Workspace-Benutzeroberfläche verfügbar. Die Einstellung gilt nur für den Workspacezugriff über einen Browser.



Automatically Launch Desktop

Disabled

Enabling and Disabling Desktop Auto-Launch

When enabled, a desktop automatically launches after sign-in when only one is available.

Save

Wenn dies deaktiviert ist (Standardeinstellung), verhindert diese Einstellung den automatischen Desktopstart in Citrix Workspace, wenn ein Abonnent sich anmeldet. Abonnenten müssen ihren Desktop nach der Anmeldung manuell starten.

Wenn dies aktiviert ist und ein Abonnent nur einen verfügbaren Desktop hat, wird der Desktop automatisch gestartet, sobald der Abonnent sich am Workspace anmeldet.

Die Anwendungen des Abonnenten werden unabhängig von der Konfiguration der Workspaces-steuerung nicht erneut verbunden.

Hinweis:

Damit Citrix Workspace einen Desktop automatisch starten kann, müssen Abonnenten, die über Internet Explorer auf die Site zugreifen, die Workspace-URL den Zonen "Lokales Intranet" oder "Vertrauenswürdige Sites" hinzufügen.

Verbundidentitätsanbietersitzungen

Wenn Workspace mit einem Verbundidentitätsanbieter konfiguriert ist, steuert dieser normalerweise die Authentifizierungssitzung und ihre Lebensdauer. Mit der Einstellung **Verbundidentitätsanbietersitzungen** kann die Steuerung an den Dienstanbieter übergeben werden. Wenn diese Option aktiviert ist (Standard), erzwingt Workspace eine Anmeldung beim Identitätsanbieter, wenn eine neue Workspace-Sitzung benötigt wird. Wenn die Option deaktiviert ist, wird der Abonnent nicht aufgefordert, sich beim Identitätsanbieter zu authentifizieren, wenn er mit einer gültigen Sitzung auf Workspace zugreift.

Wenn diese Einstellung aktiviert ist und Sie Azure AD für die Workspace-Authentifizierung verwenden, werden Abonnenten möglicherweise aufgefordert, sich erneut anzumelden, selbst wenn für ihre Sitzung ein gültiges Microsoft-Authentifizierungstoken vorhanden ist. Weitere Informationen zu diesem Szenario finden Sie unter [CTX253779](#).


Apps und Desktops starten

Die Einstellung **Apps und Desktops starten** ist für Kunden mit Zugriff auf die **Workspacekonfiguration** und die neue Workspace-Benutzeroberfläche verfügbar. Diese Einstellung steht Neu- und Bestandskunden zur Verfügung. Die Einführung dieses Features ändert jedoch keine Einstellungen für bestehende Kunden.

Die Einstellung gilt für die Art und Weise, wie Benutzer Apps und Desktops öffnen, die von **Citrix DaaS** bereitgestellt werden. Dies kann über den Dienst **Citrix DaaS** oder on-premises über das Feature [Siteaggregation](#) erfolgen. **Apps und Desktops starten** gilt beispielsweise nicht für SaaS-Apps, die von Citrix Gateway Service bereitgestellt werden.

Launching apps and desktops

Select how end users must launch apps and desktops when they access their workspace from a browser. (DaaS only)

Let end users choose 

Let end users choose between a locally installed version of the Workspace app or in a browser.

- If end users have the right to install software, prompt them to install the latest version of the Workspace app if a local app isn't detected automatically.

Do you want end users to download the Workspace Web Extension for a safer and more reliable app launch experience? Once the extension is downloaded, the Workspace detection step will no longer be displayed. [Learn more](#)

- Require end users to download the Workspace Web Extension and block access to Workspace until it is detected.
- Prompt end users to download the Workspace Web Extension but allow access to Workspace if it isn't detected.
- Do not prompt end users to download the Workspace Web Extension.

Save

Wählen Sie eine der folgenden Einstellungen:

- **In einer nativen App** (Standard): Endbenutzer müssen eine lokal installierte Version der Workspace-App verwenden.
- **In einem Browser:** Endbenutzer müssen eine Browserversion der Workspace-App für HTML5 verwenden.
- **Benutzer wählen lassen:** Endbenutzer haben die Wahl zwischen einer lokal installierten Version der Workspace-App oder dem Start von Apps und Desktops in einem Browser.

Durch eine zusätzliche Option für **In einer nativen App** und **Benutzer wählen lassen** werden Benutzer aufgefordert, die aktuelle Version der Citrix Workspace-App zu installieren, wenn keine lokale App automatisch erkannt wird. Das Entfernen dieser Option ist sinnvoll, wenn Abonnenten keine Rechte zum Installieren von Software haben.

Integration von Microsoft Teams in Workspace

Mit der Integration von Microsoft Teams können Abonnenten Karten aus ihrem Workspace-**Aktivitätsfeed** mit anderen Abonnenten über Kanäle in Microsoft Teams teilen.

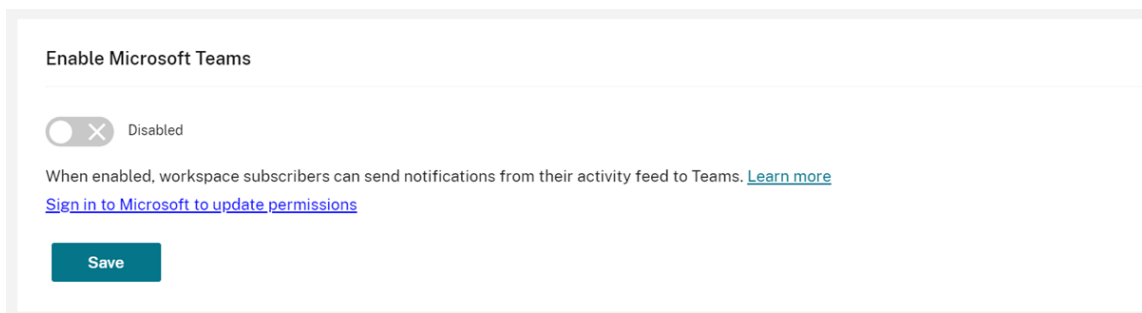
Anforderungen

- Sie können die Microsoft Teams-Integration nur als Citrix Cloud-Administrator mit **Vollzugriff** aktivieren. Administratoren mit **benutzerdefiniertem Zugriff** verfügen nicht über die erforderlichen Berechtigungen zum Aktivieren der Microsoft Teams-Integration.

- Sie müssen die Azure AD-Authentifizierung in **Identitäts- und Zugriffsverwaltung** konfigurieren. Weitere Informationen zum Konfigurieren der Azure AD-Authentifizierung finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).
- Sie können nur eine einzelne Azure AD-Instanz mit Microsoft Teams verwenden. Wenn Microsoft Teams für die von Ihnen konfigurierte Azure AD-Instanz über ein anderes Citrix Cloud-Konto aktiviert ist, können Sie die Microsoft Teams-Integration für Ihr Citrix Cloud-Konto nicht aktivieren.
- Der Feature Toggle **lwsMicrosoftTeams** muss aktiviert sein.
- Das Feature für **Aktionen und Aktivitätsfeed** muss für Workspaces aktiviert sein.
- Für Workspace-Abonnenten muss der Microsoft Teams-Desktopclient installiert sein.

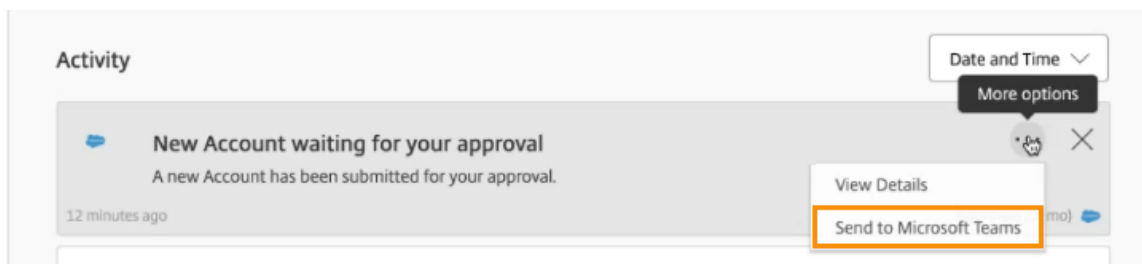
Aktivieren der Microsoft Teams-Integration

1. Nach dem Anmelden in Citrix Cloud wählen Sie **Workspacekonfiguration**.
2. Wählen Sie **Anpassen** und dann die Registerkarte **Einstellungen**.
3. Wählen Sie unter **Microsoft Teams aktivieren** den Umschalter aus, um ihn zu aktivieren.



4. Wählen Sie **Speichern**.

Workspace-Benutzer können jetzt die Option **An Microsoft Teams senden** sehen und Karten aus Workspace freigeben. Benutzer müssen möglicherweise ihren Bildschirm aktualisieren (Strg+F5).

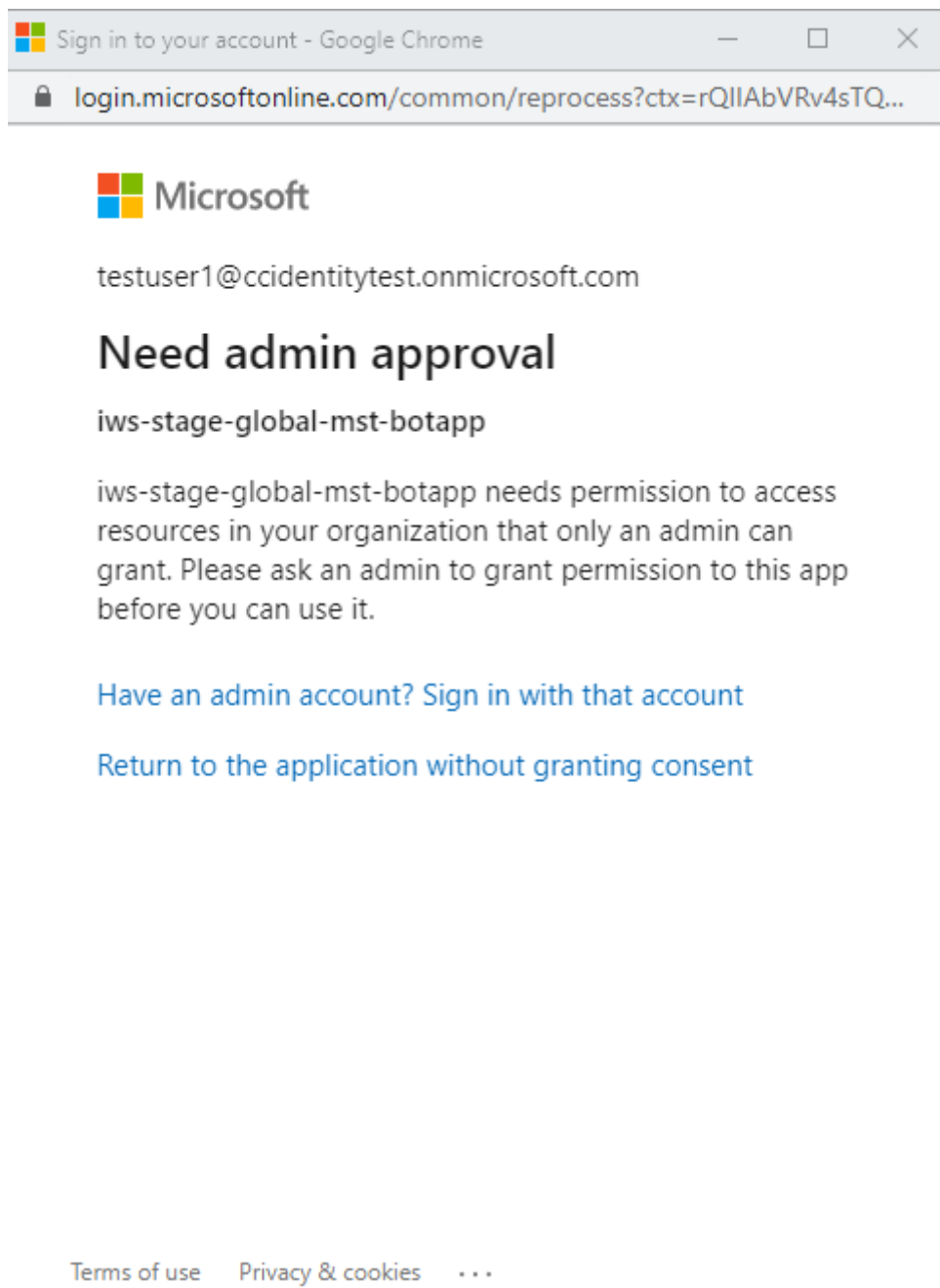


Akzeptieren von Workspace-Berechtigungen

Zum Aktivieren dieser Integration sind weitere Setupschritte erforderlich. Das **Microsoft-Administratorkonto** muss die Berechtigungen der Integration in der Workspace-Benutzeroberfläche

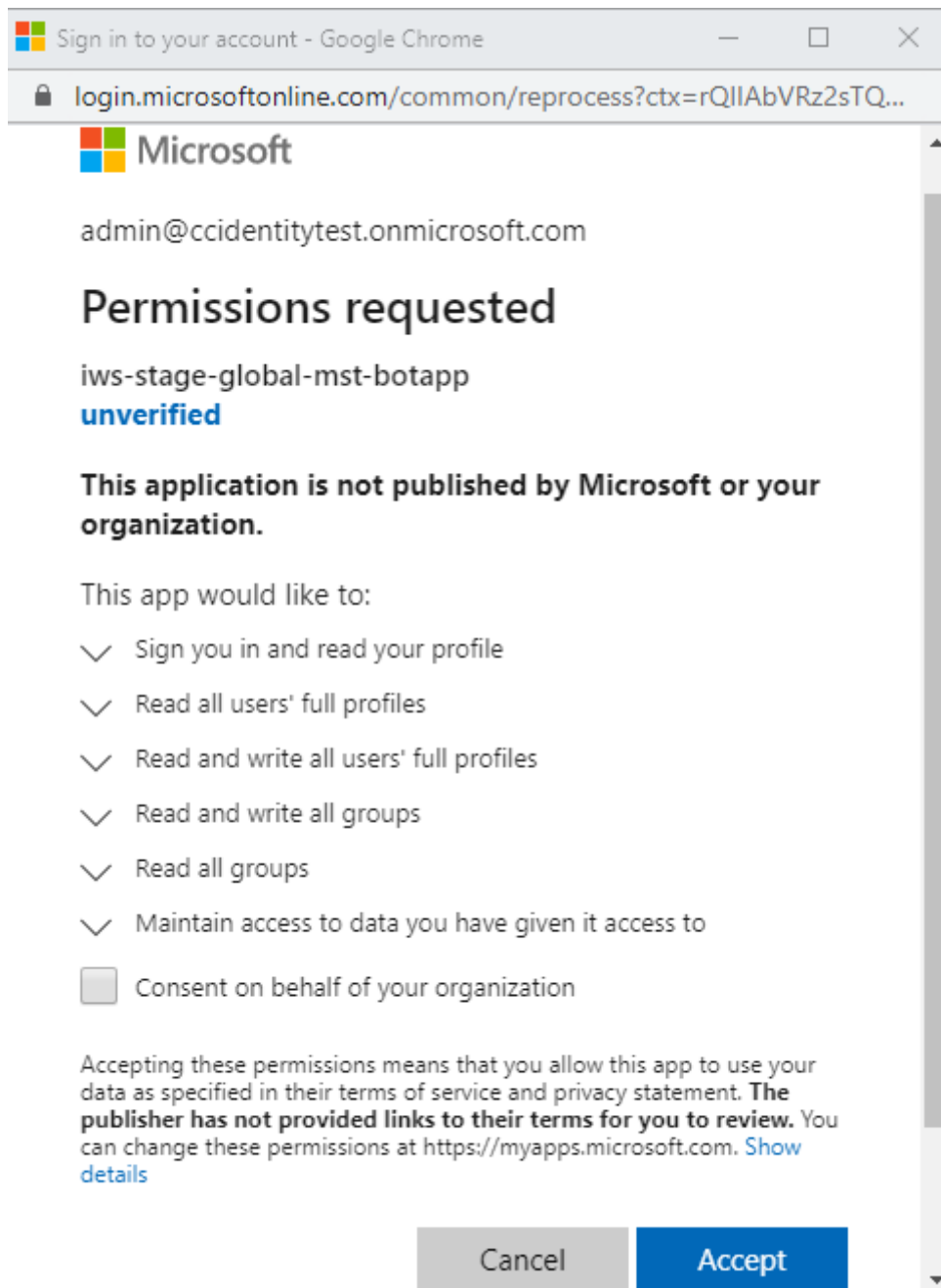
akzeptieren, damit Benutzer Ihrer Organisation Karten für Microsoft Teams freigegeben können.

1. Melden Sie sich bei einem Workspace-Konto an und versuchen Sie, eine Karte freizugeben.
2. Wenn vom **Microsoft-Administratorkonto** noch keine Berechtigungen für die Integration mit Microsoft Teams akzeptiert wurden und Sie versuchen, sich mit einem Nicht-Administratorkonto anzumelden, wird die folgende Meldung angezeigt:



3. Um Berechtigungen zu akzeptieren, melden Sie sich bei Ihrem Administratorkonto an. Wählen Sie hierfür **Wenn Sie über ein Administratorkonto verfügen, melden Sie sich mit diesem**

Konto an. Die folgenden Berechtigungen für den Zugriff auf Daten sind erforderlich, um die Integration von Microsoft Teams in Citrix Workspace zu aktivieren:



4. Wenn das Dialogfeld **Berechtigungen akzeptiert** geöffnet wird, überprüfen Sie die Optionen. Die Option für die **Zustimmung im Namen Ihrer Organisation** gewährt allen Workspace-Abonnenten Berechtigungen für diesen Administrator. Andernfalls werden Berechtigungen nur für das Administratorkonto gewährt.
5. Wählen Sie **Akzeptieren**.

Anpassen von Sicherheits- und Datenschutzrichtlinien

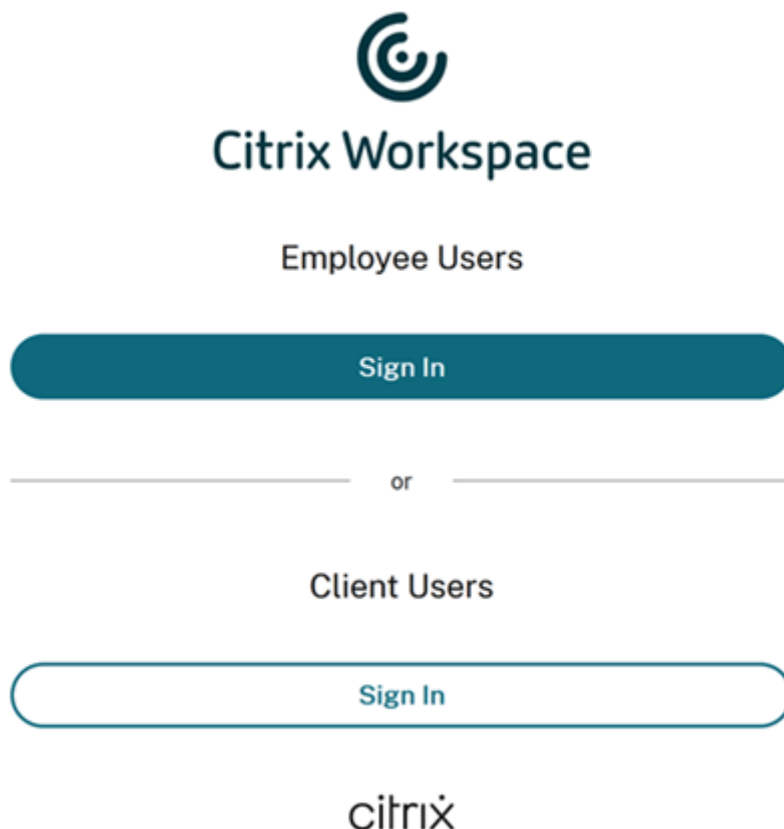
November 27, 2023

Dieser Artikel enthält Hinweise zum Anpassen des Anmeldeverfahrens, nachdem Sie den Workspace-Zugriff und die Authentifizierung konfiguriert haben.

Einen Überblick über das Verfahren zum Konfigurieren von Workspace-Zugriff und Authentifizierung finden Sie unter [Konfigurieren von Workspaces](#). Informationen zum Konfigurieren der Abonnentenauthentifizierung für Workspaces finden Sie unter [Sichere Workspaces](#).

Erstellen eines einheitlichen Workflows zur Benutzeranmeldung

Standardmäßig wird ein geteilter Bildschirm für Mitarbeiter-Benutzer und externe Clientbenutzer angezeigt.



Um den geteilten Bildschirm zu entfernen, navigieren Sie zu **Workspacekonfiguration > Authentifizierung > Einheitlicher Anmeldevorgang für Benutzer** und wählen Sie **Aktivieren**. Durch das Aktivieren dieses Features erhalten alle Benutzer dieselbe Anmeldeoption.



Citrix Workspace

Username

Password

Legen Sie für Web- und Workspace-Apps auf Desktop und Mobilgerät einen Timeout bei Inaktivität fest

Über die Einstellung **Inaktivitätstimeout für das Internet** unter **Workspacekonfiguration > Anpassen > Einstellungen** legen Sie die Leerlaufzeit fest (bis zu 8 Stunden), nach deren Ablauf Abonnenten automatisch von Citrix Workspace abgemeldet werden. Für die Workspace-App auf Desktop und Mobilgerät können Sie den Timeout bei Inaktivität auch aktivieren, indem Sie das entsprechende Konfigurationsfeld auswählen.

Workspace Sessions

Inactivity Timeout for Web

After this amount of idle time (maximum of 8 hours), your subscribers will be automatically signed out of Workspace. Applies to browser access only (not from a local Citrix Workspace app).

HOURS	MINUTES
<input type="text" value="0"/> ▾	: <input type="text" value="20"/> ▾

Im Gegensatz zur manuellen Abmeldung, bei der DaaS-Sitzungen getrennt werden, bleiben Abonnenten nach einem Inaktivitätstimeout mit ihren DaaS-Sitzungen verbunden.

Einrichten eines Neuauthentifizierungszeitraums für die Citrix Workspace-App

Über die Einstellung **Neuauthentifizierungszeitraum für die Workspace-App** unter **Workspacekonfiguration > Anpassen > Einstellungen** können Sie angeben, wie lange Abonnenten bei der Citrix Workspace-App angemeldet bleiben können, bevor eine erneute Anmeldung erforderlich wird.

Reauthentication Period for Workspace App ⓘ

This is the maximum time your subscribers can stay signed in to Workspace app before needing to reauthenticate (between 1 and 365 days).

Current Reauthentication Period: 1 Day(s) [Edit](#)

[Learn more](#) about Workspace reauthentication periods.

Save

Standardmäßig müssen sich Abonnenten alle 24 Stunden anmelden. Sie können einen Neuauthentifizierungszeitraum von bis zu 365 Tagen angeben. Bei einem längeren Neuauthentifizierungszeitraum müssen Abonnenten zustimmen, um angemeldet zu bleiben. Für Benutzer, die nach dem 27. September 2021 bereitgestellt wurden, gilt eine Frist von 30 Tagen, damit sich Abonnenten erneut anmelden können.

Während Ihres festgelegten Neuauthentifizierungszeitraums bleiben Abonnenten angemeldet, sofern sie nicht mindestens 14 Tage lang inaktiv sind. Wenn Abonnenten über einen Zeitraum von mindestens 14 Tagen inaktiv sind, werden sie beim nächsten Zugriff auf den Workspace zur erneuten Authentifizierung aufgefordert.

Sie können die Sitzung für Abonnenten ungültig machen, indem Sie dieses [PowerShell-Skript](#) herunterladen und den Anweisungen im Download folgen. Nachdem Sie Sitzungen ungültig gemacht haben, müssen Abonnenten sich innerhalb von 24 Stunden erneut bei ihrem Workspace authentifizieren.

Wenn Sie den Zeitraum für die erneute Authentifizierung für die Citrix Workspace-App auf weniger als 24 Stunden festlegen müssen, können Sie dies per PowerShell tun.

Weitere Informationen finden Sie unter [Steps to configure InactivityTimeoutInMinutes](#).

Unterstützte Workspace-App-Clients

Dieses Feature wird von den folgenden Versionen der Citrix Workspace-App unterstützt:

- Workspace-App 2106 oder höher für Windows
- Workspace-App 2106 oder höher für Mac

- Workspace-App für 21.6.5 iOS oder höher
- Workspace-App für 21.6.0 Android oder höher

Unterstützte Authentifizierungsmethoden

Die dauerhafte Anmeldung bei der Citrix Workspace-App wird für die folgenden Authentifizierungsmethoden unterstützt:

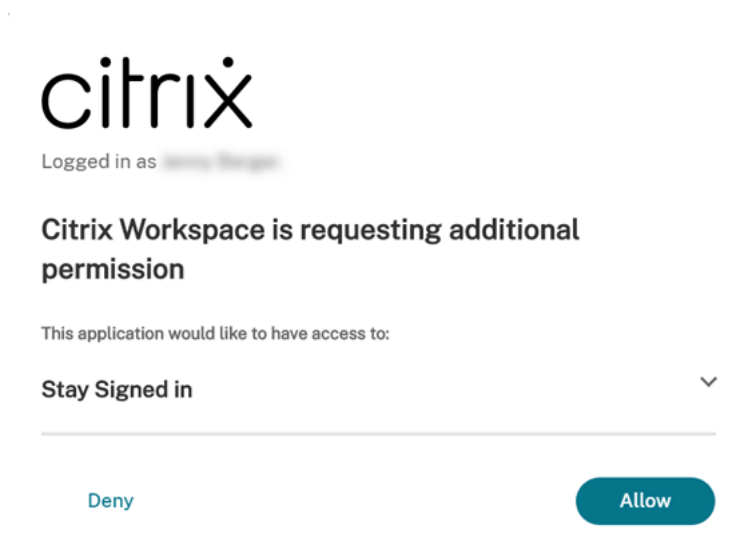
- Active Directory
- Active Directory plus Token
- Azure Active Directory
- Citrix Gateway
- Okta

Hinweis:

Um dieselbe Benutzererfahrung als Citrix DaaS-Kunde mit Okta oder Azure Active Directory zu erzielen, konfigurieren Sie den Citrix Verbundauthentifizierungsdienst (FAS). Weitere Informationen zu FAS finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Dauerhafte Anmeldung für Abonnenten

Wenn sich Abonnenten auf ihrem Gerät bei Workspace anmelden, fordert Workspace sie zu einer Einverständniserklärung für die dauerhafte Anmeldung auf.



