Citrix Secure Private Access

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Was ist neu

June 19, 2024

11. Juni 2024

- **Tool zur Politikmodellierung**

  Das Tool zur Richtlinienmodellierung (**Zugriffsrichtlinien > Richtlinienmodellierung**) hilft Administratoren dabei, Konfigurationsprobleme von der Admin-Konsole aus zu analysieren und zu beheben. Einzelheiten finden Sie unter Tool zur Richtlinienmodellierung.

- **Unterstützung für Filter im Diagramm mit den Diagnoseprotokollen**

  Mithilfe der Filteroption im Diagramm mit den **Diagnoseprotokollen** können Administratoren die Suche anhand der verschiedenen Kriterien wie App-Typ, Kategorie und Beschreibung verfeinern, um die Protokollanalyse und Problembehandlung zu vereinfachen. Einzelheiten finden Sie unter Diagnoseprotokolle.

13. März 2024

- **Unterstützung für das Beenden aktiver Benutzersitzungen und das Hinzufügen von Benutzern zur Liste der deaktivierten Benutzer**

  Administratoren können jetzt alle aktiven Endbenutzersitzungen sofort beenden und die Benutzer zur Liste der deaktivierten Benutzer hinzufügen. Das Hinzufügen eines Benutzers zu dieser Liste deaktivierter Benutzer beendet alle aktiven Secure Private Access-Anwendungssitzungen und blockiert den zukünftigen Anwendungszugriff. Einzelheiten finden Sie unter Beenden aktiver Benutzersitzungen und Hinzufügen von Benutzern zur Liste der deaktivierten Benutzer.

12. Februar 2024

- **Allgemeine Verfügbarkeit des Browsers und der Antivirenscans**

  Die vom Device Posture Service unterstützten Browser- und Antivirenscans sind jetzt allgemein verfügbar. Einzelheiten finden Sie unter Scans, die je nach Geräteposition unterstützt werden.

23. Januar 2024

- **Allgemeine Verfügbarkeit der Gerätezertifikatsprüfung mit dem Device Posture Service**

Die Überprüfung von Gerätezertifikaten mit dem Device Posture Service ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats mit dem Device Posture Service.

20. Dezember 2023

- **Allgemeine Verfügbarkeit von Secure Private Access on-premises**

  Citrix Secure Private Access for on-premises ist jetzt allgemein verfügbar. Weitere Informationen finden Sie unter Neue Features.

16. Oktober 2023

- **Vorschaufunktionen der lokalen Secure Private Access-Lösung**

  Die lokale Secure Private Access-Lösung bietet jetzt Folgendes:

  - Admin-Benutzeroberfläche für die erstmalige Einrichtung.
  - Admin-Benutzeroberfläche für die Konfiguration der Anwendungen und Zugriffsrichtlinien.
  - Protokoll-Dashboard.

  Einzelheiten finden Sie unter Secure Private Access for on-premises.

- **Vorschaufunktionen des Device Posture Service**

  Der Device Posture Service unterstützt jetzt die folgenden Prüfungen:

  - Der Device Posture Service wird jetzt auf den IGEL-Plattformen unterstützt.
  - Der Device Posture Service unterstützt jetzt Geolocation- und Netzwerkstandortprüfungen.

  Einzelheiten finden Sie unter Gerätestatus.

11. September 2023

- **Allgemeine Verfügbarkeit der Device Posture Integration mit Microsoft Intune**

  Die Device Posture Integration mit Microsoft Intune ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Microsoft Intune-Integration mit Device Posture.

30. August 2023

- **Citrix Endpoint Analysis Client für Device Posture Service verwalten**

  Der EPA-Client kann zusammen mit NetScaler und Device Posture verwendet werden. Einige Konfigurationsänderungen sind erforderlich, um den EPA-Client zu verwalten, wenn er mit NetScaler und Device Posture verwendet wird. Einzelheiten finden Sie unter Verwalten des Citrix Endpoint Analysis Client für den Device Posture Service.

28. August 2023

- **Unterstützung des Device Posture Service auf iOS-Plattformen**

  Der Device Posture Service wird jetzt auf iOS-Plattformen unterstützt. Einzelheiten finden Sie unter Gerätestatus.

  Dieses Feature ist als Preview verfügbar.

22. August 2023

- **Überprüfung des Gerätezertifikats mit dem Citrix Device Posture Service**

  Der Citrix Device Posture Service kann jetzt den kontextuellen Zugriff (Smart Access) auf Citrix DaaS- und Secure Private Access-Ressourcen ermöglichen, indem das Zertifikat des Endgeräts mit einer unternehmenseigenen Zertifizierungsstelle verglichen wird, um festzustellen, ob das Endgerät vertrauenswürdig ist. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats mit dem Device Posture Service.

  Dieses Feature ist als Preview verfügbar.

17. August 2023

- **Gerätezustandsereignisse auf Citrix DaaS Monitor**

  Device Posture Service-Ereignisse und Überwachungsprotokolle können jetzt auf DaaS Monitor durchsucht werden. Einzelheiten finden Sie unter Gerätezustandsereignisse auf Citrix DaaS Monitor.

07. Juni 2023

- **Tool zur Konfiguration von Secure Private Access for on-premises**

Für die Konfiguration von Secure Private Access for on-premises ist jetzt eine vereinfachte Benutzeroberfläche verfügbar. Das Konfigurationstool kann auf einem Citrix Virtual Apps and Desktops Delivery Controller ausgeführt werden, um schnell eine SaaS- oder Webanwendung zu erstellen. Darüber hinaus können Sie dieses Tool verwenden, um Anwendungseinschränkungen, Datenverkehrsrouting und NetScaler Gateway-Einstellungen festzulegen. Einzelheiten finden Sie unter /en-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html .

29 May 2023

- **Allgemeine Verfügbarkeit der Erstellung von Zugriffsrichtlinien mit mehreren Regeln**

  Sie können mehrere Zugriffsregeln erstellen und verschiedene Zugriffsbedingungen für verschiedene Benutzer oder Benutzergruppen innerhalb einer einzigen Richtlinie konfigurieren. Diese Regeln können getrennt für HTTP/HTTPS- und TCP/UDP-Anwendungen angewendet werden, und das alles innerhalb einer einzigen Richtlinie. Einzelheiten finden Sie unter Konfigurieren einer Zugriffsrichtlinie mit mehreren Regeln.

  [SPA-746]

10. April 2023

- **Anwendungserkennung**

  Mit der Funktion zur Anwendungserkennung erhält ein Administrator einen Überblick über die internen privaten Anwendungen wie Web-Apps und Client-Server-Apps (TCP- und UDP-basierte Apps) in seiner Organisation und über die Benutzer, die auf diese Anwendungen zugreifen. Administratoren können die Apps entdecken, indem sie den Gültigkeitsbereich der Domänen (Wildcard-Domains) oder IP-Subnetze angeben. Einzelheiten finden Sie unter Anwendungserkennung.

  [ACS-2325]

29. März 2023

- **Secure Private Access-Lösung für On-Premises-Bereitstellungen**

  Als Kunde von Citrix StoreFront und NetScaler Gateway können Sie jetzt mithilfe der Citrix Secure Private Access-Lösung für On-Premises-Bereitstellungen nahtlos auf die Web- und SaaS-Apps sowie auf Citrix Virtual Apps und virtuelle Desktops zugreifen. Einzelheiten finden Sie unter Secure Private Access for on-premises.

  [SPAOP-1]

07. März 2023

- **Konfigurieren von DNS-Suffixen**

  Die DNS-Suffix-Funktion des Citrix Secure Private Access-Dienstes kann für die folgenden Anwendungsfälle verwendet werden:

  - Ermöglichen Sie dem Citrix Secure Access Client, einen nicht vollständig qualifizierten Domänennamen (Hostnamen) in einen vollqualifizierten Domänennamen (FQDN) aufzulösen, indem Sie die DNS-Suffixdomäne für die Backend-Server hinzufügen.
  - Ermöglichen Sie Administratoren, Anwendungen mithilfe von IP-Adressen (IP-CIDR/IP-Bereich) zu konfigurieren, sodass die Endbenutzer über den entsprechenden FQDN unter der DNS-Suffixdomäne auf die Anwendungen zugreifen können.

  Einzelheiten finden Sie unter DNS-Suffixe zur Auflösung von FQDNs inIP-Adressen.

  [ACS-2490]

23. Januar 2023

- **Device Posture Service**

  Der Citrix Device Posture Service ist eine cloudbasierte Lösung, mit der Administratoren bestimmte Anforderungen durchsetzen können, die die Endgeräte erfüllen müssen, um Zugriff auf Citrix DaaS (virtuelle Apps und Desktops) oder Citrix Secure Private Access-Ressourcen (SaaS, Web-Apps, TCP- und UDP-Apps) zu erhalten. Einzelheiten finden Sie unter Gerätestatus.

  [AAUTH-90]

- **Integration von Microsoft Endpoint Manager mit Device Posture**

  Zusätzlich zu den nativen Scans, die der Device Posture Service anbietet, kann der Device Posture Service auch in andere Lösungen von Drittanbietern integriert werden. Gerätestatus ist in Microsoft Endpoint Manager (MEM) unter Windows und macOS integriert. Einzelheiten finden Sie unter Integration von Microsoft Endpoint Manager mit Device Posture.

  [ACS-1399]

22. Dezember 2022

- **Single-Sign-On-Unterstützung für die Workspace-URL für Benutzer, die über die Citrix Workspace-App angemeldet sind**

  Der Citrix Secure Access-Client unterstützt jetzt Single Sign-On für die Workspace-URL, wenn ein Benutzer bereits über die Citrix Workspace-App angemeldet ist. Diese SSO-Funktionalität

verbessert die Benutzererfahrung, indem mehrere Authentifizierungen vermieden werden. Einzelheiten finden Sie unter Single Sign-On-Unterstützung für die Workspace-URL.

[ACS-1888]

- **Zugriff auf Apps mit Zugriffsrichtlinien aktivieren**

  Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren nun Zugriffsrichtlinien mit einer entsprechenden Benutzerabonnementliste erstellen, damit die Apps für Endbenutzer verfügbar sind. Bisher mussten Admins Benutzer als Abonnenten hinzufügen, um den Zugriff zu aktivieren. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

  [ACS-3018]

03. Oktober 2022

- **Zugriffsrichtlinien, um Zugriff auf die Apps zu gewähren**

  Die Konfigurationsoption App-Abonnenten wurde im Konfigurationsassistenten aus dem Abschnitt Anwendungen entfernt. Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

  [ACS-3018]

- **Unterstützung für UDP-Apps**

  Der Secure Private Access Service unterstützt jetzt den Zugriff auf UDP-Apps. Einzelheiten finden Sie unter Vorschaufunktionen.

  [ACS-1430]

09. September 2022

- **Adaptiver Zugriff basierend auf der Risikobewertung des Benutzers**

  Administratoren können jetzt eine adaptive Zugriffsrichtlinie mit der von Citrix Analytics for Security (CAS) bereitgestellten Benutzerrisikobewertung konfigurieren. Einzelheiten finden Sie unter Adaptiver Zugriff basierend auf der Benutzerrisikobewertung.

  [ACS-877]

- **Adaptiver Zugriff basierend auf dem Netzwerkstandort des Benutzers**

  Administratoren können jetzt die adaptive Zugriffsrichtlinie basierend auf dem Standort konfigurieren, von dem aus der Benutzer auf die Anwendung zugreift. Der Standort kann das Land

sein, von dem aus der Benutzer auf die Anwendung zugreift, oder der Netzwerkstandort des Benutzers. Einzelheiten finden Sie unter Adaptiver Zugriff basierend auf dem Standort.

[ACS-99]

- **Verbesserter Generator für adaptive Zugriffsrichtlinien**

  Der Zugriff auf die Apps ist jetzt erst aktiviert, wenn die konfigurierten Bedingungen erfüllt sind. Das Apps-Abonnement allein bietet Ihren Kunden keinen Zugriff auf die Anwendungen. Administratoren müssen Zugriffsrichtlinien hinzufügen, um zusätzlich zum App-Abonnement Zugriff auf die Apps zu gewähren. Außerdem sind Benutzer oder Gruppen eine obligatorische Bedingung in den Zugriffsrichtlinien, die für den Zugriff auf die Apps erfüllt sein müssen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

  [ACS-1850]

- **Beschränken Sie Datei-Uploads in SaaS/Web-Apps**

  Mit dieser Funktion können die Kundenadministratoren steuern (zulassen oder einschränken), wer Dateien in ihre geschäftskritischen Anwendungen hochladen kann. Damit können nur autorisierte Benutzer Dateien in die Anwendungen hochladen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

  [ACS-655]

- **Verbessertes Dashboard**

  Das Secure Private Access-Dashboard bietet jetzt detaillierte Einblicke in verschiedene Benutzermetriken wie App-Nutzung, Top-App-Benutzer, Top-Apps, auf die zugegriffen wurde, Diagnoseprotokolle usw. Einzelheiten finden Sie unter Dashboard.

  [ACS-2480]

- **Abwertung der Bibliothek**

  Die Secure Private Access-Anwendungen sind jetzt in der Citrix Cloud Library nicht sichtbar. Alle mit Secure Private Access konfigurierten Anwendungen befinden sich innerhalb des Anwendungsabschnitts innerhalb der Dienstkachel Secure Private Access. Dies hilft Administratoren, die Anwendungen einfach zu navigieren, zu bearbeiten und zu konfigurieren.

  [ACS-1546]

- **Prüfprotokolle für Secure Private Access**

  Die Ereignisse, die sich auf den Dienst Citrix Secure Private Access beziehen, werden jetzt im **Citrix Cloud > Systemprotokoll erfasst.** Einzelheiten finden Sie unter Prüfprotokolle.

  [ACS-876]

- **Diagnoseprotokolle für den Zugriff auf Enterprise Web und SaaS-Apps**

Die Ereignisse von Citrix Secure Private Access sind jetzt in Citrix Analytics integriert. Citrix Analytics bietet einen öffentlichen Endpunkt, über den Administratoren auf die Ereignisse zugreifen und diese herunterladen können. Auf diese Ereignisse kann über ein PowerShell-Skript zugegriffen werden. Einzelheiten finden Sie unter Diagnoseprotokolle für den Zugriff auf Enterprise Web und SaaS-Apps.

[ACS-805]

- **Leitfaden zur Fehlerbehebung**

  Die Administratoren können den Leitfaden zur Fehlerbehebung verwenden, um Probleme im Zusammenhang mit der Konfiguration zu lösen. Einzelheiten finden Sie unter Behandeln von Problemen im Zusammenhang mit Apps.

  [ACS-2719]

15. Juli 2022

- **Zugriff auf eine Anwendung nur aktivieren, wenn eine Zugriffsrichtlinie konfiguriert ist**

  Der Zugriff auf die Apps ist jetzt erst aktiviert, nachdem der Administrator zusätzlich zum App-Abonnement eine Zugriffsrichtlinie hinzugefügt hat. Das App-Abonnement allein ermöglicht keinen Zugriff auf die Anwendungen. Mit dieser Änderung können Administratoren anpassungsfähige Sicherheit basierend auf Kontext wie Benutzer, Standort, Gerät und Risiko durchsetzen. Administratoren müssen die vorhandenen App-Sicherheitskontrollen und Zugriffsrichtlinien auf das neue Framework für Zugriffsrichtlinien migrieren. Einzelheiten finden Sie unter Migration von App-Sicherheitskontrollen und Zugriffsrichtlinien.

  [ACS-1850]

01. Juni 2022

- **Adaptive Authentifizierung**

  Adaptive Authentication ist jetzt allgemein verfügbar (GA). Weitere Informationen zur adaptiven Authentifizierung finden Sie unter Adaptive Authentication service.

  [CGS-6510]

04. April 2022

- **Änderungen beim Rebranding**

  Der Citrix Secure Workspace Access Service wurde jetzt in den Citrix Secure Private Access Service umbenannt.

[ACS-2322]

- **Admin-geführter Workflow für einfaches Onboarding und Setup**

  Secure Private Access bietet jetzt ein neues, optimiertes Administratorerlebnis mit einem schrittweisen Prozess zur Konfiguration des Zero-Trust-Netzwerkzugriffs auf SaaS-Apps, interne Web-Apps und TCP-Apps. Es umfasst die Konfiguration von Adaptive Authentication, Anwendungen wie Benutzerabonnements, Richtlinien für den adaptiven Zugriff und andere innerhalb einer einzigen Admin-Konsole. Einzelheiten finden Sie unter Admin-geführter Workflow für einfaches Onboarding und Setup.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-1102]

- **Dashboard für sicheren privaten Zugriff**

  Das Secure Private Access-Dashboard bietet Administratoren vollen Einblick in ihre Top-Apps, Top-Benutzer, Connector-Integritätsstatus, Bandbreitennutzung und an einem einzigen Ort für die Nutzung. Diese Daten werden von Citrix Analytics abgerufen. Einzelheiten finden Sie unter Secure Private Access-Dashboard.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-1169]

- **Direkter Zugriff auf Enterprise Web-Apps**

  Kunden können jetzt Zero Trust Network Access (ZTNA) für interne Web-Apps direkt von nativen Webbrowsern wie Chrome, Firefox, Safari und Microsoft Edge aus aktivieren. Einzelheiten finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

- **ZTNA agentbasierter Zugriff auf TCP/HTTPS-Apps**

  Citrix-Kunden können jetzt Zero Trust Network Access (ZTNA) für alle Client-Server-Anwendungen und IP/Port-basierten Ressourcen zusätzlich zu internen Web-Apps aktivieren. Einzelheiten finden Sie unter Unterstützung für Client-Server-Apps.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-970]

- **Adaptive Zugriffs- und Sicherheitskontrollen für Enterprise Web-, TCP- und SaaS-Anwendungen**

  Die adaptive Zugriffsfunktion des Citrix Secure Private Access-Dienstes bietet einen umfassenden Zero Trust Network Access (ZTNA) -Ansatz, der sicheren Zugriff auf die Anwendungen ermöglicht. Durch den adaptiven Zugriff können Administratoren granularen Zugriff auf die

Apps gewähren, auf die Benutzer basierend auf dem Kontext zugreifen können. Der Begriff "Kontext"bezieht sich hier auf:

- Benutzer und Gruppen (Benutzer und Benutzergruppen)
- Geräte (Desktop- oder Mobilgeräte)
- Standort (Geolocation oder Netzwerkstandort)
- Gerätestatus (Gerätestatusprüfung)
- Risiko (Benutzerrisikobewertung)

Einzelheiten finden Sie unter Adaptive Zugriffs- und Sicherheitskontrollen für Enterprise Web-, TCP- und SaaS-Anwendungen.

Diese Funktion ist jetzt allgemein verfügbar (GA).

[ACS-878, ACS-879, ACS-882]

- **Prüfprotokolle für Secure Private Access**

  Die Ereignisse, die sich auf den Dienst Citrix Secure Private Access beziehen, werden jetzt im **Citrix Cloud > Systemprotokoll erfasst.** Einzelheiten finden Sie unter Prüfprotokolle.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-876]

- **Diagnoseprotokolle für den Zugriff auf Enterprise Web und SaaS-Apps**

  Die Ereignisse von Citrix Secure Private Access sind jetzt in Citrix Analytics integriert. Citrix Analytics bietet einen öffentlichen Endpunkt, über den Administratoren auf die Ereignisse zugreifen und diese herunterladen können. Auf diese Ereignisse kann über ein PowerShell-Skript zugegriffen werden. Einzelheiten finden Sie unter Diagnoseprotokolle für den Zugriff auf Enterprise Web und SaaS-Apps.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-805]

- **Adaptiver Authentifizierungsdienst**

  Citrix Cloud-Kunden können jetzt Citrix Workspace verwenden, um Adaptive Authentifizierung für Citrix Virtual Apps and Desktops bereitzustellen. Die adaptive Authentifizierung ist ein Citrix Cloud-Dienst, der Kunden und Benutzern, die sich bei Citrix Workspace anmelden, eine verbesserte Authentifizierung ermöglicht. Adaptive Authentication Service ist ADC, das von Citrix verwaltet und von Citrix Cloud gehostet wird. Einzelheiten finden Sie unter Adaptive Authentication Service.

  Dieses Feature ist als Preview verfügbar.

  [CGS-6510]

16. Februar 2022

- **Unterstützung für Client-Server-Apps** Mit der Unterstützung von Client-Server-Anwendungen in Citrix Secure Private Access können Sie jetzt die Abhängigkeit von einer herkömmlichen VPN-Lösung beseitigen, um Remotebenutzern Zugriff auf alle privaten Apps zu ermöglichen.

  Einzelheiten finden Sie unter Unterstützung für Client-Server-Apps —Vorschau

  [ACS-870]

11. Oktober 2021

- **Zusammenführung der NetScaler Gateway Service-Kachel zu Secure Private Access in Citrix Cloud**

  Die NetScaler Gateway-Dienstkachel wird jetzt zu einem einzigen Secure Private Access in der Citrix Cloud zusammengeführt.

  - Alle Secure Private Access-Kunden, einschließlich Citrix Workspace Essentials und Citrix Workspace Standard, können jetzt eine einzige Secure Private Access-Kachel zum Konfigurieren von SaaS- und Enterprise-Web-Apps, erweiterten Sicherheitskontrollen, kontextbezogenen Richtlinien sowie Webfilterrichtlinien verwenden.
  - Alle Citrix DaaS-Kunden können den NetScaler Gateway-Dienst weiterhin als HDX-Proxy über die Workspace Configuration aktivieren. Die Verknüpfung zum Aktivieren des NetScaler Gateway Service über die Gateway Service-Kachel wurde jedoch entfernt. Sie können den NetScaler Gateway Service über **Workspace-Konfiguration > Zugriff > Externe Konnektivität**aktivieren. Einzelheiten finden Sie unter Externe Konnektivität. Sonst ändert sich die Funktionalität nicht.

  [NGSWS-16761]

30. Juli 2021

- **Kontextabhängiger Zugriff und Sicherheitskontrollen für die Enterprise Web- und SaaS-Apps basierend auf dem geografischen Standort des Benutzers**

  Der Citrix Secure Private Access Service unterstützt jetzt den kontextbezogenen Zugriff auf das Enterprise Web und SaaS-Apps basierend auf dem geografischen Standort des Benutzers.

  [ACS-833]

- **Option zum Ausblenden eines bestimmten Web oder einer SaaS-App vor dem Citrix Workspace-Portal**

Administratoren können jetzt eine bestimmte Web- oder SaaS-App vor dem Citrix Workspace-Portal ausblenden. Wenn eine App im Citrix Workspace-Portal ausgeblendet ist, gibt der NetScaler Gateway Service diese App während der Aufzählung nicht zurück. Benutzer können jedoch weiterhin auf die versteckte App zugreifen.

[ACS-944]

09. Juni 2021

- **Routentabelle zum Definieren der Regeln zur Weiterleitung des App-Datenverkehrs**

  Administratoren können jetzt die Routing-Tabelle verwenden, um die Regeln für die Weiterleitung des App-Datenverkehrs direkt ins Internet oder über den NetScaler Gateway Connector zu definieren. Die Administratoren können den Routentyp für die Apps als Extern, Intern, Interner Bypass-Proxy oder Extern über Gateway Connector definieren, je nachdem, wie sie den Verkehrsfluss definieren möchten.

  [ACS-243]

22. Mai 2021

- **Kontextabhängiger Zugriff auf Enterprise Web- und SaaS-Anwendungen**

  Die Funktion für den kontextbezogenen Zugriff auf den Dienst Citrix Secure Private Access bietet einen umfassenden Zero-Trust-Zugriffsansatz, der sicheren Zugriff auf die Anwendungen ermöglicht. Durch den kontextabhängigen Zugriff können Administratoren einen granularen Zugriff auf die Apps gewähren, auf die Benutzer basierend auf dem Kontext zugreifen können. Der Begriff "Kontext"bezieht sich hier auf Benutzer, Benutzergruppen und die Plattform (mobiles Gerät oder Desktop-Computer), von der aus der Benutzer auf die Anwendung zugreift.

  [ACS-222]

- **Rebranding der NetScaler Gateway Connector-Benutzeroberfläche**

  Die Citrix Cloud Gateway Connector-Benutzeroberfläche wird gemäß den Citrix Branding-Richtlinien umbenannt.

  [NGSWS-17100]

01. Mai 2021

- **Löschen von Kundendaten aus dem Dienstdatenspeicher von Citrix Secure Private Access**

  Kundendaten, einschließlich Backups, werden nach 90 Tagen nach Ablauf der Serviceberechtigung aus dem Citrix Secure Private Access-Dienstdatenspeicher gelöscht.

[ACS-388]

- **Vereinfachte Schritte zum Verbund einer Domäne von Azure AD mit Citrix Workspace**

  Die Schritte zum Verbund einer Domäne von Azure AD mit der Citrix Workspace-App sind jetzt vereinfacht, um ein schnelleres Onboarding in Citrix Workspace zu ermöglichen. Der Domänenverbund kann jetzt über die Benutzeroberfläche des NetScaler Gateway Service Gateway-Dienstes auf der Seite Single Sign On ausgeführt werden.

  [ACS-351]

- **Erweiterung des Konnektivitätstest-Tools**

  Das Konnektivitätstest-Tool im NetScaler Gateway Connector wurde erweitert, um Timeout-Fehler zu behandeln und die erforderlichen Protokolle zu generieren.

  [NGSWS-17212]

15. März 2021

- **Verbesserungen der Plattform**

  Es werden verschiedene Plattformverbesserungen vorgenommen, um die Zuverlässigkeit bei der Verteilung der Administrationskonfigurationen des Kunden an die NetScaler Gateway Connectors zu erhöhen.

  [ACS-85]

- **Verbesserte Leistung von Web-Apps**

  Die Leistung von Web-Apps, wenn auf die Webanwendungen über den Systembrowser mit clientless VPN zugegriffen wird, wurde verbessert.

  [NGSWS-16469]

- **Aktivieren von NetScaler Gateway Connector zur Verwendung von TLS1.2 Cipher Suites der Klasse A oder höher**

  Der NetScaler Gateway Connector verwendet jetzt TLS1.2 mit Cipher Suites der Klasse A oder höher, um eine Verbindung mit dem Citrix Cloud-Dienst und anderen Backend-Servern herzustellen.

  [NGSWS-16068]

11. November 2020

- **Umbenennung des Citrix Access Control-Dienstes**

  Der Access Control-Dienst wurde jetzt in Secure Private Access umbenannt.

[NGSWS-14934]

15. Oktober 2020

- **Verbesserte Sicherheitsoption zum Starten von SaaS- und Unternehmens-Web-Apps innerhalb des Remote Browser Isolation Service**

  Administratoren können jetzt die erweiterte Sicherheitsoption **"Anwendung immer im Citrix Remote Browser Isolationsdienst starten** "verwenden, um eine Anwendung unabhängig von anderen erweiterten Sicherheitseinstellungen immer im Remote-Browser-Isolationsdienst zu starten.

  [ACS-123]

08. Oktober 2020

- **Sitzungstimeouts für die Citrix Secure Private Access-Browsererweiterung konfigurieren**

  Administratoren können jetzt Sitzungstimeouts für die Citrix Secure Private Access-Browsererweiterung konfigurieren. Administratoren können diese Einstellung über die Registerkarte **Verwalten** in der Benutzeroberfläche des NetScaler Gateway Services konfigurieren.

  [NGSWS-13754]

- **RBAC-Steuerung in den Administratoreinstellungen der Citrix Secure Private Access-Browsererweiterung**

  Die RBAC-Steuerung wird jetzt in den Administratoreinstellungen der Citrix Secure Private Access-Browsererweiterung erzwungen.

  [NGSWS-14427]

24. September 2020

- **Aktivieren des VPN-losen Zugriffs auf Enterprise Web Apps über einen lokalen Browser**

  Sie können jetzt die **Citrix Secure Private Access-Browsererweiterung** verwenden, um den VPN-losen Zugriff auf Enterprise Web-Apps über einen lokalen Browser zu ermöglichen. Die **Citrix Secure Private Access-Browsererweiterung** wird sowohl von Google Chrome- als auch von Microsoft Edge-Browsern unterstützt.

  [ACS-286]

07. Juli 2020

- **Validierung der Kerberos-Konfiguration auf NetScaler Gateway Connector**

  Sie können jetzt die Schaltfläche **Test** im **Single Sign-On-Bereich** verwenden, um die Kerberos-Konfiguration zu überprüfen.

  [NGSWS-8581]

19. Juni 2020

- **Schreibgeschützter Zugriff für Administratoren von NetScaler Gateway Service und Citrix Secure Private Access Service**

  Sicherheitsadministratorteams, die NetScaler Gateway Service verwenden, können jetzt detaillierte Steuerelemente bereitstellen, z. B. schreibgeschützten Zugriff für Administratoren von NetScaler Gateway Service und Citrix Secure Private Access Service.

  - Administratoren mit schreibgeschütztem Zugriff auf NetScaler Gateway Service haben Zugriff, um nur die App-Details anzuzeigen.
  - Administratoren mit schreibgeschütztem Zugriff auf Citrix Secure Private Access Service können nur die Inhaltszugriffseinstellungen anzeigen.

  [ACS-205]

08. Mai 2020

- **Neue Tools zur Fehlerbehebung in NetScaler Gateway Connector 13.0**

  - **Netzwerkverfolgung:** Sie können jetzt die **Trace-Funktion** verwenden, um Probleme bei der NetScaler Gateway Connector-Registrierung zu beheben. Sie können die Trace-Datei herunterladen und zur Problembehandlung an die Administratoren weitergeben. Einzelheiten finden Sie unter Beheben von Registrierungsproblemen für NetScaler Gateway Connector.

    [NGSWS-10799]

  - **Konnektivitätstests:** Sie können jetzt die Funktion **Konnektivitätstest** verwenden, um zu bestätigen, dass in der Gateway Connector-Konfiguration keine Fehler vorliegen und der Gateway Connector eine Verbindung zu den URLs herstellen kann. Einzelheiten finden Sie unter Anmelden und Einrichten des NetScaler Gateway Connectors.

    [NGSWS-8580]

V2019.04.02

- **Unterstützung der Kerberos-Authentifizierung für NetScaler Gateway Connector zum ausgehenden Proxy** [NGSWS-6410]

  Die Kerberos-Authentifizierung wird jetzt für den Datenverkehr vom NetScaler Gateway Connector zum ausgehenden Proxy unterstützt. Gateway Connector verwendet die konfigurierten Proxy-Anmeldeinformationen zur Authentifizierung beim ausgehenden Proxy.

V2019.04.01

- **Web-/SaaS-Apps-Datenverkehr kann nun über einen Gateway-Connector im Unternehmensnetzwerk weitergeleitet werden, wodurch die Zwei-Faktor-Authentifizierung vermieden wird.** Wenn ein Kunde eine SaaS-App veröffentlicht hat, die außerhalb des Unternehmensnetzwerks gehostet wird, wird jetzt Unterstützung hinzugefügt, um den Datenverkehr zu authentifizieren, damit diese App einen on-premises Gateway Connector durchläuft.

  Bedenken Sie beispielsweise, dass ein Kunde über eine Okta geschützte SaaS-App (wie Workday) verfügt. Der Kunde möchte möglicherweise, dass der Authentifizierungsdatenverkehr zum Okta-Server über den NetScaler Gateway Service über den NetScaler Gateway Service über einen lokalen Gateway Connector geleitet wird, obwohl der tatsächliche Workday-Datenverkehr nicht über den NetScaler Gateway Service weitergeleitet wird. Dies hilft einem Kunden, eine zweite Faktorauthentifizierung vom Okta-Server zu vermeiden, da der Benutzer über das Unternehmensnetzwerk eine Verbindung zum Okta-Server herstellt.