Wählt der Abonnent **Zulassen**, bleibt er für die Dauer des Neuauthentifizierungszeitraums angemeldet. Wenn vier Tage lang keine Aktivität auf dem Gerät eines Abonnenten festgestellt

wird, wird er automatisch aufgefordert, sich erneut zu authentifizieren. Nachdem er sich bei der Citrix Workspace-App angemeldet hat, gilt der Neuauthentifizierungszeitraum, sofern er Apps und Desktops auf dem Gerät verwendet.

Wählt der Abonnent **Verweigern**, fordert Workspace ihn auf, sich erneut anzumelden. Anschließend wird der Abonnent nach Ablauf von 24 Stunden erneut zur Anmeldung aufgefordert.

Nach der Änderung des Kennworts muss der Abonnent sich über die Citrix Workspace-App abmelden und erneut anmelden, damit der Neuauthentifizierungszeitraum weiterhin funktioniert.

Änderung des Kontokennworts durch Abonnenten

Hinweis:

Der Rollout dieses Features für Kunden erfolgt schrittweise. Sie sehen das Feature möglicherweise erst, wenn der Rolloutprozess abgeschlossen ist.

Citrix möchte Citrix Workspace-Kunden neue Features und Produktupdates unverzüglich zur Verfügung zu stellen. Der Prozess ist für Sie transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Durch diese schrittweise Bereitstellung von Updates wird die Produktqualität sichergestellt und die Verfügbarkeit maximiert.

Mit der Einstellung **Ändern des Kontokennworts zulassen** unter **Workspacekonfiguration > Anpassen > Einstellungen** wird gesteuert, ob Abonnenten ihr Domänenkennwort in Citrix Workspace ändern können. Sie können Abonnenten auch anleiten, wie sie gültige Kennwörter erstellen, die der Kennwortrichtlinie Ihrer Organisation entsprechen.

Wenn diese Option aktiviert ist (Standardeinstellung), können Abonnenten ihr Kennwort jederzeit ändern, gemäß den Active Directory-Einstellungen Ihres Unternehmens. Wenn diese Option deaktiviert ist, fordert Workspace Abonnenten auf, ihr Kennwort zu ändern, wenn es abläuft. Abonnenten können jedoch ihr nicht abgelaufenes Kennwort nicht in Workspace ändern.

Unterstützte Authentifizierungsmethoden

- Active Directory
- Active Directory plus Token

Unterstützte Workspace-App-Clients

Dieses Feature wird von den folgenden Versionen der Citrix Workspace-App unterstützt:

- Workspace-App für Windows 2101 oder höher

- Workspace-App für Mac 2012 oder höher
- Workspace-App für Chrome 2010 oder höher
- Workspace-App für HTML5 2101 oder höher
- Workspace-App für Android 21.1.0 oder höher

Abonnenten können dieses Feature auch verwenden, wenn sie mit der neuesten Version der Webbrowser Edge, Chrome, Firefox oder Safari auf Workspaces zugreifen.

Dieses Feature wird in älteren Versionen der Citrix Workspace-App und der Citrix Workspace-App für Linux nicht unterstützt.

Anleitung für Kennwörter

Sie können bis zu 20 Kennwortanforderungen hinzufügen, die der Sicherheitsrichtlinie Ihrer Organisation entsprechen und die von Ihrem Identitätsanbieter erzwungen werden. Workspace zeigt diese Anforderungen zur Anleitung an, wenn Abonnenten ihr Kennwort auf ihrer Seite **Kontoeinstellungen** in Workspace ändern. Wenn Sie keine Kennwortanforderungen hinzufügen, zeigt Workspace folgende Meldung an: “Die Kennwortanforderungen Ihrer Organisation gelten weiterhin.”

Wichtig:

Citrix Workspace validiert keine neuen Kennwörter, die Ihre Abonnenten eingeben. Wenn ein Abonnent versucht, sein gültiges Kennwort über Workspace in ein ungültiges Kennwort zu ändern, lehnt Ihr Identitätsanbieter das neue Kennwort ab. Das bestehende Kennwort wird nicht geändert.

Hinzufügen von Kennwortanforderungen:

1. Navigieren Sie zu **Workspacekonfiguration > Anpassen > Einstellungen**.
2. Überprüfen Sie unter **Ändern des Kontokennworts zulassen**, ob die Einstellung aktiviert ist. Wenn diese Einstellung deaktiviert ist, aktivieren Sie sie.
3. Wählen Sie **Kennwortanforderung hinzufügen** aus.

Allow Account Password to be Changed

Enabled

When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

If no requirements are defined, subscribers see the message: **Your organization's password requirements still apply.**

[+ Add a password requirement \(20 max.\)](#)

Save

4. Geben Sie eine Anforderung ein, die den Sicherheitsanforderungen Ihrer Organisation für gültige Kennwörter entspricht. Sie können beispielsweise festlegen, dass ein Kennwort eine bestimmte Zeichenlänge haben muss. Wählen Sie **Kennwortanforderung hinzufügen** aus, um weitere Elemente für Abonnenten hinzuzufügen, wenn sie ihr Kennwort ändern.

Add a password requirement ✕

Add the password requirements that are enforced by your organization's identity provider so your subscribers understand how to create valid, complex passwords. Workspace displays these requirements to your subscribers, but does not validate subscribers' passwords.

Password must meet the following requirements: ?

- 🗑️

[+ Add a password requirement \(20 max.\)](#)

⚠️ If no requirements are defined, subscribers see the message:
Your organization's password requirements still apply.

Save

Cancel

5. Wenn Sie mit dem Hinzufügen von Anforderungen fertig sind, wählen Sie **Speichern**.
6. Wählen Sie erneut **Speichern** aus, um alle Ihre Einstellungsänderungen zu speichern.

Allow Account Password to be Changed



When enabled, subscribers can change their password by going to "Security and Sign In" in Workspace.

^ Password must meet the following 4 requirements: ?

- At least 7 characters in length.
- Contain no personal information (Part of your name, social security number, birthday).
- Must contain 3 of the following: Lower Case Letter, Upper Case Letter, Number, Other Character (!@#%&).
- Must not be a password you have used before.



Abonnenten-Benutzererfahrung beim Ändern von Kennwörtern

Tipp:

Um Ihre Abonnenten auf dieses Feature aufmerksam zu machen, sollten Sie eine Empfehlung in Ihre interne Knowledgebase aufnehmen, damit Abonnenten ihre Domänenkennwörter über Workspace ändern können. [Laden Sie diese PDF-Datei herunter](#). Die darin enthaltenen Anweisungen können Sie in Ihre eigenen Mitteilungen und Knowledgebase-Artikel integrieren.

Wenn **Ändern des Kontokennworts zulassen** aktiviert ist, können Abonnenten ihr Kennwort in Workspace ändern, indem sie zu **Kontoeinstellungen > Sicherheit & Anmeldung** navigieren.

Wählen Sie **Kennwortanforderungen anzeigen**, um alle Anforderungen anzuzeigen, die Sie unter **Workspacekonfiguration** eingegeben haben.

Change Password

You'll have to sign back in to Workspace after changing your password.

Current Password:

New Password:

Confirm Password:

▼ Hide Password Requirements

Passwords must meet the following requirements:

- Be at least ten (10) characters in length
- Contain an upper case letter
- Contain a lower case letter
- Contain a number
- Contain a symbol (e.g., !, @, \$, %...)
- Be different than the 24 previously reset passwords
- Do not include a common dictionary word
- Do not include any part of the user or login name
- Avoid padding passwords with consecutive or repetitive numbers (e.g. 123, 1234, 1111, etc.)

Nachdem Abonnenten ihr Kennwort geändert haben, werden sie automatisch bei Workspace abgemeldet und müssen sich mit dem neuen Kennwort erneut anmelden.

Benutzerdefinierte Ankündigungen senden

Senden Sie eine benutzerdefinierte Meldung, die für eine begrenzte Zeit angezeigt wird, z. B. über ein bevorstehendes Wartungsfenster.

Die benutzerdefinierte Ankündigung wird für alle Abonnenten in allen Clients angezeigt, einschließlich Web- und Mobilgeräten. Abonnenten sehen die Meldung, nachdem sie sich angemeldet haben. Abonnenten können die Ankündigung nicht verwerfen, aber sie können sie auf ihrem Mobilgerät minimieren.

1. Wählen Sie im **Citrix Cloud**-Menü **Workspace-Konfiguration > Anpassen > Einstellungen > Benutzerdefinierte Ankündigung senden > Konfigurieren**.

2. Geben Sie Titel und Text der Nachricht ein, die Sie anzeigen möchten, und wählen Sie Datum, Uhrzeit und Position (oben oder unten) für die Meldung der Nachricht für Abonnenten aus.
3. Um zu sehen, wie die Meldung für Abonnenten angezeigt wird, wählen Sie **Vorschau**.
4. Wenn Sie fertig sind, wählen Sie **Speichern**.

Konfigurieren einer Anmelderichtlinie

Erstellen Sie eine benutzerdefinierte Anmelderichtlinie, um Abonnenten über die Endbenutzerlizenzvereinbarung (EULA) Ihrer Organisation zu informieren, wenn sie sich bei ihrem Workspace anmelden.

Wenn diese Option aktiviert und konfiguriert ist, wird die Anmelderichtlinie auf allen Clients angezeigt, einschließlich Web- und Mobilgeräten. Abonnenten können die Anmelderichtlinie sehen, wenn sie sich anmelden. Abonnenten können die Richtlinie nicht umgehen und müssen sie akzeptieren, um sich bei ihrem Workspace anzumelden.

1. Wählen Sie im **Citrix Cloud**-Menü **Workspacekonfiguration > Anpassen > Einstellungen**.
2. Klicken Sie im Bereich **Anmelderichtlinie** auf **Konfigurieren**. Wenn eine Richtlinie vorliegt, heißt die Schaltfläche **Bearbeiten**.
3. Aktivieren Sie das Feature über die Umschaltfläche unter **Richtlinie aktivieren**.
4. Geben Sie in der **Richtlinienkopfzeile** einen Titel für die Richtlinie ein.
5. Geben Sie den Richtlinientext ein, dem Abonnenten vor der Anmeldung zustimmen müssen. Fügen Sie bei Bedarf übersetzten Text für andere Sprachen in dasselbe Textfeld ein.
6. Geben Sie einen Namen für die Schaltfläche ein, die Abonnenten auswählen müssen, um der Richtlinie zuzustimmen.

Sign In Policy ✕

Define the company usage policy that your subscribers must read and accept before signing in and accessing resources. [Learn more](#)


Enable policy
When enabled, the policy will be displayed to end users.

Policy header
Enter the header to display above the policy text.

Policy text
Enter the text of the sign in policy you want to display to subscribers.

Normal ⇅ **B** *I* U

Button text
Enter the text to display for the button that will allow subscribers to continue to sign in.



7. Wählen Sie **Vorschau**, um eine Vorschau der Richtlinie für Abonnenten anzuzeigen.

8. Wenn Sie fertig sind, wählen Sie **Speichern**.

Hinweis

Wenn Sie Citrix Gateway als Workspace-Identitätsanbieter konfiguriert haben, haben Sie möglicherweise bereits eine Anmelde Richtlinie im Rahmen der AAA- und nFactor-Authentifizierung festgelegt. Citrix empfiehlt, dass Sie nur eine Anmelde Richtlinie konfigurieren, entweder im Rahmen der bestehenden nFactor-Authentifizierung oder außerhalb dieses Workflows über die Citrix Cloud-Verwaltungskonsolle.

DaaS in Citrix Workspace optimieren

October 12, 2023

Mit den folgenden Optionen können Sie die Effizienz und Verfügbarkeit Ihrer DaaS-Apps und -Desktops verbessern:

- Verwendung der [Siteaggregation](#), um on-premises bereitgestellte virtuelle Apps und Desktops für Workspace-Abonnenten zur Verfügung zu stellen.
- Optimieren der Konnektivität mit der [direkten Workloadverbindung](#), bei der Netzwerkstandorte in Citrix Cloud konfiguriert werden.
- Sicherstellen der [Servicekontinuität](#) während eines Ausfalls zur Gewährleistung der resilienten Offline-Nutzung.
- Konfigurieren von Single Sign-On (SSO) für DaaS mithilfe von [Citrix FAS \(Verbundauthentifizierungsdienst\)](#).

Siteaggregation

Mit der Siteaggregation können Sie on-premises bereitgestellte virtuelle Apps und Desktops zu Ihrem Workspace hinzufügen, damit Abonnenten neben den Ressourcen in der Cloud auch auf diese Ressourcen zugreifen können.

Weitere Informationen finden Sie unter [Aggregieren von on-premises bereitgestellten virtuellen Apps und Desktops in Workspaces](#)

Weitere Informationen zu Skalierbarkeitslimits finden Sie unter [Skalierbarkeitslimits für die Workspace-Plattform](#).

Direkte Workloadverbindung

Die direkte Workloadverbindung verwendet Netzwerkstandorte, um zwischen internen und externen Routen zu den virtuellen Hostmaschinen für Ihre virtuellen Apps und Desktops zu wechseln.

Mit der direkten Workloadverbindung ermöglichen Sie Clients im Unternehmensnetzwerk, zum Direktstart von Citrix DaaS zu wechseln. Beim Direktstart müssen die HDX-Verbindungen zwischen Clients und VDAs nicht über ein Gateway geleitet werden. Zur Verwendung der direkten Workloadverbindung ist mindestens ein interner Netzwerkstandort erforderlich.

Weitere Informationen finden Sie unter [Optimieren der Konnektivität mit direkter Workloadverbindung](#).

Servicekontinuität

Durch die Servicekontinuität wird sichergestellt, dass Abonnenten bei einem Ausfall von Citrix Cloud mithilfe der Citrix Workspace-App weiter auf wichtige Apps und Desktops zugreifen können.

Die Servicekontinuität speichert Verbindungsleases auf Clientlaufwerken, auf denen die Citrix Workspace-App installiert ist. Verbindungsleases werden regelmäßig aktualisiert, wenn Clients auf den Workspace-Store zugreifen. Clients können dann Citrix DaaS starten, auf die sie vor dem Ausfall zugreifen konnten. Weitere Informationen finden Sie unter [Servicekontinuität](#).

Citrix Verbundauthentifizierungsdienst (FAS)

Citrix Workspace unterstützt den Citrix Verbundauthentifizierungsdienst (FAS) für das Single Sign-On bei Citrix DaaS. Mit FAS müssen Abonnenten, die einen Verbundidentitätsanbieter wie Azure AD oder Okta verwenden, ihre Anmeldeinformationen nur einmal eingeben, wenn sie sich bei ihrem Workspace anmelden. Ohne FAS werden solche Abonnenten mehrfach aufgefordert, ihre Anmeldeinformationen einzugeben, um auf ihre virtuellen Apps und Desktops zuzugreifen.

Für die Verwendung von FAS mit Workspace gelten folgende Anforderungen:

- Ein FAS-Server, der gemäß der Beschreibung im Abschnitt [Anforderungen](#) der FAS-Produktdokumentation konfiguriert wurde.
- Eine Verbindung zwischen Ihrem FAS-Server und Citrix Cloud, die im FAS-Installationsprogramm unter **Connect to Citrix Cloud** erstellt wurde.
- Eine Verbindung zwischen Ihrer On-Premises-Active Directory-Domäne und Citrix Cloud, wobei FAS in der **Workspacekonfiguration** aktiviert ist.

Weitere Informationen zum Bereitstellen von FAS finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

On-premises bereitgestellte virtuelle Apps und Desktops in Workspaces aggregieren

October 12, 2023

Sie können Ihre Site (Virtual Apps and Desktops-Bereitstellung) zu Citrix Workspace hinzufügen, damit Workspace-Abonnenten auf Ihre vorhandenen Apps und Desktops zugreifen können. Nach dem Hinzufügen Ihrer Site können Abonnenten sich in ihrem Workspace anmelden und neben Dateien und anderen Ressourcen auch auf virtuelle Apps und Desktops zugreifen. Dieser Prozess wird als *Siteaggregation* bezeichnet.

Die Site-Aggregation ist in allen Citrix Workspace-Editionen verfügbar. Weitere Informationen zu den Features der einzelnen Workspace-Editionen finden Sie in der [Citrix Workspace-Featurematrix](#).

Unterstützte Umgebungen

Die Siteaggregation wird nur für On-Premises-Bereitstellungen der folgenden Citrix Produkte unterstützt:

- Virtual Apps and Desktops 7 1808 oder höher
- XenApp und XenDesktop 7.0 bis 7.18

Für On-Premises-Sites, in denen ältere Versionen von XenApp oder XenApp und XenDesktop ausgeführt werden, wird die Verwendung mit Citrix Workspace nicht unterstützt.

Wichtig:

XenApp und XenDesktop 7.x schließt Versionen ein, die das Ende des Lebenszyklus erreicht haben. Die Releases von XenApp und XenDesktop vor 7.14 erreichten am 30. Juni 2018 das Ende des Lebenszyklus. Die Unterstützung für die Siteaggregation mit XenApp- und XenDesktop 7.x-Versionen, die das Ende des Lebenszyklus erreicht haben, hängt von der erfolgreichen Enumeration und dem Start von Ressourcen in Ihrer StoreFront-Bereitstellung ab.

Um die Siteaggregation mit einer On-Premises-Bereitstellung zu verwenden, die den Citrix Verbundauthentifizierungsdienst (FAS) umfasst, muss Ihre Site eine der folgenden Citrix Produktversionen verwenden:

- Virtual Apps and Desktops 7 1808 oder höher
- XenApp und XenDesktop 7.16 bis 7.18

Die Verbindung mit Citrix Cloud ist erforderlich, wenn Sie FAS mit Citrix Workspace verwenden. Aktualisieren Sie Ihre FAS-Server auf die aktuelle FAS-Softwareversion zum Herstellen einer Verbindung mit Citrix Cloud. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Skalierbarkeitslimits für die Workspace-Plattform

Die folgenden Skalierbarkeitslimits gelten für die Workspace-Plattform:

Limittyp	SLI-Metrik	SLO-Schwellenwert
Nutzungslimits	Gleichzeitige Endbenutzer für alle aggregierten On-Premises-Citrix Virtual Apps and Desktops-Sites	500
Zusätzliche Limits für Backend-/Frontend-Integration	Anzahl der On-Premises-Citrix Virtual Apps and Desktops-Sites	4

Hinweis:

Bei mehr als vier Backend-/Frontend-Integrationssites kann es zu langsamen Reaktionszeiten kommen. Servicekontinuität und LHC-Unterstützung stehen auch für On-Premises-Sites nicht zur Verfügung.

Aufgabenüberblick

Wenn Sie Ihre On-Premises-Site zu Citrix Workspace hinzufügen, führt Sie der Assistent zum **Hinzufügen einer Site** durch die folgenden Schritte:

1. Discovery der Site und Auswählen des Ressourcenstandorts, den Sie verwenden möchten.
2. Ermitteln Sie die Active Directory-Domänen, in denen Ihre Cloud Connectors installiert sind.
3. Geben Sie die Konnektivität an, die Sie zwischen Citrix Cloud und der Site verwenden möchten.

Mit dem Ressourcenstandort wird die Domäne und die Konnektivitätsoption für alle Benutzer angegeben, die auf Ihre Site zugreifen. Dabei führt Citrix Cloud einen Verbindungstest durch, um zu überprüfen, ob Ihre Site von Cloud Connectors aus erreichbar ist. Citrix Cloud zeigt dann eine Liste Ihrer Ressourcenstandorte an. Wenn Sie über Ressourcenstandorte verfügen, in denen keine Cloud Connectors installiert sind, laden Sie die erforderliche Software herunter und installieren Sie sie.

Für externe Konnektivität können Sie Ihr eigenes Citrix Gateway oder den Citrix Gateway Service verwenden. Damit nur Benutzer im Netzwerk Ihrer Site auf Anwendungen zugreifen können, legen Sie "Nur interner Zugriff" fest.

Voraussetzungen**Cloud Connectors**

Cloud Connectors ermöglichen Citrix Cloud, Ihre Site zu lokalisieren und mit ihr zu kommunizieren. Zur Minimierung der Unterbrechungen empfiehlt Citrix die Installation von Cloud Connectors, bevor Sie Ihre Site zu Citrix Workspace hinzufügen.

Für Hochverfügbarkeit empfiehlt Citrix mindestens zwei Server zum Installieren der Citrix Cloud Connector-Software. Diese Server müssen folgenden Anforderungen erfüllen:

- Die unter [Technische Daten zu Citrix Cloud Connector](#) beschriebenen Systemanforderungen müssen erfüllt sein.
- Keine anderen Citrix Komponenten installiert.
- Keine Funktion als Active Directory-Domänencontroller.
- Keine Funktion als Maschine, die für die Infrastruktur Ihres Ressourcenstandorts von entscheidender Bedeutung ist.
- Mit der Site-Domäne verbunden. Wenn Benutzer auf Anwendungen zugreifen, die sich in mehreren Domänen der Site befinden, installieren Sie in jeder Domäne mindestens zwei Cloud Connectors.
- Die Server müssen mit einem Netzwerk verbunden sein, das Ihre Site kontaktieren kann.
- Eine Verbindung mit dem Internet muss bestehen. Weitere Informationen finden Sie unter [Anforderungen an System und Konnektivität](#).

Weitere Informationen zur Installation von Cloud Connectors finden Sie unter [Cloud Connector-Installation](#).

Konfiguration eines Webproxys

Wenn Ihre Umgebung einen Webproxy verwendet, vergewissern Sie sich, dass Cloud Connectors die Konnektivität zum XML-Dienst in Ihrer Site überprüfen können. Fügen Sie alle XML-Server der Proxyumgehungsliste auf jedem Cloud Connector hinzu. Verwenden Sie keine Platzhalter oder IP-Adressen, da Cloud Connectors nur FQDNs verarbeiten können.

1. Hinzufügen der XML-Server zur Proxyumgehungsliste:
 - a) Wählen Sie auf dem Cloud Connector **Start** und geben Sie **Internetoptionen** ein.
 - b) Klicken Sie auf die Registerkarte **Verbindungen** und wählen Sie **LAN-Einstellungen**.
 - c) Wählen Sie unter **Proxyserver** die Option **Erweitert**.
 - d) Fügen Sie unter **Exceptions** den FQDN jedes XML-Servers in Ihrer Site hinzu. Verwenden Sie nur Kleinbuchstaben. Wenn diese Einträge Groß- oder Kleinbuchstaben oder nur Großbuchstaben enthalten, schlägt die Websiteaggregation möglicherweise fehl. Weitere Informationen finden Sie unter [CTX272160](#) im Citrix Support Knowledge Center.
2. Importieren Sie die Liste, damit die Cloud Connector-Dienste sie nutzen können. Geben Sie an der Eingabeaufforderung `netsh winhttp import proxy source=ie` ein.
3. Führen Sie über die **Services**-Konsole auf jeder Maschine mit Cloud Connector einen Neustart aller Citrix Cloud Services durch oder starten Sie jede Maschine neu.

Active Directory

Die Siteaggregation unterstützt Sites, die On-Premises-Active Directory verwenden.

Konfiguration von Azure Active Directory Um Sites, die Azure Active Directory verwenden, zu Citrix Workspace hinzuzufügen, konfigurieren Sie die Site so, dass sie XML-Serviceanfragen vertraut. Detaillierte Anweisungen hierzu finden Sie in folgenden Artikeln:

Weitere Informationen zu XenApp und XenDesktop 7.x sowie zu Virtual Apps and Desktops 7 1808 finden Sie unter [CTX236929](#).

Wichtig:

Wenn Sie Azure Active Directory, Okta, SAML oder einen anderen Verbundidentitätsanbieter mit Workspaces und Siteaggregation verwenden, werden die Benutzer aufgefordert, sich bei jeder Anwendung, die sie starten, zu authentifizieren.

FAS bietet Single Sign-On (SSO) für das Starten von Ressourcen mithilfe der Verbundauthentifizierung. Um SSO für Abonnenten zu aktivieren, registrieren Sie einen oder mehrere FAS-Server bei dem Ressourcenstandort, den Sie für das Hinzufügen Ihrer Site konfiguriert haben.

Vertrauensstellungen in Active Directory Wenn Sie in Active Directory separate Gesamtstrukturen für Benutzer und Ressourcen haben, müssen Sie in jeder Gesamtstruktur Cloud Connectors installieren, bevor Sie Ihre On-Premises-Site hinzufügen. Citrix Cloud erkennt über die Cloud Connectors diese Gesamtstrukturen während der Sitediscovery. Sie können dann die Benutzer und Ressourcen der Gesamtstruktur verwenden, um Workspaces für Ihre Benutzer zu erstellen.

Einschränkungen:

Wenn Sie Ihre Site hinzufügen, können Sie beim Definieren des Ressourcenstandorts keine separaten Gesamtstrukturen für Benutzer und Ressourcen verwenden. Da Cloud Connectors nicht zu möglicherweise vorhandenen gesamtstrukturübergreifenden Vertrauensstellungen gehören, kann Citrix Cloud Ihre Website nicht über die Cloud Connectors in diesen Gesamtstrukturen erkennen. Sie können diese Gesamtstrukturen verwenden, wenn Sie einen sekundären Ressourcenstandort definieren, der Benutzern eine andere Konnektivitätsoption bietet. Weitere Informationen finden Sie unter Hinzufügen von IP-Bereichen für verschiedene Konnektivitätsoptionen.

Gesamtstrukturen ohne Vertrauensstellung werden bei der Siteaggregation nicht unterstützt. Obwohl Citrix Cloud und Citrix Workspace Benutzer aus nicht vertrauenswürdigen Gesamtstrukturen unterstützen, können diese Benutzer Citrix Workspace nicht verwenden, nachdem eine On-Premises-Site per Siteaggregation hinzugefügt wurde. Benutzer können sich nur anmelden und Citrix Workspace verwenden, wenn sie in einer Gesamtstruktur sind, der die Site vertraut. Wenn sich Benutzer aus einer nicht vertrauenswürdigen Gesamtstruktur bei Citrix Workspace anmelden,

erhalten sie folgende Fehlermeldung: “Die Anmeldung ist abgelaufen. Melden Sie sich erneut an, um fortzufahren.”