  [NGSWS-6445]

- **Deaktivieren des Filterns von Website-Listen und der Website-Kategorisierung**. Das Filtern von Website-Listen und die Website-Kategorisierung können deaktiviert werden, wenn der Administrator diese Funktionen nicht für einen bestimmten Kunden anwendet.

  [NGSWS-6532]

- **Automatisches Geo-Routing für Umleitungen des Remote Browser Isolation-Dienstes.** Automatisches Geo-Routing ist jetzt für Remote Browser Isolation-Dienstumleitungen aktiviert.

  [NGSWS-6926]

V2019.03.01

- **Die Schaltfläche "Erkennen"wird auf der Seite "Gateway Connector hinzufügen"hinzugefügt.** Die Schaltfläche **Erkennen** wird verwendet, um die Liste der Connectors zu aktualisieren,

sodass der neu hinzugefügte Connector im Abschnitt Web-App-Konnektivität reflektiert werden kann.

[CGOP-6358]

- **Eine neue Kategorie "Bösartig und gefährlich"wird in den Kategorien "Access Control Web Filterung"hinzugefügt.** Eine neue Kategorie mit dem Namen **bösartig und gefährlich** in den Kategorien **Access Control Web Filtering** wird unter der Gruppe **Malware und Spam** hinzugefügt.

  [CGOP-6205]

Veraltete Funktionen

June 19, 2024

Dieser Artikel informiert Sie im Voraus über die Funktionen des Secure Private Access-Dienstes, die schrittweise eingestellt werden, sodass Sie zeitnahe Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element. Einzelheiten zum Support für den Produktlebenszyklus finden Sie in der Richtlinie zur Unterstützung des Produktlebenszyklus.

In der folgenden Tabelle sind die Secure Private Access-Dienstfunktionen aufgeführt, die veraltet sind oder deren Verwertung geplant ist.

Element	Einstellung der Unterstützung angekündigt in	Datum der Abwertung	Alternative
Clientlose VPN-Zugriffsmethode für den Zugriff auf Web-Apps	Januar 2023	1. Oktober 2023	Verwenden Sie je nach Anwendungsfall den Citrix Enterprise Browser oder Direct Access. Weitere Informationen finden Sie unter Informationen zur Abschaffung des clientlosen VPN-Zugriffs für den Zugriff auf Web-Apps.
Kategoriebasierte Webfilterung	Dezember 2022	1. Dezember 2022	Die Funktionen “Zulassen”, “Verweigern”oder “RBI-Umleitung”pro Website in Secure Private Access werden beibehalten, um selektiven Zugriff auf Websites zu ermöglichen, die nichts mit der Arbeit zu tun haben, über den Citrix Enterprise Browser.
Sicherheitssteuerung für die Navigation einschränken	April 2022	1. Juni 2022	Nicht verfügbar

Element	Einstellung der Unterstützung angekündigt in	Datum der Abwertung	Alternative
Citrix Gateway Connector	Mai 2022	1. September 2022	Connector-Appliance. Informationen zur Migration Ihres Gateway Connector zu Connector Appliance finden Sie unter Migrieren von Gateway Connector zu Connector

Informationen zur Abschaffung des clientlosen VPN-Zugriffs für den Zugriff auf Web-Apps

- Was ist die Clientless VPN-Zugriffsmethode (clientloses VPN)?

  Citrix Secure Private Access verwendet die CVPN-basierte Zugriffsmethode, wenn über Workspace für Web (Citrix Workspace-App für HTML5) auf eine interne Web-App zugegriffen wird, die ohne erweiterte Sicherheitseinschränkungen konfiguriert wurde.

  > **Hinweis:**
  >
  > Die clientlose VPN-Zugriffsmethode wird nur verwendet, wenn über Workspace für Web (Citrix Workspace-App für HTML5) auf eine interne App zugegriffen wird. Nur Apps, für die keine erweiterten Sicherheitseinschränkungen konfiguriert sind, werden blockiert.

- Warum lehnen wir diese Funktion ab?

  Die clientlose VPN-Methode verwendet clientseitige URL-Umschreibungen, was bestimmten branchenweiten technologischen Einschränkungen unterliegt. In mehreren Fällen kann es zu Fehlern beim App-Zugriff kommen, wenn bestimmte Links innerhalb der Web-Apps neu geschrieben werden. Dies führt zu einer schlechten Endbenutzererfahrung. Um unseren Kunden den bestmöglichen Zugriff auf Apps zu bieten, lehnen wir diese Funktion ab und empfehlen, zu einer der unten genannten Alternativen zu wechseln.

- Wie wirkt sich das auf die Endbenutzer aus, die auf für Secure Private Access konfigurierte Anwendungen zugreifen?

  Wenn über Workspace für Web auf eine ohne erweiterte Sicherheitseinschränkungen konfigurierte Web-App zugegriffen wird, wird der Zugriff auf diese Anwendung blockiert.

Dies hat keine Auswirkungen auf den Zugriff von Endbenutzern auf Anwendungen über Workspace Application, Direct Access, Remote Browser Isolation Service (RBI) oder Secure Access Agent.

- Was sind die Alternativen und was sollten die Admins tun?

  Citrix Enterprise Browser: Verwenden Sie die Citrix Workspace-App, um über den Citrix Enterprise Browser auf diese Anwendungen zuzugreifen. Diese Methode bietet die beste Benutzererfahrung mit erweiterten Sicherheitseinstellungen (wie Einschränkung von Downloads, Druckeinschränkungen, Wasserzeichen, Einschränkung des Zugriffs auf die Zwischenablage) und Browserverwaltung. Sicherer privater Zugriff für Citrix Workspace.
  Direktzugriff: Wenn Sie eine clientlose Methode für den Zugriff auf Webanwendungen wünschen, verwenden Sie die Direktzugriffsmethode, mit der Apps direkt von jedem nativen Browser wie Chrome aus aufgerufen werden können. Diese Methode kann für Anwendungsfälle verwendet werden, in denen die Citrix Workspace-App nicht auf dem Endgerät installiert werden kann, oder für nicht verwaltete Geräte. Weitere Informationen finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.

- Wirkt es sich auf bestehende Anwendungen aus, auf die über die Citrix Workspace-App oder den Secure Access Agent zugegriffen wird?

  Nein, wir blockieren nur den Zugriff auf Webanwendungen, auf die über Workspace for Web zugegriffen wird. Diese Veraltete Version hat keine Auswirkungen auf Apps, auf die über die Citrix Workspace-App zugegriffen wird, oder auf Secure Access-Clients, die auf Endgeräten installiert sind. Wenn auf eine Webanwendung, die mit erweiterten Sicherheitseinschränkungen konfiguriert ist, über Workspace für Web oder die HTML5-Variante der Citrix Workspace-App zugegriffen wird, wird der Zugriff auf diese Anwendungen blockiert.

- Haben Sie noch Fragen?

  Wenden Sie sich an den Citrix Support.

Erste Schritte mit Citrix Secure Private Access

December 27, 2023

In diesem Dokument erfahren Sie, wie Sie mit dem Onboarding und der erstmaligen Einrichtung der SaaS-App-Bereitstellung beginnen können. Dieses Dokument ist für Anwendungsadministratoren gedacht.

Systemanforderungen

Unterstützung von Betriebssystemen: Die Citrix Workspace App wird unter Windows 7, 8, 10 und Mac 10.11 und höher unterstützt.

Browserunterstützung: Greifen Sie mit den neuesten Versionen von Edge, Chrome, Firefox oder Safari auf Arbeitsbereiche zu.

Citrix Workspace-Unterstützung: Greifen Sie mit Citrix Workspace auf Arbeitsbereiche für eine der Desktop-Plattformen (Windows, Mac) zu.

Funktionsweise

Citrix Secure Private Access unterstützt IT- und Sicherheitsadministratoren dabei, den autorisierten Endbenutzerzugriff auf genehmigte SaaS- und von Unternehmen gehostete Web-Apps zu steuern. Benutzeridentitäten und -attribute werden verwendet, um Zugriffsrechte zu bestimmen, und Zugriffskontrollrichtlinien legen fest, welche Berechtigungen für die Ausführung von Vorgängen erforderlich sind. Sobald ein Benutzer authentifiziert wurde, autorisiert die Zugriffskontrolle die entsprechende Zugriffsebene und zulässige Aktionen, die mit den Anmeldeinformationen dieses Benutzers verknüpft sind.

Citrix Secure Private Access kombiniert Elemente verschiedener Citrix Cloud-Dienste, um Endbenutzern und Administratoren ein integriertes Erlebnis zu bieten.

Funktionalität	Service/Komponente, die die Funktionalität bereitstellt
Konsistente Benutzeroberfläche für den Zugriff auf Apps	Workspace-Erlebnis-/Workspace-App
SSO zu SaaS und Web-Apps	NetScaler Gateway-Dienststandard
Webfilterung und Kategorisierung	Webfilter-Dienst
Verbesserte Sicherheitsrichtlinien für SaaS	Cloud-App-Steuerung
Sicheres Surfen	Remote-Browser-Isolationsdienst
Einblick in den Zugriff auf Websites und riskantes Verhalten	Citrix Analytics

Erste Schritte mit dem Citrix Secure Private Access Service

1. Melden Sie sich für Citrix Cloud an.
2. Anforderung der Secure Private Access-Dienstberechtigung.

3. Nach der Berechtigung wird der Secure Private Access-Dienst unter “**Meine Dienste**”bereitgestellt.
4. Greifen Sie auf die Secure Private Access-Dienstschnittstelle zu

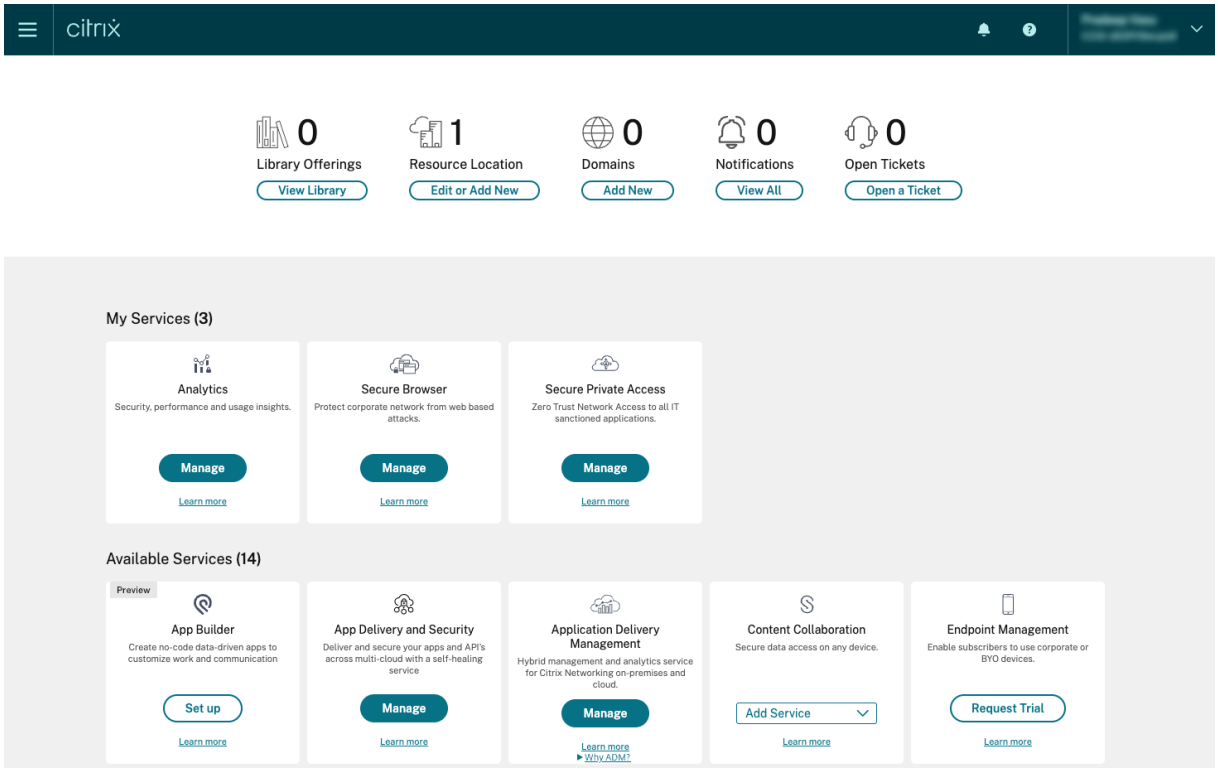
Schritt 1: **Melden Sie sich für Citrix Cloud an**

Um den Secure Private Access-Dienst verwenden zu können, müssen Sie zuerst ein Citrix Cloud-Konto erstellen oder einem vorhandenen Konto beitreten, das von einer anderen Person in Ihrem Unternehmen erstellt wurde. Detaillierte Prozesse und Anweisungen zum weiteren Vorgehen finden Sie unter Registrierung für Citrix Cloud .

Schritt 2: **Anforderung der Secure Private Access-Dienstberechtigung**

Um die Secure Private Access-Dienstberechtigung anzufordern, klicken Sie auf dem **Citrix Cloud-Bildschirm** im Abschnitt **Verfügbare Dienste** auf die Registerkarte **Testversion anfordern**, die sich in der Servicekachel Secure Private Access befindet.

Einzelheiten zur Lizenz finden Sie unter https://www.citrix.com/buy/licensing/product.html.



Schritt 3: **Nach der Berechtigung wird der Secure Private Access-Dienst unter “Meine Dienste” bereitgestellt**

Nachdem Sie die Secure Private Access-Dienstberechtigung erhalten haben, wird die Secure Private Access-Dienstkachel in den Abschnitt **Meine Dienste** verschoben.

Schritt 4: **Zugreifen auf die Secure Private Access-Dienstbenutzeroberfläche**

Klicken Sie auf der Kachel auf die Registerkarte **Verwalten**, um auf die Secure Private Access-Dienstbenutzeroberfläche zuzugreifen.

Hinweis:

- Damit Endbenutzer den Workspace verwenden und auf ihre Apps zugreifen können, müssen sie die Citrix Workspace-App herunterladen und nutzen oder die Workspace-URL verwenden. Sie müssen einige SaaS-Apps in Ihrem Workspace veröffentlicht haben, um die Citrix Secure Private Access-Lösung testen zu können. Die Workspace-App kann unter https://www.citrix.com/downloads heruntergeladen werden. Wählen Sie in der Liste "**Downloads suchen** "die **Citrix Workspace-App**aus.
- Bei konfigurierter Firewall für ausgehende Verbindungen müssen Sie sicherstellen, dass der Zugriff auf die folgenden Domänen zulässig ist.

  > – *.cloud.com
  > – *.nssvc.net
  > – *.netscalergateway.net

  Weitere Details finden Sie unter Konfiguration von Cloud Connector-Proxy und Firewall und Anforderungen an die Internetkonnektivität.
- Sie können nur ein Workspace-Konto hinzufügen.

Überblick über die Secure Private Access Service Access-Servicelösung

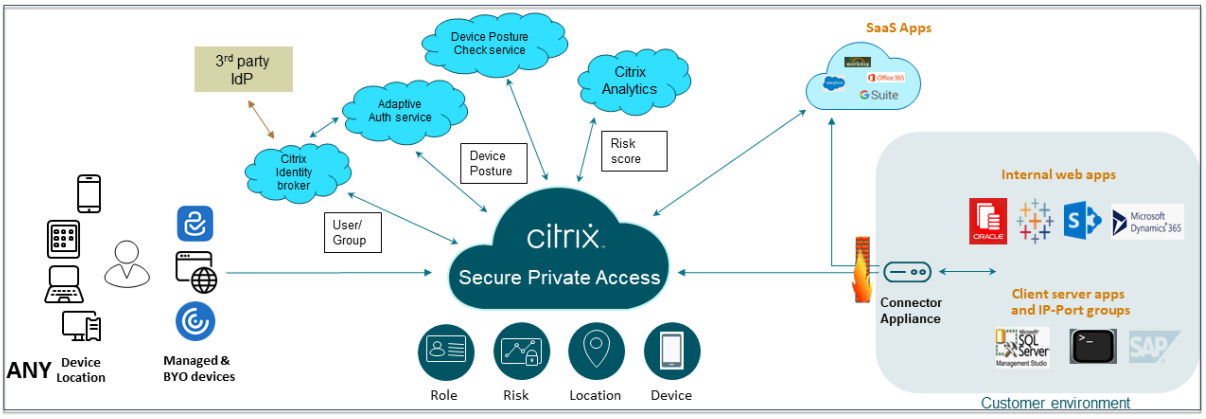
June 19, 2024

Überblick über die Lösung

Herkömmliche VPN-Lösungen erfordern die Verwaltung von Endbenutzergeräten, die Bereitstellung des Zugriffs auf Netzwerkebene und die Durchsetzung statischer Zugriffskontrollrichtlinien. Citrix Secure Private Access bietet der IT eine Reihe von Sicherheitskontrollen zum Schutz vor Bedrohungen durch BYO-Geräte, sodass Benutzer die Wahl haben, von jedem Gerät aus auf ihre IT-genehmigten Anwendungen zuzugreifen, unabhängig davon, ob es sich um ein verwaltetes Gerät oder ein BYO-Gerät handelt.

Citrix Secure Private Access bietet adaptive Authentifizierung, Single-Sign-On-Unterstützung und erweiterte Sicherheitskontrollen für die Anwendungen. Secure Private Access bietet auch die

Möglichkeit, das Endbenutzergerät vor dem Einrichten einer Sitzung mithilfe des Device Posture-Dienstes zu scannen. Basierend auf den Ergebnissen der adaptiven Authentifizierung oder des Gerätestatus können Administratoren die Authentifizierungsmethoden für die Apps definieren.



Adaptive Sicherheit

Die adaptive Authentifizierung bestimmt den richtigen Authentifizierungsablauf für die aktuelle Anfrage. Die adaptive Authentifizierung kann den Gerätestatus, den geografischen Standort, das Netzwerksegment und die Zugehörigkeit zur Benutzerorganisation/Abteilung identifizieren. Basierend auf den erhaltenen Informationen kann ein Administrator definieren, wie er Benutzer für ihre von der IT genehmigten Apps authentifizieren möchte. Auf diese Weise können Unternehmen dasselbe Authentifizierungsrichtlinien-Framework für alle Ressourcen implementieren, einschließlich öffentlicher SaaS-Apps, privater Web-Apps, privater Client-Server-Apps und Desktops as a Service (DaaS). Einzelheiten finden Sie unter Adaptive Sicherheit.

Zugriff auf Anwendungen

Secure Private Access kann eine Verbindung zu den on-premises Web-Apps herstellen, ohne auf ein VPN angewiesen zu sein. Diese VPN-lose Verbindung verwendet ein on-premises bereitgestelltes Connector Appliance. Die Connector Appliance erstellt einen ausgehenden Kontrollkanal zum Citrix Cloud-Abonnement der Organisation. Von dort aus kann Secure Private Access Verbindungen zu den internen Web-Apps tunneln, ohne dass ein VPN erforderlich ist. Einzelheiten finden Sie unter Anwendungszugriff.

Single Sign-On

Mit Adaptive Authentication können Unternehmen strenge Authentifizierungsrichtlinien bereitstellen, um das Risiko kompromittierter Benutzerkonten zu verringern. Die Single-Sign-On-Funktionen von

Secure Private Access verwenden dieselben adaptiven Authentifizierungsrichtlinien für alle SaaS-, privaten Web- und Client-Server-Apps. Einzelheiten finden Sie unter Single Sign-On.

Sicherheit des Browsers

Secure Private Access ermöglicht Endbenutzern das sichere Surfen im Internet mit einem zentral verwalteten und gesicherten Unternehmensbrowser. Wenn ein Endbenutzer eine SaaS- oder private Web-App startet, werden dynamisch mehrere Entscheidungen getroffen, um zu entscheiden, wie diese Anwendung am besten bereitgestellt werden soll. Einzelheiten finden Sie unter Browsersicherheit.

Gerätestatus

Mit dem Device Stature Service kann ein Administrator Richtlinien definieren, um den Status von Endgeräten zu überprüfen, die versuchen, remote auf Unternehmensressourcen zuzugreifen. Je nach Konformitätsstatus eines Endpunkts kann der Device Posture Service den Zugriff auf Unternehmensanwendungen und Desktops verweigern oder eingeschränkten oder vollständigen Zugriff gewähren.

Wenn ein Endbenutzer eine Verbindung mit Citrix Workspace initiiert, sammelt der Device Posture Client Informationen über die Endpunktparameter und gibt diese Informationen an den Device Posture Service weiter, um festzustellen, ob der Status des Endpunkts den Richtlinienanforderungen entspricht.

Die Integration des Device Posture Service mit Citrix Secure Private Access ermöglicht den sicheren Zugriff auf SaaS-, Web-, TCP- und UDP-Apps von überall und mit der Resilienz und Skalierbarkeit von Citrix Cloud. Einzelheiten finden Sie unter Device Posture.

Unterstützung für TCP- und UDP-Anwendungen

Manchmal benötigen Remote-Benutzer Zugriff auf private Client-Server-Apps, deren Frontend auf dem Endpunkt und ihr Backend in einem Rechenzentrum liegt. Unternehmen können zu Recht strenge Sicherheitsrichtlinien für diese internen und privaten Apps durchsetzen, wodurch es für Remote-Benutzer schwierig wird, auf diese Anwendungen zuzugreifen, ohne die Sicherheitsprotokolle zu gefährden.

Der Secure Private Access Service behebt die TCP- und UDP-Sicherheitslücken, indem er es ZTNA ermöglicht, sicheren Zugriff auf diese Apps bereitzustellen. Benutzer können jetzt mit einem systemeigenen Browser oder einer systemeigenen Clientanwendung über den Citrix Secure Access Client, der auf ihren Computern ausgeführt wird, auf alle privaten Apps, einschließlich TCP-, UDP- und HTTPS-Apps, zugreifen.

Benutzer müssen den Citrix Secure Access Client auf ihren Clientgeräten installieren.

- Für Windows kann die Client-Version (22.3.1.5 und höher) von https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html heruntergeladen werden.
- Für macOS kann die Client-Version (22.02.3 und höher) aus dem App Store heruntergeladen werden.

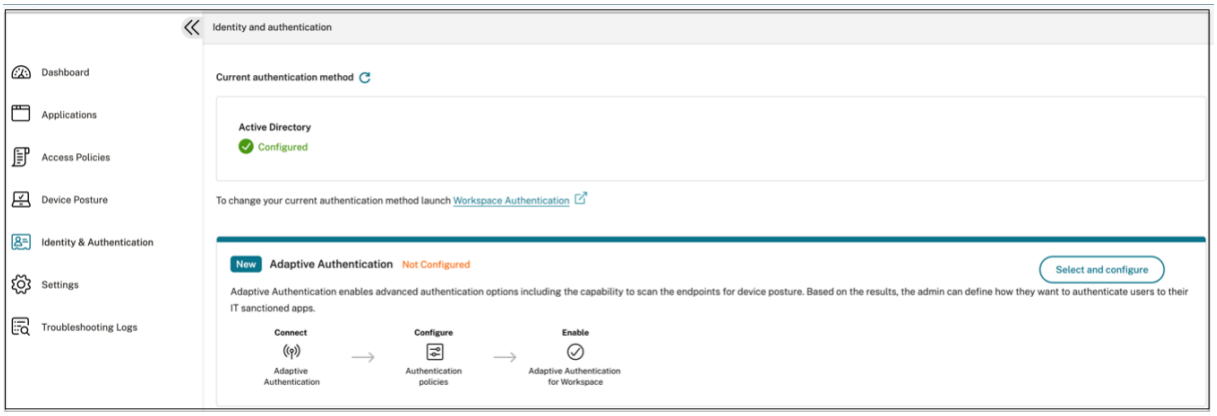
Einzelheiten finden Sie unter Unterstützung für Client-Server-Apps.

Citrix Secure Private Access einrichten

Aktivieren Sie den Zero-Trust-Netzwerkzugriff auf SaaS-Apps, interne Web-Apps, TCP- und UDP-Apps mithilfe der Secure Private Access-Administratorkonsole. Diese Konsole umfasst die Konfiguration der adaptiven Authentifizierung, Anwendungen einschließlich Benutzerabonnements und adaptiver Zugriffsrichtlinien.

Identität und Authentifizierung einrichten

Wählen Sie die Authentifizierungsmethode für die Abonnenten aus, um sich bei Citrix Workspace anzumelden. Die adaptive Authentifizierung ist ein Citrix Cloud-Dienst, der Kunden und Benutzern, die sich bei Citrix Workspace anmelden, eine verbesserte Authentifizierung ermöglicht.



Einzelheiten finden Sie unter Identität und Authentifizierung einrichten.

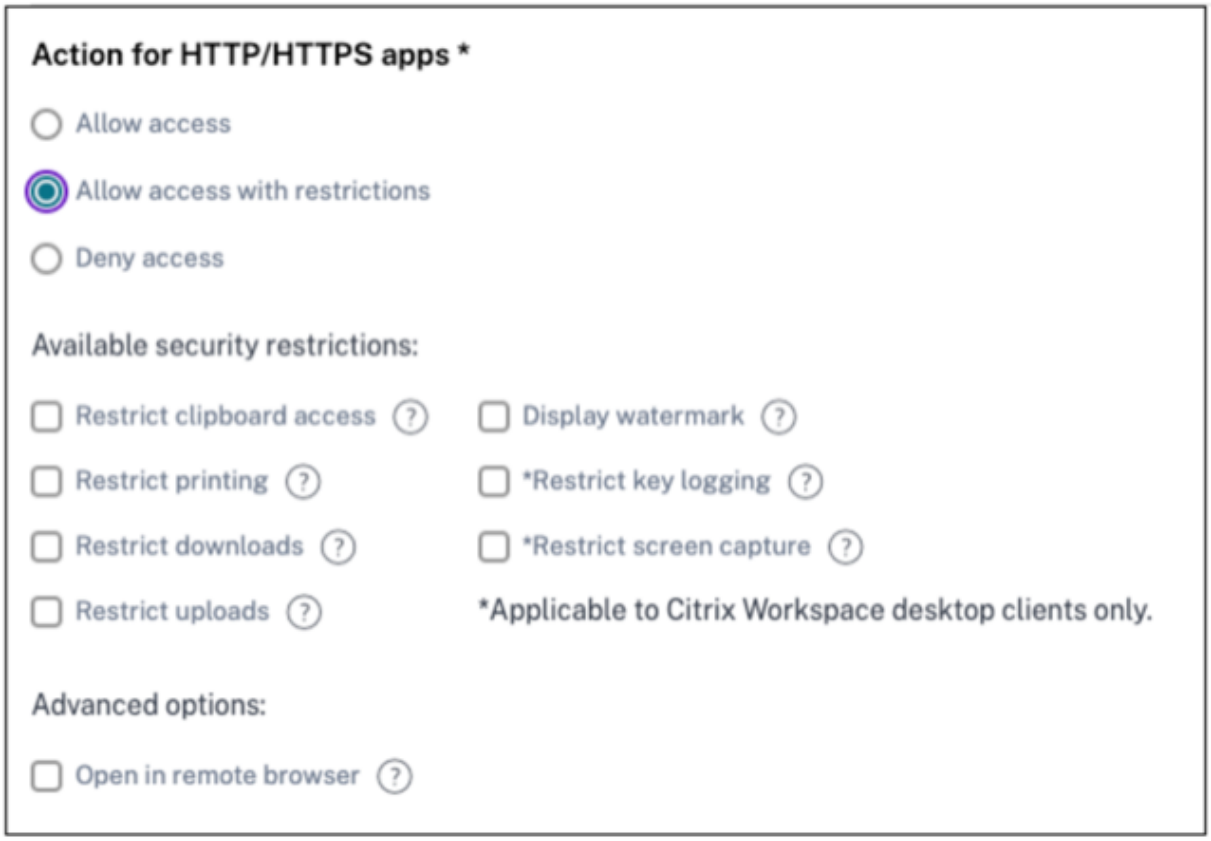
Apps auflisten und veröffentlichen

Nachdem Sie die Authentifizierungsmethode ausgewählt haben, konfigurieren Sie die Web-, SaaS- oder die TCP- und UDP-Apps mithilfe der Admin-Konsole. Einzelheiten finden Sie unter Apps hinzufügen und verwalten.

Ermöglichen Sie erweiterte Sicherheitskontrollen

Um Inhalte zu schützen, integrieren Unternehmen erweiterte Sicherheitsrichtlinien in die SaaS-Anwendungen. Jede Richtlinie erzwingt eine Einschränkung im Citrix Enterprise Browser, wenn Sie die Workspace-App für Desktop verwenden, oder im Secure Browser, wenn Sie die Workspace-App Web oder Mobile verwenden.

- **Zugriff auf die Zwischenablage einschränken**: Deaktiviert das Ausschneiden/Kopieren/Einfügen zwischen der App und der Systemzwischenablage.
- **Drucken einschränken**: Deaktiviert das Drucken im Citrix Enterprise Browser.
- **Downloads einschränken**: Deaktiviert die Fähigkeit des Benutzers, aus der App herunterzuladen.
- **Uploads einschränken**: Deaktiviert die Fähigkeit des Benutzers, innerhalb der App hochzuladen.
- **Wasserzeichen anzeigen**: Zeigt ein Wasserzeichen auf dem Bildschirm des Benutzers an, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt.
- **Beschränken Sie die Schlüsselprotokollierung**: Schützt vor Keyloggern. Wenn ein Benutzer versucht, sich mit dem Benutzernamen und dem Kennwort bei der App anzumelden, werden alle Schlüssel auf den Keyloggern verschlüsselt. Außerdem sind alle Aktivitäten, die der Benutzer in der App ausführt, vor Key-Logging geschützt. Wenn beispielsweise App-Schutzrichtlinien für Office 365 aktiviert sind und der Benutzer ein Office 365-Word-Dokument bearbeitet, werden alle Tastenanschläge auf Keyloggern verschlüsselt.
- **Bildschirmaufnahme einschränken**: Deaktiviert die Möglichkeit, die Bildschirme mit einem der Bildschirmaufnahmeprogramme oder Apps aufzunehmen. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm aufgenommen.



Einzelheiten finden Sie unter Konfigurieren einer Zugriffsrichtlinie.

Aktivieren Sie den Citrix Enterprise Browser für Anwendungsstarts

Secure Private Access ermöglicht es Endbenutzern, ihre Apps mit dem Citrix Enterprise Browser (CEB) zu starten. CEB ist ein chrombasierter Browser, der in die Citrix Workspace-App integriert ist und einen nahtlosen und sicheren Zugriff auf Web- und SaaS-Apps im Citrix Enterprise Browser ermöglicht.

CEB kann als bevorzugter Browser oder als Ihr Arbeitsbrowser für alle intern gehosteten Web-Apps oder SaaS-Apps mit Sicherheitsrichtlinien konfiguriert werden. CEB ermöglicht es Benutzern, alle konfigurierten SaaS-/Web-App-Domains in einer sicheren und kontrollierten Umgebung zu öffnen.

Aktivieren Sie den Citrix Enterprise Browser Administratoren können den Global App Configuration Service (GACS) verwenden, um den Citrix Enterprise Browser als Standardbrowser zum Starten von Web- und SaaS-Apps von der Citrix Workspace-App aus zu konfigurieren.