Interne und externe Konnektivität für Workspaceressourcen

Während Sie Ihre Site zu Citrix Workspace hinzufügen, können Sie angeben, ob Sie internen oder externen Zugriff auf die Ressourcen gewähren möchten, die Benutzern zur Verfügung stehen. Wenn Sie nur internen Benutzern den Zugriff auf Ihre Site über Citrix Workspace gestatten möchten, müssen Benutzer sich im selben Netzwerk wie die Site befinden, um auf Anwendungen zugreifen zu können.

Sie haben folgende Möglichkeiten, um externen Benutzern den Zugriff auf diese Ressourcen zu gewähren:

- Den vorhandenen Citrix Gateway zur Verarbeitung des Datenverkehrs zwischen Ihrer On-Premises-Site und Citrix Cloud verwenden. Ihr Citrix Gateway muss so konfiguriert sein, dass Cloud Connectors als STA-Server (Secure Ticket Authority) verwendet werden, **bevor** Sie Ihre Site zu Citrix Workspace hinzufügen. Anweisungen finden Sie unter [CTX232640](#).
- Den Citrix Gateway Service verwenden, wenn Sie Citrix erlauben, den Datenverkehr zwischen Ihrer Site und Citrix Cloud zu verarbeiten. Sie können eine Testversion des Service aktivieren und den Service konfigurieren, wenn Sie Ihre Site hinzufügen. Wenn Sie sich bereits für den Citrix Gateway Service angemeldet haben, erkennt Citrix Cloud Ihr Abonnement, wenn Sie diese Option auswählen.

Hinweis:

Damit Citrix Cloud Ihr Citrix Gateway-Serviceabonnement erkennt, müssen Sie dieselbe OrgID verwenden, die Sie bei der Anmeldung für den Citrix Gateway Service verwendet haben. Weitere Informationen zu OrgIDs in Citrix Cloud finden Sie unter [\[Was ist eine OrgID?\].\(/en-us/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html#what-is-an-orgid\)](#)

Anmeldeinformationen und Ports für die Sitediscovery

Während des Hinzufügens Ihrer Site zu Citrix Workspace erkennt Citrix Cloud Ihre Site und prüft, ob der von Ihnen angegebene Controller verfügbar ist. Prüfen Sie vor dem Hinzufügen Ihrer On-Premises-Site Folgendes:

- Sie verfügen über Citrix Administratorberechtigungen mindestens mit **Leseberechtigungen**. Während der Site-Discovery fordert Citrix Cloud Sie auf, diese Anmeldeinformationen anzugeben. Diese Anmeldeinformationen werden von Citrix Cloud nicht gespeichert oder zum Vornehmen von Änderungen an der Site verwendet.

Aktivieren der Sitediscovery ohne Site-Anmeldeinformationen Nur XenApp und XenDesktop 7.x und Virtual Apps and Desktops 7 1808: Wenn Sie Siteanmeldeinformationen aus Sicherheitsgründen nicht angeben möchten, können Sie Citrix Cloud so einrichten, dass Ihre Site ermittelt wird ohne nach Siteanmeldeinformationen zu fragen. Führen Sie folgenden Schritt aus, **bevor** Sie Ihre On-Premises-Site Citrix Workspace hinzufügen.

1. Installieren Sie mindestens zwei Cloud Connectors in der Domäne Ihrer Site.
2. Erstellen Sie eine Active Directory-Sicherheitsgruppe und fügen Sie ihr die Cloud Connectors Ihrer Domäne hinzu.
3. Starten Sie die Cloud Connectors neu.
4. Gewähren Sie der Sicherheitsgruppe in Studio mindestens **Leseberechtigung**.

Schritt 1: Discovery der Site

In diesem Schritt geben Sie die Informationen an, die Citrix Cloud benötigt, um Ihre Site zu finden und Ihren Ressourcenstandort auszuwählen. Mit dem Ressourcenstandort wird die Domäne und die Konnektivitätsoption für alle Benutzer angegeben, die auf Ihre Site zugreifen. Wenn Sie Cloud Connectors in der Domäne Ihrer Site installieren müssen, können Sie dies jetzt tun. Wenn Sie Cloud Connectors bereits installiert haben, wählen Sie diese aus, wenn Sie dazu aufgefordert werden.

1. Rufen Sie im Citrix Cloud-Menü auf **Workspacekonfiguration > Sites > Site hinzufügen** auf.
2. Wählen Sie den Typ der On-Premises-Site aus, die Sie hinzufügen möchten, und fahren Sie fort.
Citrix Cloud ermittelt Ressourcenstandorte und Cloud Connectors in Ihrer Domäne und zeigt eine Liste an, aus der Sie auswählen können.
3. Führen Sie eine der folgenden Aktionen aus:
 - Wenn in der Domäne Ihrer Site keine Cloud Connectors installiert sind, wählen Sie **Connector installieren**. Citrix Cloud fordert Sie auf, die Cloud Connector-Software herunterzuladen und den Installationsassistenten abzuschließen.
 - Wenn Cloud Connectors bereits installiert sind, zeigt Citrix Cloud die Connectors in den Domänen an, in denen sie gefunden wurden. Wählen Sie den Ressourcenstandort aus, den Sie Citrix Workspace hinzufügen möchten. Dieser Ressourcenstandort wird zum Standardressourcenstandort.
 - Wenn Cloud Connectors installiert sind, aber nicht angezeigt werden, wählen Sie **Ermitteln**.
4. Wählen Sie die Ressourcenstandort/Cloud Connector-Kombination für die Site-Discovery.
5. Geben Sie unter **Serveradresse eingeben** die IP-Adresse oder den FQDN eines Controllers in der Site ein und wählen Sie **Ermitteln**.

Hinweis:

Wenn Sie einen FQDN verwenden, müssen Sie einen DNS-Eintrag haben, der auf den Delivery Controller verweist, den Sie ermitteln möchten.

Bei XenApp- und XenDesktop 7.x-Sites erkennt Citrix Cloud automatisch den XML-Serverport.

6. Wenn Sie dazu aufgefordert werden, geben Sie die Citrix Administrator-Anmeldeinformationen für die Site ein.

Citrix Cloud führt einen Verbindungstest durch, um zu überprüfen, ob Ihre Site erreichbar ist. Die Discovery kann je nach Art und Größe der Site einige Minuten dauern.

7. Wenn eine Meldung angezeigt wird, die angibt, dass die Site erfolgreich erkannt wurde, wählen Sie **Weiter**.

Schritt 2: Verifizieren der Active Directory-Verbindung

In **Active Directory-Verbindung verifizieren** zeigt Citrix Cloud die Domänen an, die mit Ihrer Site verwendet werden, und ob Cloud Connectors in diesen Domänen installiert sind.

Wenn in einer Domäne keine Cloud Connectors vorhanden sind, können Benutzer in der Domäne Citrix Workspace nicht für den Zugriff auf die dort veröffentlichten Anwendungen verwenden. Wenn Sie nur einen Cloud Connector in Ihrer Domäne haben, haben Sie zwei Möglichkeiten:

- Installieren weiterer Cloud Connectors, indem **Sie Connector installieren** auswählen
- Fortfahren, ohne weitere Cloud Connectors zu installieren, indem Sie **Ich verstehe, dass für hohe Verfügbarkeit in jeder Domäne zwei Connectors installiert sein müssen** auswählen

Wenn Ihre Anwendungen in Ihrer Site lokale Benutzer zugewiesen sind, wählen Sie **Benutzerliste (CSV-Datei) herunterladen**.

Nachdem Sie Ihre Active Directory-Verbindung überprüft haben, wählen Sie **Weiter**.

Aufgabe 3: Konnektivität konfigurieren

In diesem Schritt geben Sie an, ob Sie nur externen oder nur internen Benutzerzugriff auf Ihre Site über Citrix Workspace erlauben. Interne Konnektivität erfordert, dass die Benutzer im selben Netzwerk wie Ihre Site und VDAs sind, die Ihre veröffentlichten Ressourcen hosten. Für externe Konnektivität können Sie Ihr vorhandenes On-Premises-Citrix Gateway oder den cloudgehosteten Citrix Gateway Service verwenden.

Wählen Sie unter **Konnektivitätstyp auswählen > Konnektivität konfigurieren** eine der folgenden Optionen aus:

- **Vorhandenes Gateway hinzufügen:** Wählen Sie diese Option, um einen externen Zugriff über Ihr vorhandenes Citrix Gateway zu ermöglichen.
- **Citrix Gateway-Dienst:** Wählen Sie diese Option, um eine Testversion zu aktivieren oder Ihr bestehendes Abonnement für Ihre Site zu verwenden.
- **Nur interne:** Wählen Sie diese Option, wenn keine andere Konfiguration erforderlich ist.

Wenn **Vorhandenes Gateway hinzufügen** ausgewählt ist, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Bearbeiten** und geben Sie die öffentliche URL des Citrix Gateway ein.
2. Stellen Sie sicher, dass Citrix Gateway für die Verwendung Ihrer Cloud Connectors als STA-Server konfiguriert ist, wie in [CTX232640](#) beschrieben.
3. Wählen Sie **STA testen** und, wenn der Test bestanden wurde, **Weiter**. Wenn der Test nicht erfolgreich ist, finden Sie Informationen zur Problembehandlung in [CTX232517](#).

Wenn **Citrix Gateway-Dienst** ausgewählt ist, der Dienst für Ihr Citrix Cloud-Konto aber nicht als Testversion oder als erworbener Dienst aktiviert ist, können Sie **60-tägige Testversion starten** wählen. Citrix Cloud aktiviert den Dienst als Testversion für Sie. Wenn der Dienst zu einem früheren Zeitpunkt aktiviert wurde, erkennt Citrix Cloud den Dienst und zeigt noch verbleibende Testtage an.

Wenn Sie die Aufgaben abgeschlossen haben, wählen Sie **Weiter**.

Aufgabe 4: Siteaggregation bestätigen

Überprüfen Sie in diesem Schritt die Siteaggregation. Dies umfasst den XML-Port, die XML-Server, die Active Directory-Domänen und den Konnektivitätstyp, den Sie zuvor ausgewählt haben.

Citrix Cloud zeigt bis zu fünf XML-Server an, mit denen es eine Verbindung herstellen kann. Wenn in Ihrer Site mehrere XML-Server sind, aber nur einer angezeigt wird, zeigt Citrix Cloud eine Warnung an. Informationen zur Behebung dieses Problems finden Sie unter [CTX232516](#).

1. Überprüfen Sie in **Siteaggregation bestätigen** den XML-Port, die XML-Server, die Active Directory-Domänen und den Konnektivitätstyp, die Sie zuvor ausgewählt haben.
2. Wählen Sie **Speichern und schließen**. Die neu hinzugefügte Site wird auf der Seite **Sites** angezeigt.

Wenn Sie verschiedene XML-Server angeben möchten, können Sie diese Werte für Ihre Site ändern, nachdem Sie **Speichern und schließen** ausgewählt haben.

Aufgabe 5: Serviceintegrationen verwalten

Nachdem Sie Ihre erste Site hinzugefügt haben, müssen Sie die **Serviceintegration** für Virtual Apps and Desktops-On-Premises-Sites aktivieren, die standardmäßig deaktiviert ist. Abonnenten können

Ressourcen der Site erst sehen, wenn Sie sie aktiviert haben.

1. Gehen Sie zu **Workspace-Konfiguration > Serviceintegrationen > Virtual Apps and Desktops > Lokale Sites** und wählen Sie die Punkte, um das Menü mit den Siteaktionen zu öffnen.
2. Aktivieren Sie die Serviceintegration, damit sich Abonnenten bei ihren Workspaces anmelden und Ressourcen der Site sehen können.

Ändern der Sitekonfiguration

Erneute Discovery Ihrer Site

Wenn Sie Ihrer Site Delivery Controller hinzufügen oder XML-Ports ändern, können Sie die Discovery erneut initiieren, um zu überprüfen, ob Ihre Site in Citrix Workspace noch erreichbar ist.

1. Gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die Site, die Sie aktualisieren möchten, und wählen Sie dann **Site bearbeiten**.
2. Geben Sie unter **Serveradresse** die IP-Adresse oder den FQDN eines Delivery Controllers der Site ein und wählen Sie **Erneute Discovery**.

Hinzufügen oder Ändern von XML-Servern

Wenn Sie Citrix Workspace eine Site hinzufügen, erkennt Citrix Cloud automatisch XML-Server in Ihrer Site und zeigt in Ihrer Sitekonfiguration bis zu fünf XML-Server an. Sie können XML-Server nach Bedarf Ihrer Sitekonfiguration hinzufügen und daraus entfernen. Das Anzeigelimit ist fünf XML-Server.

Hinzufügen eines XML-Servers

1. Gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die Site, die Sie aktualisieren möchten, und wählen Sie **Site bearbeiten**.
2. Geben Sie im Abschnitt **XML-Server** den XML-Serverport ein und wählen Sie ggf. **SSL verwenden**.
3. Wählen Sie eine Konnektivitätsoption:
 - **Mit Lastausgleich:** Mit dieser Option kann Citrix Cloud einen beliebigen XML-Server aus der Liste auswählen.
 - **Failover:** Mit dieser Option verwendet Citrix Cloud die aufgelisteten XML-Server in der Reihenfolge, in der sie in der Liste aufgeführt sind. Nur der erste XML-Dienst in der Liste wird für den Start verwendet. Ist er nicht verfügbar, wird der zweite Server verwendet. Sie können die Liste neu ordnen, indem Sie die einzelnen Server an die gewünschte Position ziehen.
4. Wählen Sie **Änderungen speichern**.

Wenn beim Hinzufügen eines XML-Servers ein Fehler auftritt, finden Sie Informationen zur Fehlerbehebung in [CTX232516](#).

Hinzufügen von IP-Bereichen für verschiedene Konnektivitätsoptionen

Wenn Sie VDAs oder Sitzungshosts in verschiedenen Subnetzen haben, können Sie für jeden VDA einen IP-Bereich mit einem anderen Konnektivitätstyp angeben. Jedem IP-Bereich kann auch ein anderer Ressourcenstandort zugeordnet sein. Beispielsweise ist Folgendes möglich: Sie haben einen IP-Bereich für Maschinen in der EU, in dem Benutzer interne Verbindungen herstellen, einen IP-Bereich für Maschinen in der EU, in dem Benutzer über Ihr Citrix Gateway Verbindungen herstellen, und einen IP-Bereich für Maschinen in den USA, in dem Benutzer über den Citrix Gateway Service Verbindungen herstellen.

1. Gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die Site, die Sie aktualisieren möchten, und wählen Sie **Site bearbeiten**.
2. Wählen Sie im Bereich **Konnektivität** die Option **IP-Bereich mit einer anderen Konnektivitätsoption hinzufügen** und geben Sie einen IP-Bereich im CIDR-Format ein.

Erstellen eines Ressourcenstandorts:

1. Wählen Sie **Einen neuen Ressourcenstandort hinzufügen** und geben Sie einen Anzeigenamen ein.
2. Wählen Sie unter **Konnektivität auswählen** aus, ob Sie nur internen Zugriff gewähren oder externen Zugriff über Ihr Citrix Gateway oder den Citrix Gateway Service zulassen möchten.

Zuweisen eines bestehenden Ressourcenstandorts zum IP-Bereich:

1. Wählen Sie **Vorhandenen Ressourcenstandort auswählen**.
2. Wählen Sie den gewünschten Ressourcenstandort.
3. Wenn Sie einen Ressourcenstandort mit nur einem installierten Cloud Connector auswählen, aktivieren Sie die Option **Ich verstehe, dass für hohe Verfügbarkeit in einem Ressourcenstandort zwei Connectors installiert sein müssen**.
4. Wählen Sie **Hinzufügen** aus.

Hinzufügen von weiteren Active Directory-Domänen

Wenn Sie Cloud Connectors in zusätzlichen Domänen installieren und Ihre Site Active Directory-Benutzer enthält, können Sie sich vergewissern, dass sie Ihrer Sitekonfiguration in Citrix Workspace hinzugefügt werden.

1. Gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die Site, die Sie aktualisieren möchten, und wählen Sie dann **Site bearbeiten**.
2. Wählen Sie unter Active Directory die Option **Aktualisieren**.

Deaktivieren von Sites

Wenn Ihre On-Premises-Site nicht mehr für Benutzer in Citrix Workspace verfügbar sein soll, können Sie die Site deaktivieren. Sie können eine einzelne On-Premises-Site oder alle On-Premises-Sites deaktivieren, die Sie Citrix Workspace hinzugefügt haben.

Wenn Sites deaktiviert sind, können Benutzer nicht über Citrix Workspace auf die On-Premises-Anwendungen in diesen Sites zugreifen. Die Konfiguration dieser Sites bleibt jedoch erhalten. Wenn Sie eine Site später wieder aktivieren, werden der Standardstandort der Site, die Domäne, der XML-Server und die Konnektivitätseinstellungen der Site beibehalten.

So deaktivieren Sie eine On-Premises-Site

1. Gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die gewünschte Site und wählen Sie dann **Deaktivieren**.
2. Eine Bestätigungsmeldung wird angezeigt. Wählen Sie erneut **Deaktivieren**.

So deaktivieren Sie alle On-Premises-Sites

Um alle Sites auf der Seite **Sites** zu deaktivieren, deaktivieren Sie die Workspace-Service-Integration für alle On-Premises-Sites für Virtual Apps and Desktops. Anweisungen finden Sie unter [Deaktivieren der Workspaceintegration für einen Service](#).

Um eine einzelne On-Premises-Site wieder zu aktivieren oder später eine neue Site hinzuzufügen, müssen Sie zunächst die Workspace-Service-Integration für alle Sites auf der Seite **Serviceintegrationen** wieder aktivieren.

Löschen einer Site aus Citrix Workspace

Wenn Ihre On-Premises-Sitekonfiguration nicht mehr in Citrix Workspace verfügbar sein soll, können Sie die Site löschen. Beim Löschen einer Site wird nur die Konfiguration der Site aus Citrix Workspace entfernt. Citrix Cloud ändert Ihre Site nicht.

Um eine Site zu löschen, gehen Sie zu **Workspace-Konfiguration > Sites**, wählen Sie das Punktemenü für die gewünschte Site und wählen Sie dann **Löschen**.

Optimieren der Konnektivität zu Workspaces mit einer direkten Workloadverbindung

November 27, 2023

Mit der direkten Workloadverbindung in Citrix Cloud optimieren Sie den internen Datenverkehr zu Apps und Desktops in Workspaces und können so HDX-Sitzungen beschleunigen. In der Regel verbinden sich Benutzer in internen und externen Netzwerken über ein externes Gateway mit VDAs. Dieses Gateway kann on-premises in Ihrer Organisation sein oder als Citrix Dienst dem Ressourcenstandort in Citrix Cloud hinzugefügt werden. Mit der direkten Workloadverbindung können interne Benutzer das Gateway umgehen und sich direkt mit VDAs verbinden, wodurch die Latenz für den internen Netzwerkverkehr verringert wird.

Um eine direkte Workloadverbindung einzurichten, benötigen Sie Netzwerkstandorte, die dem Standort entsprechen, an dem Clients Apps und Desktops in Ihrer Umgebung starten. Fügen Sie mit dem Netzwerkpositionsdienst (NLS) eine öffentliche Adresse für jeden Bürostandort hinzu, an dem sich diese Clients befinden. Sie haben zwei Möglichkeiten, Netzwerkspeicherorte zu konfigurieren:

- Menüoption **Netzwerkspeicherorte** in Citrix Cloud.
- Verwenden eines von Citrix bereitgestellten PowerShell-Moduls.

Netzwerkspeicherorte entsprechen den öffentlichen IP-Bereichen der Netzwerke, von denen aus interne Benutzer eine Verbindung herstellen (z. B. Ihre Bürostandorte oder Zweigstellen). Citrix Cloud bestimmt anhand öffentlicher IP-Adressen, ob Netzwerke, aus denen virtuelle Apps oder Desktops gestartet werden, innerhalb oder außerhalb des Unternehmensnetzwerks liegen. Wenn ein Abonnent sich über das interne Netzwerk verbindet, leitet Citrix Cloud die Verbindung direkt an den VDA weiter und umgeht NetScaler Gateway. Wenn ein Abonnent eine externe Verbindung herstellt, leitet Citrix Cloud ihn über NetScaler Gateway und dann den Datenverkehr der Sitzung über Citrix Cloud Connector an den VDA im internen Netzwerk weiter. Wenn Citrix Gateway Service verwendet wird und das [Rendezvous-Protokoll](#) aktiviert ist, leitet Citrix Cloud externe Benutzer über den Gateway Service an den VDA im internen Netzwerk weiter. Roaming-Clients wie Laptops können eine dieser Netzwerkrouthen verwenden, je nachdem, ob sich der Client zum Startzeitpunkt innerhalb oder außerhalb des Unternehmensnetzwerks befindet.

Wichtig:

Wenn es in Ihrer Umgebung neben On-Premises-VDAs auch Citrix DaaS Standard für Azure gibt und Sie die direkte Workloadverbindung konfigurieren, schlägt der Start im internen Netzwerk fehl.

Die Ressourcenstarts von Remote Browser Isolation, Citrix Virtual Apps Essentials und Citrix Virtual Desktops Essentials werden immer über das Gateway geleitet. Bei diesen Starts kommt es daher zu

keiner Leistungsverbesserung durch die direkte Workloadverbindung.

Anforderungen

Netzwerkanforderungen

- Das Unternehmensnetzwerk und Gast-WiFi-Netzwerke müssen separate öffentliche IP-Adressen haben. Wenn Ihr Unternehmens- und Gastnetzwerk dieselbe öffentliche IP-Adresse verwendet, können Benutzer im Gastnetzwerk keine DaaS-Sitzungen starten.
- Verwenden Sie die öffentlichen IP-Adressbereiche der Netzwerke, von denen aus interne Benutzer eine Verbindung herstellen. Interne Benutzer in diesen Netzwerken müssen über eine direkte Verbindung zu den VDAs verfügen. Andernfalls schlägt der Start virtueller Ressourcen fehl, da Workspace versucht, interne Benutzer direkt an den VDA weiterzuleiten. Diese Verbindung ist jedoch nicht möglich.
- Obwohl sich VDAs normalerweise in Ihrem On-Premises-Netzwerk befinden, können Sie auch VDAs verwenden, die in einer öffentlichen Cloud wie Microsoft Azure gehostet werden. Für den Start von Clients muss eine Netzwerkroute zum Kontakt der VDAs vorliegen, die nicht von einer Firewall blockiert wird. Dies erfordert einen VPN-Tunnel vom On-Premises-Netzwerk zu einem virtuellen Netzwerk, in dem sich die VDAs befinden.

TLS-Anforderungen

TLS 1.2 muss in PowerShell aktiviert sein, wenn Sie Ihre Netzwerkspeicherorte konfigurieren. Um in PowerShell TLS 1.2 zu erzwingen, verwenden Sie den folgenden Befehl, bevor Sie das PowerShell-Modul verwenden:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Workspaceanforderungen

- Sie haben einen Workspace in Citrix Cloud konfiguriert.
- Citrix DaaS ist unter **Workspacekonfiguration > Serviceintegrationen** aktiviert.

Aktivieren von TLS für Workspace-App für HTML5-Verbindungen

Wenn Ihre Abonnenten die Citrix Workspace-App für HTML5 zum Starten von Apps und Desktops verwenden, empfiehlt Citrix, auf den VDAs im internen Netzwerk TLS zu konfigurieren. Das Konfigurieren von TLS-Verbindungen für Ihre VDAs ermöglicht Direktstarts auf den VDAs. Ohne aktivierte TLS auf

VDAs müssen App- und Desktopstarts über ein Gateway geleitet werden, wenn Abonnenten die Citrix Workspace-App für HTML5 verwenden. Starts mit dem Desktop Viewer sind davon nicht betroffen. Weitere Informationen zum Schutz direkter VDA-Verbindungen mit TLS finden Sie unter [CTX134123](#) im Citrix Support Knowledge Center.

Netzwerkspeicherorte über die GUI hinzufügen

Die Konfiguration einer direkten Workloadverbindung über Citrix Cloud umfasst das Erstellen von Netzwerkspeicherorten unter Verwendung der öffentlichen IP-Adressbereiche jedes Zweigstandorts, von dem aus sich interne Benutzer verbinden.

1. Wählen Sie in der Citrix Cloud-Konsole **Netzwerkspeicherorte**.
2. Klicken Sie auf **Netzwerkspeicherort hinzufügen**.
3. Geben Sie einen Namen und einen öffentlichen IP-Adressbereich für den Netzwerkspeicherort ein.

Add a Network Location ✕

Adaptive access based on network locations allow you to specify networks in your organization. Administrators can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.

Location name

Argentina ✕

Public IP address range

✕

Save

4. Klicken Sie auf **Speichern**.
5. Wiederholen Sie diese Schritte für jeden Netzwerkspeicherort, den Sie hinzufügen möchten.

Hinweis:

Tags für den Ort sind für die direkte Workloadverbindung nicht erforderlich, da der Konnektivitätstyp immer **Intern** ist. Das Feld **Tags für den Ort** ist nur dann auf der Seite **Netzwerkspeicherort hinzufügen** sichtbar (**Citrix Cloud > Netzwerkspeicherort > Netzwerkspeicherort hinzufügen**).

gen > Tags für den Ort), wenn die Funktion “Adaptiver Zugriff” aktiviert ist. Einzelheiten siehe [Adaptiven Zugriff aktivieren](#).

Ändern oder Entfernen von Netzwerkspeicherorten

1. Wählen Sie in der Citrix Cloud-Konsole im Hauptmenü **Netzwerkspeicherorte**.
2. Suchen Sie den gewünschten Netzwerkspeicherort und klicken Sie auf die Auslassungspunkte.

Adaptive access based on network locations allow you to specify the internal networks in your organization. Admin can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.

Search... + Add network location

Location name	Public IP address range	
testloc02	192.167.100.100/32	...
testloc01	192.167.1.1/29	...
sydmobip02	1344.2739/32	...
sp_nls_namatch	69.181.66.45/32	...
sp_mac_office_internal	192.221.154.0/24	...
sp_mac_internal	69.181.66.39/32	...