Konfiguration über API:

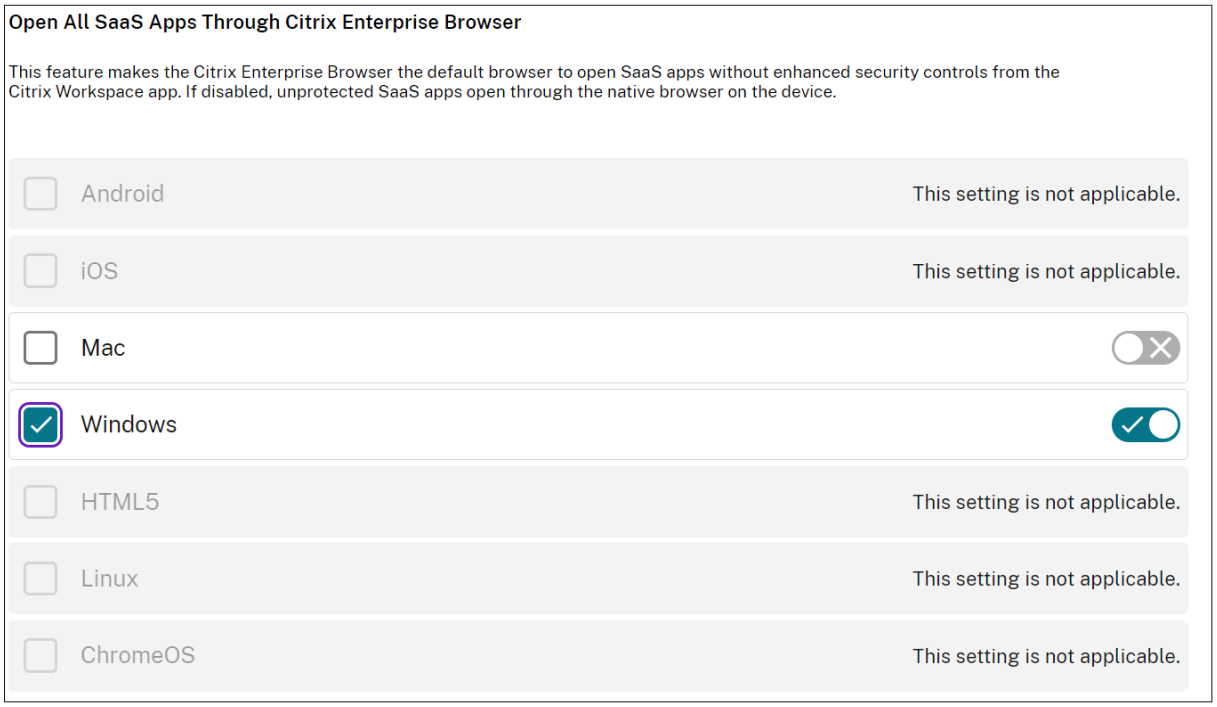
Zur Konfiguration finden Sie hier eine Beispiel-JSON-Datei, um den Citrix Enterprise Browser standardmäßig für alle Apps zu aktivieren:


```
"settings": [
                    {

                       "name": "open all apps in ceb",
                       "value": "true"
                     }

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

Der Standardwert ist true.

Konfiguration über GUI:

Wählen Sie die Geräte aus, für die CEB zum Standardbrowser für die App-Starts gemacht werden muss.



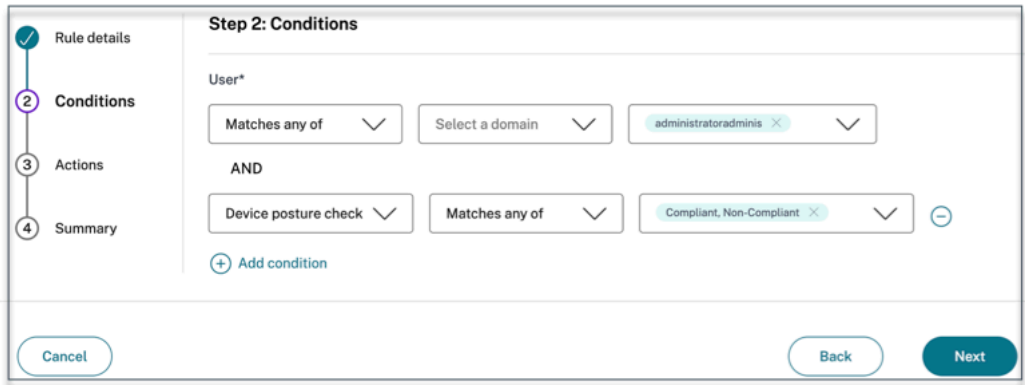
Einzelheiten finden Sie unter Citrix Enterprise Browser über GACS verwalten.

Konfigurieren Sie Tags für den kontextuellen Zugriff mithilfe von Device Posture

Nach der Überprüfung der Geräteposition darf sich das Gerät anmelden und das Gerät wird als konform oder nicht konform eingestuft. Diese Klassifizierung wird dem Secure Private Access Service als Tags zur Verfügung gestellt und wird verwendet, um kontextabhängigen Zugriff auf der Grundlage des Gerätestatus bereitzustellen.

1. Melden Sie sich bei Citrix Cloud an.

2. Klicken Sie auf der Kachel Secure Private Access auf **Verwalten** .
3. Klicken Sie im linken Navigationsbereich auf **Richtlinien zugreifen** und dann auf **Richtlinie erstellen**.
4. Geben Sie den Richtliniennamen und die Beschreibung der Richtlinie ein.
5. Wählen Sie unter **Anwendungen** die App oder die Gruppe von Apps aus, für die diese Richtlinie durchgesetzt werden muss.
6. Klicken Sie auf **Regel erstellen**, um Regeln für die Richtlinie zu erstellen.
7. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein, und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Bedingungen der Benutzer aus. Die Benutzerbedingung ist eine zwingende Voraussetzung, die erfüllt sein muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren.
9. Klicken Sie auf **+**, um den Zustand der Gerätehaltung hinzuzufügen.
10. Wählen Sie **Device Posture Check** und den logischen Ausdruck aus dem Drop-down-Menü aus.
11. Geben Sie einen der folgenden Werte in benutzerdefinierte Tags ein:



- **Konform** —Für konforme Geräte
- **Nicht konform** —Für Geräte, die nicht konform sind

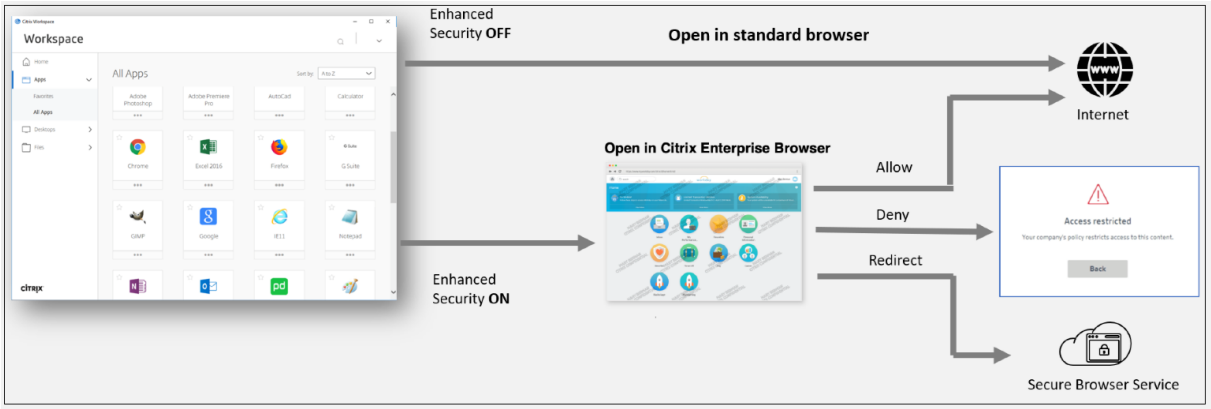
12. Klicken Sie auf **Weiter**.
13. Wählen Sie die Aktionen aus, die auf der Grundlage der Zustandsbewertung angewendet werden müssen, und klicken Sie dann auf **Weiter**.

    Auf der Übersichtsseite werden die Richtliniendetails angezeigt.
14. Überprüfen Sie die Angaben und klicken Sie auf **Fertig** stellen .

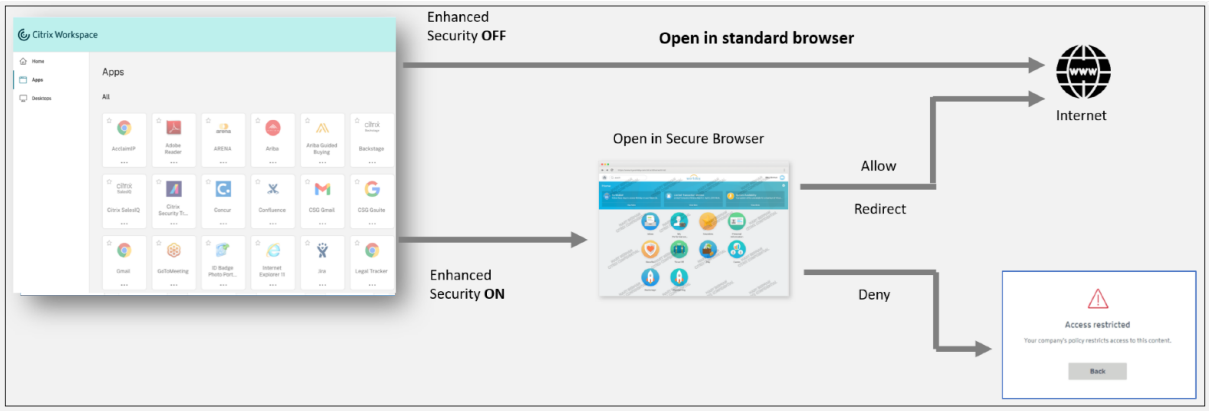
> **Hinweis:**
>
> Jede Secure Private Access-Anwendung, die in der Zugriffsrichtlinie nicht als konform oder nicht konform gekennzeichnet ist, wird als Standardanwendung behandelt und ist unabhängig vom Gerätestatus auf allen Endpunkten zugänglich.

Erfahrung für Endbenutzer

Der Citrix Administrator ist befugt, die Sicherheitskontrolle mithilfe von Citrix Secure Private Access zu erweitern. Die Citrix Workspace-App ist ein Einstiegspunkt für den sicheren Zugriff auf alle Ressourcen. Endbenutzer können über die Citrix Workspace-App auf virtuelle Apps, Desktops, SaaS-Apps und Dateien zugreifen. Mit Citrix Secure Private Access können Administratoren steuern, wie der Endbenutzer über die Citrix Workspace Experience-Webbenutzeroberfläche oder den nativen Citrix Workspace-App-Client auf eine SaaS-Anwendung zugreift.



Wenn der Benutzer die Workspace-App auf dem Endpunkt startet, sieht er seine Anwendungen, Desktops, Dateien und SaaS-Apps. Wenn ein Benutzer auf die SaaS-Anwendung klickt, während die erweiterte Sicherheit deaktiviert ist, wird die Anwendung in einem Standardbrowser geöffnet, der lokal installiert ist. Wenn der Administrator die erweiterte Sicherheit aktiviert hat, werden die SaaS-Apps auf dem CEB in der Workspace-App geöffnet. Der Zugriff auf Hyperlinks in SaaS-Apps und Web-Apps wird auf der Grundlage der Richtlinien für nicht genehmigte Websites kontrolliert. Einzelheiten zu nicht genehmigten Websites finden Sie unter UnsanktionierteWebsites.



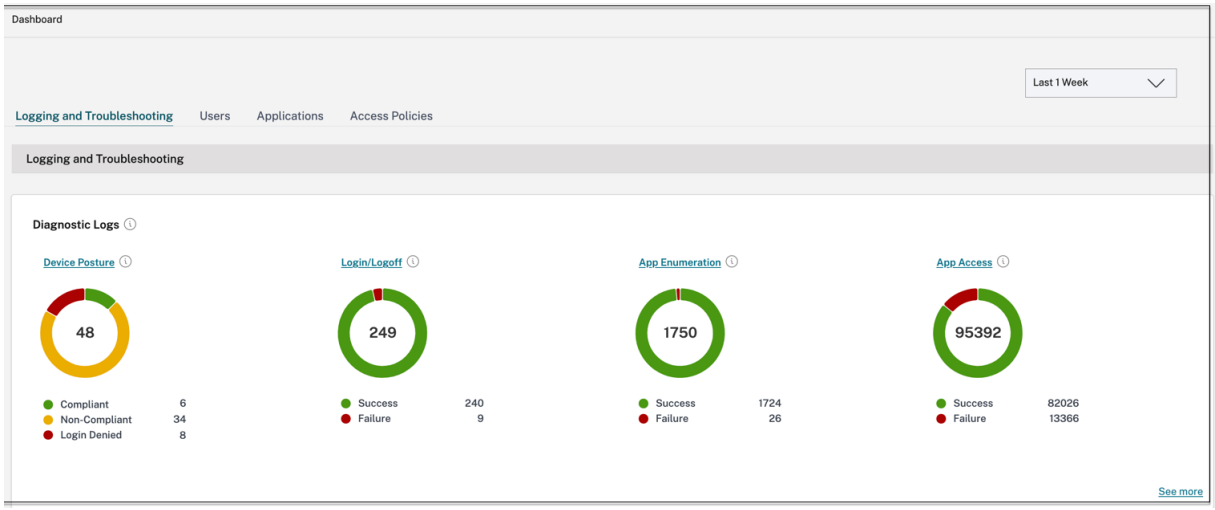
Ähnlich werden SaaS-Anwendungen beim Workspace-Webportal, wenn die erweiterte Sicherheit deaktiviert ist, in einem Standardbrowser geöffnet, der nativ installiert ist. Wenn die erweiterte Sicherheit aktiviert ist, werden SaaS-Apps im sicheren Remote-Browser geöffnet. Benutzer können auf der Grundlage der Richtlinien für nicht genehmigte Websites innerhalb von SaaS-Apps auf die Websites zugreifen. Einzelheiten zu nicht genehmigten Websites finden Sie unter UnsanktionierteWebsites.

Analytics-Dashboard

Das Secure Private Access Service Access-Dienst-Dashboard zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Das Dashboard bietet Administratoren einen vollständigen Überblick über ihre Apps, Benutzer, Konnektoren, den Gesundheitszustand und die Bandbreitennutzung an einem einzigen Ort für den Verbrauch. Diese Daten werden von Citrix Analytics abgerufen. Die Kennzahlen sind grob in die folgenden Kategorien unterteilt.

- Protokollierung und Problembehandlung
- Benutzer
- Anwendungen
- Richtlinien für den Zugriff

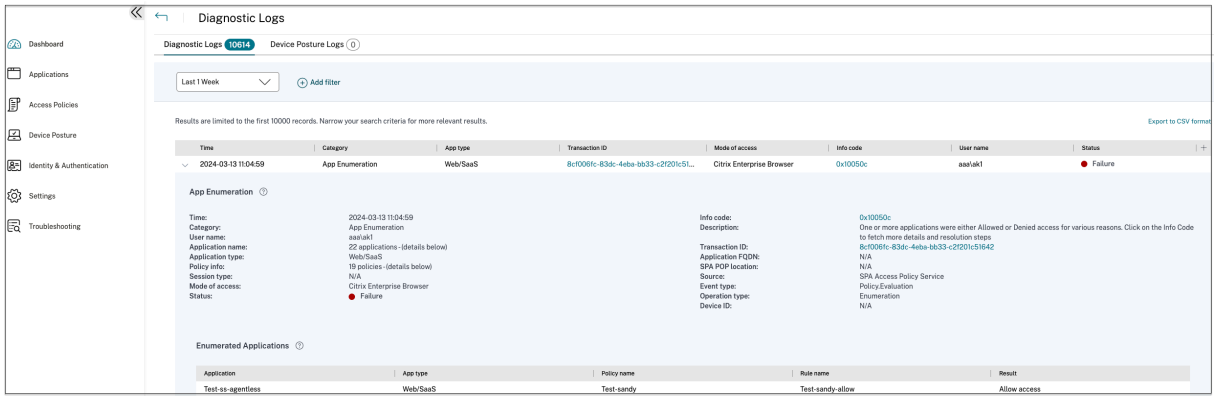
Einzelheiten finden Sie unter Dashboard.



App-Probleme beheben

Das Diagramm mit den Diagnoseprotokollen im Secure Private Access-Dashboard bietet einen Überblick über die Protokolle zur Authentifizierung, zum Anwendungsstart, zur App-Aufzählung und zum Gerätestatus.

- **Infocode**: Einigen Protokollereignissen wie Ausfällen ist ein Infocode zugeordnet. Wenn Sie auf den Infocode klicken, werden die Benutzer zu den Lösungsschritten oder zu weiteren Informationen zu diesem Ereignis weitergeleitet.
- **Transaktions-ID**: In den Diagnoseprotokollen wird auch eine Transaktions-ID angezeigt, die alle Secure Private Access-Protokolle für eine Zugriffsanforderung miteinander verknüpft. Für eine App-Zugriffsanforderung können mehrere Protokolle generiert werden, angefangen mit der Authentifizierung, dann der App-Aufzählung innerhalb der Workspace-App und dann dem App-Zugriff selbst. All diese Ereignisse generieren ihre eigenen Protokolle. Die Transaktions-ID wird verwendet, um all diese Protokolle zu korrelieren. Sie können die Diagnoseprotokolle anhand der Transaktions-ID filtern, um alle Protokolle zu finden, die sich auf eine bestimmte App-Zugriffsanforderung beziehen.
  Einzelheiten finden Sie unter Problembehandlung bei Secure Private Access.



Beispiele für Anwendungsfälle

- Greifen Sie mithilfe eines Zero-Trust-Ansatzes auf interne Anwendungen (Web/TCP/UDP) zu, ohne eingehenden Datenverkehr auf der Firewall zu öffnen
- Gehen Sie zu einem Zero-Trust-Ansatz über, indem Sie Anwendungen ermitteln, auf die Benutzer zugreifen
- Beschränken Sie den Zugriff auf SaaS-Anwendungen auf Citrix Enterprise Browser
- Beschränken Sie den Zugriff auf SaaS-Anwendungen auf unternehmenseigene öffentliche IP-Adressen
- Verbesserte Sicherheit für von Azure verwaltete SaaS-Apps
- Verbesserte Sicherheit für Office 365
- Verbesserte Sicherheit für Okta-Apps

Referenz

- Einführung in Secure Private Access
- Technischer Überblick
- Referenzarchitektur
- Citrix Enterprise Browser
- Citrix Enterprise Browser über GACS verwalten
- Admin-geführter Workflow für einfaches Onboarding und Einrichten

Referenzvideos

- Zero-Trust-Netzwerkzugriff (ZTNA) auf Apps
- Zugriff auf private Web-Apps mit Citrix Secure Private Access
- Zugriff auf öffentliche SaaS-Apps mit Citrix Secure Private Access
- Zugriff auf private Client-Server-Apps mit Citrix Secure Private Access

- Keylogger-Schutz mit Citrix Secure Private Access
- Schutz vor Bildschirmübertragung mit Citrix Secure Private Access
- Endbenutzererlebnis mit Citrix Secure Private Access
- ZTNA versus VPN-Anmeldeerfahrung mit Citrix Secure Private Access
- ZTNA im Vergleich zu VPN-Port-Scans mit Citrix Secure Private Access

Was gibt es Neues bei verwandten Produkten

- Citrix Enterprise Browser: Über dieses Release
- Citrix Workspace: Was ist neu
- Citrix DaaS: Was ist neu
- Citrix Secure Access-Client NetScaler Gateway-Clients

Admin-geführter Workflow für einfaches Onboarding und Einrichten

June 19, 2024

Eine neue optimierte Admin-Erfahrung mit schrittweisem Prozess zur Konfiguration von Zero Trust Network Access für SaaS-Apps, interne Web-Apps und TCP-Apps ist im Secure Private Access-Dienst verfügbar. Es umfasst die Konfiguration von Adaptive Authentication, Anwendungen wie Benutzerabonnements, Richtlinien für den adaptiven Zugriff und andere innerhalb einer einzigen Admin-Konsole.

Dieser Assistent hilft Administratoren dabei, eine fehlerfreie Konfiguration zu erreichen, entweder beim Onboarding oder bei wiederkehrender Verwendung. Außerdem ist ein neues Dashboard mit vollständigem Einblick in die allgemeinen Nutzungsmetriken und andere wichtige Informationen verfügbar.

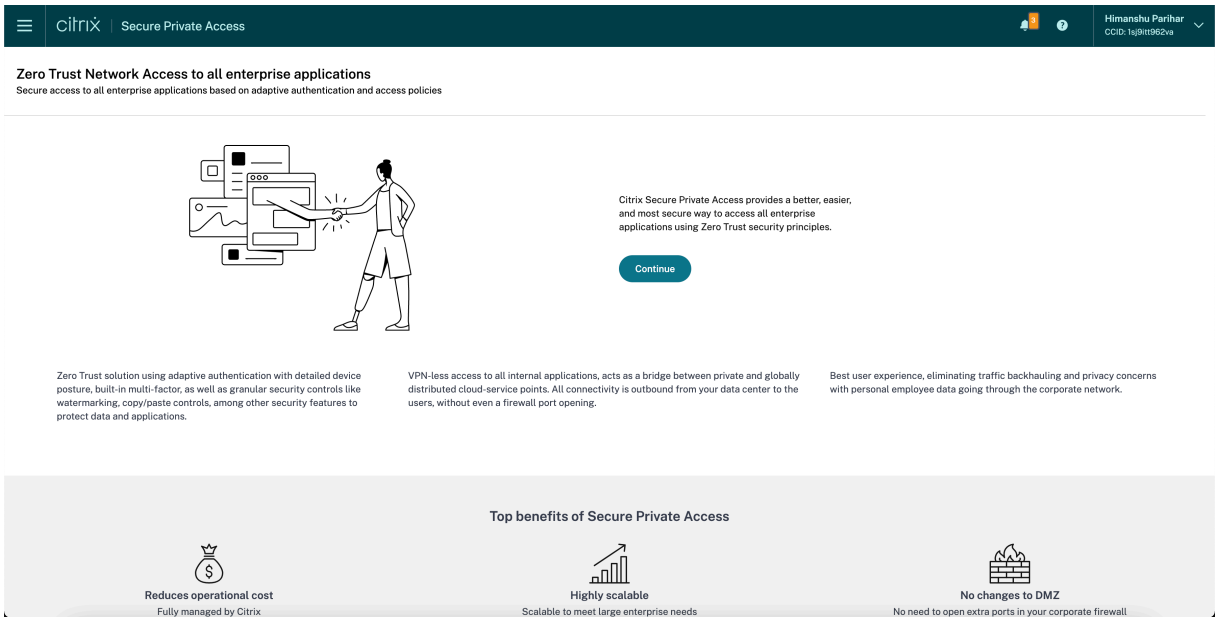
Zu den allgemeinen Schritten gehören die folgenden:

1. Wählen Sie die Authentifizierungsmethode, mit der sich die Abonnenten bei Citrix Workspace anmelden möchten.
2. Fügen Sie Anwendungen für Ihre Benutzer hinzu.
3. Weist Berechtigungen für den App-Zugriff zu, indem die erforderlichen Zugriffsrichtlinien erstellt werden.
4. Überprüfen Sie die Konfiguration der App.

Greifen Sie auf den administrativen Workflow-Assistenten Secure Private Access zu

Führen Sie die folgenden Schritte aus, um auf den Assistenten zuzugreifen.

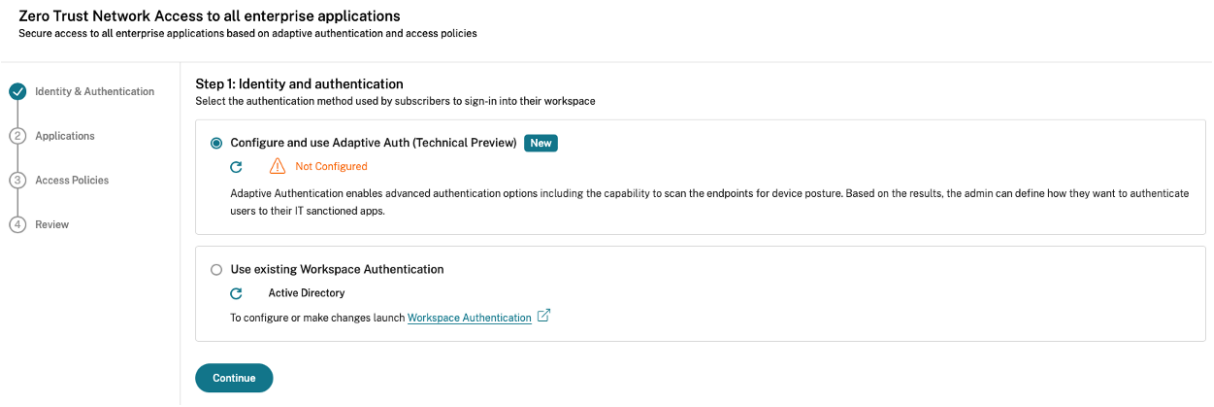
1. Klicken Sie auf der **Secure Private Access-Dienstkachel** auf **Verwalten**.
2. Klicken Sie auf der Übersichtsseite auf **Weiter**.



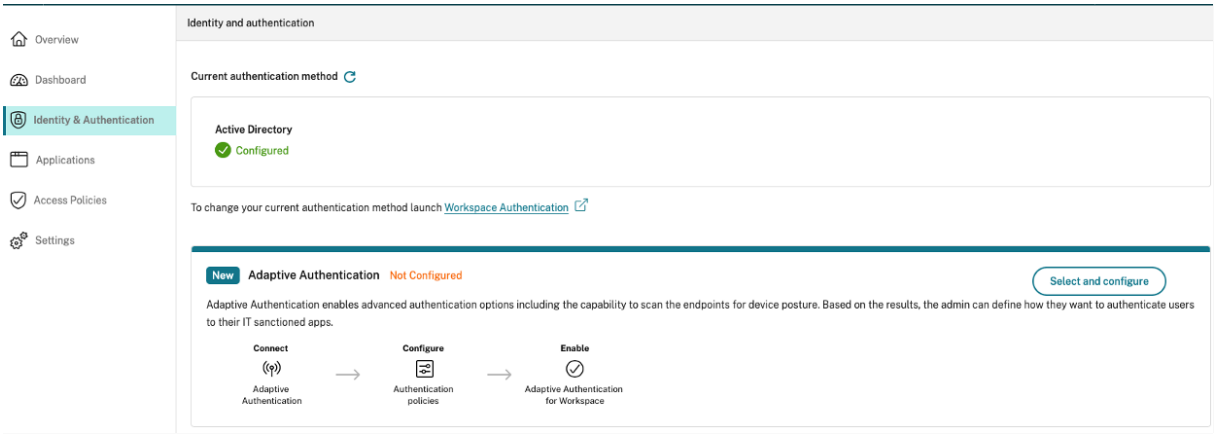
Schritt 1: Identität und Authentifizierung einrichten

Wählen Sie die Authentifizierungsmethode für die Abonnenten aus, um sich bei Citrix Workspace anzumelden. Die adaptive Authentifizierung ist ein Citrix Cloud-Dienst, der Kunden und Benutzern, die sich bei Citrix Workspace anmelden, eine verbesserte Authentifizierung ermöglicht. Der Adaptive Authentication Service ist ein von Citrix gehosteter, von Citrix verwalteter, Cloud-gehosteter Citrix ADC, der alle erweiterten Authentifizierungsfunktionen wie die folgenden bietet.

- Multifaktorauthentifizierung
- Gerätestatusscans
- Bedingte Authentifizierung
- Adaptiver Zugriff auf Citrix Virtual Apps and Desktops
- Um die Adaptive Authentifizierung zu **konfigurieren, wählen Sie Adaptive Auth (Technical Preview) konfigurieren und verwenden** und schließen Sie dann die Konfiguration ab. Weitere Informationen zur adaptiven Authentifizierung finden Sie unter Adaptive Authentication Service. Nachdem Sie die adaptive Authentifizierung konfiguriert haben, können Sie auf **Verwalten** klicken, um die Konfiguration bei Bedarf zu ändern.



- Wenn Sie anfangs eine andere Authentifizierungsmethode ausgewählt haben und zur adaptiven Authentifizierung wechseln möchten, klicken Sie auf **Auswählen und konfigurieren**, und schließen Sie dann die Konfiguration ab.

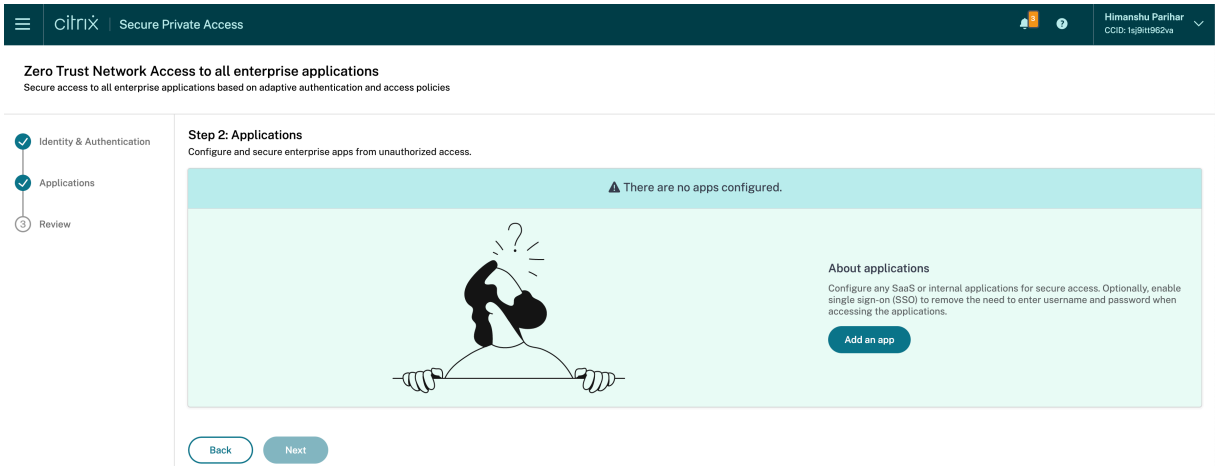


Um die vorhandene Authentifizierungsmethode oder die vorhandene Authentifizierungsmethode zu ändern, klicken Sie auf **Workspace-Authentifizierung**.

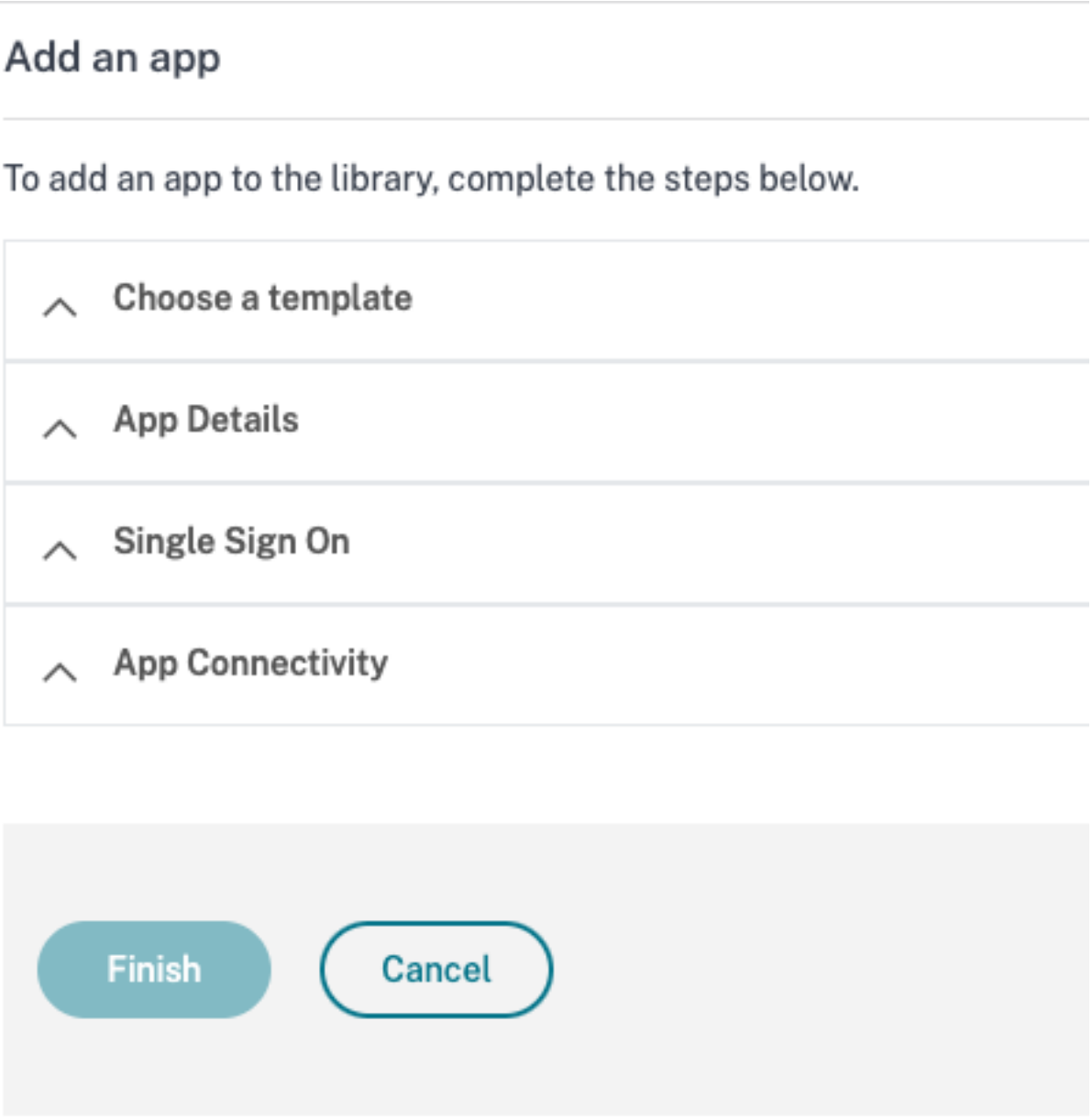
Schritt 2: Anwendungen hinzufügen und verwalten

Nachdem Sie die Authentifizierungsmethode ausgewählt haben, konfigurieren Sie die Anwendungen. Für Erstbenutzer werden auf der Zielseite **Anwendungen** keine Anwendungen angezeigt. Fügen Sie eine App hinzu, indem Sie auf **App hinzufügen**klicken. Auf dieser Seite können Sie SaaS-Apps, Web-Apps und TCP/UDP-Apps hinzufügen. Um eine App hinzuzufügen, klicken Sie auf **App hinzufügen**.

Sobald Sie eine App hinzugefügt haben, können Sie sie hier sehen.



Führen Sie die in der folgenden Abbildung angezeigten Schritte aus, um eine App hinzuzufügen.



- **Hinzufügen einer Enterprise Web-App**
  - Unterstützung für unternehmenseigene Web-Apps
  - Direkter Zugriff auf Web-Apps konfigurieren
- **Eine SaaS-App hinzufügen**
  - Unterstützung für Software as a Service App
  - Serverspezifische Konfiguration für SaaS App
- **Client-Server-Apps konfigurieren**
  - Unterstützung für Client-Server-Apps

- **Starten Sie eine App**
  - Starten einer konfigurierten App - Endbenutzerworkflow
- **Nur-Lese-Zugriff für Admins aktivieren**
  - Schreibgeschützter Zugriff für Administratoren auf SaaS und Web-Apps

Schritt 3: Konfigurieren Sie eine Zugriffsrichtlinie mit mehreren Regeln

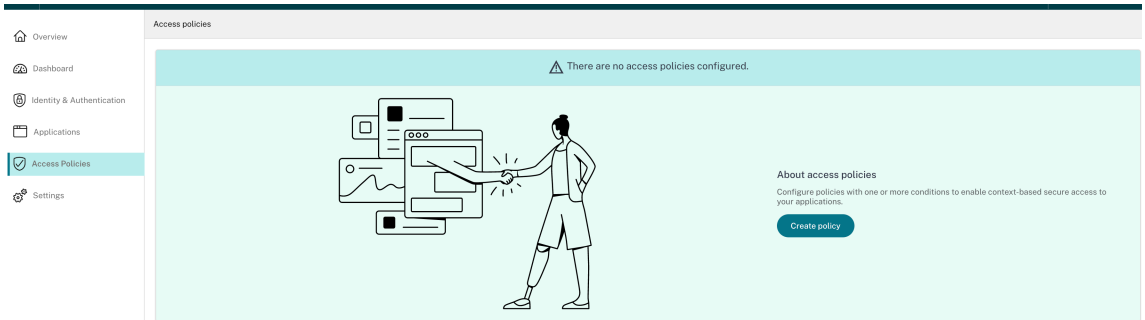
Sie können mehrere Zugriffsregeln erstellen und verschiedene Zugriffsbedingungen für verschiedene Benutzer oder Benutzergruppen innerhalb einer einzigen Richtlinie konfigurieren. Diese Regeln können getrennt für HTTP/HTTPS- und TCP/UDP-Anwendungen angewendet werden, und das alles innerhalb einer einzigen Richtlinie.

Mit den Zugriffsrichtlinien in Secure Private Access können Sie den Zugriff auf die Apps je nach Kontext des Benutzers oder Benutzergeräts aktivieren oder deaktivieren. Darüber hinaus können Sie den eingeschränkten Zugriff auf die Apps aktivieren, indem Sie die folgenden Sicherheitseinschränkungen hinzufügen:

- Zugriff auf Zwischenablage einschränken
- Drucken einschränken
- Downloads einschränken
- Uploads einschränken
- Wasserzeichen anzeigen
- Schlüsselprotokollierung einschränken
- Bildschirmaufnahme einschränken

Weitere Informationen zu diesen Einschränkungen finden Sie unter Verfügbare Zugriffsbeschränkungsoptionen.

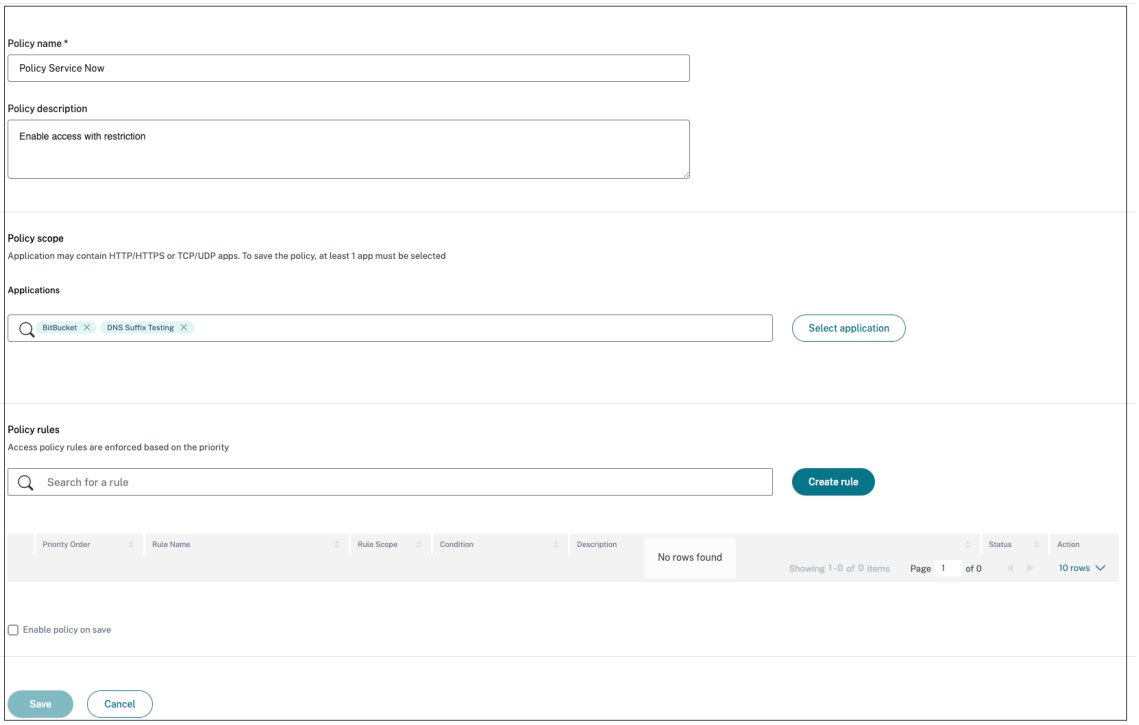
1. Klicken Sie im Navigationsbereich auf **Zugriffsrichtlinien** und dann auf **Richtlinie erstellen**.



   Für Erstbenutzer werden **auf der Zielseite Zugriffsrichtlinien** keine Richtlinien angezeigt. Sobald Sie eine Richtlinie erstellt haben, können Sie sie hier sehen.

2. Geben Sie den Richtliniennamen und die Beschreibung der Richtlinie ein.

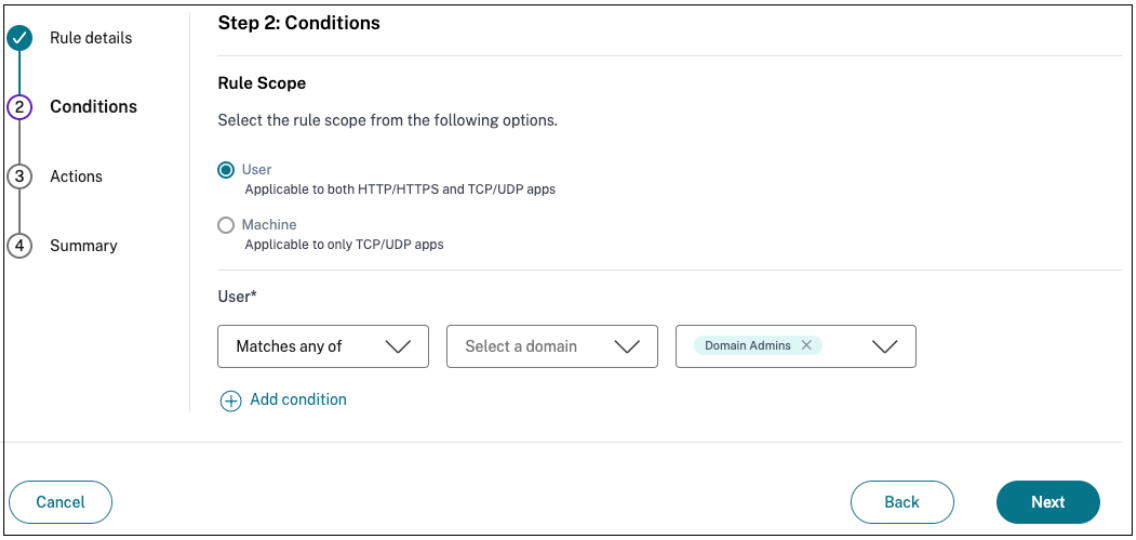
3. Wählen Sie unter **Anwendungen** die App oder die Gruppe von Apps aus, für die diese Richtlinie durchgesetzt werden muss.
4. Klicken Sie auf **Regel erstellen**, um Regeln für die Richtlinie zu erstellen.



5. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein, und klicken Sie dann auf **Weiter**.

6. Wählen Sie die Bedingungen der Benutzer aus. Die **Benutzerbedingung** ist eine zwingende Voraussetzung, die erfüllt sein muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren. Wählen Sie eine Option aus:

- **Entspricht einem von** —Nur die Benutzer oder Gruppen, die mit einem der im Feld aufgeführten Namen übereinstimmen und zur ausgewählten Domäne gehören, haben Zugriff.
- **Entspricht keinem** — Alle Benutzer oder Gruppen mit Ausnahme der im Feld aufgeführten Benutzer oder Gruppen, die zur ausgewählten Domäne gehören, sind berechtigt, darauf zuzugreifen.



7. (Optional) Klicken Sie auf +, um je nach Kontext mehrere Bedingungen hinzuzufügen.

   Wenn Sie Bedingungen hinzufügen, die auf einem Kontext basieren, wird eine UND-Operation auf die Bedingungen angewendet, wobei die Richtlinie nur ausgewertet wird, wenn die **Benutzerbedingungen** und die optionalen kontextbezogenen Bedingungen erfüllt sind. Sie können die folgenden Bedingungen je nach Kontext anwenden.

   - **Desktop** oder **Mobilgerät** —Wählen Sie das Gerät aus, für das Sie den Zugriff auf die Apps aktivieren möchten.
   - **Geografischer Standort** —Wählen Sie die Bedingung und den geografischen Standort aus, von dem aus die Benutzer auf die Apps zugreifen.
     - **Entspricht einem von:** Nur Benutzern oder Benutzergruppen, die von einem der aufgelisteten geografischen Standorte aus auf die Apps zugreifen, wird der Zugriff auf die Apps gewährt.
     - **Entspricht keinem:** Alle Benutzer oder Benutzergruppen außer denen aus den aufgelisteten geografischen Standorten haben Zugriff.
   - **Netzwerkstandort** —Wählen Sie die Bedingung und das Netzwerk aus, über das die Benutzer auf die Apps zugreifen.
     - **Entspricht einem von:** Nur Benutzern oder Benutzergruppen, die von einem der aufgelisteten Netzwerkstandorte aus auf die Apps zugreifen, wird der Zugriff auf die Apps gewährt.

- **Entspricht keinem:** Alle Benutzer oder Benutzergruppen außer denen von den aufgelisteten Netzwerkstandorten haben Zugriff.

- **Gerätestatusprüfung** —Wählen Sie die Bedingungen aus, die das Benutzergerät für den Zugriff auf die Anwendung erfüllen muss.
- **Risikobewertung für Benutzer** —Wählen Sie die Risikobewertungskategorien aus, auf deren Grundlage die Benutzer Zugriff auf die Anwendung erhalten müssen.
- **Workspace-URL**—Administratoren können Filter auf der Grundlage des vollqualifizierten Domainnamens angeben, der dem Workspace entspricht.
  - **Entspricht einer der**Optionen —Zugriff nur zulassen, wenn die eingehende Benutzerverbindung einer der konfigurierten Workspace-URLs entspricht.
  - **Entspricht allen** —Erlaubt den Zugriff nur, wenn die eingehende Benutzerverbindung alle konfigurierten Workspace-URLs erfüllt.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie die Aktionen aus, die auf der Grundlage der Zustandsbewertung angewendet werden müssen.

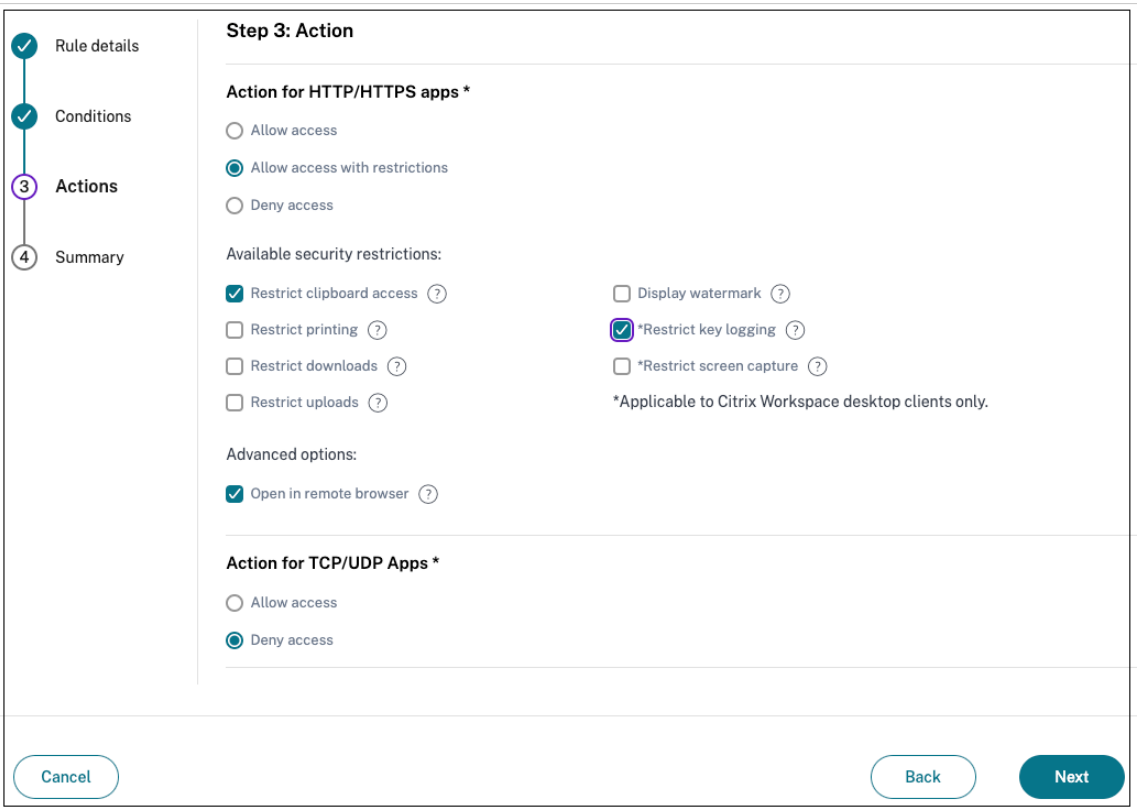
   - Für HTTP/HTTPS-Apps können Sie Folgendes auswählen:

     - **Zugriff erlauben**
     - **Zugriff mit Einschränkungen zulassen**
     - **Zugriff verweigern**

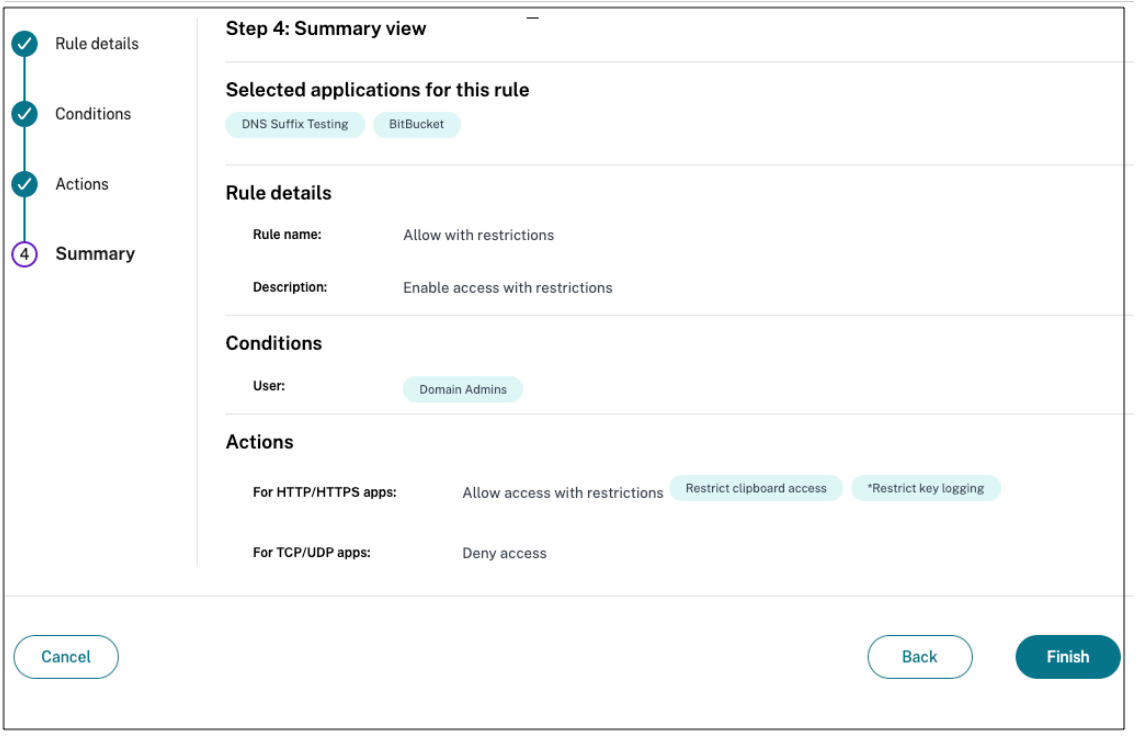
     > **Hinweis:**
     >
     > Wenn Sie **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie die Einschränkungen auswählen, die Sie für die Apps erzwingen möchten. Einzelheiten zu den Einschränkungen finden Sie unter Verfügbare Optionen für Zugriffsbeschränkungen . Sie können auch angeben, ob die App in einem Remote-Browser oder im Citrix Secure Browser geöffnet werden soll.

   - Für den TCP/UDP-Zugriff können Sie Folgendes auswählen:

     - **Zugriff erlauben**
     - **Zugriff verweigern**



10. Klicken Sie auf **Weiter**. Auf der Übersichtsseite werden die Richtliniendetails angezeigt.
11. Sie können die Details überprüfen und auf **Fertig stellen**klicken.



Punkte, die Sie sich nach der Erstellung einer Richtlinie merken sollten

- Die von Ihnen erstellte Richtlinie wird im Abschnitt Richtlinienregeln angezeigt und ist standardmäßig aktiviert. Sie können die Regeln bei Bedarf deaktivieren. Stellen Sie jedoch sicher, dass mindestens eine Regel aktiviert ist, damit die Richtlinie aktiv ist.
- Der Richtlinie ist standardmäßig eine Prioritätsreihenfolge zugewiesen. Die Priorität mit einem niedrigeren Wert hat die höchste Präferenz. Die Regel mit der niedrigsten Prioritätsnummer wird zuerst bewertet. Wenn die Regel (n) nicht den definierten Bedingungen entspricht, wird die nächste Regel (n+1) ausgewertet und so weiter.

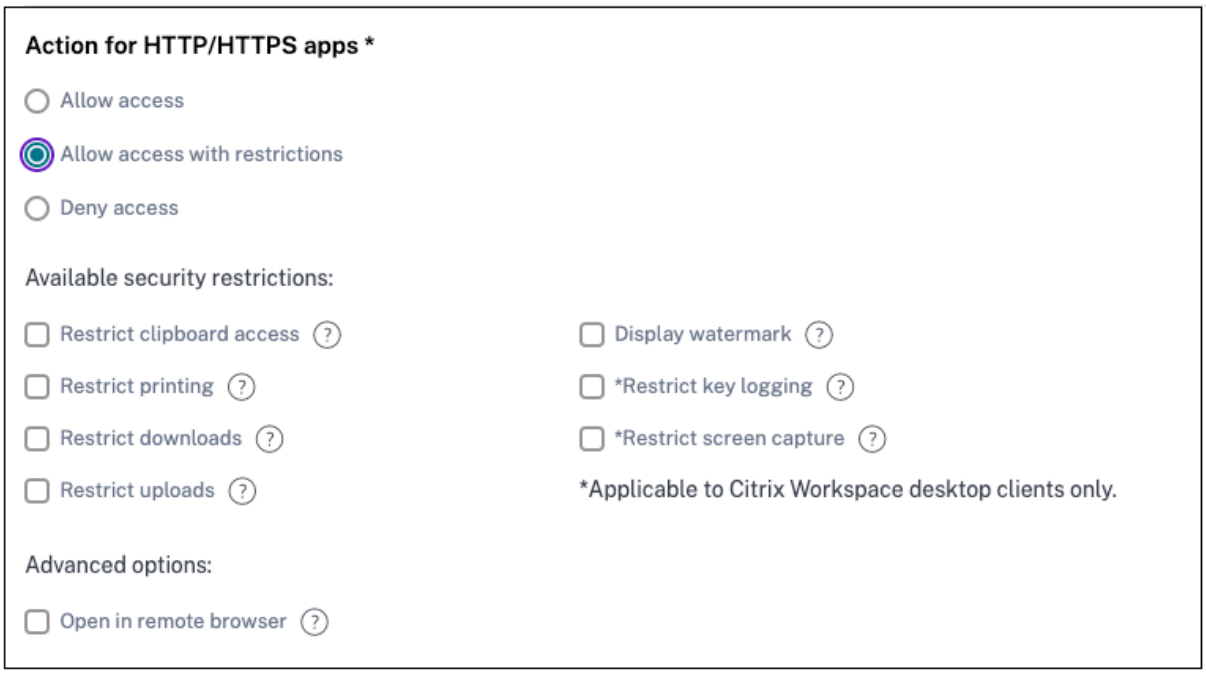
Beispiel für die Bewertung von Regeln mit Prioritätsreihenfolge:

Bedenken Sie, dass Sie zwei Regeln erstellt haben, Regel 1 und Regel 2.
Regel 1 wird Benutzer A zugewiesen und Regel 2 wird Benutzer B zugewiesen, dann werden beide Regeln ausgewertet.
Bedenken Sie, dass beide Regeln Regel 1 und Regel 2 dem Benutzer A zugewiesen sind. In diesem Fall hat Regel 1 die höhere Priorität. Wenn die Bedingung in Regel 1 erfüllt ist, wird Regel 1 angewendet und Regel 2 wird übersprungen. Andernfalls, wenn die Bedingung in Regel 1 nicht erfüllt ist, wird Regel 2 auf Benutzer A angewendet.

> **Hinweis:**
>
> Wenn keine der Regeln ausgewertet wird, wird die App für die Benutzer nicht aufgeführt.

Verfügbare Optionen für Zugriffsbeschränkungen

Wenn Sie die Aktion **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie mindestens eine der Sicherheitseinschränkungen auswählen. Diese Sicherheitseinschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen. Die folgenden Sicherheitseinschränkungen können für die Anwendung aktiviert werden.



- **Zugriff auf die Zwischenablage einschränken:**Deaktiviert Ausschneiden/Kopieren/Einfügen zwischen der App und der Systemzwischenablage.
- **Drucken einschränken:**Deaktiviert die Möglichkeit, im Citrix Enterprise Browser zu drucken.
- **Downloads einschränken:**Deaktiviert die Fähigkeit des Benutzers, von der App aus herunterzuladen.
- **Uploads einschränken:**Deaktiviert die Fähigkeit des Benutzers, innerhalb der App hochzuladen.
- **Wasserzeichen anzeigen:**Zeigt auf dem Bildschirm des Benutzers ein Wasserzeichen an, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt.
- **Key-Logging einschränken:**Schützt vor Keyloggern. Wenn ein Benutzer versucht, sich mit dem Benutzernamen und dem Kennwort bei der App anzumelden, werden alle Schlüssel auf den Keyloggern verschlüsselt. Außerdem sind alle Aktivitäten, die der Benutzer in der App ausführt, vor Key-Logging geschützt. Wenn beispielsweise App-Schutzrichtlinien für Office 365 aktiviert sind und der Benutzer ein Office 365-Word-Dokument bearbeitet, werden alle Tastenanschläge auf Keyloggern verschlüsselt.

- **Bildschirmaufnahme einschränken:**Deaktiviert die Möglichkeit, die Bildschirme mit einem der Bildschirmaufnahmeprogramme oder Apps aufzunehmen. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm aufgenommen.
- **Im Remote-Browser öffnen:**Öffnet die App im Citrix Remote Browser.
  - Wenn Sie **Im Remote-Browser öffnen** auswählen und die Remote-Browser-Kataloge für Secure Private Access fehlen, wird die folgende Meldung angezeigt:

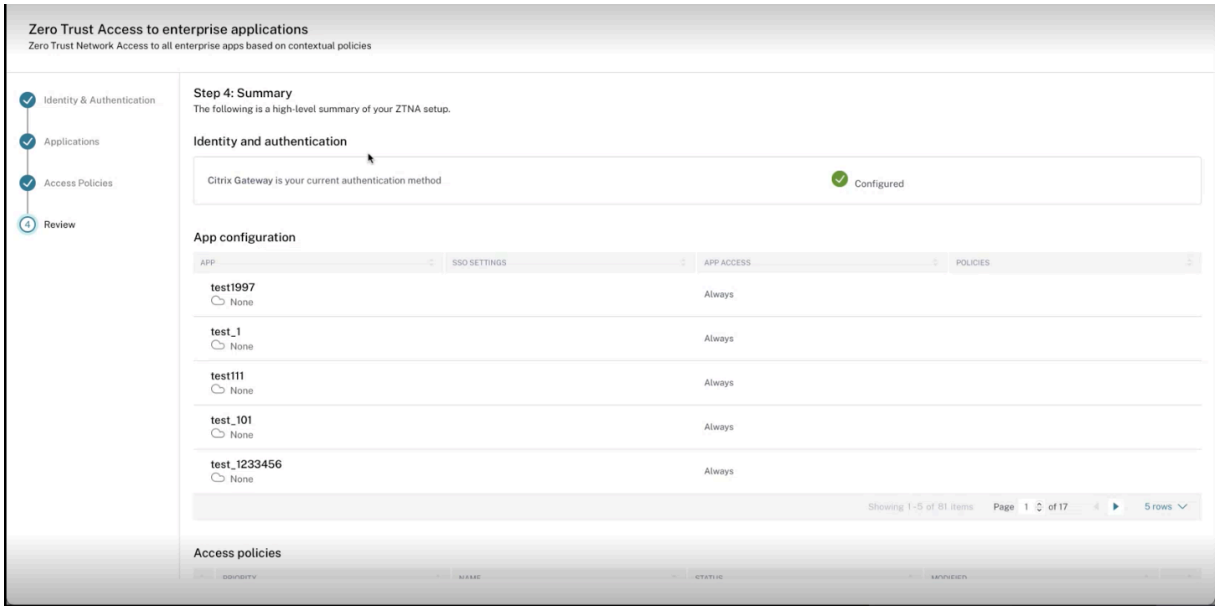
    Es ist kein veröffentlichter Remote-Isolationskatalog verfügbar, um diese Anwendung zu hosten. Rufen Sie die Remote Browser Isolation-Konsole auf, um den Katalog zu veröffentlichen.
  - Wenn Sie versuchen, eine Web- oder SaaS-App zu starten, schlägt der App-Start außerdem fehl, wenn die RBI-Kataloge fehlen und die folgende Meldung erscheint:

    Es wurden keine Kataloge erstellt, um diese Anfrage zu bearbeiten. Wenden Sie sich an den Administrator.

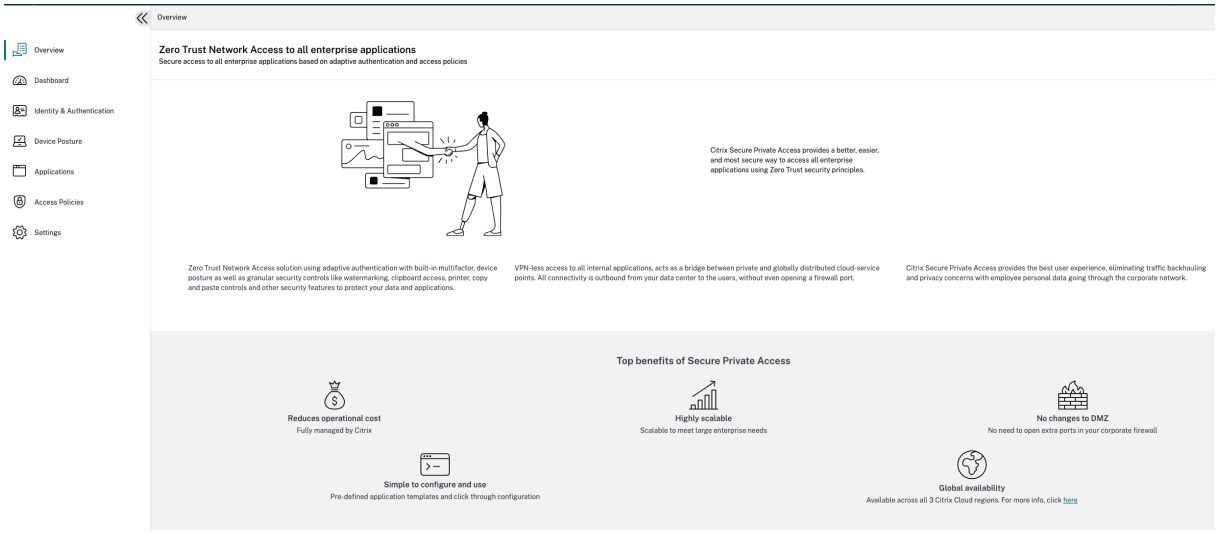
  Weitere Informationen zur Citrix Remotebrowser-Isolierung finden Sie unter Remote-Browser-Isolierung.

Schritt 4: Überprüfen Sie die Zusammenfassung jeder Konfiguration

Auf der Seite Überprüfen können Sie die vollständige App-Konfiguration anzeigen und dann auf **Schließen**klicken.

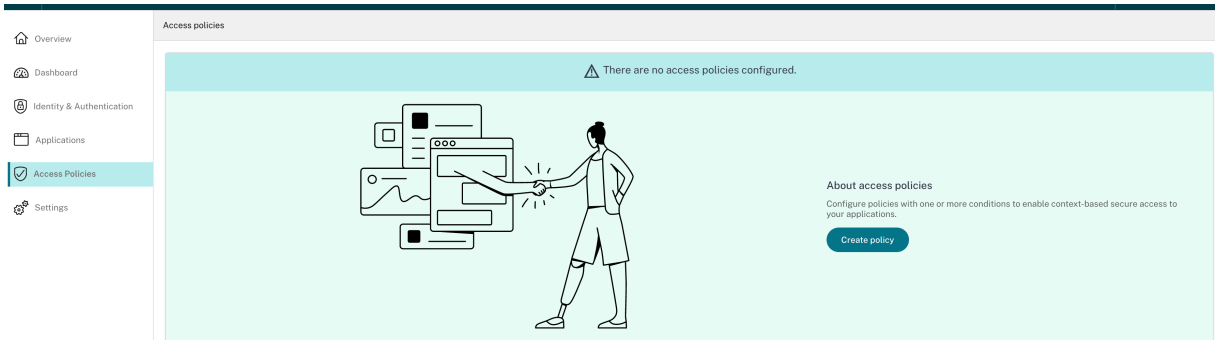


Die folgende Abbildung zeigt die Seite an, nachdem Sie die 4-stufige Konfiguration abgeschlossen haben.



Wichtig:

- Nachdem Sie die Konfiguration mit dem Assistenten abgeschlossen haben, können Sie die Konfiguration eines Abschnitts ändern, indem Sie direkt zu diesem Abschnitt gehen. Sie müssen die Reihenfolge nicht einhalten.
- Wenn Sie alle konfigurierten Apps oder Richtlinien löschen, müssen Sie sie erneut hinzufügen. In diesem Fall wird das folgende Fenster angezeigt, wenn Sie alle Richtlinien gelöscht haben.



Tool zur Politikmodellierung

June 19, 2024

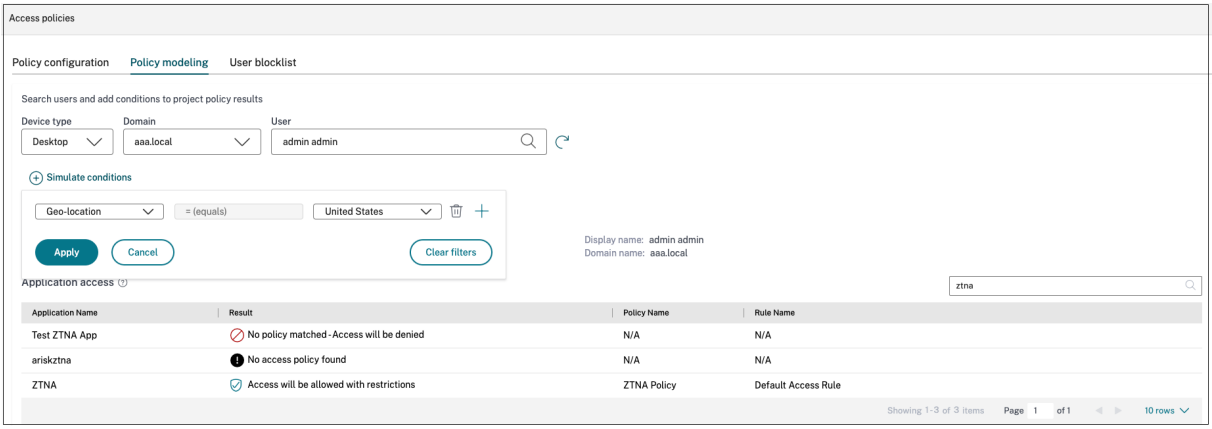