3. Wählen Sie einen der folgenden Befehle:
 - **Bearbeiten**, um die Netzwerkadresse zu ändern. Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **Speichern**.
 - **Löschen**, um den Netzwerkspeicherort zu entfernen. Wählen Sie **Ja, löschen**, um den Löschvorgang zu bestätigen. Sie können diese Aktion nicht rückgängig machen.

Netzwerkstandorte mit PowerShell hinzufügen und ändern

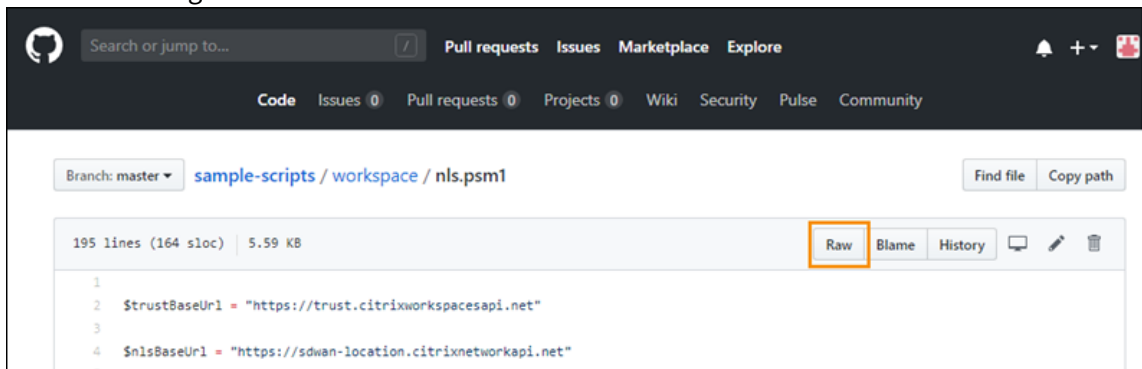
Statt der Citrix Cloud-Verwaltungskonsole können Sie das PowerShell-Skript verwenden, um die direkte Workloadverbindung zu konfigurieren. Die Konfiguration der direkten Workloadverbindung mit PowerShell umfasst die folgenden Aufgaben:

1. Bestimmen Sie die öffentlichen IP-Adressbereiche der einzelnen Zweigstellen, von denen interne Benutzer eine Verbindung herstellen.
2. Download des PowerShell-Moduls.
3. Erstellen Sie einen sicheren API-Client in Citrix Cloud und notieren Sie sich die Client-ID und den geheimen Clientschlüssel.
4. Importieren Sie das PowerShell-Modul und stellen Sie eine Verbindung zum Netzwerkpositionsdienst (NLS) mit Ihren API-Clientdetails her.
5. Erstellen Sie NLS-Sites für jeden Ihrer Zweigstellen mit den öffentlichen IP-Adressbereichen, die Sie zuvor festgelegt haben. Die direkte Workloadverbindung wird automatisch für alle Starts aktiviert, die von den von Ihnen angegebenen internen Netzwerkspeicherorten stammen.
6. Starten Sie eine App oder einen Desktop von einem Gerät in Ihrem internen Netzwerk und prüfen Sie, ob die Verbindung direkt zum VDA geht, also das Gateway umgeht. Weitere Informationen finden Sie unter [ICA-Dateiprotokollierung](#) in diesem Artikel.

Download des PowerShell-Moduls

Vor dem Einrichten Ihrer Netzwerkstandorte laden Sie das von Citrix bereitgestellte [PowerShell-Modul](#) (nls.psm1) aus dem Citrix GitHub-Repository herunter. Mit diesem Modul können Sie beliebig viele Netzwerkspeicherorte für Ihre VDAs einrichten.

1. Rufen Sie in einem Webbrowser <https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1> auf.
2. Klicken Sie bei gedrückter **ALT**-Taste auf die Schaltfläche **Raw**.



3. Wählen Sie einen Speicherort auf Ihrem Computer und klicken Sie auf **Speichern**.

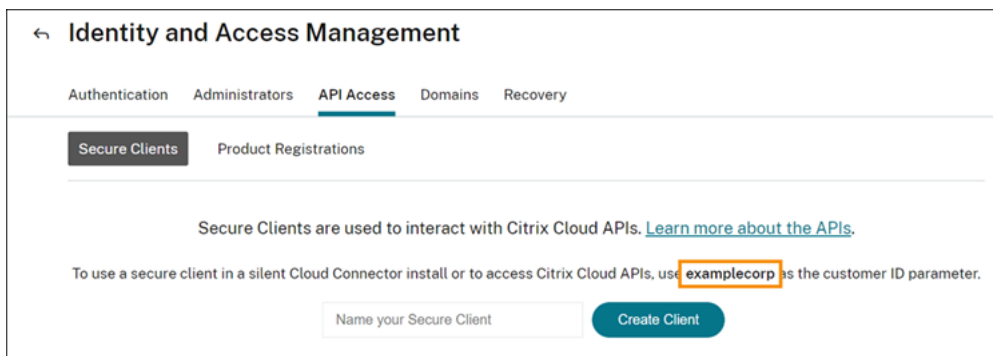
Erforderliche Konfigurationsdetails

Zum Einrichten Ihrer Netzwerkspeicherorte sind folgende Informationen erforderlich:

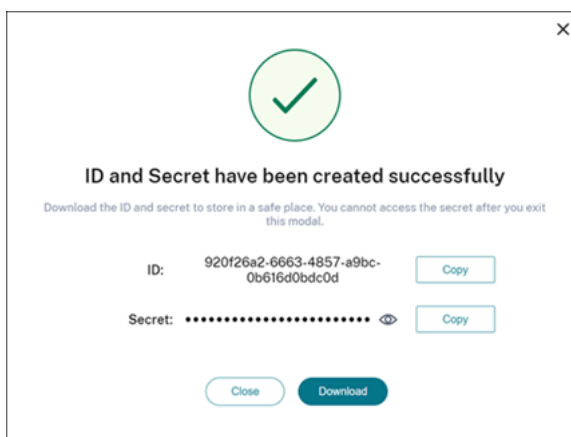
- Kunden-ID, Client-ID und Clientgeheimnis für den sicheren Client in Citrix Cloud. Informationen zum Abrufen dieser Werte finden Sie unter Erstellen eines sicheren Clients in diesem Artikel.
- Öffentliche IP-Adressbereiche für die Netzwerke, von denen Ihre internen Benutzer eine Verbindung herstellen. Weitere Informationen zu diesen öffentlichen IP-Adressbereichen finden Sie unter Anforderungen in diesem Artikel.

Erstellen eines sicheren Clients

1. Melden Sie sich bei Citrix Cloud auf <https://citrix.cloud.com> an.
2. Wählen Sie im Menü "Citrix Cloud" **Identitäts- und Zugriffsverwaltung** und dann **API-Zugriff**.
3. Notieren Sie sich die Kunden-ID auf der Registerkarte **Sichere Clients**.



4. Geben Sie einen Namen für den Client ein und wählen Sie **Client erstellen**.
5. Kopieren Sie die Client-ID und das Clientgeheimnis.



Konfigurieren von Netzwerkstandorten

1. Öffnen Sie ein PowerShell-Befehlsfenster und gehen Sie zum Verzeichnis, in dem Sie das PowerShell-Modul gespeichert haben.
2. Importieren Sie das Modul: `Import-Module .\nls.psm1 -Force`
3. Legen Sie die erforderlichen Variablen fest. Verwenden Sie hierfür die Angaben zum sicheren Client, die Sie unter Erstellen eines sicheren Clients erfasst haben:
 - `$clientId = "YourSecureClientID"`
 - `$customer = "YourCustomerID"`
 - `$clientSecret = "YourSecureClientSecret"`
4. Verbinden Sie sich mit den Anmeldeinformationen für Ihren sicheren Client mit dem Netzwerkpositionsdienst:

```
1 Connect-NLS -clientId $clientId -clientSecret $clientSecret -
  customer $customer
```


- Erstellen Sie einen Netzwerkspeicherort und ersetzen Sie die Parameterwerte durch die Werte für das interne Netzwerk, von dem Ihre internen Benutzer eine direkte Verbindung herstellen:

```
1 New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
  ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
  12.3456 -internal $True
```

Um keinen Bereich, sondern eine einzelne IP-Adresse anzugeben, fügen Sie **/32** am Ende der IP-Adresse hinzu. Beispiel:

```
1 New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
  ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
  12.3456 -internal $True
```

Wichtig:

Wenn Sie den Befehl `New-NLSSite` verwenden, müssen Sie für jeden Parameter mindestens einen Wert einfügen. Wenn Sie diesen Befehl ohne Befehlszeilenargumente ausführen, werden Sie von PowerShell aufgefordert, für jeden Parameter nacheinander die entsprechenden Werte einzugeben. Die Eigenschaft `internal` ist eine erforderliche boolesche Eigenschaft mit den möglichen Werten `$True` oder `$False`, die über PowerShell der Benutzeroberfläche zugeordnet werden. Beispiel: `(UI)Network Internal -> (PowerShell)-internal=$True`.

Wenn der Netzwerkspeicherort erfolgreich erstellt wurde, werden im Befehlsfenster die Details des Netzwerkspeicherorts angezeigt.

- Wiederholen Sie Schritt 5 für alle Netzwerkspeicherorte, von denen die Benutzer eine Verbindung herstellen.
- Der Befehl `Get-NLSSite` gibt eine Liste aller Sites zurück, die Sie mit NLS konfiguriert haben. Überprüfen Sie, ob die Details korrekt sind.

Ändern von Netzwerkspeicherorten

Ändern eines Netzwerkspeicherorts:

- Listen Sie alle vorhandenen Netzwerkspeicherorte in einem PowerShell-Befehlsfenster auf: `Get-NLSSite`
- Zum Ändern des IP-Bereichs für einen bestimmten Netzwerkspeicherort geben Sie ein:

```
(Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32", "
4.3.2.1/32")
```

Dabei ist `[N]` die Ziffer, die der Position in der Liste entspricht (beginnend mit Null) und `"1.2.3.4/32"`, `"4.3.2.1/32"` sind die durch Kommas getrennten IP-Bereiche, die Sie ver-

wenden möchten. Um beispielsweise den ersten aufgelisteten Standort zu ändern, geben Sie folgenden Befehl ein:

```
(Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32",  
141.43.0.0/24")
```

Entfernen von Netzwerkspeicherorten

Wenn Sie Netzwerkspeicherort entfernen müssen, die Sie nicht mehr verwenden, gehen Sie folgendermaßen vor:

1. Listen Sie alle vorhandenen Netzwerkspeicherorte in einem PowerShell-Befehlsfenster auf: `Get-NLSSite`
2. Um alle Netzwerkspeicherorte zu entfernen, geben Sie ein: `Get-NLSSite | Remove-NLSSite`
3. Um bestimmte Netzwerkspeicherorte zu entfernen, geben Sie ein: `(Get-NLSSite)[N] | Remove-NLSSite`. Dabei ist `[N]` die Ziffer, die der Position in der Liste entspricht. Um beispielsweise den ersten aufgelisteten Standort zu entfernen, geben Sie folgenden Befehl ein: `(Get-NLSSite)[0] | Remove-NLSSite`

Überprüfen der fehlerfreien Weiterleitung interner Startvorgänge

Verwenden Sie eine der folgenden Methoden, um zu überprüfen, ob interne Starts direkt auf VDAs zugreifen:

- Zeigen Sie VDA-Verbindungen über die DaaS-Konsole an.
- Überprüfen Sie mit der ICA-Dateiprotokollierung die korrekte Adressierung der Clientverbindung.

Citrix DaaS-Konsole

Wählen Sie **Verwalten > Überwachen** und suchen Sie einen Benutzer mit aktiver Sitzung. Im Abschnitt **Sitzungsdetails** der Konsole werden direkte VDA-Verbindungen als UDP-Verbindungen angezeigt, während Gateway-Verbindungen als TCP-Verbindungen angezeigt werden.

Wird UDP in der DaaS-Konsole nicht angezeigt, müssen Sie die Richtlinie "Adaptiver HDX-Transport" für die VDAs aktivieren.

ICA-Dateiprotokollierung

Aktivieren Sie die ICA-Dateiprotokollierung auf dem Clientcomputer wie unter [Aktivieren der Protokollierung für die Datei launch.ica](#) beschrieben. Überprüfen Sie nach dem Start von Sitzungen die Einträge **Address** und **SSLProxyHost** in der Protokolldatei.

Direkte VDA-Verbindungen Bei einer Direktverbindung zum VDA enthält die Eigenschaft **Address** die IP-Adresse und den Port des VDA.

Dies ist ein Beispiel für eine ICA-Datei, wenn ein Client eine Anwendung über NLS startet:

```
1 [Notepad++ Cloud]
2 Address=;10.0.1.54:1494
3 SSLEnable=Off
4 <!--NeedCopy-->
```

Die Eigenschaft **SSLProxyHost** ist in dieser Datei nicht vorhanden. Diese Eigenschaft ist nur für Starts über ein Gateway enthalten.

Gateway-Verbindungen Bei Gateway-Verbindungen enthält die Eigenschaft **Address** das STA-Ticket von Citrix Cloud. Die Eigenschaft **SSLEnable** ist auf **Ein** festgelegt und die Eigenschaft **SSLProxyHost** enthält den FQDN und Port des Gateways.

Dies ist das Beispiel einer ICA-Datei, wenn ein Client über den Citrix Gateway Service verbunden ist und eine Anwendung startet:

```
1 [PowerShell ISE Cloud]
2 Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
3 SSLEnable=On
4 SSLProxyHost=global.g.nssvcstaging.net:443
5 <!--NeedCopy-->
```

Dies ist das Beispiel einer ICA-Datei, wenn ein Client über ein On-Premises-Gateway verbunden ist und eine Anwendung über ein On-Premises-Gateway startet, das innerhalb des Ressourcenstandorts konfiguriert ist:

```
1 [PowerShell ISE Cloud]
2 Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
3 SSLEnable=On
4 SSLProxyHost=onpremgateway.domain.com:443
5 <!--NeedCopy-->
```

Hinweis:

Virtuelle On-Premises-Gatewayserver, die zum Starten virtueller Apps und Desktops verwendet werden, müssen virtuelle VPN-Server sein, keine virtuellen nFactor-Authentifizierungsserver. Virtuelle nFactor-Authentifizierungsserver dienen nur der Benutzerauthentifizierung und nicht als Proxy für den HDX- und ICA-Startdatenverkehr.

Beispielskript

Das Beispielskript enthält alle Befehle, die Sie zum Hinzufügen, Ändern und Entfernen der öffentlichen IP-Adressbereiche für Ihre Zweigstellen benötigen. Sie müssen jedoch nicht alle Befehle ausführen,

um eine einzelne Funktion auszuführen. Damit das Skript ausgeführt werden kann, müssen Sie stets die ersten 10 Zeilen angeben, von **Import-Module** bis einschließlich **Connect-NLS**. Anschließend können Sie nur die Befehle für die Funktionen angeben, die Sie ausführen möchten.

```
1 Import-Module .\nls.psm1 -Force
2
3 $clientId = "XXXX" #Replace with your clientId
4 $clientSecret = "YYY" #Replace with your clientSecret
5 $customer = "CCCCCC" #Replace with your customerid
6
7 # Connect to Network Location Service
8 Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
   $customer
9
10 # Create a new Network Location Service Site (Replace with details
   corresponding to your branch locations)
11 New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("
   1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True
12
13 # Get the existing Network Location Service Sites (optional)
14 Get-NLSSite
15
16 # Update the IP Address ranges of your first Network Location Service
   Site (optional)
17 $s = (Get-NLSSite)[0]
18 $s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
19 \ $s | Set-NLSSite
20
21 # Remove all Network Location Service Sites (optional)
22 Get-NLSSite | Remove-NLSSite
23
24 # Remove your third site (optional)
25 \ (Get-NLSSite)\[2] | Remove-NLSSite
```

Problembehandlung

Fehler beim VDA-Start

Wenn VDA-Sitzungen nicht gestartet werden, müssen Sie sicherstellen, dass Sie öffentliche IP-Adressbereiche aus dem richtigen Netzwerk verwenden. Beim Konfigurieren Ihrer Netzwerkspeicherorte müssen Sie die öffentlichen IP-Adressbereiche des Netzwerks verwenden, von dem aus Ihre internen Benutzer eine Verbindung zum Internet herstellen. Weitere Informationen finden Sie unter Anforderungen in diesem Artikel.

Interne VDA-Starts werden weiterhin über das Gateway geleitet

Wenn intern gestartete VDA-Sitzungen weiterhin über das Gateway geleitet werden (als wären sie externe Sitzungen), müssen Sie sicherstellen, dass Sie die richtige öffentliche IP-Adresse verwenden, von denen Ihre internen Benutzer eine Verbindung zum Workspace herstellen. Die auf der NLS-Site aufgeführte öffentliche IP-Adresse muss der Adresse entsprechen, die der Client, der Ressourcen startet, für den Zugriff auf das Internet verwendet. Um die korrekte öffentliche IP-Adresse für den Client zu erhalten, melden Sie sich an der Clientmaschine an, öffnen dann eine Suchmaschine und geben dort "what is my ip" in die Suchleiste ein.

Alle Clients, die Ressourcen innerhalb desselben Bürostandorts starten, greifen in der Regel über dieselbe ausgehende öffentliche IP-Adresse im Netzwerk auf das Internet zu. Für diese Clients muss eine Internetnetzwerkroute zu den Subnetzen mit den VDAs vorliegen, die nicht durch eine Firewall blockiert wird. Weitere Informationen finden Sie unter Anforderungen in diesem Artikel.

Fehler beim Ausführen von PowerShell-Cmdlets auf Nicht-Windows-Plattformen

Wenn beim Ausführen von Cmdlets mit den richtigen Parametern in PowerShell Core Fehler auftreten, stellen Sie sicher, dass der Vorgang erfolgreich ausgeführt wurde. Wenn beispielsweise beim Ausführen des Cmdlets "New-NLSSite" Fehler auftreten, führen Sie `Get-NLSSite` aus, um zu prüfen, ob die Site erstellt wurde. Beim Ausführen dieser Cmdlets unter macOS oder Linux mit PowerShell Core werden evtl. Fehler gemeldet, obwohl der Vorgang erfolgreich ausgeführt wurde.

Wenn das Problem beim Ausführen von Cmdlets mit den richtigen Parametern unter Windows mit PowerShell auftritt, stellen Sie sicher, dass Sie die neueste PowerShell-Modulversion verwenden. Bei Verwendung der neuesten Version des PowerShell-Moduls tritt dieses Problem unter Windows nicht auf.

Zusätzliche Hilfe und Unterstützung

Bei Fragen oder Problemen wenden Sie sich bitte an Ihren Citrix Vertriebsmitarbeiter oder an den [Citrix Support](#).

Servicekontinuität

November 27, 2023

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

Servicekontinuität ermöglicht Benutzern auch bei Ausfällen den Zugriff auf ihre DaaS-Apps und -Desktops, solange eine Netzwerkverbindung zwischen Benutzergerät und Ressourcenstandort besteht. Bei Ausfällen in Citrix Cloud-Komponenten oder öffentlichen und privaten Clouds können Benutzer sich weiterhin mit DaaS-Apps und -Desktops verbinden. Benutzer können sich direkt mit dem Ressourcenstandort oder über den Citrix Gateway Service verbinden.

Durch Einsatz der Service Worker-Technologie von Progressive Web Apps werden Ressourcen in der Benutzeroberfläche zwischengespeichert, was die visuelle Darstellung veröffentlichter Ressourcen bei Ausfällen verbessert.

Servicekontinuität verwendet Workspace-Verbindungsleases, um Benutzern bei einem Ausfall den Zugriff auf Apps und Desktops zu ermöglichen. Workspace-Verbindungsleases sind langlebige Autorisierungstoken. Die Workspace-Verbindungsleasedateien werden im Cache des Benutzergeräts gespeichert. Wenn ein Benutzer sich bei Citrix Workspace anmeldet, werden im Benutzerprofil Workspace-Verbindungsleasedateien für jede für den Benutzer veröffentlichte Ressource gespeichert. Mit Servicekontinuität können Benutzer während eines Ausfalls selbst dann auf Apps und Desktops zugreifen, wenn sie eine App oder einen Desktop nie zuvor gestartet haben. Workspace-Verbindungsleasedateien sind signiert, verschlüsselt und mit dem Benutzer und dem Benutzergerät verknüpft. Bei aktivierter Servicekontinuität ermöglicht ein Workspace-Verbindungslease Benutzern standardmäßig für sieben Tage den Zugriff auf Apps und Desktops. Sie können Workspace-Verbindungsleases so konfigurieren, dass sie den Zugriff für bis zu 30 Tage ermöglichen.

Wenn Benutzer die Citrix Workspace-App beenden, wird nur die Citrix Workspace-App geschlossen. Die Workspace-Verbindungsleases werden beibehalten. Benutzer beenden die Citrix Workspace-App, indem sie mit der rechten Maustaste auf das Symbol in der Taskleiste klicken oder das Benutzergerät neu starten. Sie können Servicekontinuität so konfigurieren, dass Workspace-Verbindungsleases gelöscht oder beibehalten werden, wenn Benutzer sich während eines Ausfalls bei Citrix Workspace abmelden. Standardmäßig werden Workspace-Verbindungsleases von Benutzergeräten gelöscht, wenn Benutzer sich während eines Ausfalls abmelden.

Servicekontinuität wird für Double-Hop-Szenarien unterstützt, wenn die Citrix Workspace-App auf einem virtuellen Desktop installiert ist.

Einen ausführlichen technischen Artikel über Servicekontinuität und andere Citrix Cloud-Features zur Verbindungsstabilität finden Sie unter [Resilienz von Citrix Cloud](#).

Hinweis:

Das veraltete Citrix DaaS-Feature "Verbindungsleasing" ähnelt Workspace-Verbindungsleases insofern, als dass es ebenfalls die Verbindungsstabilität bei Ausfällen verbesserte. Ansonsten stehen das veraltete Feature und Servicekontinuität nicht im Zusammenhang.

Einrichten des Benutzergeräts

Damit Benutzer während eines Ausfalls auf Ressourcen zugreifen zu können, müssen sie sich vor dem Ausfall bei Citrix Workspace anmelden. Wenn Sie das Servicekontinuität-Feature aktivieren, müssen Benutzer die folgenden Schritte auf ihren Geräten ausführen:

1. Laden Sie eine unterstützte Version der Citrix Workspace-App herunter und installieren Sie sie.
2. Hinzufügen der Workspace-URL für Ihre Organisation zur Citrix Workspace-App (z. B. <https://example.cloud.com>).
3. Anmelden bei Citrix Workspace.

Wenn sich ein Benutzer zum ersten Mal bei Citrix Workspace anmeldet, lädt die Servicekontinuität Workspace-Verbindungsleases auf sein Gerät herunter.

Das Herunterladen von Workspace-Verbindungsleases kann bei der erstmaligen Anmeldung bis zu 15 Minuten dauern. Benutzer können während des Downloads weiterhin veröffentlichte Ressourcen starten.

Benutzererfahrung während eines Ausfalls

Bei aktivierter Servicekontinuität wird die Benutzererfahrung während eines Ausfalls von mehreren Faktoren bestimmt:

- Welche Art von Ausfall liegt vor?
- Ist die Citrix Workspace-App mit Domänen-Passthrough-Authentifizierung konfiguriert?
- Ist für die App oder den Desktop, mit dem bzw. der sich der Benutzer verbindet, die Sitzungs-freigabe aktiviert?

Bei einigen Ausfällen können Benutzer ohne Beeinträchtigung weiter auf DaaS zugreifen. Bei anderen Ausfällen ändert sich möglicherweise die Darstellung von Workspace oder der Benutzer wird aufgefordert, Maßnahmen zu ergreifen.

In dieser Tabelle wird zusammengefasst, wie die Servicekontinuität den Zugriff von Benutzern auf Apps und Desktops bei Ausfällen verschiedenen Typs unterstützt.

Wo tritt der Ausfall auf	Wie bleibt der Benutzerzugriff erhalten	Benutzererfahrung während des Ausfalls
Citrix Workspace-Dienst	Die Citrix Workspace-App enumeriert Apps und Desktops basierend auf dem lokalen Cache des Benutzergeräts.	Die Symbole nicht verfügbarer Apps und Desktops werden abgeblendet angezeigt. Die Benutzer können weiterhin auf Apps und Desktops zugreifen, deren Symbole nicht abgeblendet sind. Nach dem Klicken auf ein nicht abgeblendetes Symbol werden die Benutzer evtl. aufgefordert, ihre Anmeldeinformationen erneut am VDA einzugeben. Um wieder Zugriff auf alle ihre Apps und Desktops zu erhalten, können Benutzer versuchen, die Verbindung zu Workspace herzustellen, indem sie auf den Link "Verbindung mit Workspace wiederherstellen" klicken.
Identitätsanbieter	Die Citrix Workspace-App enumeriert Apps und Desktops basierend auf dem lokalen Cache des Benutzergeräts.	Die Benutzer können sich möglicherweise nicht bei Workspace anmelden. Benutzer klicken auf den Link "Workspace offline verwenden" , um, ähnlich wie bei einem Ausfall des Workspace-Diensts, auf einige Apps und Desktops zuzugreifen.