Administratoren können mehrere Richtlinien erstellen und diese Richtlinien mehreren Anwendungen zuweisen. Infolgedessen kann es für Administratoren schwierig werden, die Ergebnisse des Anwendungszugriffs für ihre Endbenutzer zu verstehen, d. h., ob dem Endbenutzer der Zugriff auf der Grundlage der Anwendungs- und Zugriffsrichtlinienkonfigurationen gewährt oder verweigert wird.

Das Tool zur Richtlinienmodellierung (**Zugriffsrichtlinien > Richtlinienmodellierung**) hilft bei der Lösung dieser Probleme, indem es den Administratoren einen vollständigen Überblick über das erwartete Ergebnis des Anwendungszugriffs (erlaubt/erlaubt mit Einschränkung/Verweigerung) bietet. Administratoren können die Zugriffsergebnisse für bestimmte Benutzer überprüfen und Benutzerbedingungen wie Gerätetyp, Gerätestatus, Geolocation, Netzwerkstandort, Benutzerrisikobewertung und Workspace-URL hinzufügen. Das Tool zeigt auch die Liste der Richtlinien und Regelnamen an, die den Anwendungen zugeordnet sind.

Gehen Sie wie folgt vor, um die Konfiguration der Zugriffsrichtlinie zu analysieren.

1. Klicken Sie in der Secure Private Access-Konsole auf **Zugriffsrichtlinien** und dann auf die Registerkarte **Richtlinienmodellierung** .
2. Fügen Sie die folgenden Details hinzu:
    - **Gerätetyp**: Wählen Sie den Gerätetyp des Endbenutzers aus. (Desktop ist standardmäßig ausgewählt.)
    - **Domain**: Wählen Sie die Domain aus, die dem Benutzer zugeordnet ist.
    - **Benutzer**: Wählen Sie den Benutzernamen aus, für den Sie die Anwendungen und die zugehörigen Richtlinien analysieren möchten.
3. Sie können auch eine Reihe von Bedingungen/Einschränkungen für den Endbenutzer und seine Geräte simulieren.
4. Klicken Sie auf **Bedingungen simulieren**.
5. Wählen Sie die Bedingung aus (Gerätestatus, Geolokalisierung, Netzwerkstandort, Risikobewertung des Benutzers und Workspace-URL) und wählen Sie dann den zugehörigen Wert aus.
6. Klicken Sie auf das **Pluszeichen** , um zusätzliche Bedingungen hinzuzufügen.
7. Klicken Sie auf **Anwenden**.

Die Anwendungen, zugehörigen Richtlinien und Regeln für den ausgewählten Benutzer werden in tabellarischer Form angezeigt.



Dashboard-Übersicht

June 19, 2024

Das Secure Private Access Service Access-Dienst-Dashboard zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Das Dashboard bietet Administratoren einen vollständigen Überblick über ihre Apps, Benutzer, Konnektoren, den Gesundheitszustand und die Bandbreitennutzung an einem einzigen Ort für den Verbrauch. Diese Daten werden von Citrix Analytics abgerufen. Die Daten für die verschiedenen Entitäten können für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitleiste angezeigt werden. Für einige der Entitäten können Sie einen Drilldown durchführen, um weitere Details anzuzeigen.

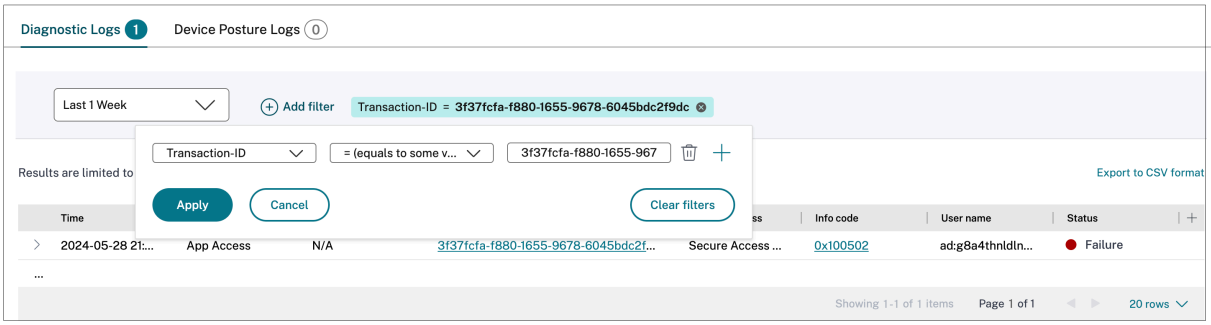
Die Kennzahlen sind grob in die folgenden Kategorien unterteilt.

- **Protokollierung und Problembehandlung**
  - Diagnoseprotokolle: Protokolle im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Aufzählung und Gerätezustandsprüfungen.
- **Benutzer**
  - Aktive Benutzer: Gesamtzahl der eindeutigen Benutzer, die für das ausgewählte Zeitintervall auf die Anwendungen (SaaS, Web und TCP) zugreifen.
  - Uploads: Das gesamte Datenvolumen, das über den Secure Private Access Service für das ausgewählte Zeitintervall hochgeladen wurde.
  - Downloads: Gesamtvolumen der Daten, die über den Secure Private Access Service für das ausgewählte Zeitintervall heruntergeladen wurden.
- **Anwendungen:**
  - Anwendungen: Gesamtzahl der aktuell konfigurierten Anwendungen (unabhängig vom Zeitintervall).
  - Anzahl der Anwendungsstarts: Gesamtzahl der Anwendungen (App-Sitzungen), die von jedem Benutzer für das ausgewählte Zeitintervall gestartet wurden.
  - Konfigurierte Domänen: Gesamtzahl der für das ausgewählte Zeitintervall konfigurierten Domänen.
  - Entdeckte Anwendungen: Gesamtzahl der eindeutigen, individuellen Domänen, auf die zugegriffen wurde, die aber keiner App zugeordnet sind
- **Richtlinien für den Zugriff**
  - Zugriffsrichtlinien: Gesamtzahl der aktuell konfigurierten Zugriffsrichtlinien (unabhängig vom Zeitintervall).

Diagnoseprotokolle

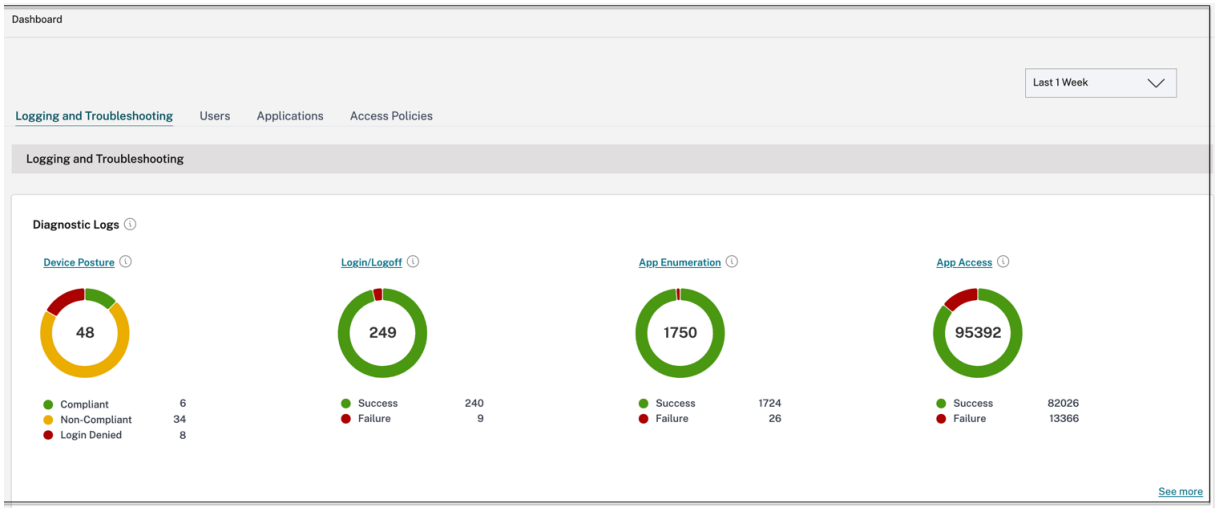
Verwenden Sie das Diagramm mit den **Diagnoseprotokollen**, um die Protokolle zur Authentifizierung, zum Anwendungsstart, zur App-Aufzählung sowie zur Geräteposition anzuzeigen. Sie können auf den Link **Weitere Informationen** klicken, um die Details der Protokolle anzuzeigen. Die Details werden in einem tabellarischen Format dargestellt. Sie können die Protokolle für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitleiste anzeigen. Sie können dem Diagramm Spalten hinzufügen, indem Sie auf das Pluszeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerprotokolle in das CSV-Format exportieren.

- Sie können die Option **Filter hinzufügen** verwenden, um Ihre Suche anhand der verschiedenen Kriterien wie App-Typ, Kategorie, Beschreibung usw. zu verfeinern. Beispielsweise können Sie in den Suchfeldern diese Reihenfolge auswählen und eingeben `Transaction ID=(equals to some value)7456c0fb-a60d-4bb9-a2a2-edab8340bb15`, um nach allen Protokollen zu suchen, die sich auf diese Transaktions-ID beziehen. Einzelheiten zu Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.

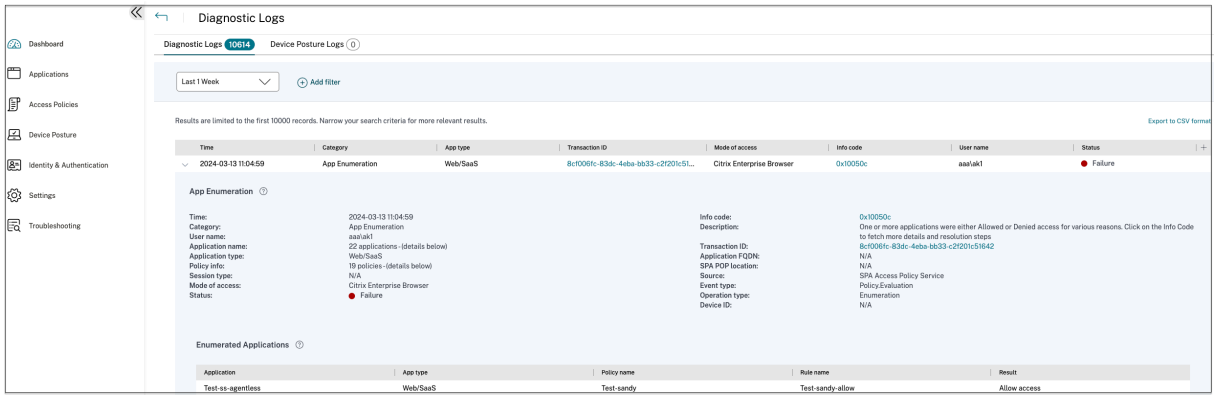


- **Protokolle zum Gerätestatus:** Sie können Ihre Suche anhand der Richtlinienergebnisse verfeinern (**konform, nicht konform und Anmeldung verweigert**). Einzelheiten zum Gerätestatus finden Sie unter Gerätestatus.

> **Hinweis:**
>
> - Jedem Fehlerereignis im Dashboard der Secure Private Access-Diagnoseprotokolle ist ein Infocode zugeordnet. Einzelheiten finden Sie unter Infocode.
> - Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanfrage. Einzelheiten finden Sie unter Transaktions-ID.



- Sie können auf das Erweiterungssymbol (>) klicken, um die vollständigen Details der Protokolle anzuzeigen.
- Auf der Seite "**Diagnoseprotokolle** "werden die eingebetteten Domänen für jede der Haupt-URLs angezeigt, auf die zugegriffen wird. Administratoren können die eingebetteten Domains einsehen, indem sie in der Haupt-URL auf das Erweiterungssymbol (>) klicken. Administratoren können die Liste der eingebetteten Domains verwenden, um Probleme im Zusammenhang mit dem App-Zugriff oder dem App-Rendern zu lösen. Wenn beispielsweise eine Domain in der Anwendungskonfiguration fehlt, kann der Endbenutzer nicht auf die jeweilige App zugreifen. In diesem Fall kann der Administrator die Liste der eingebetteten Domains einsehen, die fehlende Domain identifizieren und dann die App-Konfiguration mit der fehlenden Domain aktualisieren.

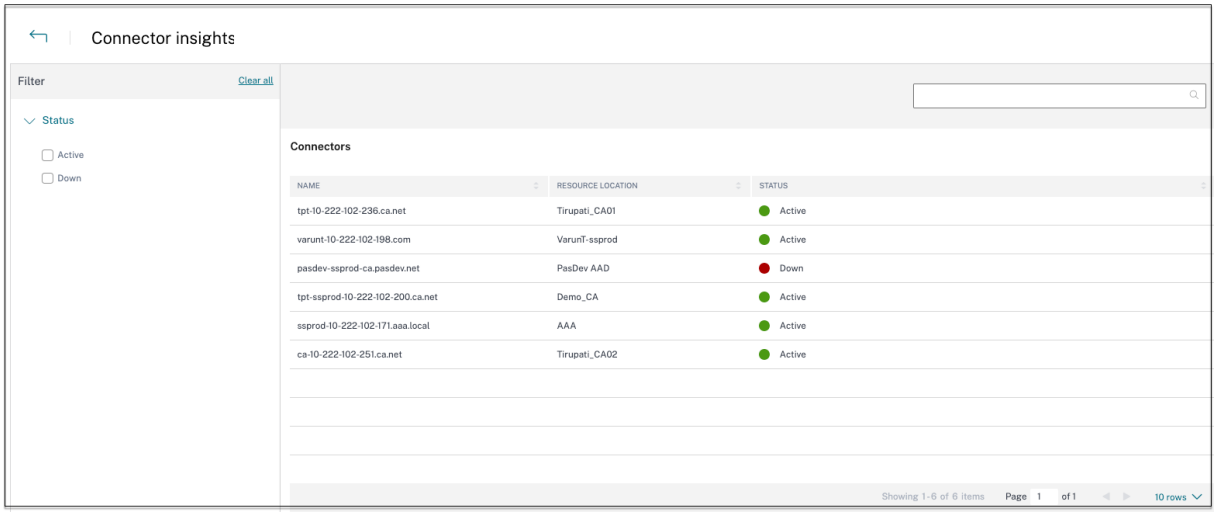


Hinweis:

- Standardmäßig werden auf der Seite "**Diagnoseprotokolle** "die Daten der aktuellen Woche und nur die letzten 10.000 Datensätze angezeigt. Verwenden Sie die benutzerdefinierte Datumssuche und Filter, um Ihre Suchergebnisse weiter zu verfeinern.

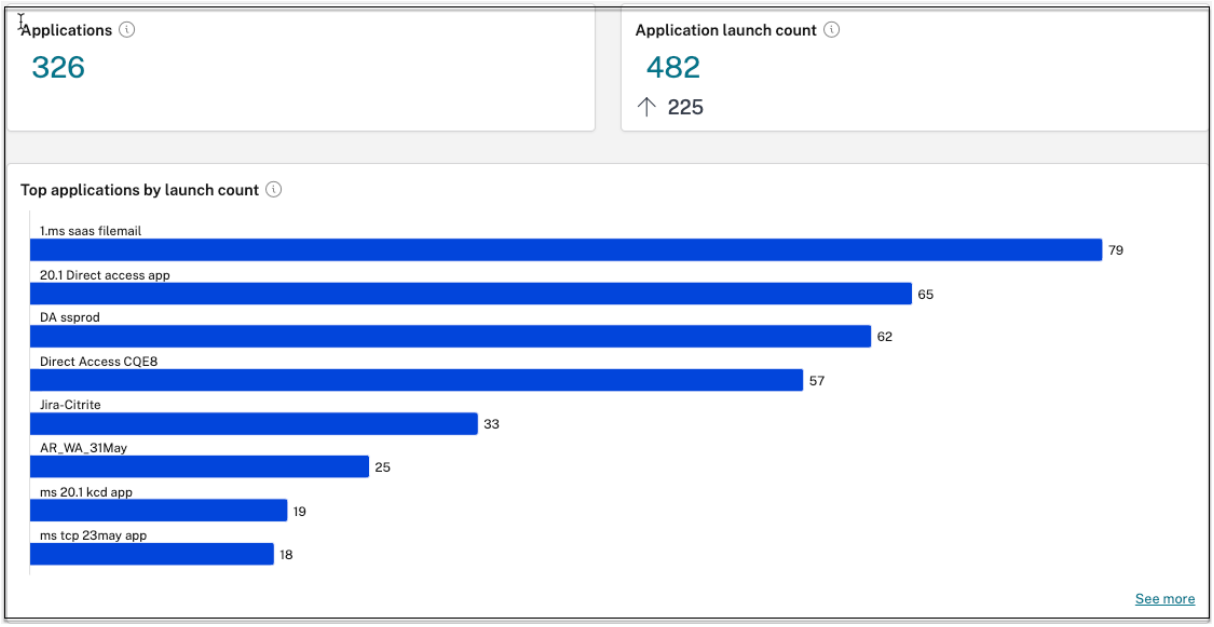
Connector-Status

Verwenden Sie das **Connector-Statusdiagramm**, um den Status der Connectors und die Ressourcenstandorte anzuzeigen, an denen die Connectors bereitgestellt werden. Klicken Sie auf den Link **Weitere** Informationen, um die Details anzuzeigen. Auf der Seite **Connector-Insights** können Sie die Filter **Aktiv** oder **Inaktiv** verwenden, um die Connectors nach ihrem Status zu filtern.



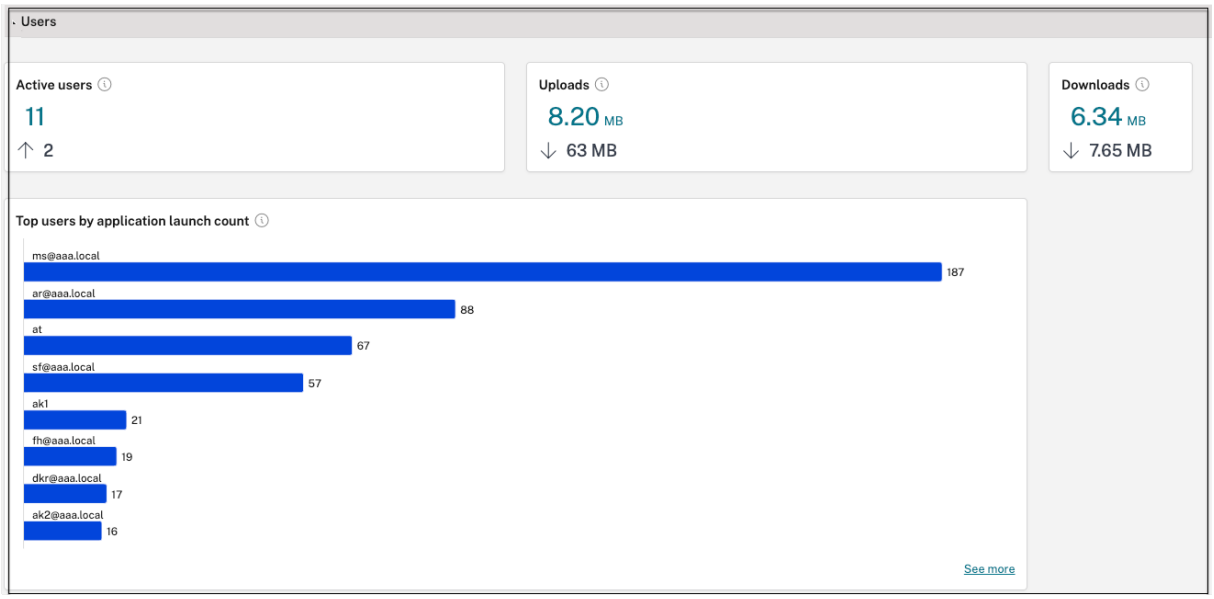
Top-Anwendungen nach Anzahl der Starts

Verwenden Sie das Diagramm **Häufigste Anwendungen nach Anzahl der Starts**, um die Liste der häufigsten Anwendungen anzuzeigen, basierend auf der Häufigkeit, mit der die App gestartet wurde, dem Gesamtvolumen der auf den App-Server hochgeladenen Daten und dem Gesamtvolumen der vom App-Server heruntergeladenen Daten. Sie können die Filter **SaaS-Apps**, **Web-Apps**oder **TCP/UDP-Apps** anwenden, um Ihre Suche auf bestimmte Apps einzugrenzen. Sie können die Daten nach einer voreingestellten Zeitleiste oder nach einer benutzerdefinierten Zeitleiste filtern.



Top-Benutzer nach Anzahl der Anwendungsstarts

Verwenden Sie das Diagramm mit der **Top-Benutzer nach Anzahl der Anwendungsstarts**, um die Daten pro Benutzer anzuzeigen. Zum Beispiel die Häufigkeit, mit der ein Benutzer die TCP-App gestartet hat, das Gesamtvolumen der auf den App-Server hochgeladenen Daten und das Gesamtvolumen der vom App-Server heruntergeladenen Daten. Sie können die Daten nach einer voreingestellten Zeitleiste oder nach einer benutzerdefinierten Zeitleiste filtern.

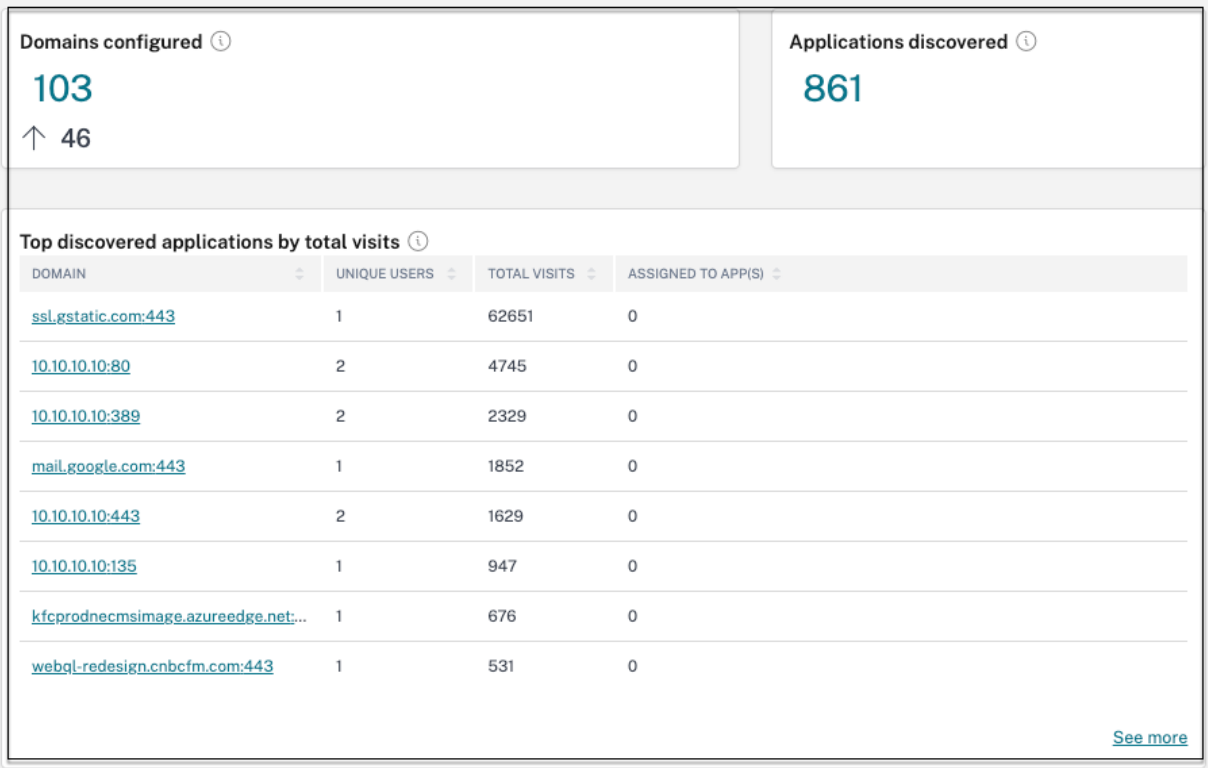


Top-Zugriffsrichtlinien nach Durchsetzung

Verwenden Sie das Diagramm **Top-Zugriffsrichtlinien nach Durchsetzung**, um die Liste der Zugriffsrichtlinien anzuzeigen, die für die Apps durchgesetzt werden. Klicken Sie auf den Link **Weitere** anzeigen, um die Liste der Richtlinien anzuzeigen, die mit den Apps verknüpft sind, sowie die Häufigkeit, mit der die Richtlinien durchgesetzt werden. Sie können auch die **Suchoption** auf der Seite Zugriffsrichtlinien verwenden, um die Richtlinien basierend auf dem Richtliniennamen zu filtern. Sie können auch mithilfe der Suchoperatoren nach bestimmten Richtlinien suchen, um Ihre Suche weiter zu verfeinern. Einzelheiten finden Sie unter Suchoperatoren.

Am häufigsten entdeckte Anwendungen

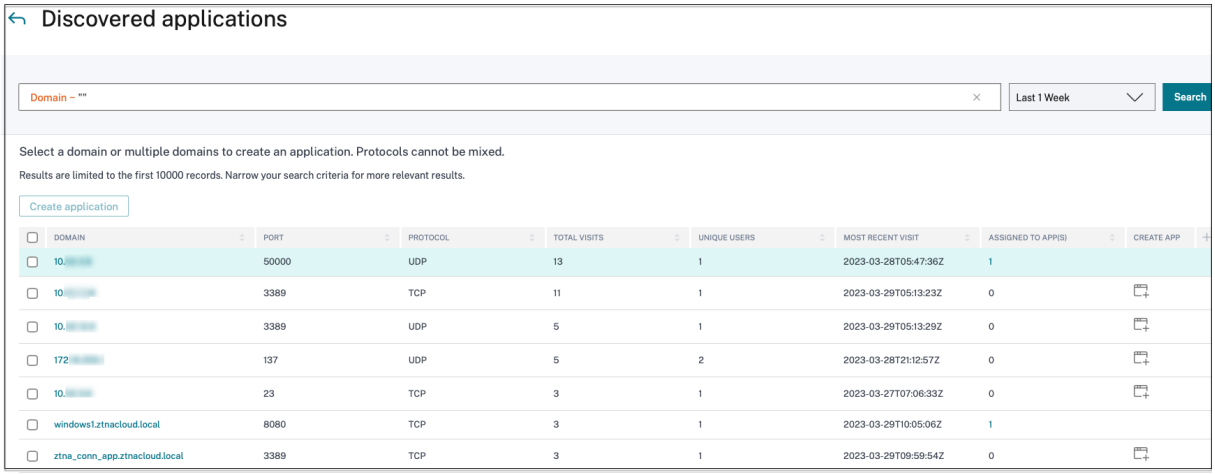
Verwenden Sie das **Diagramm "Häufigste entdeckte Anwendungen nach Gesamtzahl der Besuche** ", um die Liste der eindeutigen, individuellen Domains anzuzeigen, auf die zu einem bestimmten Zeitpunkt zugegriffen wurde, die jedoch mit keiner App verknüpft sind. Diese Domains werden auf der Grundlage der Gesamtzahl der Besuche dieser Domains aufgelistet. Administratoren können dieses Diagramm verwenden, um zu sehen, ob eine Domain von besonderem Interesse von vielen Benutzern aufgerufen wird. In solchen Fällen können Administratoren eine App mit dieser Domain erstellen, um den Zugriff zu erleichtern.



Im Diagramm wird in der Spalte **APPs ZUGEWIESEN** die Gesamtzahl der Anwendungen angezeigt, für die diese Domain als Teil ihrer zugehörigen URL- oder Ziel-URL-Werte konfiguriert ist. Wenn Sie auf

die Zahl klicken, werden die Apps angezeigt, die dieser Domain zugewiesen sind.

Sie können auf den Link **Mehr** anzeigen klicken, um weitere Informationen zu allen Domains zu erhalten.



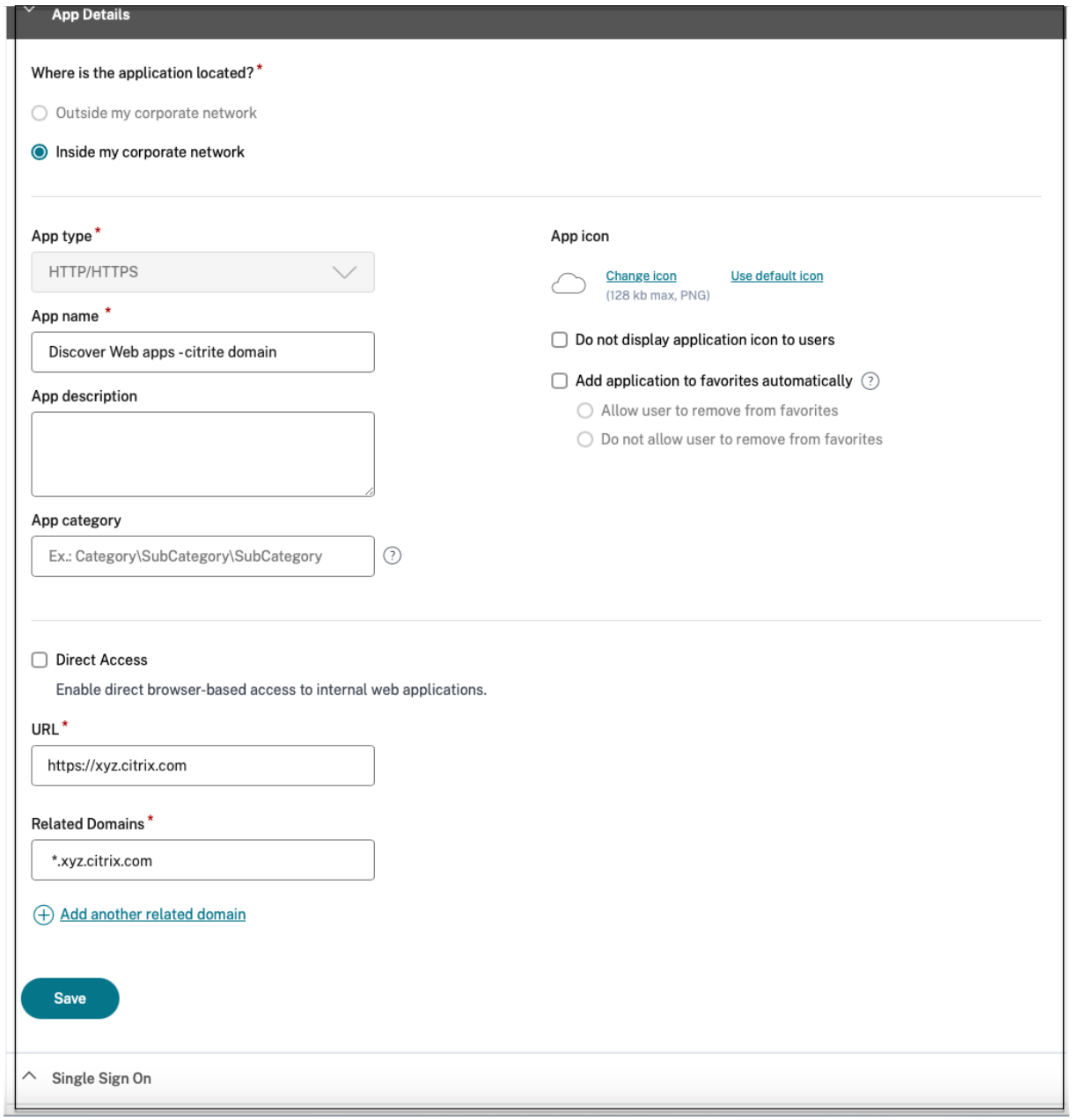
Auf der Seite Entdeckte **Anwendungen** werden die Details der Domänen wie Domainname, Port, Protokoll, Gesamtzahl der Besuche, einzelne Benutzer und das Datum des letzten Besuchs angezeigt. Alle Spalten im Diagramm sind sortierbar. Sie können die Suchleiste verwenden, um anhand einer Domain zu suchen.

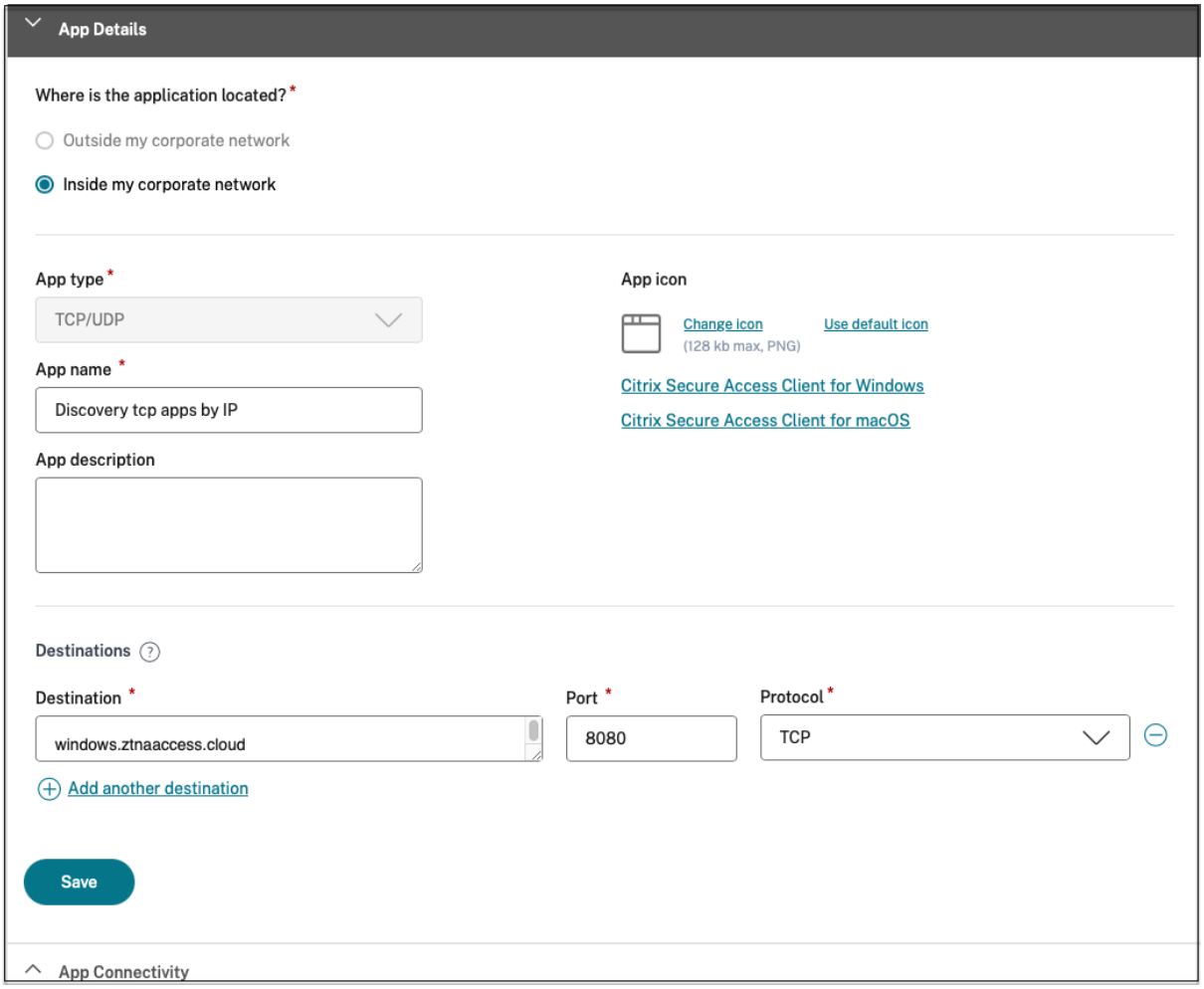
> **Hinweis:**
>
> - Die Protokolle werden auf der Grundlage der von Kunden verwendeten Standardports abgeleitet.
> - Die Liste der entdeckten Domänen ist auf 10000 Datensätze begrenzt.

Eine App aus dem Diagramm erstellen

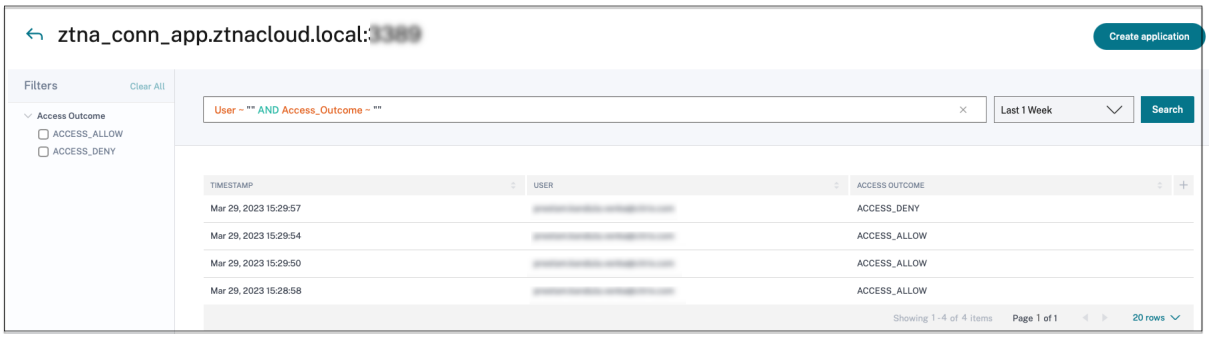
Klicken Sie auf das **+-Symbol** neben der jeweiligen Domain, um eine App zu erstellen. Der Assistent zur App-Konfiguration wird angezeigt. Das Symbol “App erstellen“wird nicht für die Zeilen angezeigt, in denen eine App bereits mit derselben Kombination aus Domäne, Port und Protokoll erstellt wurde und sich im Status “Vollständig“befindet.

- Der App-Typ wird basierend auf dem von Ihnen ausgewählten App-Protokoll automatisch ausgefüllt. Sie können den Typ jedoch bei Bedarf ändern.
- Die Werte in den Feldern **URL, Verwandte Domänen, Ziel, Port und Protokoll** werden alle automatisch ausgefüllt. Gehen Sie wie folgt vor, um eine App hinzuzufügen. Einzelheiten finden Sie unter Vom Administrator geführter Arbeitsablauf für einfaches Onboarding und Einrichtung.





Sie können auch auf den Link zur eindeutigen Domain klicken, um weitere Details zu sehen und einen Antrag für diese Domain zu erstellen. Wenn Sie auf einen Domain-Link klicken, werden die Benutzerauthentifizierungsprotokolle für die Domain angezeigt. Klicken Sie auf die Schaltfläche **Anwendung erstellen** . Gehen Sie wie folgt vor, um eine App hinzuzufügen.



Suchoperatoren

Die folgenden Suchoperatoren können Sie verwenden, um Ihre Suche zu verfeinern:

- **= (entspricht einem bestimmten Wert): Um**nach den Protokollen/Richtlinien zu suchen, die genau den Suchkriterien entsprechen.
- **! = (entspricht nicht einem bestimmten Wert)**: Um nach Protokollen/Richtlinien zu suchen, die die angegebenen Kriterien nicht enthalten.
- **~ (enthält einen Wert): Um nach den Protokollen/Richtlinien zu suchen, die den Suchkriterien teilweise**entsprechen.
- **! ~ (enthält keinen Wert)**: Um nach Protokollen/Richtlinien zu suchen, die einige der angegebenen Kriterien nicht enthalten.

Anwendungserkennung

December 27, 2023

Mit der Funktion zur Anwendungserkennung erhält ein Administrator einen Überblick über die internen privaten Anwendungen wie Web-Apps und Client-Server-Apps (TCP- und UDP-basierte Apps) in seiner Organisation und über die Benutzer, die auf diese Anwendungen zugreifen. Administratoren können die Apps entdecken, indem sie den Gültigkeitsbereich der Domänen (Wildcard-Domains) oder IP-Subnetze angeben. Um die App-Discovery-Funktion im Citrix Secure Private Access-Dienst zu aktivieren, müssen Administratoren die Subnetze oder die Wildcard-Domänen oder beide konfigurieren, innerhalb derer Anwendungen und Benutzerzugriffe erkannt und gemeldet werden müssen. Administratoren verwenden den Anwendungskonfigurationsworkflow, um die breiten Subnetze und Platzhalterdomänen zu definieren und denselben Workflow für Anwendungszugriffsrichtlinien durchzuführen, der für alle Anwendungsdefinitionskonfigurationen verwendet wird.

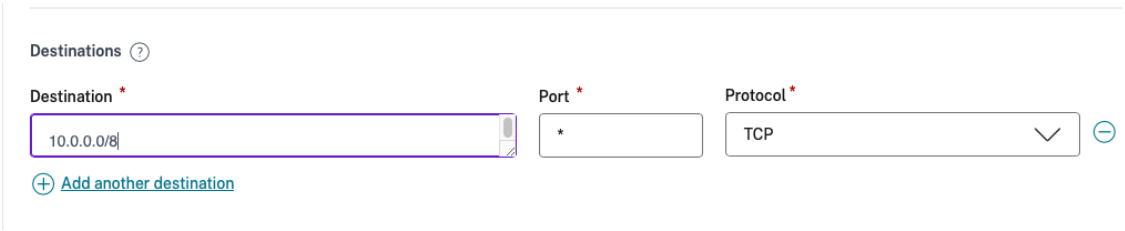
Anwendungserkennung konfigurieren

Die Anwendungserkennung kann auf eine der folgenden Arten erfolgen:

- Konfigurieren Sie das System so, dass die genauen IP-Adressen, Ziele und Ports, die auf TCP/UDP basieren, überwacht und gemeldet werden.

  Geben Sie das Subnetz zusammen mit dem TCP/UDP-Protokoll und dem Portbereich an (geben Sie * ein, um den gesamten Bereich einzubeziehen). Auf diese Weise können alle TCP- und UDP-Apps vom Secure Access Agent aus erkannt werden.

  Beispiel: 10.0.0.0/8: TCP: Port (*)



- Konfigurieren Sie das System so, dass die Hostnamen oder vollqualifizierten Domänen (FQDNs) oder beides für die Apps, auf die über das TCP- oder UDP-Protokoll zugegriffen wird, überwacht und gemeldet werden.

  Geben Sie die Wildcard-Domain an, die zu den Web-Apps gehört, die überwacht und gemeldet werden müssen.

  Beispiel:`*.citrix.com : TCP : Port (*)`

- Konfigurieren Sie das System so, dass es die vollqualifizierten Domänen (FQDNs) überwacht und protokolliert, auf die über den Citrix Enterprise Browser zugegriffen werden kann.

  Geben Sie mindestens einen FQDN für eine Web-App an, die zu der Domain oder Subdomain gehört, innerhalb der Sie interne Web-Apps entdecken möchten. Konfigurieren Sie die zugehörige Domain so, dass sie die Wildcard-Domain enthält, zu der die App gehört.

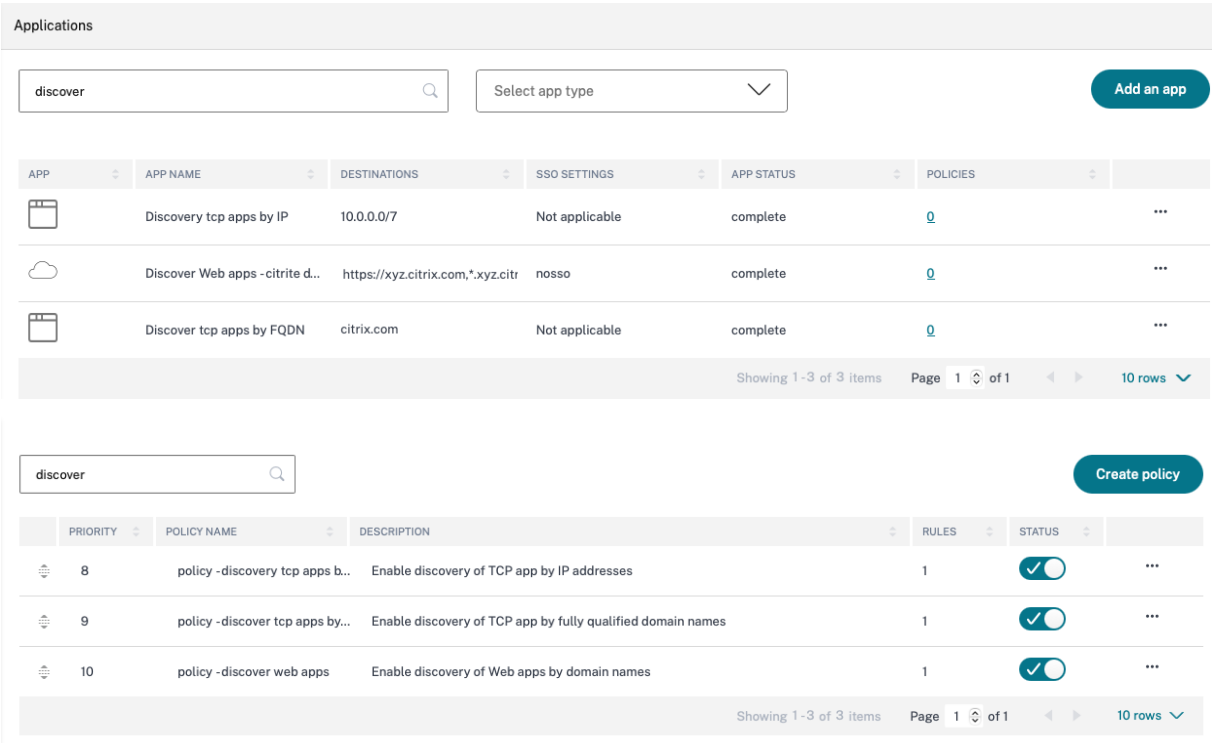
  Beispiel:

  URL der Web-App: `https://test.citrix.com/`

  Verwandte Domain: *.citrix.com

Wichtig:

- Neben der Erstellung der Apps müssen Sie auch Benutzer definieren, denen der Zugriff auf Apps mit den konfigurierten Domänen und IP-Subnetzen gestattet ist. Dies dient dazu, unbefugten oder versehentlichen Zugriff durch andere Benutzergruppen zu verhindern, die sich außerhalb der zulässigen Benutzergruppen befinden.
- Fügen Sie dem App-Namen das Präfix **Discover** hinzu, um anzuzeigen, dass es sich um eine spezielle App-Konfiguration handelt, die die Überwachung und Berichterstattung von Entdeckungen ermöglicht. Diese Benennung hilft Ihnen dabei, die Platzhalterdomänen oder IP-Subnetze oder beides zu identifizieren oder zu entfernen, sodass Sie die gesamte App-Zugriffszone später in Wochen oder einem Monat auf nur die spezifischen FQDNs und IP/Port-Kombinationen reduzieren können.



Nach dem Erstellen der Anwendungen und der entsprechenden Zugriffsrichtlinien können Benutzer weiterhin über die Citrix Workspace-App auf Anwendungen zugreifen und auf verschiedene Domänen zugreifen. Für den Zugriff auf TCP/UDP-Apps müssen Benutzer den Citrix Secure Access Agent verwenden. Der App-Zugriff über verschiedene Zugriffsmethoden wird auf der Grundlage der Domänen- und Subnetzkonfiguration der Apps überwacht und in den Dashboards gemeldet.

Konfiguration und Verwaltung von Apps

December 27, 2023

Die Bereitstellung von Apps mithilfe des Citrix Secure Private Access Access-Dienstes bietet Ihnen eine einfache, sichere, robuste und skalierbare Lösung zur Verwaltung der Apps. In der Cloud bereitgestellte Apps haben folgende Vorteile:

- Einfache Konfiguration: einfach zu bedienen, zu aktualisieren und zu nutzen.
- Single Sign-On —Problemlose Anmeldung mit Single Sign-On.
- Standardvorlage für verschiedene SaaS-Apps —Vorlagenbasierte Konfiguration beliebter Apps. Diese Vorlagen füllen viele der für die Konfiguration von Anwendungen erforderlichen Informationen vorab aus. Nur die kundenspezifischen Informationen müssen weiterhin zur Verfügung gestellt werden.

Unterstützung für unternehmenseigene Web-Apps

June 19, 2024

Durch die Bereitstellung von Web-Apps mithilfe des Secure Private Access Service können unternehmensspezifische Anwendungen remote als webbasierter Dienst bereitgestellt werden. Häufig verwendete Web-Apps sind SharePoint, Confluence, OneBug und so weiter.

Auf Web-Apps kann mit Citrix Workspace mit dem Secure Private Access-Dienst zugegriffen werden. Der Secure Private Access-Dienst in Verbindung mit Citrix Workspace bietet eine einheitliche Benutzererfahrung für die konfigurierten Web-Apps, SaaS-Apps, konfigurierten virtuellen Apps oder andere Workspace-Ressourcen.

SSO und Remote-Zugriff auf Web-Apps sind als Teil der folgenden Servicepakete verfügbar:

- Secure Private Access Standard
- Secure Private Access Advanced

Systemanforderungen

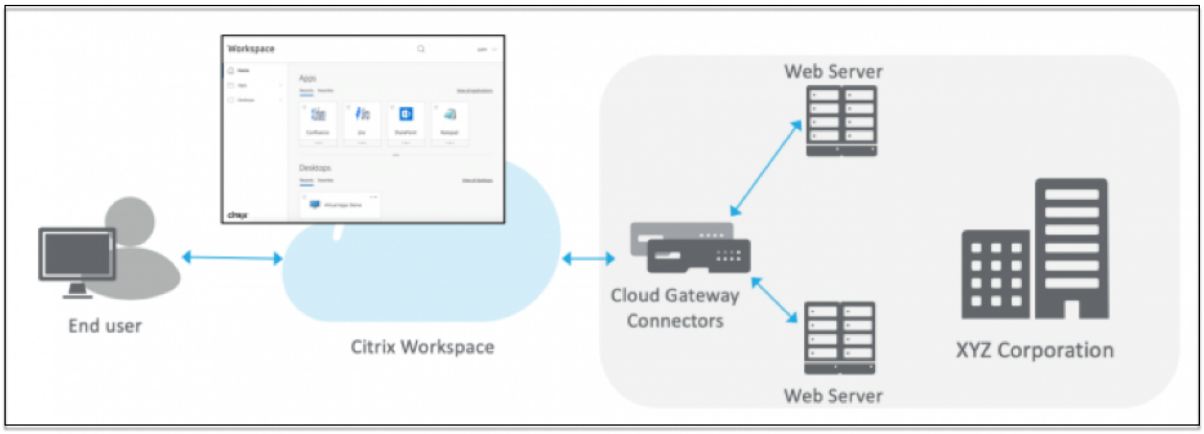
Connector Appliance —Verwenden Sie die Connector Appliance mit dem Citrix Secure Private Access Service, um den VPN-freien Zugriff auf die Enterprise Web-Apps im Rechenzentrum des Kunden zu unterstützen. Einzelheiten finden Sie unter Secure Workspace Access mit Connector Appliance.

Funktionsweise

Der Citrix Secure Private Access Service stellt mithilfe des Connectors, der on-premises bereitgestellt wird, eine sichere Verbindung zum on-premises Rechenzentrum her. Dieser Connector dient als Brücke zwischen on-premises bereitgestellten Enterprise-Web-Apps und dem Citrix Secure Private Access Service. Diese Connectors können in einem HA-Paar bereitgestellt werden und erfordern nur eine ausgehende Verbindung.

Eine TLS-Verbindung zwischen der Connector Appliance und dem Citrix Secure Private Access-Dienst in der Cloud schützt die lokalen Anwendungen, die im Cloud-Dienst aufgeführt sind. Auf Webanwendungen wird über Workspace über eine VPN-Verbindung zugegriffen und bereitgestellt.

Die folgende Abbildung zeigt den Zugriff auf Webanwendungen mit Citrix Workspace.



Web-App konfigurieren

Die Konfiguration einer Web-App umfasst die folgenden allgemeinen Schritte.

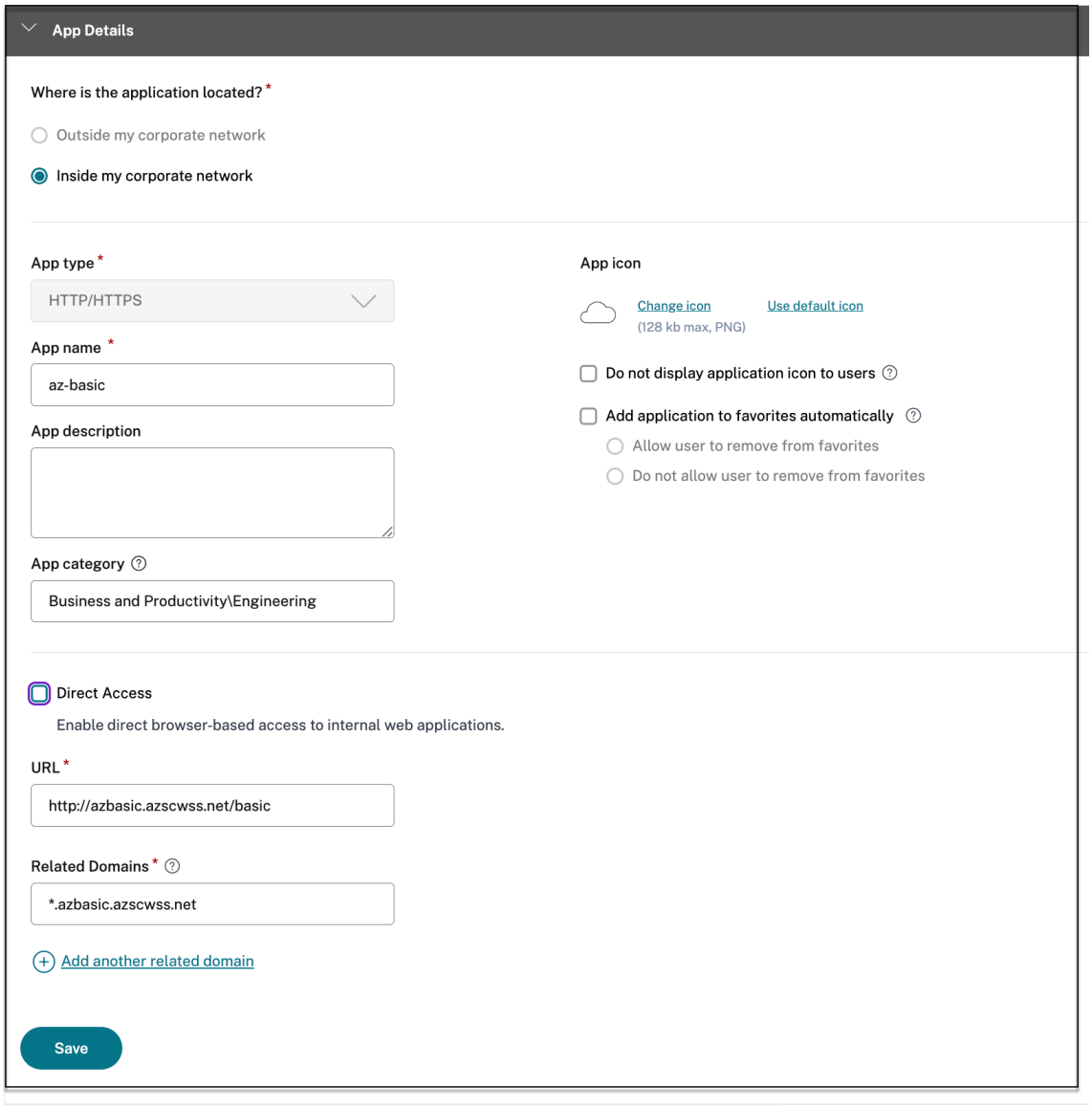
1. Konfigurieren Sie die Anwendungsdetails
2. Stellen Sie die bevorzugte Anmeldemethode ein
3. Anwendungsrouting definieren

Anwendungsdetails konfigurieren

1. Klicken Sie auf der Kachel **Secure Private Access** auf **Verwalten.**
2. Klicken Sie auf der Landingpage von Secure Private Access auf **Weiter** und dann auf **App hinzufügen**.

   > **Hinweis:**
   >
   > Die Schaltfläche **Weiter** wird nur angezeigt, wenn Sie den Assistenten zum ersten Mal verwenden. Bei den nachfolgenden Verwendungen können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen**klicken.

3. Wählen Sie die App aus, die Sie hinzufügen möchten, und klicken Sie auf **Überspringen.**
4. In **Wo ist die Anwendung?**, wählen Sie den Standort aus.
5. Geben Sie im Abschnitt **App-Details die folgenden Details** ein und klicken Sie auf **Weiter.**

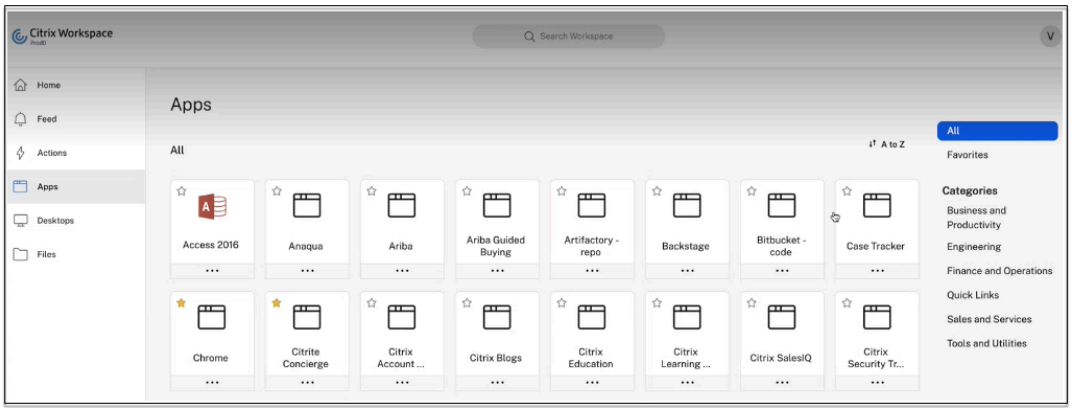


- **App-Typ** —Wählen Sie den App-Typ aus. Sie können zwischen **HTTP/HTTPS** - oder **UDP/TCP-Apps** wählen.
- **Appname** —Name der Anwendung.
- **App-Beschreibung** —Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Workspace angezeigt.
- **App-Kategorie** —Fügen Sie die Kategorie und den Namen der Unterkategorie (falls zutreffend) hinzu, unter denen die App, die Sie veröffentlichen, in der Citrix Workspace-Benutzeroberfläche erscheinen muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien über die Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angegeben haben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie

angezeigt.

- Die Kategorie/Unterkategorien sind vom Administrator konfigurierbar und Admins können für jede App eine neue Kategorie hinzufügen.
- Das Feld **App-Kategorie** gilt für HTTP/HTTPS-Apps und ist für TCP/UDP-Apps ausgeblendet.
- Die Namen der Kategorie/Unterkategorien müssen durch einen Backslash getrennt werden. Zum Beispiel **Business And Productivity\ Engineering** . Außerdem unterscheidet dieses Feld zwischen Groß- und Kleinschreibung. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn der Name in der Citrix Workspace-Benutzeroberfläche nicht mit dem im Feld **App-Kategorie eingegebenen Kategorienamen** übereinstimmt, wird die Kategorie als neue Kategorie aufgeführt.

  Wenn Sie beispielsweise die Kategorie **Geschäft und Produktivität** falsch als **Geschäft und Produktivität** in das Feld **App-Kategorie** eingeben, wird in der Citrix Workspace Workspace-Benutzeroberfläche zusätzlich zur Kategorie **Geschäft und Produktivität** eine neue Kategorie mit dem Namen **Geschäft und Produktivität** aufgeführt.



- **App-Symbol** —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Icon-Datei muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

  Wenn Sie das App-Symbol nicht anzeigen möchten, wählen Sie **Anwendungssymbol nicht für Benutzer anzeigen aus.**

- Wählen Sie **Direktzugriff**, damit Benutzer direkt von einem Client-Browser aus auf die App zugreifen können. Einzelheiten finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.
- **URL** —URL mit Ihrer Kunden-ID. Die URL muss Ihre Kunden-ID (Citrix Cloud-Kunden-ID) enthalten. Informationen zum Abrufen Ihrer Kunden-ID finden Sie unter Anmelden für Citrix Cloud. Falls SSO fehlschlägt oder Sie SSO nicht verwenden möchten, wird der Benutzer

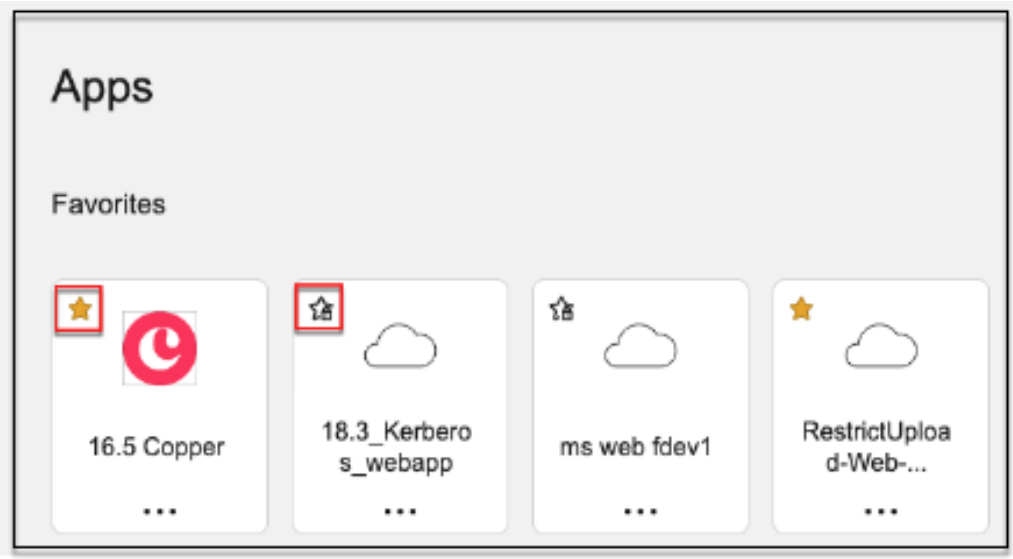
zu dieser URL umgeleitet.

Kundendomänenname und **Kundendomänen-ID** - Der Domänenname und die ID des Kunden werden verwendet, um die App-URL und andere nachfolgende URLs auf der SAML-SSO-Seite zu erstellen.

Wenn Sie beispielsweise eine Salesforce-Anwendung hinzufügen, Ihr Domänenname `salesforceformyorg` und die ID 123754 sind, dann lautet die Anwendungs-URL `https://salesforceformyorg.my.salesforce.com/?so=123754`.