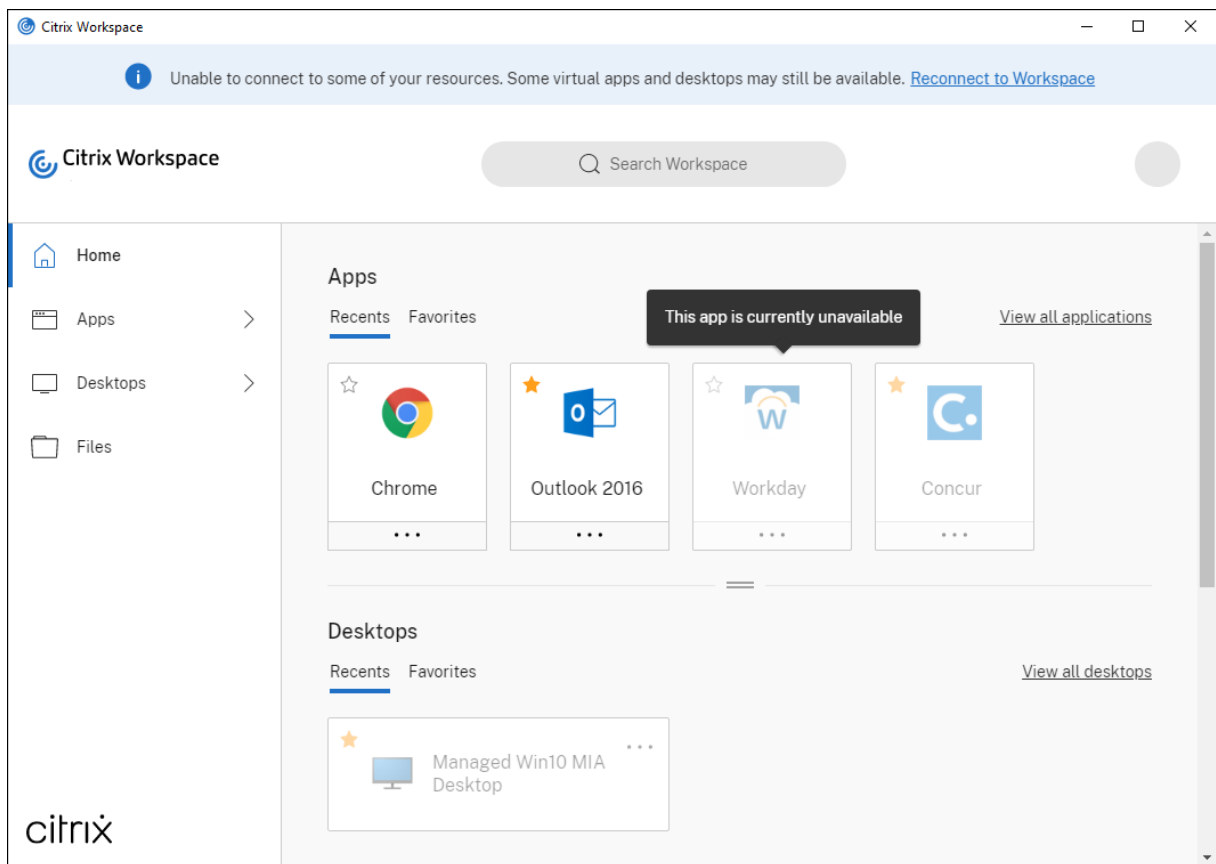
Wo tritt der Ausfall auf	Wie bleibt der Benutzerzugriff erhalten	Benutzererfahrung während des Ausfalls
Citrix Cloud Broker-Dienst	Der Hochverfügbarkeitsdienst im Cloud Connector übernimmt die das Brokering. Alle VDAs, die beim Cloud Broker Service registriert wurden, registrieren sich beim Hochverfügbarkeitsdienst.	Manche Benutzer können evtl. nicht auf virtuelle Ressourcen zugreifen, während sich die VDAs beim Hochverfügbarkeitsdienst registrieren. Bestehende Sitzungen sind nicht betroffen. Keine Benutzeraktion erforderlich.
Secure Ticket Authority	Workspace-Verbindungsleases bieten Zugriff auf virtuelle Ressourcen, wenn dies durch ICA-Dateien nicht möglich ist.	Sitzungsstarts können einige Sekunden länger dauern. Keine Benutzeraktion erforderlich.
Citrix Gateway Service	Der Netzwerkverkehr wird zum nächsten fehlerfreien Citrix Gateway Service-PoP weitergeleitet.	Bei bestehenden Sitzungen kann es einige Sekunden dauern, bis die Verbindung wiederhergestellt ist. Keine Benutzeraktion erforderlich.

Wo tritt der Ausfall auf	Wie bleibt der Benutzerzugriff erhalten	Benutzererfahrung während des Ausfalls
Internetverbindung im LAN	Die Citrix Workspace-App enumeriert Apps und Desktops basierend auf dem lokalen Cache des Benutzergeräts. Besteht eine direkte Netzwerkverbindung zum Ressourcenstandort, umgeht die Citrix Workspace-App den Citrix Gateway Service, wenn ein Benutzer auf nicht abgeblendete Symbole klickt. Die Citrix Workspace-App kontaktiert den Cloud Connector über TCP 2598 und VDAs über TCP 2598 oder UDP 2598.	Die Symbole nicht verfügbarer Apps und Desktops werden abgeblendet angezeigt. Die Benutzer können weiterhin auf Apps und Desktops zugreifen, deren Symbole nicht abgeblendet sind. Nach dem Klicken auf ein nicht abgeblendetes Symbol werden die Benutzer evtl. aufgefordert, ihre Anmeldeinformationen erneut am VDA einzugeben. Um wieder Zugriff auf alle ihre Apps und Desktops zu erhalten, können Benutzer versuchen, die Verbindung zu Workspace herzustellen, indem sie auf den Link "Verbindung mit Workspace wiederherstellen" klicken.

Hinweis:

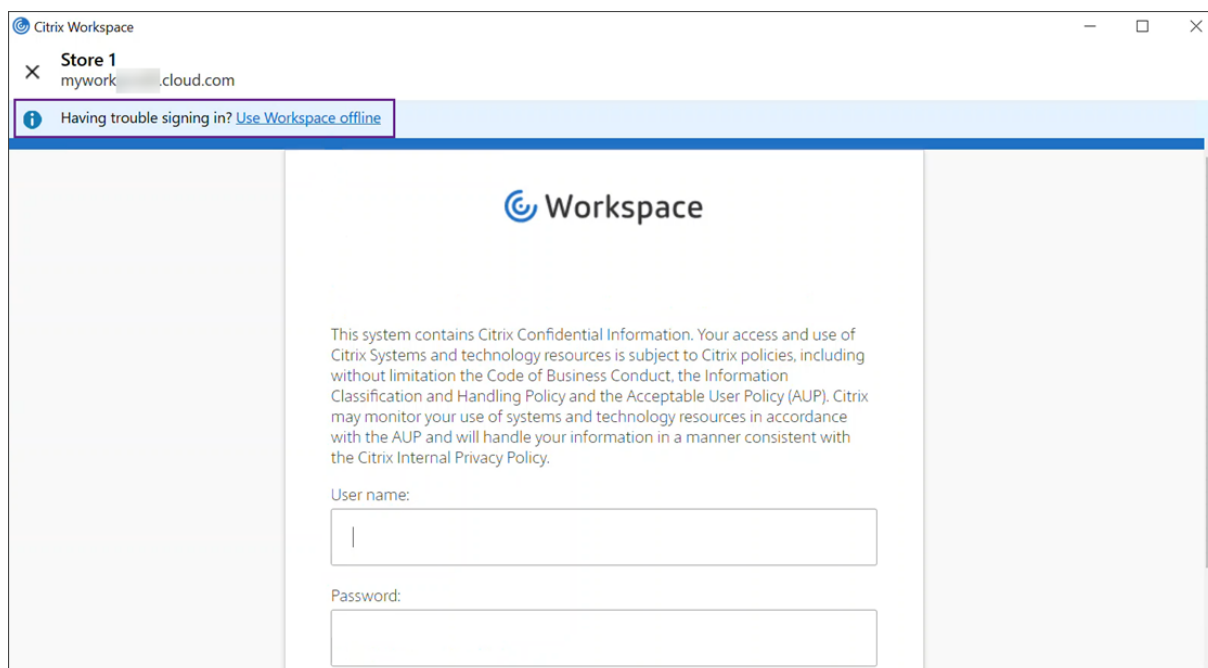
Informationen zur Validierung von Ausfallszenarien in einer Nicht-Produktionsumgebung finden Sie in dem Dokument [Service Continuity Companion Guide](#).

Bei einem Ausfall von Citrix Workspace wird über der Citrix Workspace-Homepage folgende Meldung angezeigt: "Es kann keine Verbindung zu einigen Ihrer Ressourcen hergestellt werden. Einige virtuelle Apps und Desktops sind möglicherweise noch verfügbar." Benutzer sehen Apps und Desktops, auf die sie während des Ausfalls zugreifen können. Wenn die App oder der Desktop nicht verfügbar ist, erscheint das Symbol abgeblendet.



Um auf Ressourcen zuzugreifen, die während eines Ausfalls verfügbar sind, wählen Benutzer ein Ressourcensymbol aus, das nicht abgedunkelt ist. Nach Aufforderung geben Benutzer ihre AD-Anmeldeinformationen am VDA erneut ein, bevor sie auf Ressourcen zugreifen.

Bei einem Ausfall des Identitätsanbieters für die Workspace-Authentifizierung können Benutzer sich möglicherweise nicht über die Workspace-Anmeldeseite bei Citrix Workspace anmelden. Nach 40 Sekunden wird folgende Meldung auf der Citrix Workspace-Homepage angezeigt.



Danach wird die Homepage von Citrix Workspace angezeigt. Der Zugriff auf Ressourcen erfolgt dann wie bei einem Ausfall von Citrix Workspace.

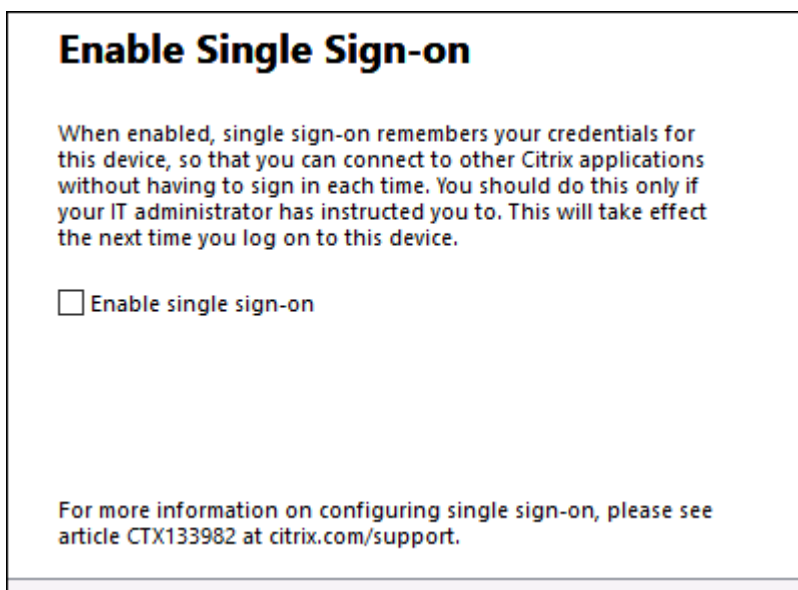
Unabhängig von der Art des Ausfalls können Benutzer weiterhin auf Ressourcen zugreifen, wenn sie die Citrix Workspace-App beenden und neu starten. Benutzer können ihre Benutzergeräte neu starten, ohne den Zugriff auf Ressourcen zu verlieren.

In der Standardkonfiguration der Servicekontinuität verlieren Benutzer den Zugriff auf ihre Ressourcen, wenn sie sich bei Citrix Workspace abmelden. Wenn Sie möchten, dass die Benutzer nach dem Abmelden weiterhin Zugriff auf ihre Ressourcen haben, geben Sie an, dass Workspace-Verbindungsleases beibehalten werden, wenn sich die Benutzer abmelden. Siehe Konfigurieren von Servicekontinuität.

Je nach Konfiguration von Citrix Workspace-App und VDAs werden Benutzer bei einem Ausfall gegebenenfalls aufgefordert, ihre Anmeldeinformationen im Windows-Anmeldebildschirm einzugeben. In diesem Fall geben Benutzer ihre Active Directory (AD)-Anmeldeinformationen oder Ihre Smartcard-PIN ein, um auf Apps oder Desktops zuzugreifen. Dieser Schritt ist erforderlich, wenn Benutzeranmeldeinformationen bei einem Ausfall nicht weitergegeben werden. Benutzer müssen sich erneut beim VDA authentifizieren, bevor sie auf Apps oder Desktops zugreifen können.

In folgenden Fällen können Benutzer auch ohne Eingabe ihrer AD-Anmeldedaten auf Ressourcen zugreifen:

- Citrix Workspace wird während der Installation für Single Sign-On konfiguriert, indem Sie das Kontrollkästchen für den Single Sign-On aktivieren.



- Die Citrix Workspace-App ist mit Domänen-Passthrough-Authentifizierung konfiguriert. Benutzer können während eines Citrix Workspace-Ausfalls auf alle verfügbaren Ressourcen zugreifen, ohne ihre Anmeldeinformationen einzugeben. Informationen zum Konfigurieren der Domänen-Passthrough-Authentifizierung für die Citrix Workspace-App für Windows finden Sie unter [Konfigurieren von Single Sign-On über die grafische Benutzeroberfläche](#) (siehe Dokumentation zur **Authentifizierung**).

Hinweis

StoreFront ist nicht erforderlich, um während eines Ausfalls Single Sign-On auf Ihrem VDA zuzulassen.

- Die Sitzungsfreigabe ist aktiviert. Benutzer können auf diverse Apps oder Desktops auf einem VDA zugreifen, nachdem sie ihre Anmeldeinformationen für eine einzelne Ressource auf diesem VDA bereitgestellt haben. Die Sitzungsfreigabe ist für die Anwendungsgruppe konfiguriert, die die Ressource auf dem VDA enthält. Informationen zum Konfigurieren von Anwendungsgruppen finden Sie unter [Erstellen von Anwendungsgruppen](#).

In allen anderen Konfigurationen werden Benutzer aufgefordert, ihre AD-Anmeldeinformationen am VDA erneut einzugeben, bevor sie auf Ressourcen zugreifen.

Anforderungen und Einschränkungen

Site-Anforderungen

- Wird in allen Editionen von Citrix DaaS und Citrix DaaS Standard für Azure unterstützt, wenn die Workspace-Benutzeroberfläche verwendet wird.

- Nicht unterstützt für Citrix Workspace mit Siteaggregation für on-premises Virtual Apps und Desktops.
- Nicht unterstützt, On-Premises-Citrix Gateway als ICA-Proxy verwendet wird. (Die Verwendung von Citrix Gateway als Workspace-Authentifizierungsmethode wird unterstützt.)

Anforderungen für Benutzergeräte

Unterstützte Mindestversionen der Citrix Workspace-App:

- Citrix Workspace-App für Windows 2106
- Citrix Workspace-App für Linux 2106
- Citrix Workspace-App für Mac 2106
- Citrix Workspace-App für Android 22.2.0
- Citrix Workspace-App für iOS 22.4.5
- Citrix Workspace-App für ChromeOS 2301

Hinweis:

Informationen zur Installation der Citrix Workspace-App für Linux und zu ihrer Verwendung mit Servicekontinuität finden Sie unter [Citrix Workspace-App für Linux](#).

- Bei Zugriff auf Apps und Desktops über einen Browser:
 - Google Chrome oder Microsoft Edge
 - Citrix Workspace-App 2109 für Windows (Mindestversion). Unterstützt von Google Chrome und Microsoft Edge.
 - Mindestens Citrix Workspace-App für Mac Version 2112 zur Verwendung mit Google Chrome.
 - Mindestens Citrix Workspace-App für Mac Version 2206 zur Verwendung mit dem Safari-Browser.

Siehe Servicekontinuität im Browser.

- Nur ein Benutzer pro Gerät unterstützt. Kiosk- oder “Hot Desk”-Benutzergeräte werden nicht unterstützt.

Unterstützte Workspace-Authentifizierungsverfahren

- Active Directory
- Active Directory plus Token
- Azure Active Directory
- Okta

- Citrix Gateway (Anspruch des primären Benutzers muss von AD stammen)
- SAML 2.0

Authentifizierungsbeschränkungen

- Single Sign-On mit Citrix Verbundauthentifizierungsdienst (FAS) wird nicht unterstützt. Die Benutzer geben ihre AD-Anmeldeinformationen in die Windows-Benutzeroberfläche zur Anmeldung des VDAs ein.
- Single Sign-On bei VDA wird nicht unterstützt.
- Lokale zugeordnete Konten werden nicht unterstützt.
- Mit Azure AD verbundene VDAs werden nicht unterstützt. Alle VDAs müssen einer AD-Domäne beigetreten sein.

Skalierung und Größe von Citrix Cloud Connector

- 4 vCPUs oder mehr
- 4 GB Speicher oder mehr

Citrix Cloud Connector Powershell Security

Stellen Sie sicher, dass das Ausführen von Skripten aktiviert ist, indem Sie die Ausführenrichtlinie auf den für Ihre Umgebung geeigneten Wert für **remotedSigned** setzen.

Andere Rechte zum Ausführen von Skripten können ebenfalls funktionieren, wie **Default** oder **AllSigned**.

Citrix Cloud Connector-Konnektivität

Citrix Cloud Connector muss <https://rootoftrust.apps.cloud.com> erreichen können. Konfigurieren Sie Ihre Firewall entsprechend. Weitere Informationen zur Cloud Connector-Firewall finden Sie unter [Konfiguration von Cloud Connector-Proxy und Firewall](#).

Netzwerkonnktivität der Workspace-App

Wenn Sie die Verbindung zu Ihrem Ressourcenstandort von außerhalb Ihres LAN konfigurieren, muss die Workspace-App auf den Benutzergeräten den FQDN des Citrix Gateway Service (https://*.g.nssvc.net) erreichen können. Stellen Sie sicher, dass Ihre Firewall so konfiguriert ist, dass ausgehender Datenverkehr an <https://global-s.g.nssvc.net:433> zugelassen ist, damit die Benutzergeräte jederzeit eine Verbindung zum Citrix Gateway Service herstellen können.

Einschränkungen bei der Verbindungsoptimierung

Advanced Endpoint Analysis (EPA) wird nicht unterstützt.

Enlightened Data Transport (EDT) wird bei Ausfällen nicht unterstützt.

VDA-Anforderungen und -Einschränkungen

- Unterstützt wird VDA 7.15 LTSR oder eine andere aktuelle Version, die noch nicht das EOL (Ende des Lebenszyklus) erreicht hat.
- Mit Azure AD verbundene VDAs werden nicht unterstützt. Alle VDAs müssen einer AD-Domäne beigetreten sein.
- VDAs müssen online sein, damit Benutzer während eines Ausfalls auf VDA-Ressourcen zugreifen können. VDA-Ressourcen sind bei einem Ausfall folgender Komponenten nicht verfügbar:
 - AWS
 - Azure
 - Cloud Delivery Controller, es sei denn, Autoscale ist für die Bereitstellungsgruppe aktiviert, die die Ressource bereitstellt
- Während eines Ausfalls unterstützte VDA-Workloads:
 - Gehostete freigegebene Apps und Desktops
 - Zufällige, nicht beständige Desktops (gepoolte VDI-Desktops) mit Energieverwaltung
 - Statische, nicht beständige Desktops
 - Statische, permanente Desktops, einschließlich Remote-PC-Zugriff

Hinweis:

Eine Zuweisung bei erster Verwendung (Assign on First Use) wird bei Ausfällen nicht unterstützt. Zufällige, nicht beständige Desktops mit Energieverwaltung sind standardmäßig nicht verfügbar, wenn die Verbindung von Cloud Connectors mit Citrix Cloud getrennt wird, es sei denn `ReuseMachinesWithoutShutdownInOutage` ist für die Bereitstellungsgruppe konfiguriert. Weitere Informationen finden Sie unter [Unterstützung für Anwendungen und Desktops](#).

Weitere Informationen zu verfügbaren VDA-Funktionen während Ausfällen finden Sie unter Verwaltung von VDAs bei Ausfällen.

Anforderungen und Einschränkungen für die lokale Tastaturzuordnung

Der Windows-Anmeldebildschirm, in dem Benutzer sich erneut auf dem VDA authentifizieren sollen, unterstützt keine lokale Tastaturzuordnung. Laden Sie im Voraus die von Benutzern benötigten Tas-

taturlayouts, damit Benutzer mit lokaler Tastaturzuordnung sich bei einem Ausfall erneut authentifizieren können.

Warnung:

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Bearbeiten Sie diesen Registrierungsschlüssel im VDA-Image:

`HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`

Das entsprechende Sprachpaket im Image des virtuellen Desktops muss installiert sein.

Eine Liste mit Tastatur-IDs für verschiedene Tastatursprachen finden Sie unter [Keyboard Identifiers and Input Method Editors for Windows](#).

Konfigurieren der Netzwerkkonnektivität des Ressourcenstandorts für Servicekontinuität

Sie können Ihren Ressourcenstandort so konfigurieren, dass er Verbindungen von außerhalb und/oder innerhalb Ihres LANs akzeptiert.

Konfigurieren von Verbindungen innerhalb Ihres LANs

1. Gehen Sie im Citrix Cloud-Menü zu **Workspacekonfiguration > Zugriff**.
2. Wählen Sie **Konnektivität konfigurieren**.
3. Wählen Sie **Nur interne** als Konnektivitätstyp.
4. Klicken Sie auf **Speichern**.

Konfigurieren Sie die Citrix Cloud Connector- und die VDA-Firewall so, dass sie Verbindungen über den TCP-Port 2598 des Common Gateway Protocol (CGP) akzeptieren. Diese Konfiguration ist die Standardeinstellung.

Konfigurieren von Verbindungen von außerhalb Ihres LANs

1. Gehen Sie im Citrix Cloud-Menü zu **Workspacekonfiguration > Zugriff**.
2. Wählen Sie **Konnektivität konfigurieren**.
3. Wählen Sie **Gateway Service** als Konnektivitätstyp.
4. Klicken Sie auf **Speichern**.

Konfigurieren von Verbindungen sowohl von außerhalb als auch innerhalb Ihres LANs

Führen Sie folgenden PowerShell-Befehl aus:

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocation
)-EnableHybridConnectivityForResourceLeases $true
```

Ersetzen Sie `YourResourceLocationExternalUid` durch die externe UID des Ressourcenstandorts.

Dieser Befehl ermöglicht bei Ausfällen direkte Verbindungen zum FQDN des Citrix Cloud Connector über TCP 2598. Wenn diese Verbindung fehlschlägt, wird Gateway Service als Fallback verwendet. Zur Verringerung der Latenz ermöglichen Sie internen Benutzern, das Gateway zu umgehen und sich direkt mit dem Ressourcenstandort zu verbinden.

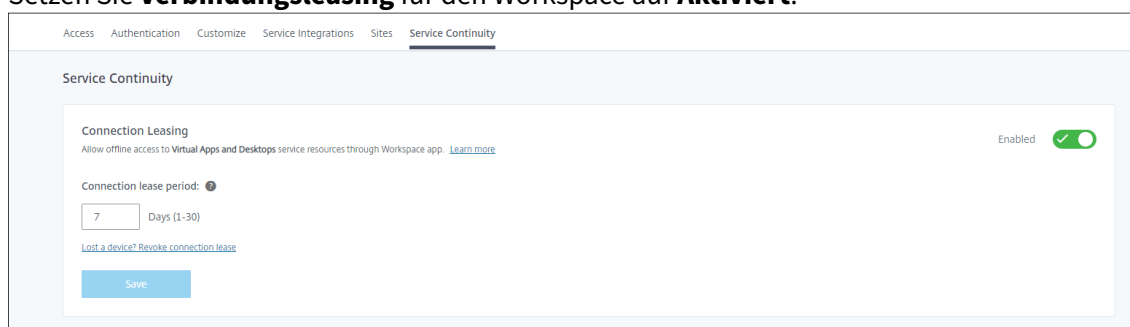
Hinweis:

Dieser PowerShell-Befehl ähnelt der direkten Workloadverbindung insofern, als er zur Optimierung der Workspace-Konnektivität internen Benutzern die Herstellung einer direkten Verbindung zu VDAs unter Umgehung des Gateways ermöglicht. Bei aktivierter Servicekontinuität ist die direkte Workloadverbindung bei Ausfällen nicht verfügbar.

Konfigurieren von Servicekontinuität

So aktivieren Sie das Servicekontinuität-Feature für Ihre Site:

1. Gehen Sie im Citrix Cloud-Menü zu **Workspacekonfiguration > Servicekontinuität**.
2. Setzen Sie **Verbindungsleasing** für den Workspace auf **Aktiviert**.



3. Legen Sie unter **Verbindungsleasingzeitraum** fest, wie viele Tage eine Verbindung mit einem Workspace-Verbindungslease aufrechterhalten werden kann. Der Workspace-Verbindungsleasingzeitraum gilt für alle Workspace-Verbindungsleases auf Ihrer Site. Der Workspace-Verbindungsleasingzeitraum beginnt mit der ersten Anmeldung eines Benutzers beim Citrix Cloud Workspace-Store. Workspace-Verbindungsleases werden mit jeder Anmeldung des Benutzers aktualisiert, bis zu einmal am Tag. Der Workspace-Verbindungsleasingzeitraum kann 1 bis 30 Tage lang sein. Der Standardwert beträgt sieben Tage.

4. Klicken Sie auf **Speichern**.

Wenn Sie die Servicekontinuität aktivieren, wird sie für alle Bereitstellungsgruppen Ihrer Site aktiviert. Verwenden Sie den folgenden PowerShell-Befehl, um die Servicekontinuität für eine Bereitstellungsgruppe zu deaktivieren:

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

Ersetzen Sie `deliverygroup` durch den Namen der Bereitstellungsgruppe.

Standardmäßig werden Workspace-Verbindungsleases von einem Benutzergerät gelöscht, wenn der Benutzer sich während eines Ausfalls von Citrix Workspace abmeldet. Um Workspace-Verbindungsleases auf Benutzergeräten nach dem Abmelden von Benutzern aufrechtzuerhalten, verwenden Sie folgenden PowerShell-Befehl:

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

Hinweis:

Workspace-Verbindungsleases können für Verbindungen per Citrix Workspace-App für Mac nicht so eingestellt werden, dass sie nach der Abmeldung auf Benutzergeräten verbleiben. Citrix Workspace für Mac kann den Wert der Eigenschaft `DeleteResourceLeaseOnLogOff` nicht lesen.

Funktionsweise von Servicekontinuität

Wenn kein Ausfall vorliegt, erfolgt der Benutzerzugriff auf virtuelle Apps und Desktops mit ICA-Dateien. Citrix Workspace generiert eine eindeutige ICA-Datei, sobald ein Benutzer das Symbol einer virtuellen App oder eines virtuellen Desktops auswählt. Jede ICA-Datei enthält ein STA-Ticket und ein Anmeldeticket, das jeweils nur einmal eingelöst werden kann, um autorisierten Zugriff auf virtuelle Ressourcen zu erhalten. Die Tickets in jeder ICA-Datei sind nur etwa 90 Sekunden gültig. Nachdem das Ticket in einer ICA-Datei verwendet wurde oder abläuft, benötigt der Benutzer eine andere ICA-Datei von Citrix Workspace, um auf Ressourcen zuzugreifen. Bei nicht aktivierter Servicekontinuität können Ausfälle den Benutzerzugriff auf Ressourcen verhindern, wenn Citrix Workspace keine ICA-Datei generieren kann.

Citrix Workspace generiert ICA-Dateien, wenn Benutzer virtuelle Apps und Desktops starten, unabhängig davon, ob Serviceaktivität aktiviert ist. Bei aktivierter Servicekontinuität generiert Citrix Workspace auch den eindeutigen Satz von Dateien, aus denen ein Workspace-Verbindungslease besteht. Im Gegensatz zu ICA-Dateien werden Workspace-Verbindungsleasedateien generiert, wenn der Benutzer sich bei Citrix Workspace anmeldet, nicht wenn der Benutzer die Ressource startet. Wenn ein Benutzer sich bei Citrix Workspace anmeldet, werden Verbindungsleasedateien für jede für diesen Benutzer veröffentlichte Ressource generiert. Workspace-Verbindungsleases enthalten Informationen,

die dem Benutzer Zugriff auf virtuelle Ressourcen ermöglichen. Wenn ein Benutzer aufgrund eines Ausfalls sich weder bei Citrix Workspace anmelden noch mit einer ICA-Datei auf Ressourcen zugreifen kann, gewährt das Verbindungslease autorisierten Zugriff auf die Ressource.

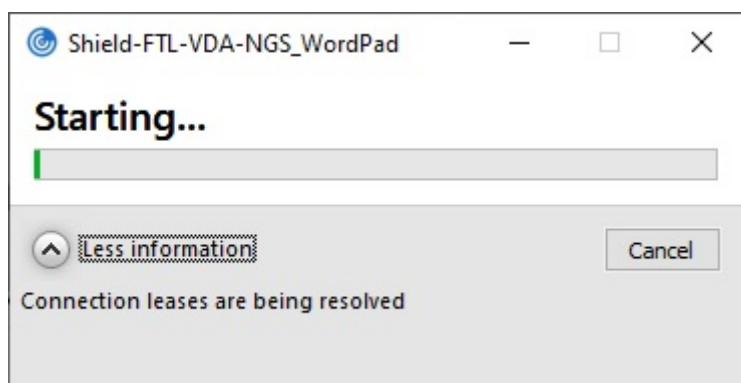
Start von Sitzungen bei Ausfällen

Wenn Benutzer während eines Ausfalls auf das Symbol einer App oder eines Desktops klicken, findet die Citrix Workspace-App die entsprechende Workspace-Verbindungslease auf dem Benutzergerät. Die Citrix Workspace-App öffnet dann eine Verbindung. Wenn die Konnektivität mit dem Ressourcenstandort, der die App oder den Desktop hostet, so konfiguriert ist, dass LAN-externe Verbindungen akzeptiert werden, wird eine Verbindung zu Citrix Gateway Service hergestellt. Wenn Sie die Konnektivität mit dem Ressourcenstandort, der die App oder den Desktop hostet, so konfigurieren, dass nur LAN-interne Verbindungen akzeptiert werden, wird eine Verbindung zum Cloud Connector hergestellt.

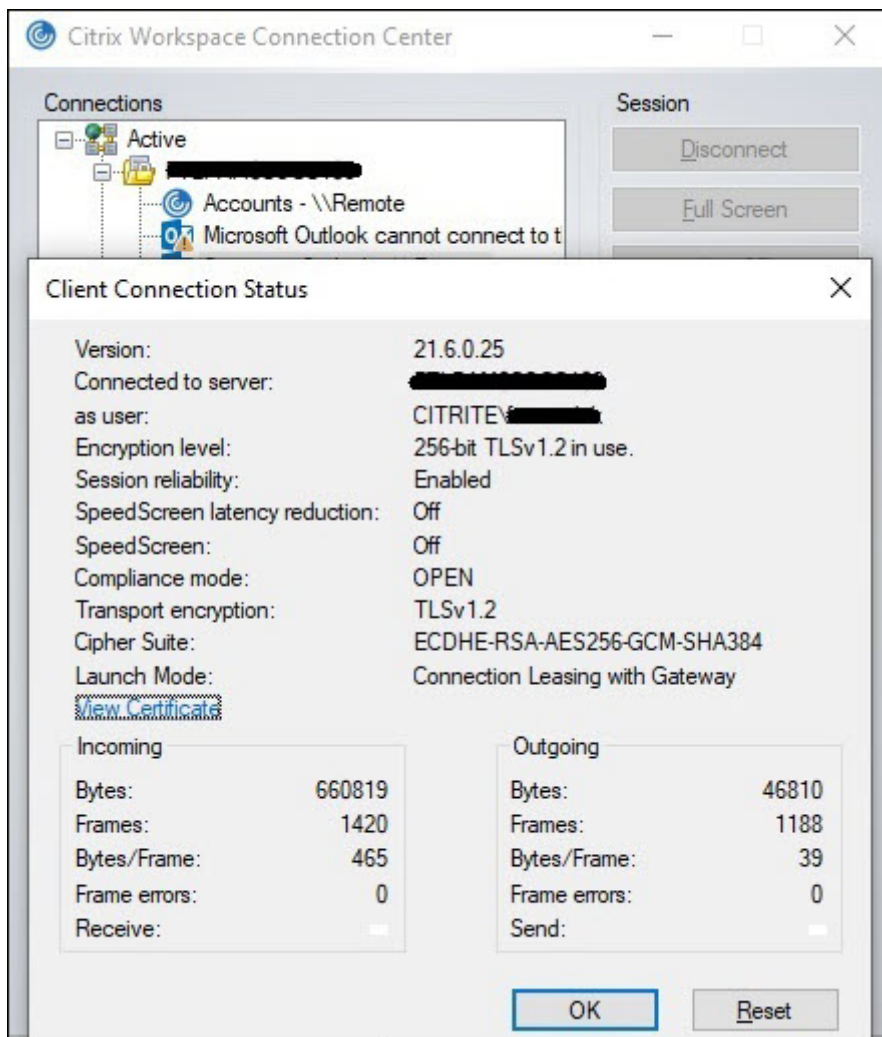
Wenn der Citrix Cloud-Broker online ist, verwendet der Cloud Connector den Citrix Cloud-Broker, um zu ermitteln, welcher VDA verfügbar ist. Ist der Citrix Cloud-Broker offline, prüft der sekundäre Broker für den Cloud Connector ("Hochverfügbarkeitsdienst") auf Verbindungsanfragen und verarbeitet sie.

Verbundene Benutzer können bei einem Ausfall ohne Unterbrechung weiterarbeiten. Bei Wiederverbindungen und neuen Verbindungen treten minimale Verbindungsverzögerungen auf. Diese Funktionalität ähnelt der des lokalen Hostcache, erfordert jedoch kein lokales StoreFront.

Wenn ein Benutzer eine Sitzung während eines Ausfalls startet, wird eine Meldung angezeigt, dass Workspace-Verbindungsleases für den Sitzungsstart verwendet wurden:

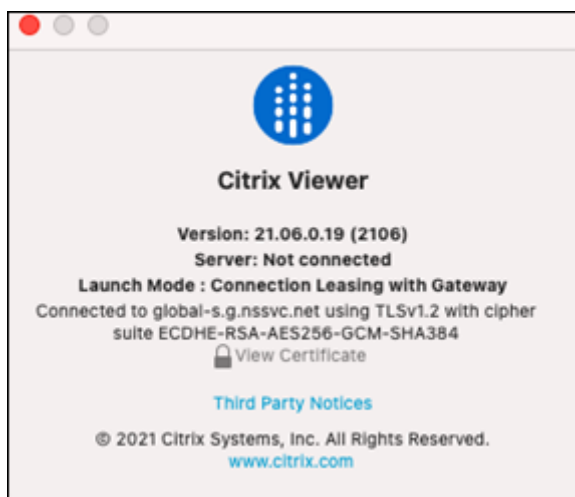


Wenn der Benutzer sich bei der Sitzung angemeldet hat, werden folgende Eigenschaften im Workspace Connection Center angezeigt:



Die Eigenschaft "Startmodus" enthält Informationen zu den Workspace-Verbindungsleases, die zum Starten der Sitzung verwendet wurden.

Auf Geräten mit der Citrix Workspace-App für Mac zeigt Citrix Viewer an, dass Workspace-Verbindungsleases für den Sitzungsstart verwendet wurden:



Sicherheitsgrundlagen

Alle vertraulichen Informationen in den Workspace-Verbindungsleasedateien werden mit AES-256 verschlüsselt. Workspace-Verbindungsleases sind an ein öffentliches/privates Schlüsselpaar gebunden, das eindeutig mit dem jeweiligen Clientgerät verknüpft ist und auf keinem anderen Gerät verwendet werden kann. Ein integrierter kryptografischer Mechanismus erzwingt die Verwendung des eindeutigen Schlüsselpaars auf jedem Gerät.

Workspace-Verbindungsleases werden auf dem Benutzergerät unter `AppData\Local\Citrix\SelfService\Connection` gespeichert.

Die Sicherheitsarchitektur von Servicekontinuität basiert auf Public-Key-Kryptographie, ähnlich einer Public Key-Infrastruktur (PKI), jedoch ohne Zertifikatsketten und Zertifizierungsstellen. Stattdessen vertrauen alle Komponenten in transitiver Vertrauensstellung einem neuen Citrix Cloud Service, der als "Root of Trust" bezeichnet wird und als Zertifizierungsstelle agiert.

Blockieren von Verbindungsleases

Wenn ein Benutzergerät verloren oder gestohlen wird oder ein Benutzerkonto geschlossen oder manipuliert wurde, können Sie Workspace-Verbindungsleases blockieren. Wenn Sie mit einem Benutzer verknüpfte Workspace-Verbindungslease blockieren kann der Benutzer keine Verbindung zu Ressourcen herstellen. Citrix Cloud generiert oder synchronisiert für den Benutzer keine Workspace-Verbindungsleases mehr.

Wenn Sie die einem Benutzerkonto zugeordneten Workspace-Verbindungsleases blockieren, blockieren Sie die Verbindung mit diesem Konto auf allen damit verknüpften Geräten. Sie können Workspace-Verbindungsleases für einen Benutzer oder für alle Benutzer in einer Benutzergruppe blockieren.

Verwenden Sie diesen PowerShell-Befehl, um Workspace-Verbindungsleases für einen einzelnen Benutzer oder eine Benutzergruppe zu widerrufen:

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays  
Days
```

Ersetzen Sie `username` durch den Benutzer, der mit dem Konto verknüpft ist, für das Sie Verbindungen blockieren möchten. Ersetzen Sie `username` durch eine Benutzergruppe, um die Verbindung von allen Konten in der Benutzergruppe zu blockieren. Ersetzen Sie `Days` durch die Anzahl an Tagen, die die Verbindungen gesperrt sind.

Um beispielsweise Verbindungen für `xd.local/user1` für die nächsten 7 Tage zu blockieren, geben Sie Folgendes ein:

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -  
LeaseRevocationDays 7
```

Mit dem folgenden PowerShell-Befehl können Sie den Zeitraum anzeigen, für den Workspace-Verbindungsleases widerrufen sind:

```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

Ersetzen Sie `username` durch den Benutzer oder die Benutzergruppe, für die Sie den Zeitraum anzeigen möchten.

Um beispielsweise den Zeitraum anzuzeigen, für den Workspace-Verbindungsleases für `xd.local/user1` widerrufen sind, geben Sie Folgendes ein:

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

Diese Informationen werden angezeigt:

```
1 FullName           :  
2 Name               : XD\user2  
3 UPN                :  
4 Sid                : S-1-5-21-nnnnnn  
5 LeaseRevocationDays : 2  
6 LeaseRevocationDateTimeInUtc : 2020-12-17T17:34:25Z  
7 LastUpdateDateTimeInUtc   : 2020-12-19T17:34:25Z
```

Anhand dieser Daten können Sie sehen, dass für Benutzer `xd.local/user2` Workspace-Verbindungsleases für zwei Tage widerrufen sind, vom 17. Dezember 2020 bis zum 19. Dezember 2020, jeweils um 17:34:25 UTC.

Um für ein Benutzerkonto mit widerrufenen Workspace-Verbindungsleases Verbindungen erneut zuzulassen, verwenden Sie folgenden PowerShell-Befehl:

```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

Ersetzen Sie `username` durch den blockierten Benutzer oder die blockierte Benutzergruppe, die

Verbindungen empfangen sollen. Um allen blockierten Benutzerkonten den Verbindungsempfang zu gestatten, lassen Sie die Option **Name** weg.

Double-Hop-Szenarios

Servicekontinuität kann Benutzern den Zugriff auf virtuelle Ressourcen während eines Ausfalls im Double-Hop-Szenario ermöglichen, wenn sie sich vor dem Ausfall bei Citrix Workspace angemeldet haben. In einem Double-Hop-Szenario stellt ein physisches Benutzergerät eine Verbindung zu einem virtuellen Desktop her, auf dem die Citrix Workspace-App installiert ist. Der virtuelle Desktop verbindet sich dann mit einer weiteren virtuellen Ressource.

Im Double-Hop-Szenario kann Servicekontinuität Benutzern unabhängig von der Art des virtuellen Desktops den Zugriff auf virtuelle Ressourcen während eines Ausfalls ermöglichen. Behält der virtuelle Desktop Benutzeränderungen bei, kann Servicekontinuität außerdem bei Ausfällen Zugriff auf virtuelle Ressourcen bieten, wenn ein Benutzer nicht angemeldet ist.

Servicekontinuität behandelt das physische Benutzergerät und das virtuelle Gerät in einem Double-Hop-Szenario als einzelne Clientendpunkte. Jedes Gerät hat eigene Workspace-Verbindungsleases. Wenn sich ein Benutzer auf einem physischen Gerät bei Citrix Workspace anmeldet, werden Workspace-Verbindungsleasedateien heruntergeladen und im Benutzerprofil auf dem physischen Gerät gespeichert. Der Benutzer greift dann auf einen virtuellen Desktop zu und meldet sich dort bei Citrix Workspace an. Es wird dann ein weiterer Satz Workspace-Verbindungsleases heruntergeladen und im Benutzerprofil auf dem virtuellen Desktop gespeichert. Workspace-Verbindungsleasedateien sind mit dem Gerät verknüpft, auf das sie heruntergeladen werden. Workspace-Verbindungsleasedateien können nicht auf ein anderes Gerät kopiert und wiederverwendet werden (auch nicht von demselben Benutzer). Daher kann Servicekontinuität bei Ausfällen nach Sitzungsende keinen Zugriff auf Ressourcen bieten, wenn der virtuelle Desktop während einer Benutzersitzung vorgenommene Änderungen nicht beibehält. Bei dieser Art von virtuellem Desktop gehören Workspace-Verbindungsleases zu den Änderungen, die verworfen werden.

Servicekontinuität funktioniert in Double-Hop-Szenarios bei den verschiedenen Typen unterstützter virtueller Desktops wie nachfolgend beschrieben.

Double-Hop-Umgebung	Servicekontinuität bietet Zugriff auf virtuelle Ressourcen
Gehostete gemeinsam genutzte Desktops	Wenn der Ausfall auftritt, während der Benutzer beim virtuellen Desktop angemeldet ist.
Zufällige, nicht beständige Desktops (gepoolte VDI-Desktops)	Wenn der Ausfall auftritt, während der Benutzer beim virtuellen Desktop angemeldet ist.

Double-Hop-Umgebung	Servicekontinuität bietet Zugriff auf virtuelle Ressourcen
Statische, nicht beständige Desktops	Wenn der virtuelle Desktop seit der letzten Anmeldung des Benutzers nicht neu gestartet wurde
Statisch beständige Desktops	Jederzeit bei einem Ausfall

Verwaltung von VDAs bei Ausfällen

Servicekontinuität verwendet die Funktion [Lokaler Hostcache](#) innerhalb des Citrix Cloud Connector. Der lokale Hostcache ermöglicht das fortgesetzte Verbindungsbrokering in einer Site, wenn die Verbindung zwischen dem Cloud Delivery Controller und dem Cloud Connector getrennt wird. Da Servicekontinuität den lokalen Hostcache verwendet, gelten für das Feature zum Teil dieselben Einschränkungen wie für den lokalen Hostcache.

Hinweis:

Obwohl Servicekontinuität den lokalen Hostcache innerhalb des Cloud Connector verwendet, wird das Feature anders als der lokale Hostcache nicht mit on-premises StoreFront unterstützt.

Energieverwaltung von VDAs bei Ausfällen

Wenn die Verbindung von Cloud Connectors zu Citrix Cloud getrennt wird, können die Connectors keine Hypervisor-Anmeldeinformationen von Citrix Cloud empfangen. Das bedeutet:

- Während eines Ausfalls befinden sich alle Maschinen im unbekanntem Energiezustand und es können keine Energieverwaltungsvorgänge ausgeführt werden. Auf dem Host eingeschaltete VMs können jedoch für Verbindungsanfragen verwendet werden.

Standardmäßig sind energieverwaltungste Desktop-VDAs in gepoolten Bereitstellungsgruppen, für die die Eigenschaft **ShutdownDesktopsAfterUse** aktiviert ist, bei einem Ausfall nicht für neue Verbindungen verfügbar, wenn die Verbindung zwischen Cloud Connectors und Citrix Cloud getrennt wird. Sie können [diese Einstellung ändern](#), sodass die Desktops bei einer Verbindungsunterbrechung zwischen Cloud Connectors und Citrix Cloud verwendet werden können, indem Sie das Flag [ReuseMachinesWithoutShutdownInOutage](#) für die Bereitstellungsgruppen konfigurieren. Das Ändern des Parameters [ReuseMachinesWithoutShutdownInOutage](#) auf “\$true” kann dazu führen, dass Daten aus früheren Benutzersitzungen auf dem VDA verbleiben, bis dieser neu gestartet wird.

Die Energieverwaltung wird fortgesetzt, sobald der Normalbetrieb nach einem Ausfall wieder aufgenommen wird.

Maschinenzuweisung und automatische Registrierung

Zugewiesene Maschinen können nur verwendet werden, wenn die Zuweisung während des normalen Betriebs erfolgte. Neue Zuweisungen sind bei einem Ausfall nicht möglich.

Die automatische Registrierung und Konfiguration von Remote-PC-Zugriff-Maschinen ist nicht möglich. Im normalen Betrieb registrierte und konfigurierte Maschinen können dagegen verwendet werden.

VDA-Ressourcen in verschiedenen Zonen

Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt, wenn die Ressourcen in verschiedenen Zonen sind.

Im Gegensatz zum lokalen Hostcache kann das Servicekontinuität-Feature Apps und Desktops von registrierten VDAs in verschiedenen Zonen starten, sofern die Ressource in mehr als einer Zone veröffentlicht ist. Die Citrix Workspace-App benötigt möglicherweise länger, um eine betriebsbereite Zone zu finden, da sie sequenziell alle Zonen im Workspace-Verbindungslease durchläuft.

Überwachung und Fehlersuche

Servicekontinuität führt primär zwei Aktionen aus:

- Download von Workspace-Verbindungsleases auf das Benutzergerät. Workspace-Verbindungsleases werden generiert und mit der Citrix Workspace-App synchronisiert.
- Virtuelle Desktops und Apps über Workspace-Verbindungsleases starten.

Problembehandlung beim Download von Workspace-Verbindungsleases

Sie können Workspace-Verbindungsleases an diesem Speicherort auf dem Benutzergerät anzeigen.

Windows-Geräte:

```
C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\  
Store GUID\User GUID\leases
```

Username ist der Benutzername.

Store GUID ist der global eindeutige Bezeichner des Workspace-Stores.

User GUID ist der global eindeutige Bezeichner des Benutzers.

Mac-Geräte:

`$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot`

Öffnen Sie zum Beispiel `/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot`.

Unter Linux:

`$HOME/.ICAClient/cache/ConnectionLease`

Öffnen Sie zum Beispiel `/home/user1/.ICAClient/cache/ConnectionLease`.

Workspace-Verbindungsleases werden generiert, wenn die Citrix Workspace-App sich mit dem Workspace-Store verbindet. Zeigen Sie Registrierungsschlüsselwerte auf dem Benutzergerät an, um festzustellen, ob die Citrix Workspace-App den Workspace-Verbindungsleasingdienst in Citrix Cloud erfolgreich kontaktiert hat.

Öffnen Sie `regedit` auf dem Benutzergerät und zeigen Sie diesen Schlüssel an:

`HKCU\Software\Citrix\Dazzle\Sites\store-xxxx`

Wenn diese Werte im Registrierungsschlüssel angezeigt werden, hat die Citrix Workspace-App den Workspace-Verbindungsleasingdienst kontaktiert oder versucht, ihn zu kontaktieren:

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

Wenn die Citrix Workspace-App erfolglos versucht hat, den Workspace-Verbindungsleasingdienst zu kontaktieren, zeigt `leaseLastCallHomeTime` einen Fehler mit ungültigem Zeitstempel an:

`leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM`

Wenn `leaseLastCallHomeTime` nicht initialisiert ist, hat die Citrix Workspace-App nie versucht, den Workspace-Verbindungsleasingdienst zu kontaktieren. Um dieses Problem zu beheben, entfernen Sie das Konto aus der Citrix Workspace-App und fügen Sie es erneut hinzu.

Fehlercodes der Citrix Workspace-App für Workspace-Verbindungsleases

Bei einem Servicekontinuitätsfehler auf dem Benutzergerät wird in der Fehlermeldung ein Fehlercode angezeigt. Dies sind häufige Fehler:

Fehlercode	Beschreibung
3000	Keine Verbindungsleasedateien vorhanden
3002	Verbindungslease kann nicht gelesen oder gefunden werden
3003	Kein Ressourcenstandort gefunden

Fehlercode	Beschreibung
3004	Keine Verbindungsdetails in Leases vorhanden
3005	ICA-Datei ist leer
3006	Verbindungslease ist abgelaufen. Melden Sie sich erneut bei Workspace an.
3007	Verbindungslease ist ungültig
3008	Ergebnis der Verbindungsleasevalidierung: leer
3009	Ergebnis der Verbindungsleasevalidierung: ungültig
3010	Parameter fehlt
3020	Verbindungsleasevalidierung fehlgeschlagen
3021	Kein Ressourcenstandort gefunden, wo die App veröffentlicht ist
3022	Ergebnis der Verbindungsleasevalidierung: verweigert
3023	Timeout der Citrix Workspace-App
3024	Benutzer hat den leasebasierten Start während der Ausführung abgebrochen
3025	Anzahl der Startwiederholungsversuche überschritten
3026	Ausgehandelte Ressource (App oder Desktop) kann nicht gestartet werden

Zugriff auf `selfservice.txt`

Gehen Sie wie folgt vor, um auf die Datei `selfservice.txt` zur Problembehandlung in Eigenregie zuzugreifen:

1. Erstellen Sie eine leere Textdatei und benennen Sie sie `enableshieldandlogging.reg`.
2. Kopieren Sie den folgenden Text in die Datei und speichern Sie sie:

```
Windows Registrierungs-Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle]
```