Die Felder "Kundendomänenname"und "Kunden-ID"sind spezifisch für bestimmte Apps.

- **Verwandte Domains** —Die zugehörige Domain wird basierend auf der von Ihnen angegebenen URL automatisch ausgefüllt. Verwandte Domain hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domain hinzufügen.
- Klicken Sie auf **Anwendung automatisch zu Favoriten hinzufügen**, um diese App als Lieblings-App in der Citrix Workspace-App hinzuzufügen.
  - Klicken Sie auf **Allow user to remove from favorites**, um App-Abonnenten zu ermöglichen, die App aus der Favoriten-Liste der Apps in der Citrix Workspace-App zu entfernen. Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein gelber Stern angezeigt.
  - Klicken Sie auf **Do not allow user to remove from favorites**, um zu verhindern, dass Abonnenten die App aus der Favoritenliste der Citrix Workspace-App entfernen. Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein Sternsymbol mit einem Vorhängeschloss angezeigt.



Wenn Sie die als Favoriten markierten Apps aus der Secure Private Access Service-

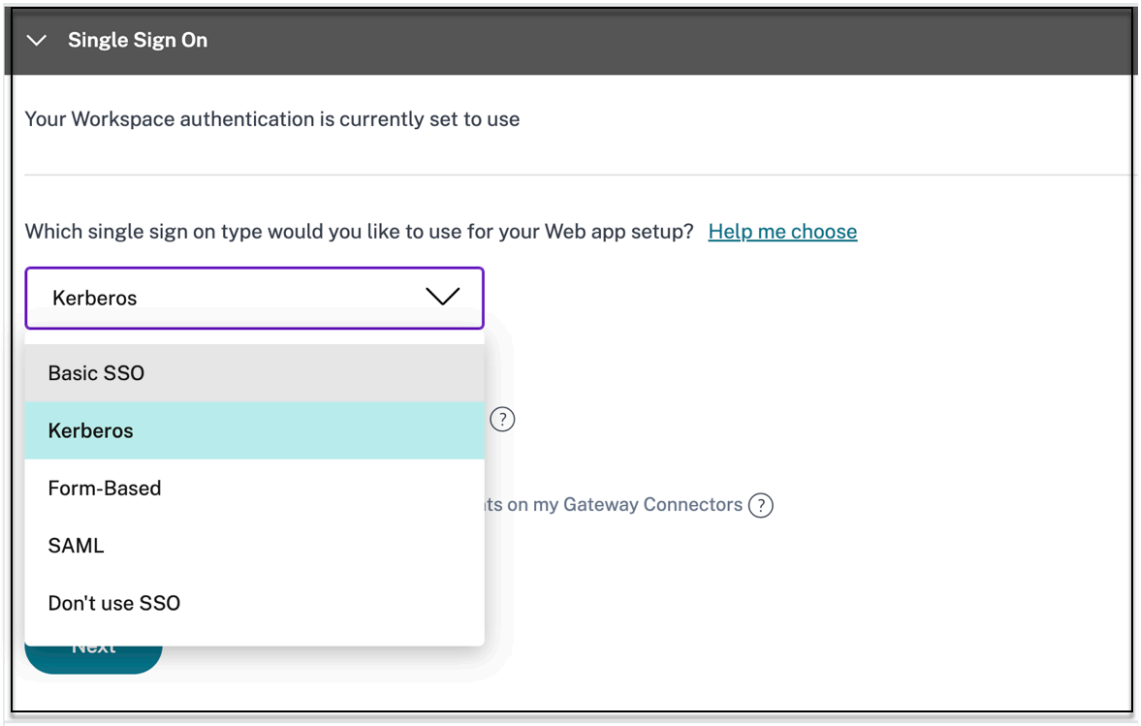
Konsole entfernen, müssen diese Apps manuell aus der Favoritenliste in Citrix Workspace entfernt werden. Die Apps werden nicht automatisch aus der Workspace-App gelöscht, wenn sie aus der Secure Private Access Service Access-Servicekonsole entfernt werden.

6. Klicken Sie auf **Weiter.**

> **Wichtig:**
>
> - Um den Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps ist nur aktiviert, wenn der Anwendung eine Zugriffsrichtlinie zugeordnet ist. Einzelheiten zum Erstellen von Zugriffsrichtlinien finden Sie unter Zugriffsrichtlinien erstellen.
> - Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, kann dies zu einer widersprüchlichen Konfiguration führen. Informationen zur Vermeidung von Konfigurationskonflikten finden Sie unter Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen.

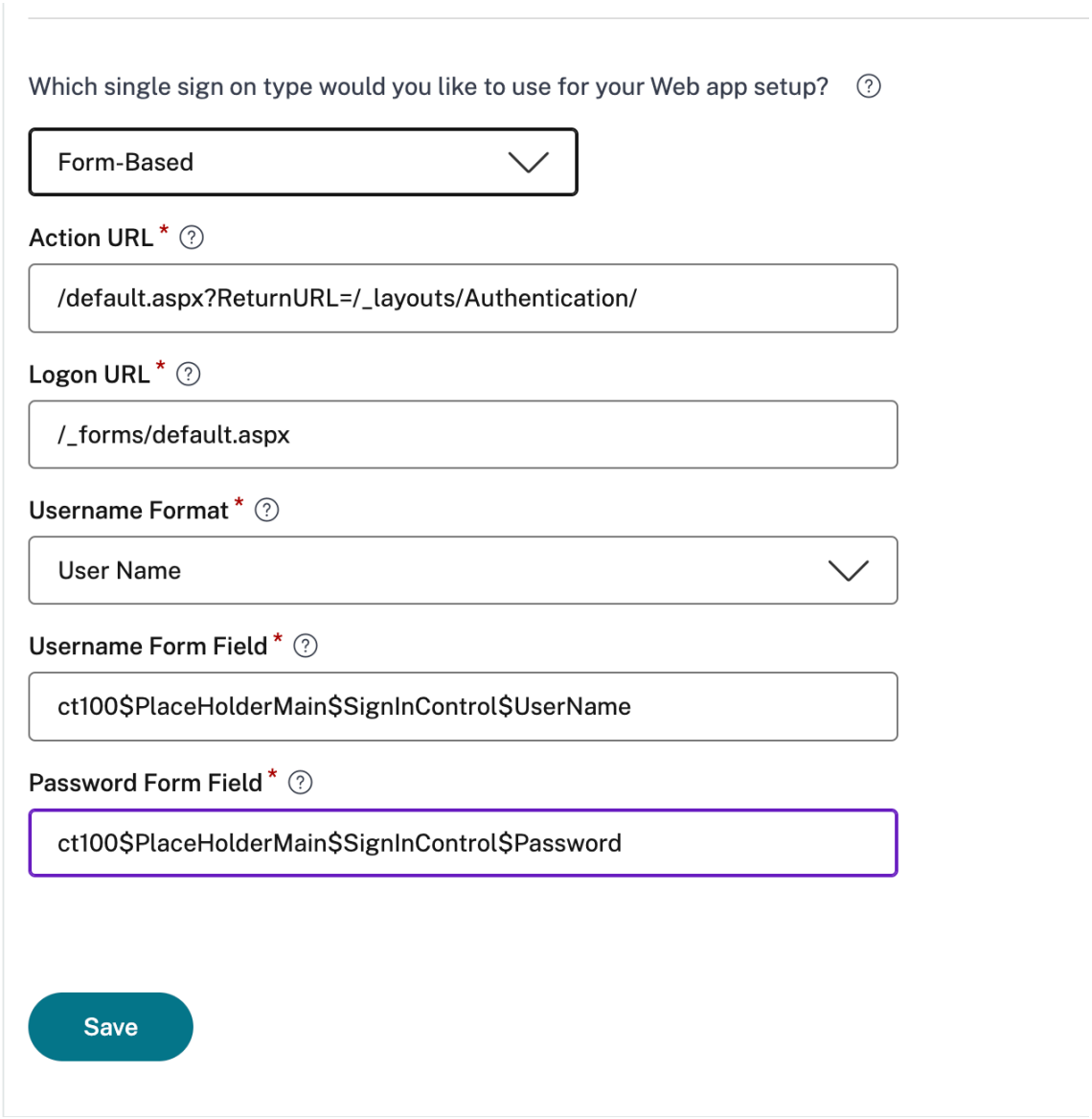
Stellen Sie die bevorzugte Anmeldemethode ein

1. Wählen Sie im Abschnitt **Single Sign On** Ihren bevorzugten Single Sign-On-Typ aus, der für Ihre Anwendung verwendet werden soll, und klicken Sie auf **Speichern**. Die folgenden Single-Sign-On-Typen sind verfügbar.



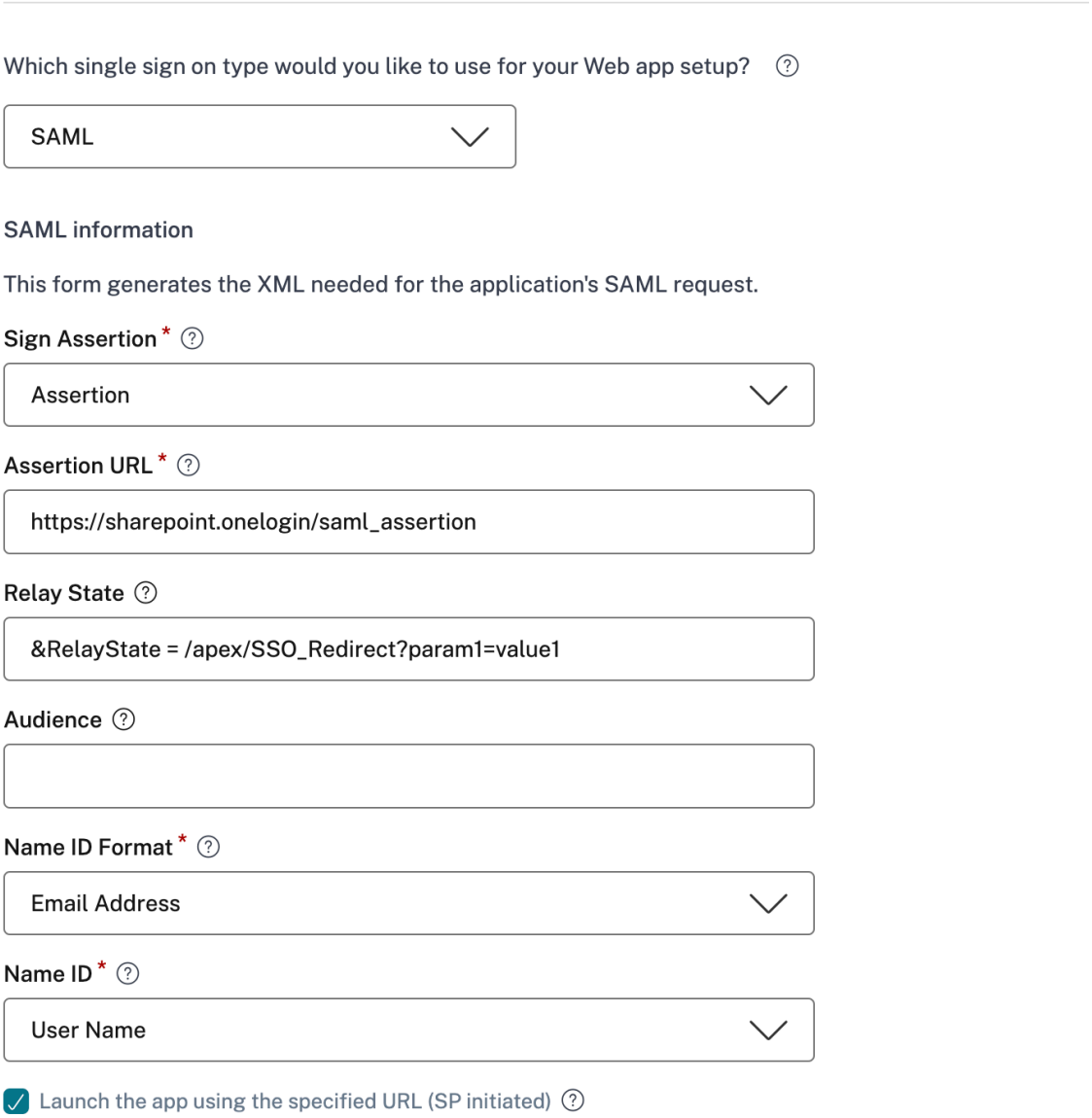
- **Basic** —Wenn Ihr Back-End-Server Ihnen eine Basic-401-Herausforderung stellt, wählen Sie **Basic SSO** . Sie müssen keine Konfigurationsdetails für den **Basis-SSO** Typ angeben.
- **Kerberos** —Wenn Ihr Back-End-Server Ihnen die negotiate-401 Challenge präsentiert, wählen Sie **Kerberos**. Sie müssen keine Konfigurationsdetails für den **Kerberos-SSO** Typ angeben.
- **Formularbasiert** —Wenn Ihr Backend-Server Ihnen ein HTML-Formular zur Authentifizierung präsentiert, wählen Sie **Formularbasiert** . Geben Sie die Konfigurationsdetails für den Typ "**Formularbasiertes** SSO"ein.
- **SAML** - Wählen Sie **SAML** für SAML-basiertes SSO in Webanwendungen. Geben Sie die Konfigurationsdetails für den **SAML**-SSO-Typ ein.
- **SSO nicht verwenden** —Verwenden Sie die Option **SSO nicht verwenden**, wenn Sie keinen Benutzer auf dem Backend-Server authentifizieren müssen. Wenn die Option "**SSO nicht verwenden** "ausgewählt ist, wird der Benutzer zu der im Abschnitt "**App-Details** "konfigurierten URL weitergeleitet.

Formularbasierte Details: Geben Sie im Abschnitt Single Sign On die folgenden formularbasierten Konfigurationsdetails ein und klicken Sie auf Speichern.



- **Aktions-URL** - Geben Sie die URL ein, an die das ausgefüllte Formular gesendet wird.
- **Anmeldeformular-URL** —Geben Sie die URL ein, auf der das Anmeldeformular angezeigt wird.
- **Benutzername-Format** - Wählen Sie ein Format für den Benutzernamen aus.
- **Formularfeld für Benutzernamen** —Geben Sie ein Benutzernamen-Attribut ein
- **Formularfeld Kennwort** —Geben Sie ein Kennwortattribut ein.

SAML: Geben Sie im Abschnitt Anmeldung die folgenden Details ein und klicken Sie auf Speichern.



- **Assertion signieren** - Das Signieren der Assertion oder Antwort gewährleistet die Integrität der Nachricht, wenn die Antwort oder Assertion an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Response, Both** oder **None** auswählen.
- **Assertion-URL** —Assertion-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.
- **Relay State** —Der Relay State-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die die Benutzer zugreifen, nachdem sie angemeldet und an den Verbundserver der vertrauenden Partei weitergeleitet wurden. Relay-Status generiert eine einzelne URL für die Benutzer. Benutzer können auf diese URL klicken, um sich bei der Zielanwendung anzumelden.
- **Zielgruppe** —Die Zielgruppe wird vom Anwendungsanbieter bereitgestellt. Dieser Wert

bestätigt, dass die SAML-Assertion für die richtige Anwendung generiert wurde.

- **Namens-ID-Format** —Wählen Sie das unterstützte Format für Namensbezeichner
- **Name-ID** —Wählen Sie die unterstützte Namen-ID aus.

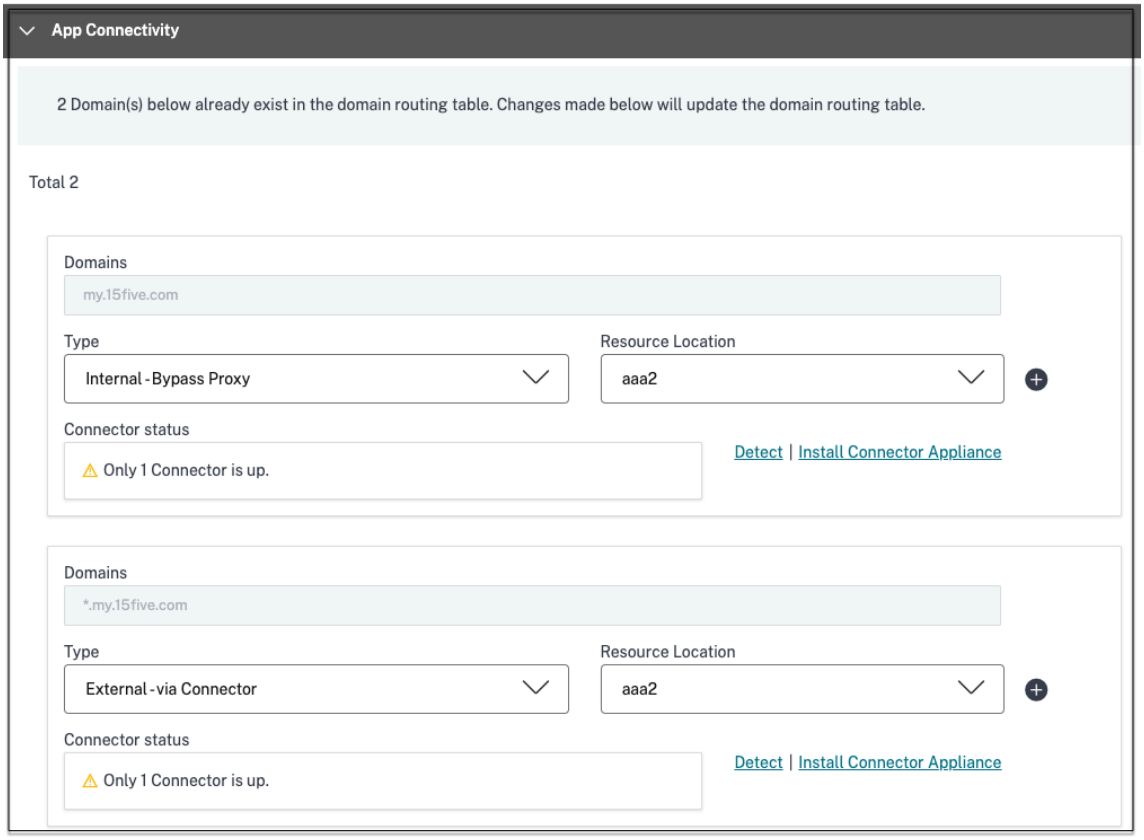
2. Fügen Sie unter **Erweiterte Attribute (optional)**zusätzliche Informationen über den Benutzer hinzu, die für Zugriffskontrollentscheidungen an die Anwendung gesendet werden.
3. Laden Sie die Metadatendatei herunter, indem Sie auf den Link unter **SAML-Metadaten**klicken. Verwenden Sie die heruntergeladene Metadatendatei, um SSO auf dem SaaS-Apps-Server zu konfigurieren.

> **Hinweis:**
>
> - Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.
> - Sie können das Zertifikat auch aus der **Zertifikatsliste** herunterladen und das Zertifikat verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.

4. Klicken Sie auf **Weiter.**

Anwendungsrouting definieren

1. Im Abschnitt **App Connectivity** definieren Sie das Routing für die zugehörigen Anwendungsdomänen, wenn die Domänen extern oder intern über das Citrix Connector Appliance weitergeleitet werden müssen. Einzelheiten finden Sie unter Weiterleiten von Tabellen zur Lösung von Konflikten, wenn die zugehörigen Domänen sowohl in SaaS als auch in Web-Apps identisch sind.

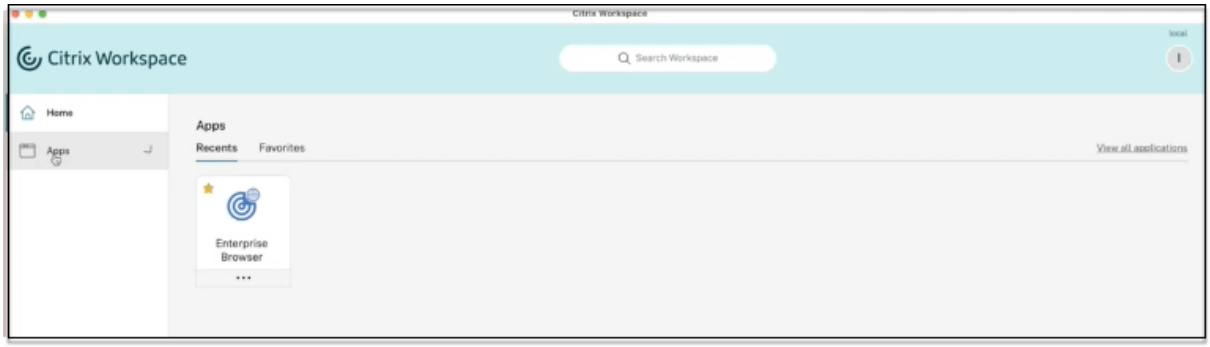


2. Klicken Sie auf **Fertig stellen.**

   Nachdem Sie auf **Fertig stellen**geklickt haben, wird die App zur Seite Anwendungen hinzugefügt. Sie können eine App auf der Seite “Anwendungen“bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu in einer App auf die Ellipsenschaltfläche und wählen Sie die Aktionen entsprechend aus.

   - **Anwendung bearbeiten**
   - **Löschen**

Wenn Sie eine Web- oder SaaS-App über den Secure Private Access Service veröffentlichen und diese App nicht ausgeblendet ist, wird die Citrix Enterprise Browser App automatisch in der Citrix Workspace-Benutzeroberfläche angezeigt. Darüber hinaus wird der Citrix Enterprise Browser standardmäßig als Lieblings-App hinzugefügt. Endbenutzer können den Workspace-Browser ohne URL starten und mit den Workspace-Browsern auf interne Websites zugreifen.



Wichtig:

- Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

Connector-Appliance für sicheren privaten Zugriff

June 21, 2024

Das Connectorgerät ist eine Citrix-Komponente, die in Ihrem Hypervisor gehostet wird. Es dient als Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten und ermöglicht die Cloudverwaltung ohne komplexe Netzwerk- oder Infrastrukturkonfiguration. Durch das Connectorgerät können Sie sich ganz auf die Ressourcen konzentrieren, die Ihren Benutzern einen Mehrwert bieten.

Alle Verbindungen werden vom Connectorgerät zur Cloud über den HTTPS-Standardport (443) und per TCP-Protokoll hergestellt. Es werden keine eingehenden Verbindungen akzeptiert. TCP-Port 443, mit den folgenden FQDNs sind ausgehend erlaubt:

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

Secure Private Access mit Connector-Appliance konfigurieren

1. Installieren Sie zwei oder mehr Connector-Appliances an Ihrem Ressourcenstandort.

   Weitere Informationen zum Einrichten von Connectorgeräten finden Sie unter Connectorgerät für Cloudservices.

2. Um Secure Private Access für die Verbindung mit on-premises Web-Apps mithilfe von KCD zu konfigurieren, konfigurieren Sie KCD, indem Sie die folgenden Schritte ausführen:

   a) Verbinden Sie Ihr Connectorgerät mit einer Active Directory-Domäne.

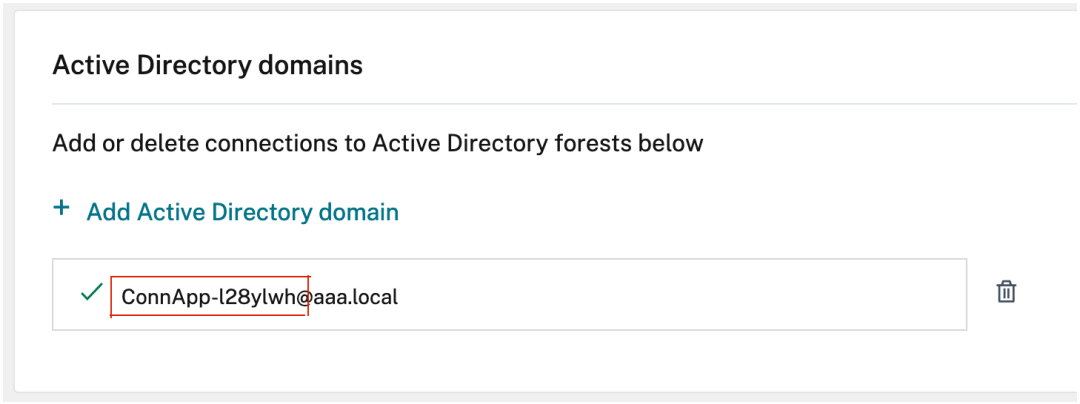
      Durch den Beitritt zu einer Active Directory-Gesamtstruktur können Sie die eingeschränkte Kerberos-Delegierung (KCD) bei der Konfiguration von Secure Private Access verwenden. Identitätsanforderungen oder Authentifizierung zur Verwendung des Connectorgeräts werden jedoch nicht aktiviert.

      - Stellen Sie in Ihrem Browser über die in der Connector Appliance-Konsole angegebene IP-Adresse eine Verbindung zur Connector Appliance-Verwaltungsseite her.
      - Klicken Sie im Abschnitt **Active Directory-Domänen** auf **+ Active Directory-Domäne hinzufügen**.

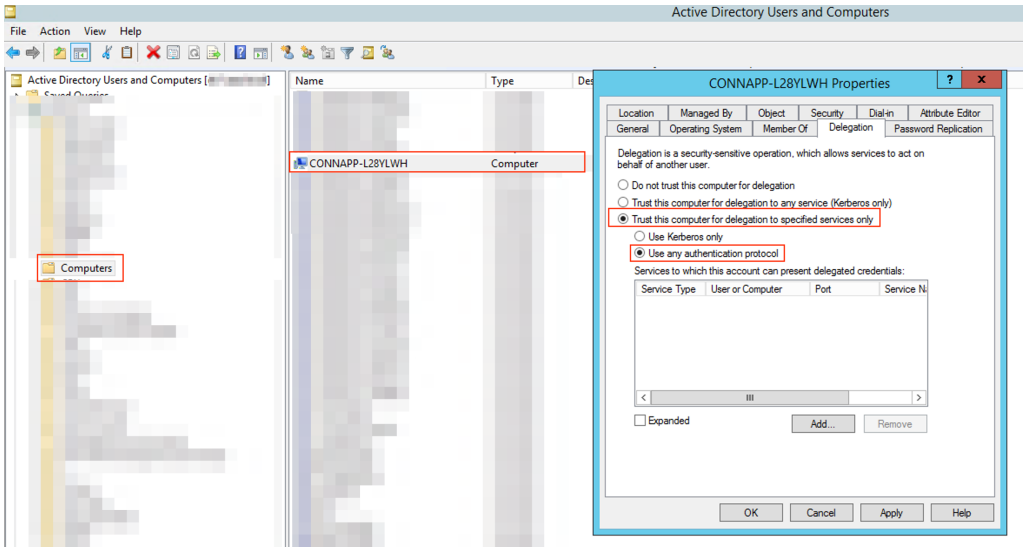
        Wenn Ihre Verwaltungsseite keinen Abschnitt **Active Directory-Domänen** enthält, wenden Sie sich an Citrix, um die Registrierung für die Preview anzufordern.
      - Geben Sie den Domänennamen in das Feld **Domänenname** ein. Klicken Sie auf **Hinzufügen**.
      - Die Connector Appliance überprüft die Domäne. Wenn die Prüfung erfolgreich ist, wird das Dialogfeld **Active Directory beitreten** geöffnet.
      - Geben Sie den Benutzernamen und das Kennwort eines Active Directory-Benutzers ein, der über eine Beitrittsberechtigung für diese Domäne verfügt.
      - Die Connector Appliance schlägt einen Maschinennamen vor. Sie können den vorgeschlagenen Namen überschreiben und Ihren eigenen Maschinennamen mit einer Länge von bis zu 15 Zeichen angeben. Notieren Sie sich den Namen des Maschinenkontos.

        Dieser Maschinenname wird in der Active Directory-Domäne erstellt, wenn die Connector Appliance beitritt.
      - Klicken Sie auf **Beitreten**.

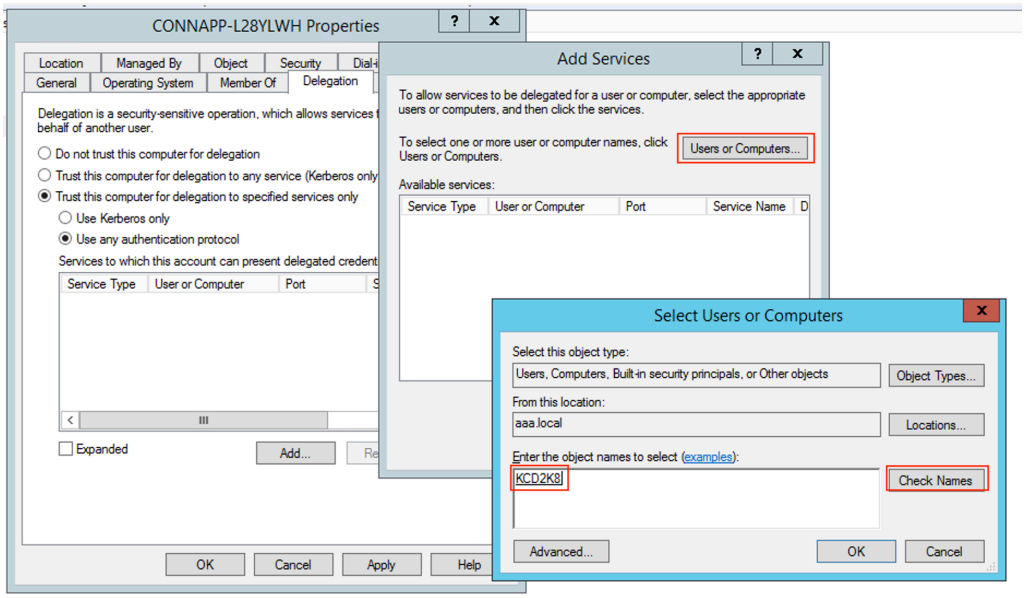
   b) Konfigurieren Sie die Kerberos-Einschränkungsdelegierung für Webserver ohne Load Balancer.



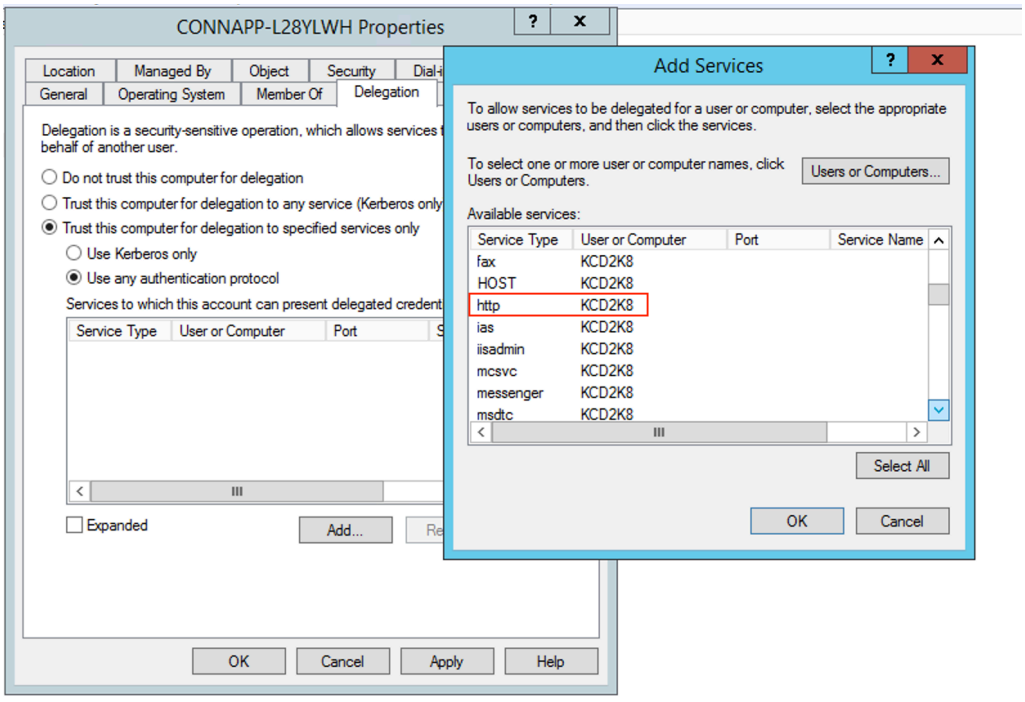
- Identifizieren Sie den Computernamen des Connector-Geräts Sie können diesen Namen entweder von dem Ort erhalten, an dem Sie gehostet haben, oder einfach von der Connector-Benutzeroberfläche.
- Suchen Sie auf Ihrem Active Directory-Controller nach dem Connector-Appliance-Computer.
- Wechseln Sie zu den Eigenschaften des Connector-Appliance-Computerkontos, und navigieren Sie zur Registerkarte **Delegierung**.
- Wählen Sie **Computer nur für die Delegierung an angegebene Dienste vertrauen** aus. Wählen Sie dann **Beliebiges Authentifizierungsprotokoll verwenden** aus.



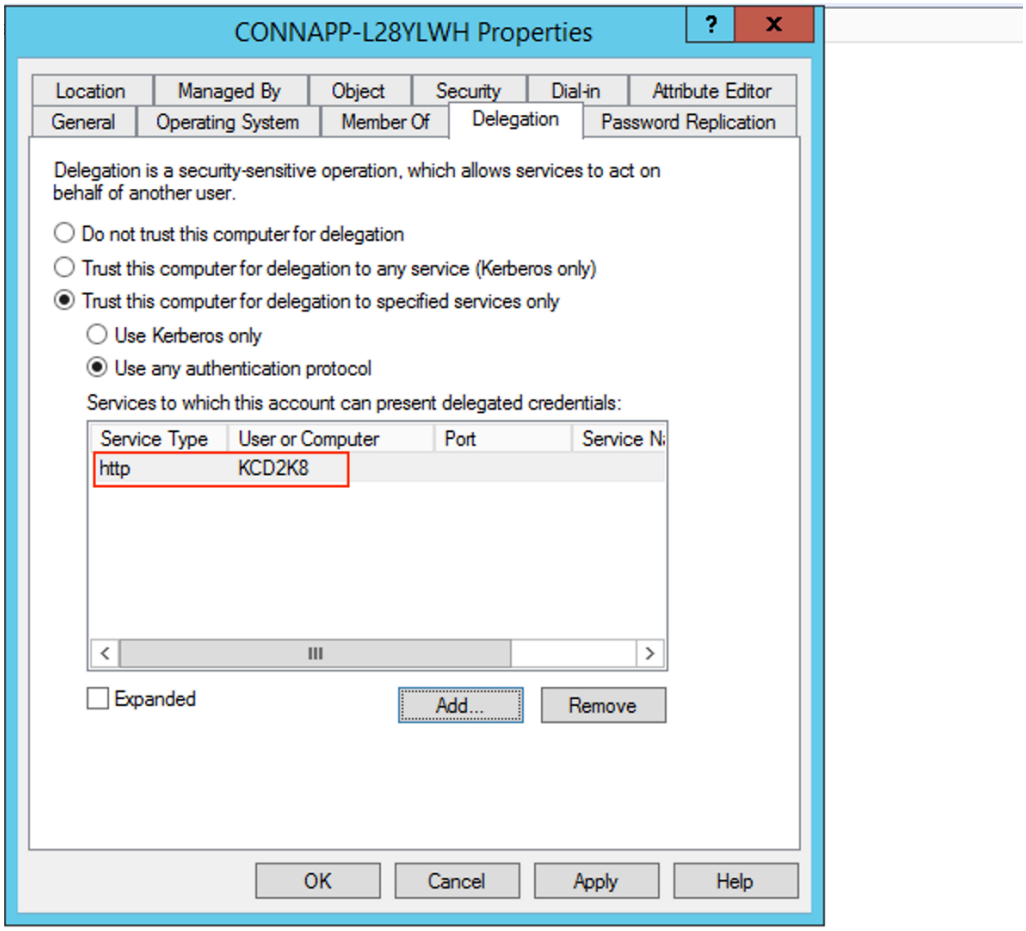
- Klicken Sie auf **Hinzufügen.**
- Klicken Sie auf **Benutzer oder Computer**.
- Geben Sie den Namen des Ziel-Webservers ein, und klicken Sie dann auf **Namen überprüfen**. In der vorherigen Abbildung ist **KCD2K8** der Webserver.



- klicken Sie auf **OK.**
- Wählen Sie den Diensttyp **http** aus.



- Klicken Sie auf **OK**.
- Klicken Sie auf **Anwenden** und dann auf **OK**.



Damit ist das Verfahren zum Hinzufügen der Delegierung für einen Webserver abgeschlossen.

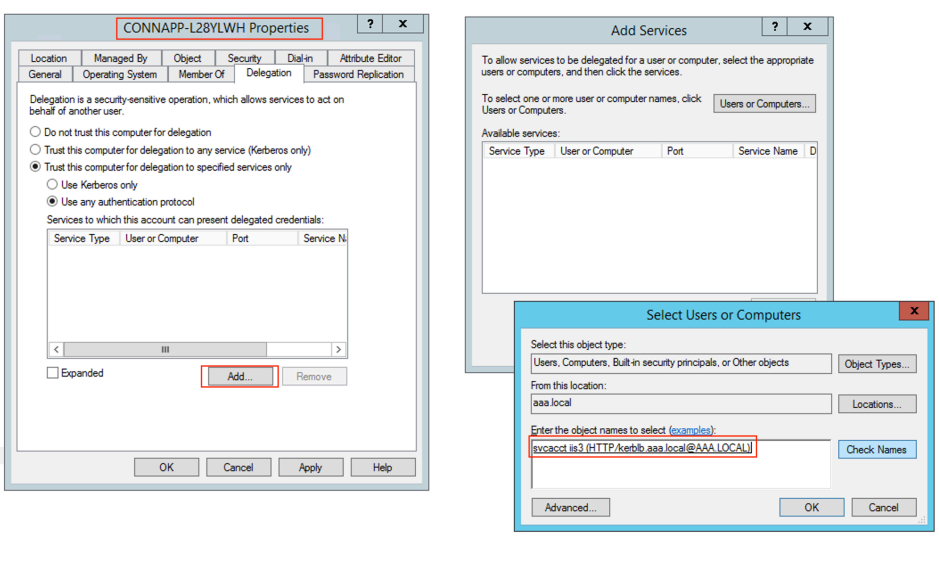
c) Konfigurieren Sie die eingeschränkte Kerberos-Delegierung (KCD) für einen Webserver hinter einem Load Balancer.

- Fügen Sie den Load Balancer-SPN mit dem folgenden Befehl `setspn` zum Dienstkonto hinzu.
  `setspn -S HTTP/<web_server_fqdn> <service_account>`

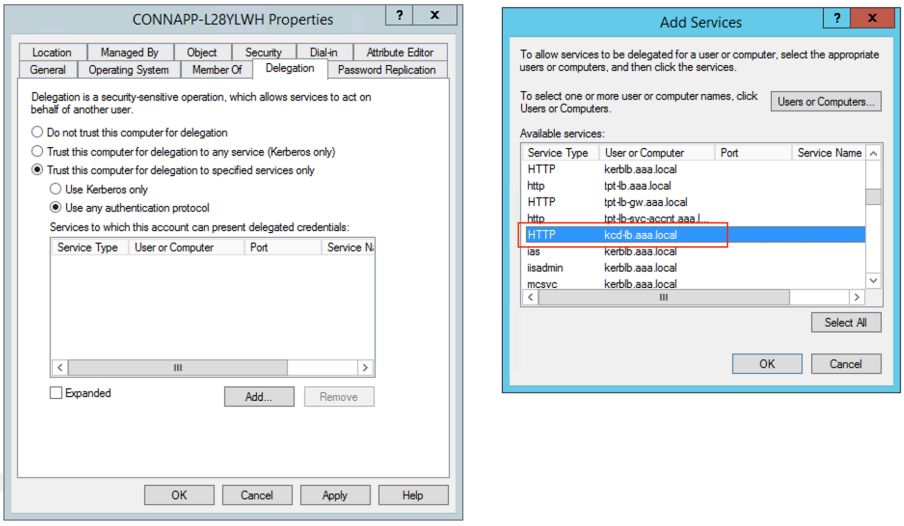
```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local