```
“Tracing”=”True”
```

```
“AuxTracing”=”True”
```

```
“DefaultTracingConfiguration”=”global all -detail”
```

```
“ConnectionLeasingEnabled”=”True”
```

```
[HKEY_CURRENT_USER\Software\Citrix\Dazzle]
```

```
“RemoteDebuggingPort”=”8088”
```

3. Speichern Sie Ihre gespeicherte Datei auf dem Client-Endpunkt.
4. Die Datei `selfservice.txt` ist jetzt im Pfad `%LocalAppData%\Citrix\SelfService` auffindbar.

Servicekontinuität im Browser

Erweiterungen für Google Chrome und Microsoft Edge bieten Servicekontinuität für Benutzer, die über diese Browser auf ihre Apps und Desktops zugreifen. Die Erweiterungen heißen Citrix Workspace Web und sind im [Chrome Web Store](#) bzw. auf der [Microsoft Edge Add-On-Website](#) verfügbar.

Diese Browsererweiterungen erfordern eine native Citrix Workspace-App auf dem Benutzergerät, um die Servicekontinuität zu unterstützen. Folgende Versionen werden unterstützt:

- Citrix Workspace-App 2109 für Windows (Mindestversion). Unterstützt von Google Chrome und Microsoft Edge.
- Citrix Workspace-App für Mac 2112 (Mindestversion). Unterstützt von Google Chrome.
- Mindestens Citrix Workspace-App für Mac Version 2206 zur Verwendung mit dem Safari-Browser.

Die Citrix Workspace-App für Windows (Store) wird nicht unterstützt.

Die native Workspace-App kommuniziert mit der Citrix Workspace Web-Erweiterung unter Verwendung des nativen Messaging-Hostprotokolls für Browsererweiterungen. Die native Workspace-App und die Workspace Web-Erweiterung verwenden gemeinsam Workspace-Verbindungsleases, um bei Ausfällen den Zugriff auf Apps und Desktops über einen Browser zu ermöglichen.

Dieses Video zeigt, wie die Servicekontinuität im Browser installiert und verwendet wird.

[Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen](#)

Benutzergeräteeinrichtung für Browserbenutzer

Um das Servicekontinuität-Feature in einem Browser zu verwenden, müssen Benutzer die folgenden Schritte auf ihren Geräten ausführen:

1. Laden Sie eine für Browser unterstützte Version der Citrix Workspace-App herunter und installieren Sie sie.

2. Laden Sie außerdem die Citrix Workspace Web-Erweiterung für Chrome oder Edge herunter und installieren Sie sie.

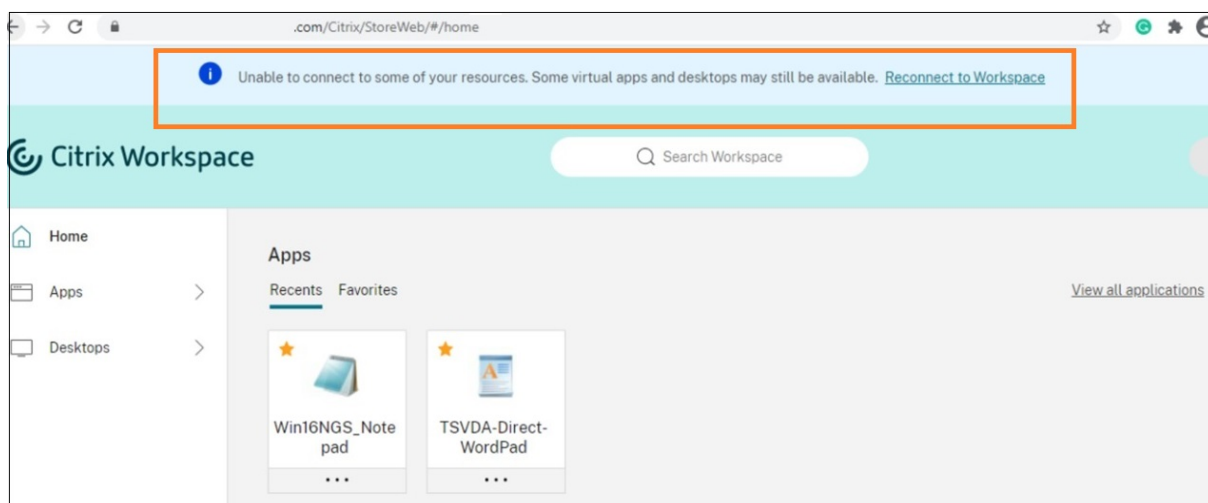
Browser-Benutzererfahrung

Wenn Benutzer auf ihre Apps oder Desktops klicken, werden diese sofort geöffnet, ohne dass Benutzer zuvor **Citrix Workspace Launcher** öffnen müssen.

Browser-Benutzererfahrung bei Ausfall

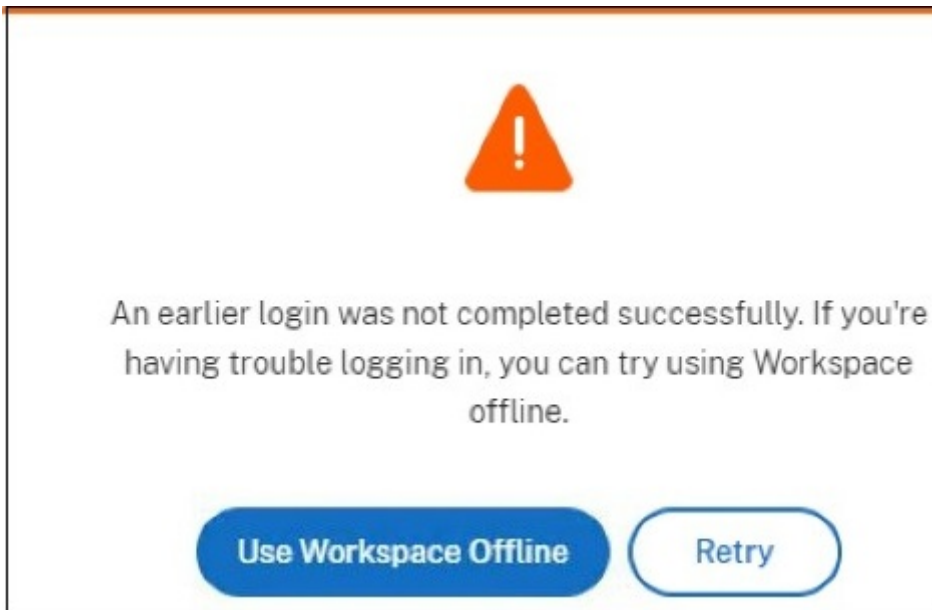
Benutzer können bei Ausfällen per Browser auf Apps und Desktops zugreifen, sofern eine Netzwerkverbindung zwischen Benutzergerät und einem Ressourcenstandort besteht.

Wenn ein Ausfall auftritt, während der Benutzer über einen Browser bei Workspace angemeldet ist, wird diese Meldung oben im Browserfenster angezeigt:



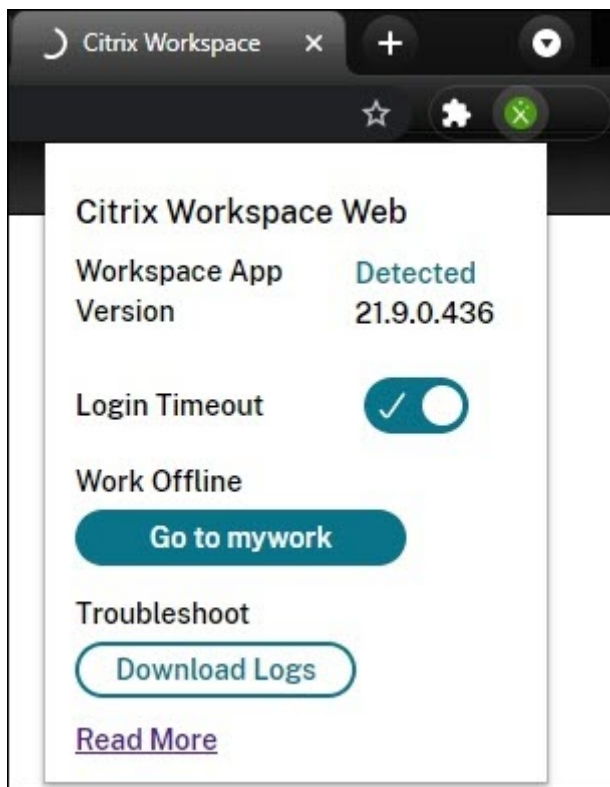
Benutzer können auf Apps und Desktops zugreifen, die offline verfügbar sind, indem sie auf ein beliebiges Symbol klicken, das nicht abgeblendet ist. Benutzer können auch versuchen, die Verbindung wiederherzustellen, indem sie auf **Verbindung mit Workspace wiederherstellen** klicken.

Wenn Benutzer sich bei einem Ausfall nicht über einen Browser bei Workspace anmelden können, werden sie aufgefordert, offline weiterzuarbeiten oder sich neu anzumelden. Um auf verfügbare Apps und Desktops offline zuzugreifen, klicken Benutzer auf **Workspace offline verwenden**.



Wenn Benutzer sich bei einem Ausfall nicht bei Workspace anmelden können, nachdem sie die Workspace-URL aufrufen, wird das Fenster nach einem festgelegten Timeoutintervall angezeigt. Standardmäßig wird das Fenster 30 Sekunden nach dem Aufrufen der Workspace-URL angezeigt. Sie können diesen Wert auf 15, 30, 45 oder 60 Sekunden festlegen. Sie können das Anmeldetimeout auch deaktivieren. Bei deaktiviertem Anmeldetimeout werden Benutzer beim Aufrufen der Workspace-URL aufgefordert, offline zu arbeiten.

Um das Anmeldetimeout zu konfigurieren, klicken Sie auf dem Benutzergerät auf das Erweiterungssymbol im Browser. Aktivieren oder deaktivieren Sie im angezeigten Fenster das Anmeldetimeout und legen Sie die Timeoutdauer fest:



Benutzer können sich bei einem Ausfall möglicherweise nicht anmelden, wenn der Browser an die Authentifizierungsseite eines externen Identitätsanbieters umgeleitet wurde. In diesem Fall kann der Benutzer die Workspace-URL in den Browser eingeben und wird dann aufgefordert, offline zu arbeiten. Der Benutzer muss nicht das Intervall des Anmeldetimeouts abwarten, bis das entsprechende Fenster angezeigt wird.

Benutzer können auf diese Weise auch während eines Ausfalls auf verfügbare Apps und Desktops zugreifen:

1. Klicken Sie im Browser auf das Erweiterungssymbol.
2. Klicken Sie im angezeigten Fenster auf die Schaltfläche unter **Offline arbeiten**. Auf der Schaltfläche steht **Gehe zu** und der Name des Workspace-Stores.
3. Klicken Sie im angezeigten Fenster auf **Workspace offline verwenden**.

Bei einigen Ausfällen wird bei erkannten Workspace-Problemen automatisch das Fenster angezeigt, in dem Benutzer zur Offlinearbeit aufgefordert werden. Der Benutzer muss keine Aktion ausführen und nicht das Intervall für das Anmeldetimeout abwarten.

Browser-Einschränkungen

Wenn Benutzer während eines Ausfalls Cookies und andere Sitedaten im Browser löschen, funktioniert die Servicekontinuität erst, wenn Benutzer sich erneut bei Workspace authentifizieren.

Der Benutzer muss die Ausführung im Incognito-Modus für die Erweiterung aktivieren, damit die Servicekontinuität in diesem Modus unterstützt wird.

Fehlerbehebung an Browsern

Stellen Sie sicher, dass im Menü **Erweitert** der Kontoeinstellungen der Citrix Workspace Browser-App die Einstellung “Startpräferenz für Apps und Desktops” auf **Citrix Workspace App verwenden** festgelegt ist. Wenn diese Option auf **Webbrowser verwenden** eingestellt ist, wird die Servicekontinuität im Browser nicht unterstützt.

Vergewissern Sie sich, dass das Erweiterungssymbol im Browser grün angezeigt wird, nachdem der Browser die Workspace-URL geladen hat.

Um Protokolle herunterzuladen, klicken Sie im Browser auf das Erweiterungssymbol. Klicken Sie dann auf **Protokolle herunterladen**.

Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS)

October 12, 2023

Der Citrix Verbundauthentifizierungsdienst (FAS) unterstützt Single Sign-On (SSO) für DaaS in Citrix Workspace. FAS wird normalerweise verwendet, wenn Sie einen der folgenden Identitätsanbieter für die Authentifizierung in Citrix Workspace verwenden:

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

Mit FAS geben Abonnenten ihre Anmeldeinformationen nur einmal ein, um auf ihre DaaS-Apps und -Desktops zuzugreifen.

Wenn Sie Active Directory (AD), AD plus Token oder bestimmte Konfigurationen von Citrix Gateway verwenden, ist FAS für Single Sign-On (SSO) bei DaaS nicht erforderlich. Weitere Informationen zum Konfigurieren von Citrix Gateway finden Sie unter [Create an OAuth IdP policy on the on-premises Citrix Gateway](#).

FAS-Server

Sie können an jedem Ressourcenstandort mehrere FAS-Server mit Citrix Cloud verbinden, um Lastausgleich und Failover zu ermöglichen.

Citrix Cloud unterstützt die Verwendung von FAS-Servern in den folgenden Szenarios:

In beiden Szenarios geben Abonnenten, die sich über einen Verbundidentitätsanbieter bei ihrem Workspace anmelden, ihre Anmeldeinformationen nur einmal ein, um auf Apps und Desktops zuzugreifen.

FAS-Server mit Verbindung zu einem einzelnen Ressourcenstandort

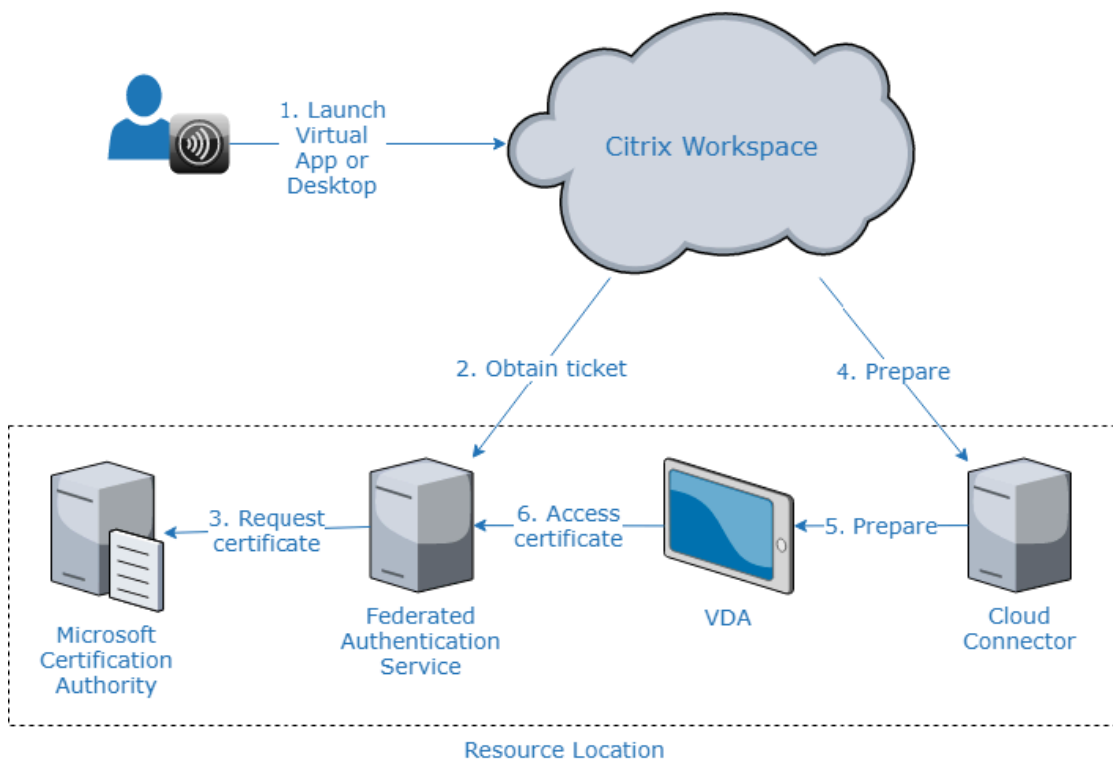
Wenn Ihre Ressourcenstandorte eine hybride Infrastruktur enthalten (z. B. unterschiedliche Active Directory-Gesamtstrukturen), stellen Sie FAS-Server am Ressourcenstandort mit den VDAs bereit. Single Sign-On ist nur an Ressourcenstandorten mit mindestens einem verbundenen FAS-Server aktiv.

FAS-Server mit Verbindung zu mehreren Ressourcenstandorten

Wenn zwischen den Ressourcenstandorten eine Netzwerkverbindung besteht und die Standorte eine ähnliche Infrastruktur aufweisen, können Sie die FAS-Server mit mehreren Ressourcenstandorten verbinden. Single Sign-On ist für Workspace-Abonnenten aktiv, die sich mit Apps und Desktops an diesen Ressourcenstandorten verbinden. Es müssen dann keine separaten FAS-Server mit jedem Ressourcenstandort verbunden werden.

Wenn Abonnenten eine virtuelle App oder einen Desktop starten, wählt Citrix Cloud einen FAS-Server aus, der sich am gleichen Ressourcenstandort wie die/der gestartete App oder Desktop befindet. Citrix Cloud kontaktiert den ausgewählten FAS-Server, um ein Ticket zu erhalten, das Zugriff auf ein auf dem FAS-Server gespeichertes Benutzerzertifikat gewährt. Der VDA stellt eine Verbindung mit dem FAS-Server her und präsentiert das Ticket, um den Abonnenten zu authentifizieren.

Bei korrekter Regelkonfiguration können Sie denselben FAS-Server verwenden, um sich on-premises oder über Citrix Cloud anzumelden.



Failoverpriorität bei mehreren Ressourcenstandorten

Bei Verwendung von FAS-Servern mit mehreren Ressourcenstandorten können die Server an einem Ressourcenstandort ein Failover für diejenigen an anderen Ressourcenstandorten bieten. Wenn Sie FAS-Server zu anderen Ressourcenstandorten hinzufügen, weisen Sie jeden Server als primären oder sekundären Server aus. Wenn Abonnenten eine virtuelle App oder einen virtuellen Desktop starten, verwendet Citrix Cloud diese Ausweisung zur Auswahl des FAS-Servers wie folgt:

- FAS-Server, die an einem Ressourcenstandort als primär festgelegt sind, werden zuerst berücksichtigt.
- Wenn keine Primärserver verfügbar sind, fällt die Wahl auf sekundäre FAS-Server.
- Wenn keine sekundären Server verfügbar sind, wird der Start fortgesetzt, es erfolgt jedoch kein Single Sign-On.

Überblick im Video

Einen Überblick über den Verbundauthentifizierungsdienst für Citrix Workspace bietet folgendes Tech Insight-Video:



Anforderungen

Konnektivitätsanforderungen

Verwenden Sie die FAS-Verwaltungskonsole, um einen FAS-Server mit Citrix Cloud zu verbinden. Sie können diese Konsole zum Konfigurieren eines lokalen oder remote vorhandenen FAS-Servers verwenden. Zum Aktivieren von Single Sign-On für Workspaces mit FAS greifen die FAS-Verwaltungskonsole und der FAS-Dienst über das Konto des Konsolenbenutzers bzw. das Netzwerkdienstkonto auf die folgenden Adressen zu.

- FAS-Verwaltungskonsole, über das Konto des Konsolenbenutzers:
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - Adressen, die von einem externen Identitätsanbieter benötigt werden (sofern dieser in Ihrer Umgebung verwendet wird)
- FAS-Dienst, über das Netzwerkdienstkonto:
 - *.citrixworkspacesapi.net

- https://*.citrixnetworkapi.net/

Wenn Ihre Umgebung Proxyserver enthält, konfigurieren Sie den Benutzerproxy mit den Adressen für die FAS-Verwaltungskonsole. Stellen Sie außerdem sicher, dass die Adresse für das Netzwerkdienstkonto entsprechend Ihrer Umgebung konfiguriert ist.

FAS-Systemvoraussetzungen

Die in diesem Abschnitt aufgeführten Anforderungen gelten für alle FAS-Server, die Sie mit Citrix Cloud verbinden.

Die vollständigen Systemvoraussetzungen für den FAS-Server werden im Abschnitt [Systemanforderungen](#) der FAS-Produktdokumentation beschrieben.

Auf FAS-Servern in Ihrer On-Premises-Umgebung für Citrix Virtual Apps and Desktops muss der Verbundauthentifizierungsdienst 2003 (Version 10.1) oder höher installiert sein.

Wenn Ihr FAS-Server älter ist als Version 10, können Sie die aktuelle FAS-Software von Citrix herunterladen und den Server vor Ort aktualisieren, bevor Sie diese Verbindung herstellen. Beim Erstellen der Verbindung wählen Sie den Ressourcenstandort für Ihren FAS-Server. SSO ist für Abonnenten nur an Ressourcenstandorten mit FAS-Server aktiv.

Weitere Informationen zum Upgrade eines bestehenden FAS-Servers finden Sie unter [Installation und Konfiguration](#) in der FAS-Produktdokumentation. Für Workspace- und On-Premises-Bereitstellungen kann derselbe FAS-Server verwendet werden.

Citrix Workspace

Sie müssen Citrix DaaS in Workspace bereitgestellt und aktiviert haben. DaaS ist nach dem Abonnieren standardmäßig in der Workspacekonfiguration aktiviert. Sie müssen jedoch Citrix Cloud Connectors bereitstellen, damit Citrix Cloud mit Ihrer On-Premises-Umgebung kommunizieren kann.

Cloud Connectors

Citrix Cloud Connectors ermöglichen die Kommunikation zwischen Ihrem Ressourcenstandort (wo sich die VDAs befinden) und Citrix Cloud. Stellen Sie mindestens zwei Cloud Connectors bereit, um eine hohe Verfügbarkeit sicherzustellen. Die Server, auf denen Sie die Cloud Connector-Software installieren, müssen die folgenden Anforderungen erfüllen:

- Systemanforderungen (siehe [Technische Daten zu Citrix Cloud Connector](#))
- Es dürfen keine anderen Komponenten von Citrix installiert sein. Die Server dürfen keine Active Directory-Domänencontroller oder Maschinen sein, die für Ihre Ressourcenstandortinfrastruktur kritisch sind.

- Sie müssen mit der Domäne verbunden sein, in der sich die VDAs befinden.

Weitere Informationen zum Bereitstellen von Cloud Connectors finden Sie in den folgenden Artikeln:

- [Cloud Connector-Proxy und Firewall konfigurieren](#)
- [Cloud Connector-Installation](#)

Übersicht über die Einrichtung

1. Wenn Sie neue FAS-Server bereitstellen, lesen Sie die Hinweise unter Anforderungen und folgen Sie den Anweisungen unter Installieren und Konfigurieren von FAS in diesem Artikel.
2. Verbinden Sie Ihren FAS-Server mit Citrix Cloud (siehe Verbinden eines FAS-Servers mit Citrix Cloud). Bei diesem Verfahren wird der FAS-Server mit einem einzelnen Ressourcenstandort verbunden.
3. Wenn Sie Ihren FAS-Server mit mehreren Ressourcenstandorten verbinden möchten, folgen Sie den Anweisungen unter Hinzufügen eines FAS-Servers zu mehreren Ressourcenstandorten in diesem Artikel.

Installieren und Konfigurieren von FAS

Folgen Sie dem FAS-Installations- und Konfigurationsprozess in der [FAS-Produktdokumentation](#). Die Konfigurationsschritte für StoreFront und den Delivery Controller sind nicht erforderlich.

Tipp:

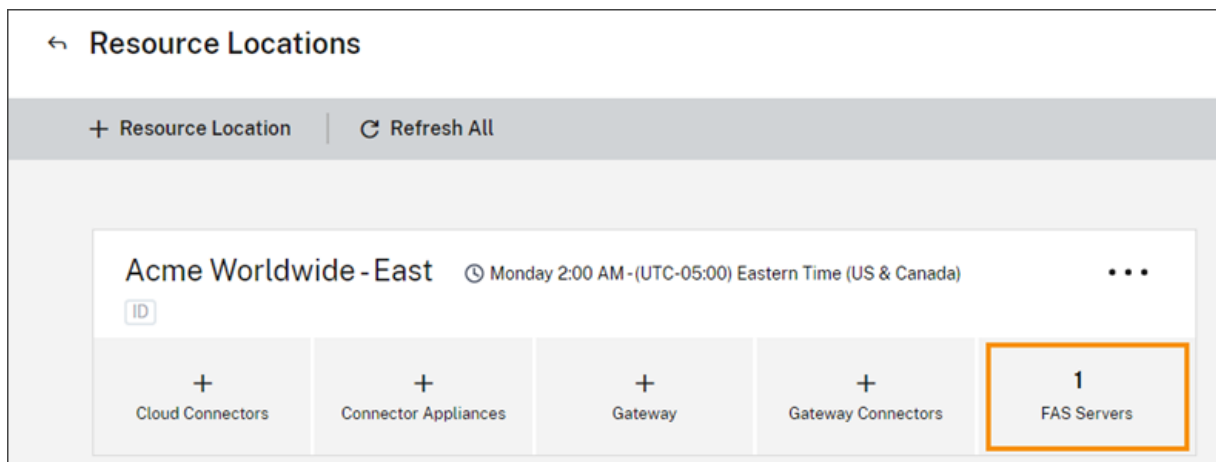
Sie können auch das Installationsprogramm für den Verbundauthentifizierungsdienst von der Citrix Cloud-Konsole herunterladen:

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Wählen Sie die Kachel **FAS-Server** und klicken Sie auf **Download**.

Verbinden von FAS-Servern mit Citrix Cloud

Verwenden Sie die FAS-Verwaltungskonsole zum Verbinden des FAS-Servers mit Citrix Cloud (siehe [Installation und Konfiguration](#) in der FAS-Produktdokumentation).

Nach Abschluss des Konfigurationsschritts **Mit Citrix Cloud verbinden** registriert Citrix Cloud den FAS-Server und zeigt ihn auf der Seite Ressourcenstandorte in Ihrem Citrix Cloud-Konto an.



Wenn Sie die Seite “Ressourcenstandorte” bereits im Browser geladen haben, müssen Sie die Seite aktualisieren, um den registrierten FAS-Server anzuzeigen.

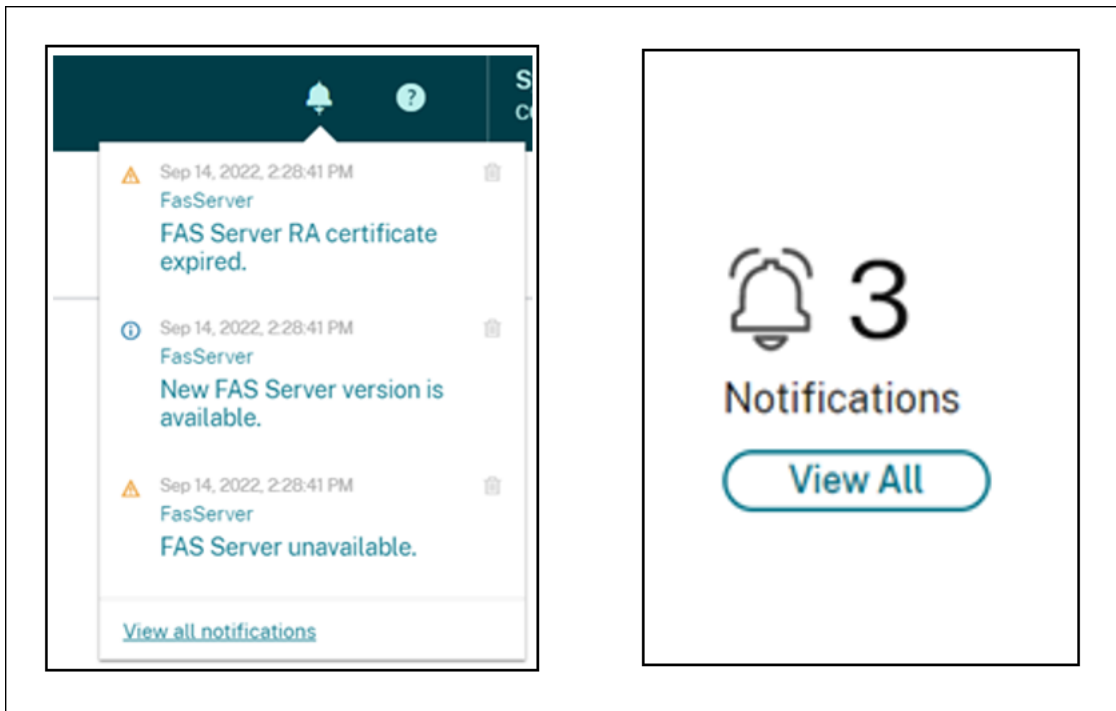
Unterstützung für Cloudbenachrichtigungen

FAS unterstützt jetzt Cloudbenachrichtigungen. Mit den neuen Cloudbenachrichtigungen für FAS-Server erhalten Sie Benachrichtigungen in den folgenden Situationen:

- Ein FAS-Server ist ausgefallen oder nicht verfügbar.
- Das Registrierungsstellenzertifikat eines FAS-Servers ist abgelaufen oder läuft bald ab.
- Eine neue Version des FAS steht zum Download zur Verfügung.

Benachrichtigungen

Die Citrix Cloud-Verwaltungskonsole prüft regelmäßig auf neue Benachrichtigungen. Die Benachrichtigungen werden unter dem Glockensymbol oben rechts in der Citrix Cloud-Verwaltungskonsole angezeigt. Wählen Sie auf dem Benachrichtigungssymbol **Alle anzeigen**, um alle Benachrichtigungen anzuzeigen. Weitere Informationen finden Sie unter [Benachrichtigungen](#).



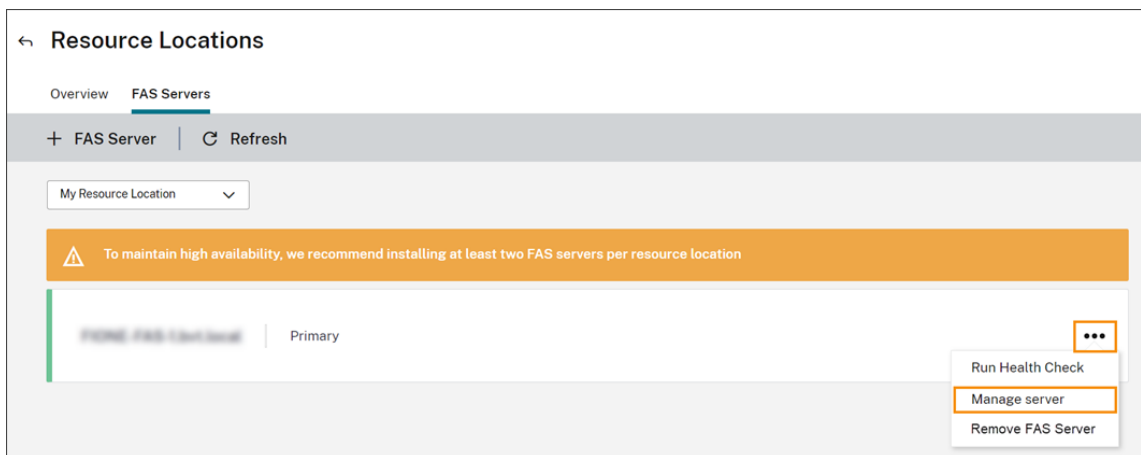
Hinweis:

Sobald eine Benachrichtigung ausgelöst wurde, wird sie von Zeit zu Zeit wieder ausgelöst, wenn das Problem nicht behoben ist.

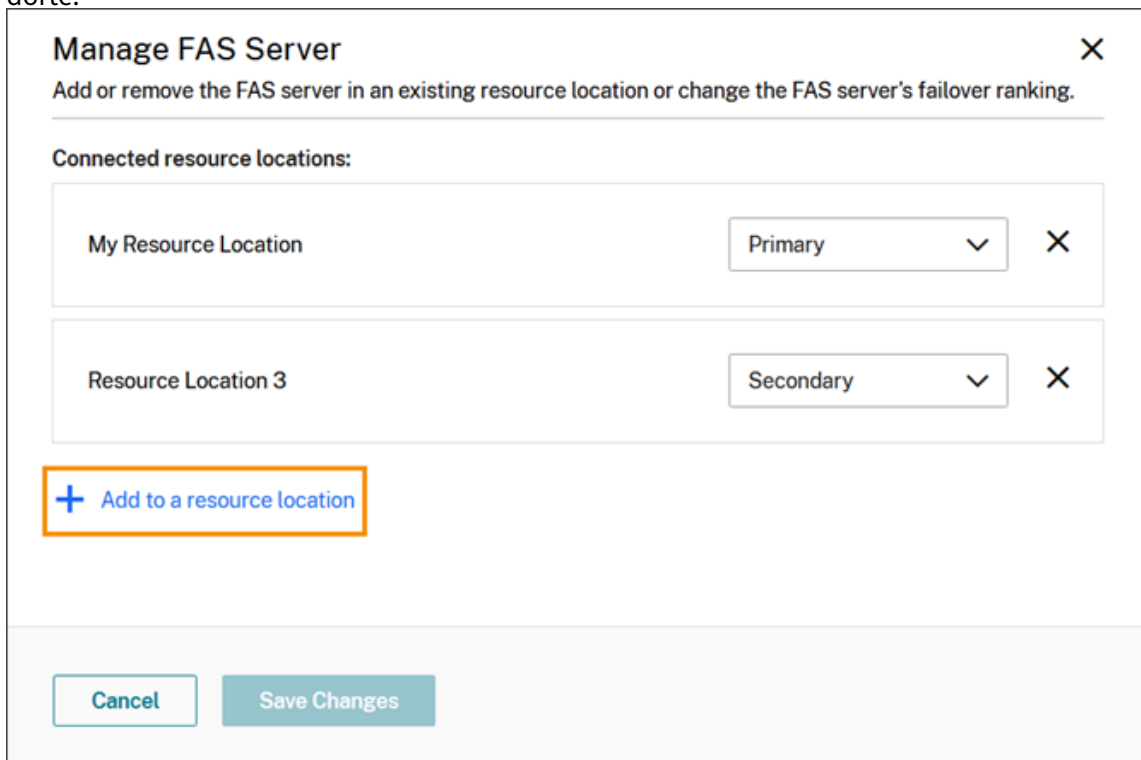
Alle Benachrichtigungen enthalten den FQDN des beeinträchtigten FAS-Servers. Die Benachrichtigung über den RA-Zertifikatablauf wird nur für FAS-Server mit Version 10.10.0.14 und höher angezeigt.

Hinzufügen eines FAS-Servers zu mehreren Ressourcenstandorten

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte** und dann die Registerkarte **FAS-Server**.
2. Suchen Sie den FAS-Server, den Sie verwalten möchten, klicken Sie rechts neben dem Eintrag auf die Auslassungspunkte und wählen Sie **Server verwalten**.



3. Wählen Sie **Zu Ressourcenstandort hinzufügen** und dann die gewünschten Ressourcenstandorte.



4. Wählen Sie **Primär** oder **Sekundär** für die Failoverpriorität des FAS-Servers an jedem ausgewählten Ressourcenstandort.
5. Wählen Sie **Änderungen speichern**.

Um den hinzugefügten FAS-Server anzuzeigen, wählen Sie im **Citrix Cloud**-Menü die Option **Ressourcenstandorte** und dann die Registerkarte **FAS-Server**. Eine Liste aller FAS-Server für alle verbundenen Ressourcenstandorte wird angezeigt. Um die FAS-Server eines bestimmten Ressourcenstandorts anzuzeigen, wählen Sie diesen aus der Dropdownliste aus.

Ändern der Failoverpriorität eines FAS-Servers

1. Wählen Sie auf der Seite **Ressourcenstandorte** die Kachel **FAS-Server** für den Ressourcenstandort, den Sie verwalten möchten.
2. Wählen Sie die Registerkarte **FAS-Server**.
3. Suchen Sie den FAS-Server, den Sie verwalten möchten, klicken Sie rechts neben dem Eintrag auf die Auslassungspunkte und wählen Sie **Server verwalten**.
4. Suchen Sie den Ressourcenstandort, für den Sie die Priorität ändern möchten, und wählen Sie die neue Priorität aus der Dropdownliste aus.

Manage FAS Server ✕

Add or remove the FAS server in an existing resource location or change the FAS server's failover ranking.

Connected resource locations:

My Resource Location	Primary ▼	✕
Resource Location 3	Secondary ▼	✕

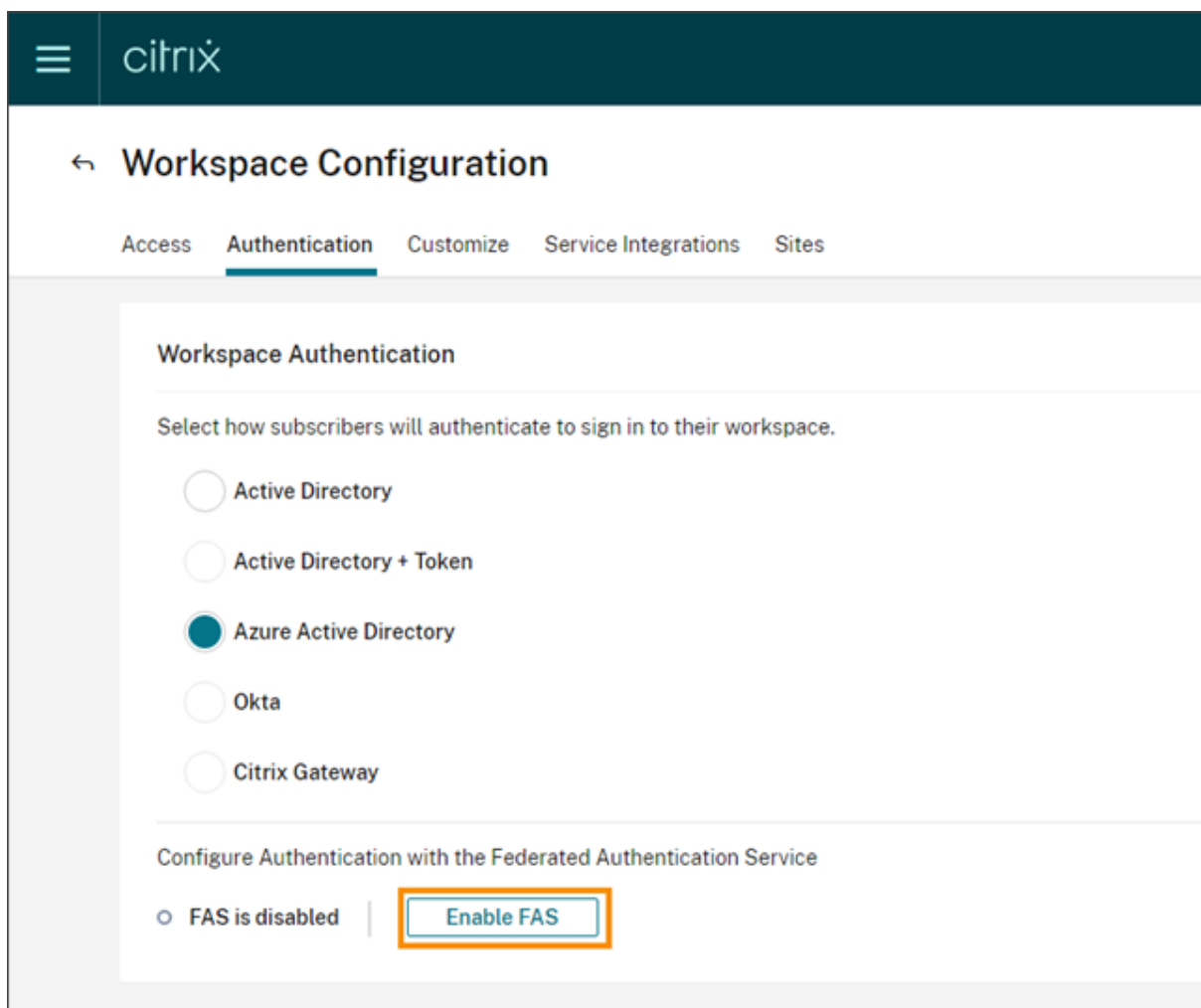
[+ Add to a resource location](#)

Cancel Save Changes

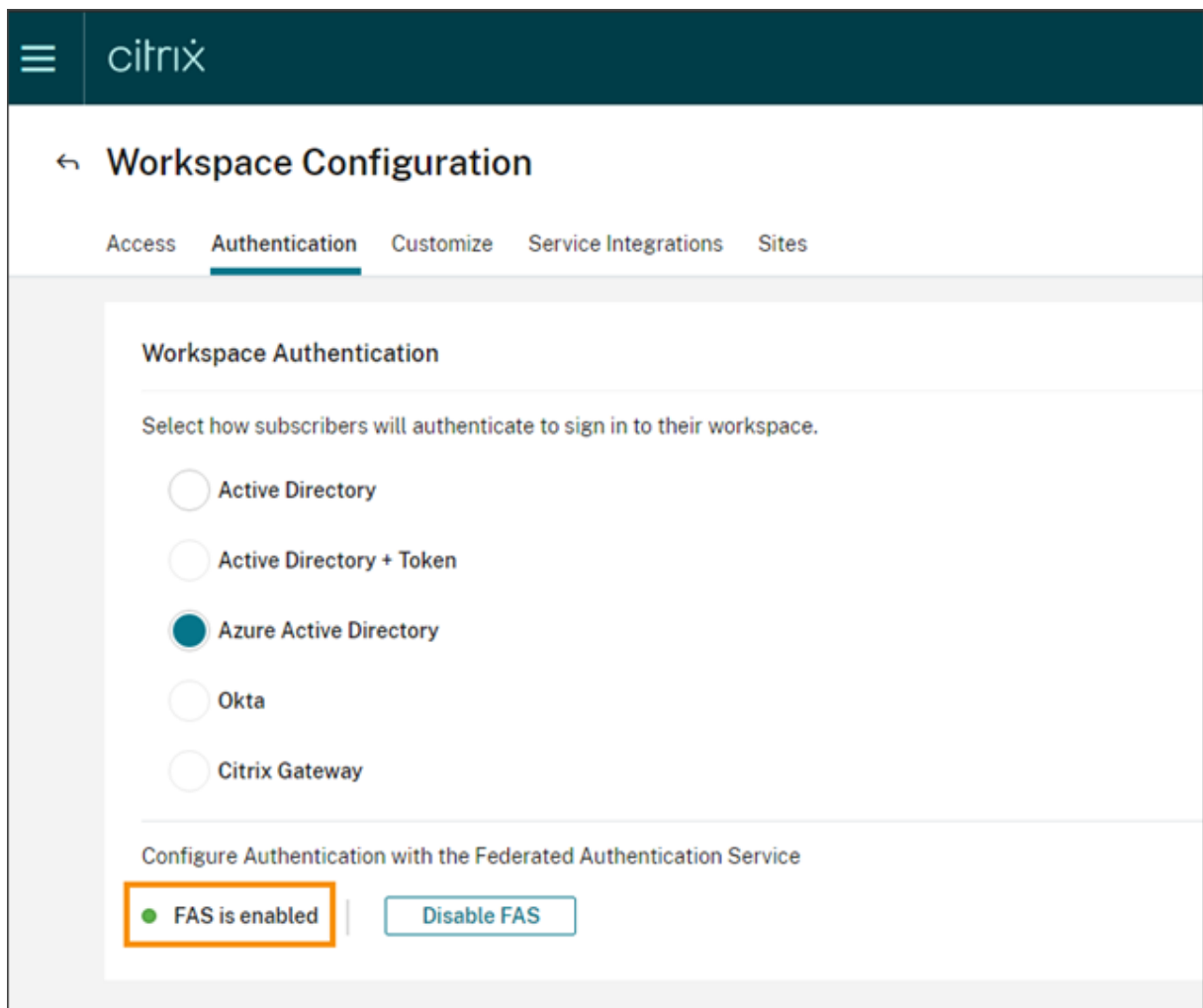
5. Wählen Sie **Änderungen speichern**.

Aktivieren der Verbundauthentifizierung für Workspaces

1. Wählen Sie im Citrix Cloud-Menü zunächst **Workspacekonfiguration** und dann **Authentifizierung**.
2. Klicken Sie auf **FAS aktivieren**. Es kann bis zu fünf Minuten dauern, bis die Änderung auf Teilnehmersitzungen angewendet wird.



Anschließend ist der Verbundauthentifizierungsdienst für alle Starts virtueller Apps und Desktops in Citrix Workspace aktiv.



Wenn sich Abonnenten bei ihrem Workspace anmelden und eine virtuelle App oder einen virtuellen Desktop am Ressourcenstandort des FAS-Servers starten, erfolgt der Start ohne Aufforderung zur Eingabe von Anmeldeinformationen.

Hinweis:

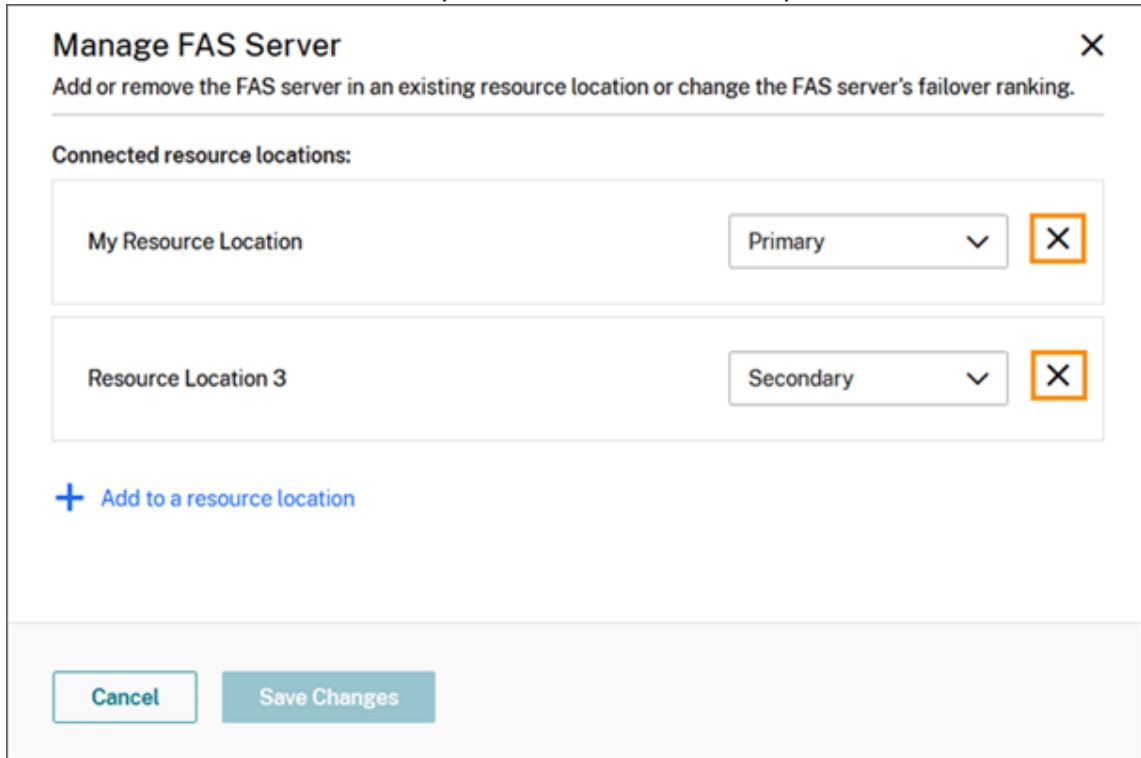
Wenn alle FAS-Server an einem Ressourcenstandort ausgefallen sind oder sich im Wartungsmodus befinden, wird die Anwendung erfolgreich gestartet, aber Single Sign-On ist nicht aktiv. Abonnenten müssen dann bei jedem Zugriff auf eine App oder einen Desktop ihre AD-Anmeldeinformationen eingeben.

Entfernen eines FAS-Servers

Entfernen eines FAS-Servers aus einem Ressourcenstandort:

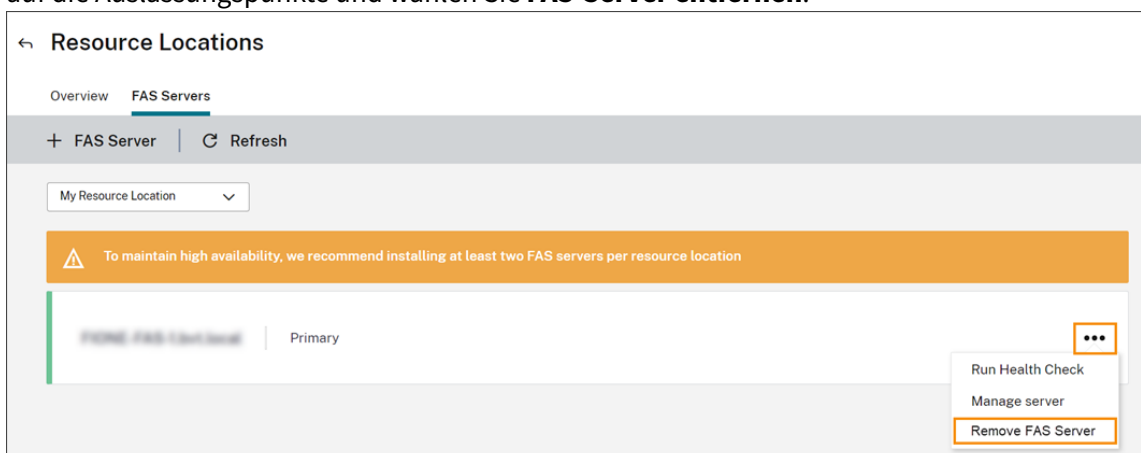
1. Wählen Sie auf der Seite **Ressourcenstandorte** die Kachel **FAS-Server** für den Ressourcenstandort, den Sie verwalten möchten.

2. Wählen Sie die Registerkarte **FAS-Server**.
3. Suchen Sie den FAS-Server, den Sie verwalten möchten, klicken Sie rechts neben dem Eintrag auf die Auslassungspunkte und wählen Sie **Server verwalten**.
4. Suchen Sie den Ressourcenstandort, den Sie entfernen möchten, und klicken Sie auf das **X**.

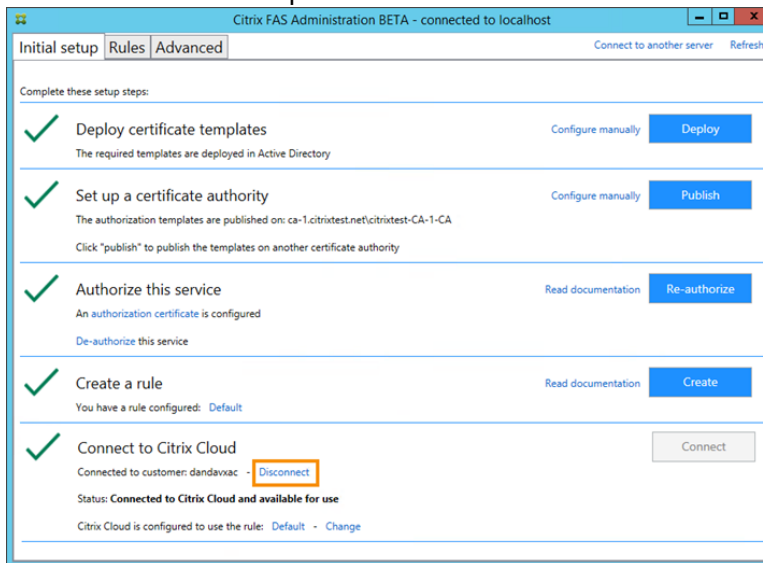


Entfernen eines FAS-Servers aus allen verbundenen Ressourcenstandorten:

1. Wählen Sie im Citrix Cloud-Menü die Option **Ressourcenstandorte**.
2. Suchen Sie den Ressourcenstandort, den Sie verwalten möchten, und wählen Sie die Kachel **FAS-Server**.
3. Suchen Sie den FAS-Server, den Sie entfernen möchten, klicken Sie rechts neben dem Eintrag auf die Auslassungspunkte und wählen Sie **FAS-Server entfernen**.

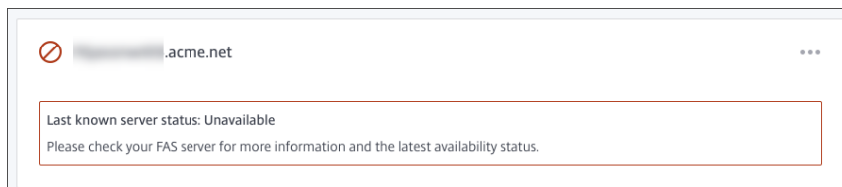


4. Wählen Sie in der FAS-Verwaltungskonsolle (auf Ihrem On-Premises-FAS-Server) unter **Mit Citrix Cloud verbinden** die Option **Trennen**. Alternativ können Sie FAS deinstallieren.

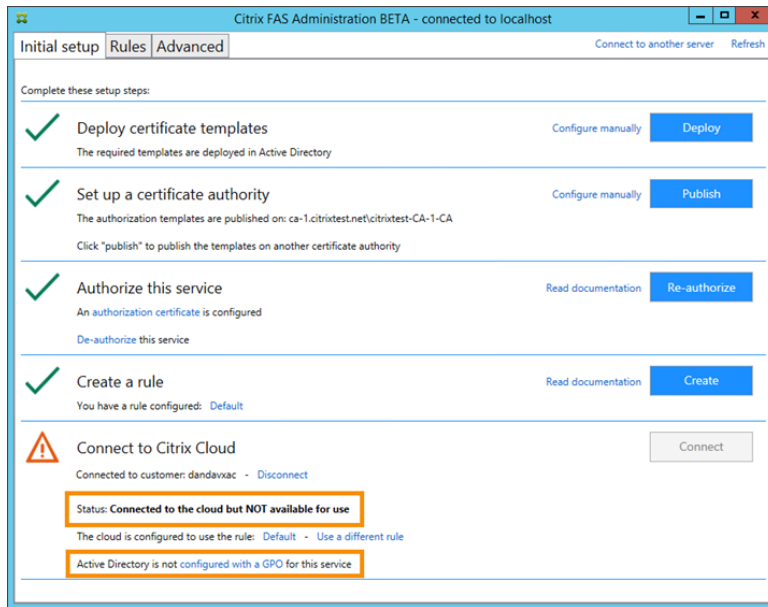


Problembehandlung

Wenn der FAS-Server nicht verfügbar ist, wird auf der Seite "FAS-Server" eine Warnmeldung angezeigt.



Um das Problem zu untersuchen, öffnen Sie die FAS-Verwaltungskonsolle auf Ihrem On-Premises-FAS-Server und überprüfen Sie den Status. Beispiel, wenn der FAS-Server nicht im FAS-Server-Gruppenrichtlinienobjekt vorhanden ist:



Wenn in der FAS-Verwaltungskonsolle angezeigt wird, dass der Server ordnungsgemäß funktioniert, es aber dennoch VDA-Anmeldeprobleme gibt, konsultieren Sie die [Anleitung zur FAS-Problembehandlung](#).

Weitere Informationen

[Konfigurieren von Single Sign-On für die Workspace-App](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).