Registering ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=
local
        HTTP/kcd-lb.aaa.local
Updated object

C:\Windows\system32>_
```

- Bestätigen Sie die SPNs für das Dienstkonto mit dem folgenden Befehl.
  `setspn -l <service_account>`

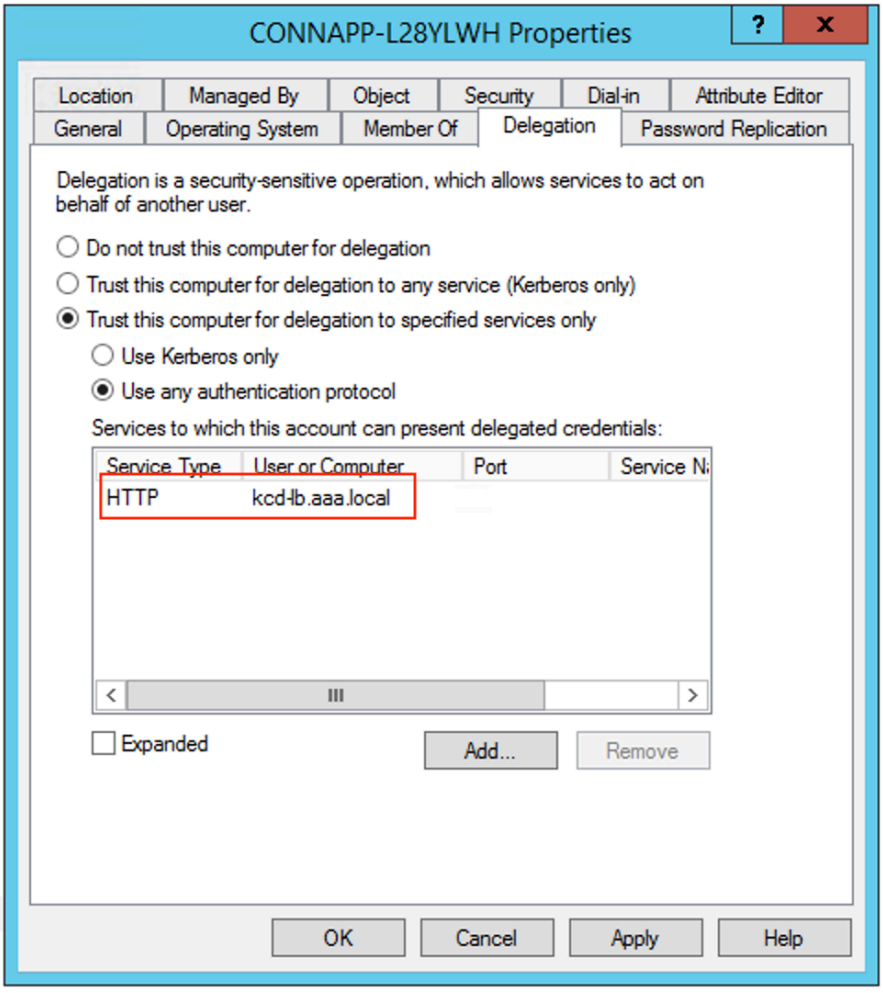
- Erstellen Sie eine Delegierung für das Computerkonto der Connector-Appliance.
  - Führen Sie die Schritte zum *Konfigurieren der Kerberos-Beschränkungsdelegierung für den Webserver* ohne Load Balancer aus, um den CA-Computer zu identifizieren und zur Delegierungs-Benutzeroberfläche zu navigieren.
  - Wählen Sie unter **Benutzer und Computer**die Option Dienstkonto aus (z. B. aaa\svc_iis3).



  - Wählen Sie in den Diensten den Eintrag **ServiceType: HTTP** und Benutzer oder Computer: Webserver (z. B. `kcd-lb.aaa.local`)



- Klicken Sie auf **OK**.
- Klicken Sie auf **Anwenden** und dann auf **OK**.

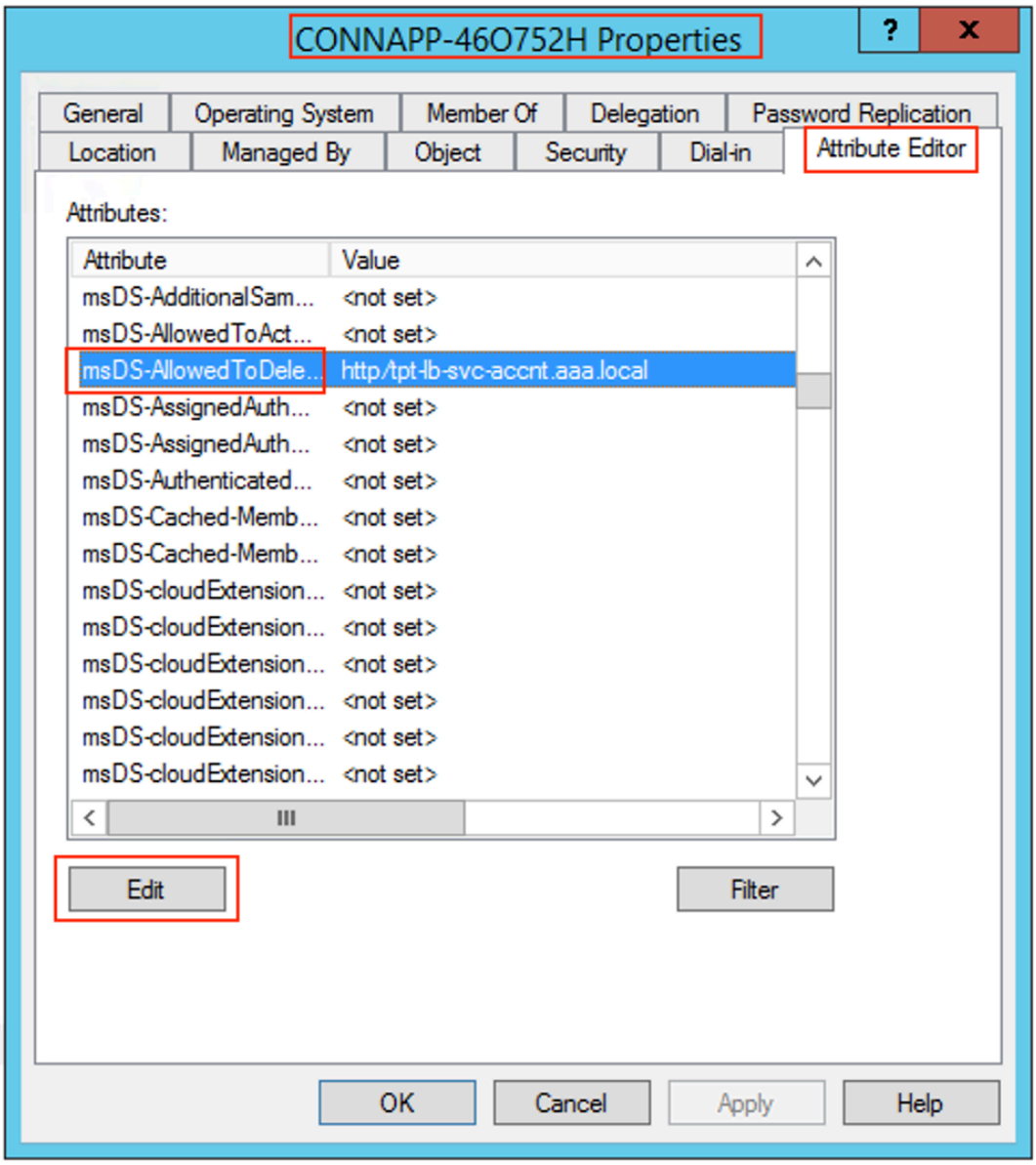


d) Konfigurieren Sie die eingeschränkte Kerberos-Delegierung (KCD) für ein gruppenverwaltetes Dienstkonto.

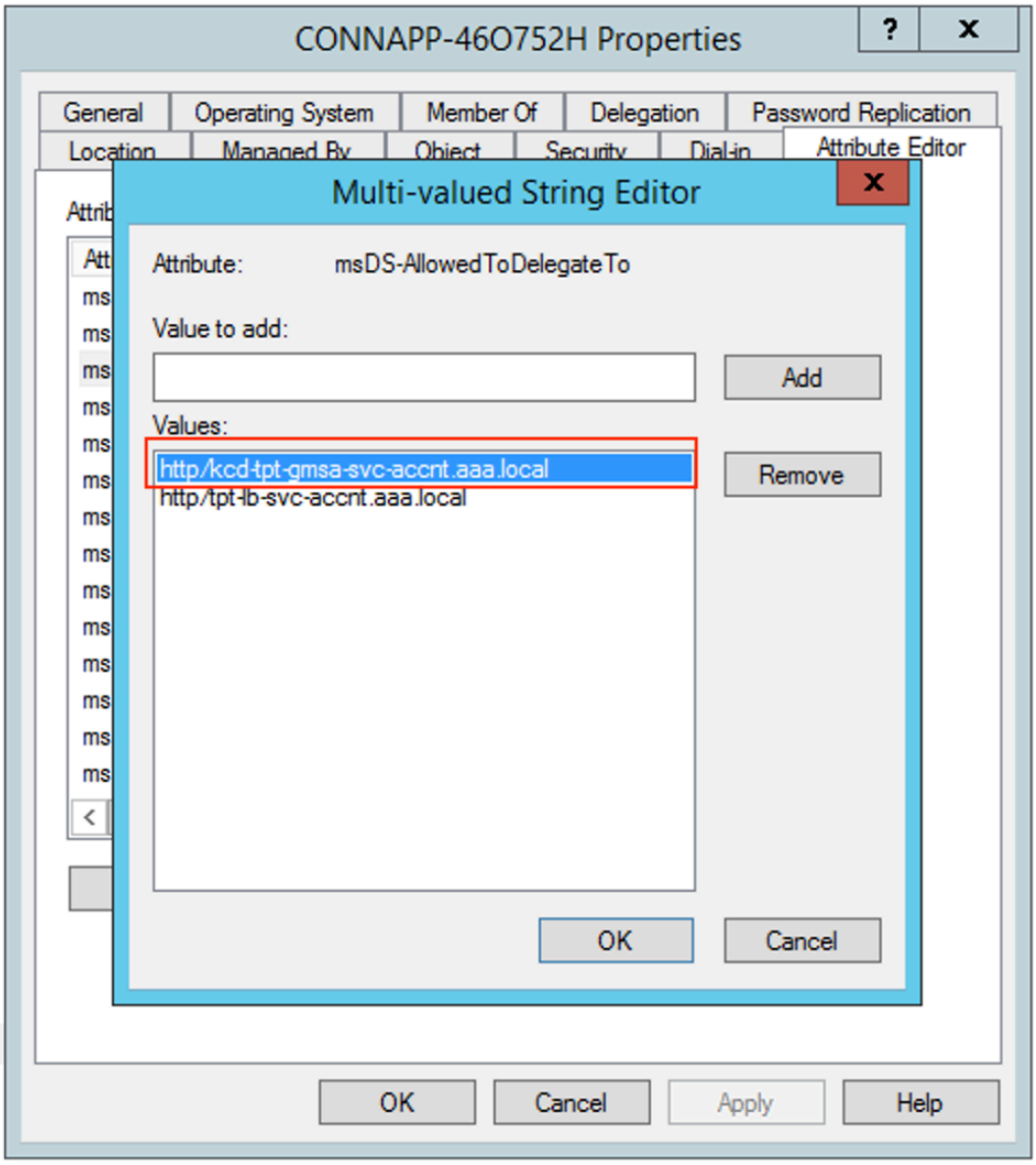
- Fügen Sie SPN dem gruppenverwalteten Dienstkonto hinzu, falls dies noch nicht geschehen ist.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Bestätigen Sie den SPN mit dem folgenden Befehl.
  `setspn -l <group_manged_service_account>`

Da das gruppenverwaltete Dienstkonto beim Hinzufügen des Delegierungseintrags für das Computerkonto nicht in der Suche `Users and Computers` angezeigt werden kann, können Sie die Delegierung für ein Computerkonto nicht auf die übliche Weise hinzufügen. Daher können Sie diesen SPN als delegierten Eintrag zum CA-Computerkonto hinzufügen, indem Sie den Attribut-Editor durchlaufen.

- Navigieren Sie in den Computereigenschaften der Connector-Appliance zur Registerkarte **Attribut-Editor**, und suchen Sie nach dem Attribut `msDA-AllowedToDeleteTo`.
- Bearbeiten Sie `msDA-AllowedToDeleteTo attribute`, und fügen Sie dann den SPN hinzu.



)

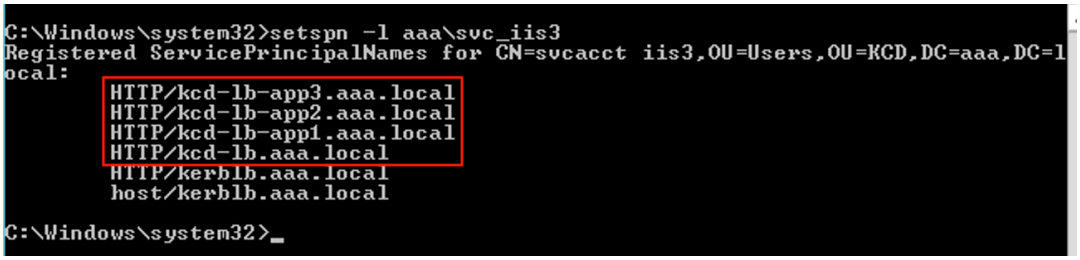


)

e) Migrieren von NetScaler Gateway Connector zur Citrix Connector Appliance.

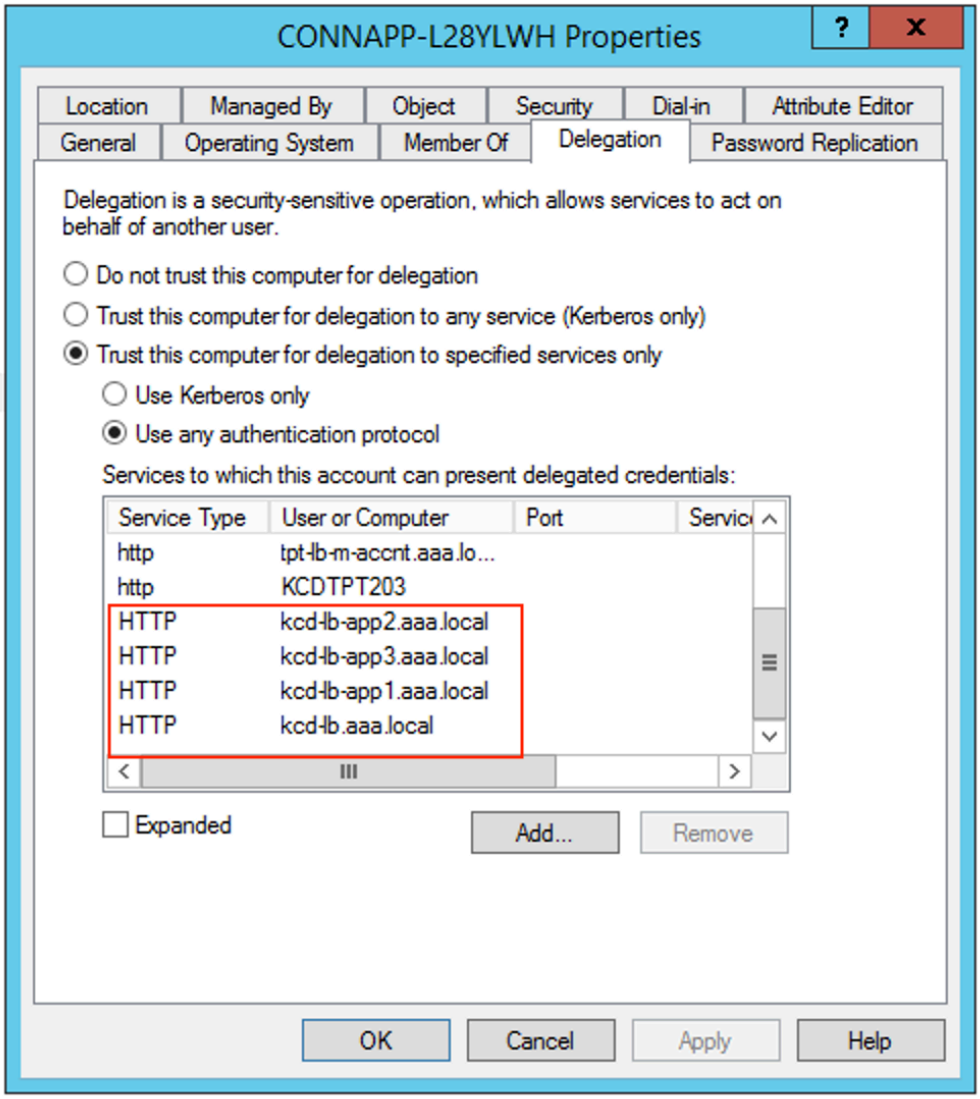
- Da SPNs bei der Konfiguration des Gateway-Connectors bereits auf Dienstkonto festgelegt sind, müssen Sie keine weiteren SPNs für das Dienstkonto hinzufügen, wenn keine neue Kerberos-App konfiguriert ist. Sie können die Liste aller SPNs anzeigen, die für das Dienstkonto zugewiesen sind, indem Sie den folgenden Befehl ausführen und sie als delegierte Einträge für das CA-Computerkonto zuweisen.

```
setspn -l <service_account>
```

In diesem Beispiel sind die SPNs (`kcd-lb.aaa.local`, `kcd-lb-app1.aaa.local`, `kcd-lb-app2.aaa.local`, `kcd-lb-app3.aaa.local`) für KCD konfiguriert.

- Fügen Sie dem Computerkonto der Connector-Appliance die erforderlichen SPNs als delegierten Eintrag hinzu. Einzelheiten finden Sie im Schritt *Erstellen einer Delegierung für das Computerkonto der Connector-Appliance*.



In diesem Beispiel wird der erforderliche SPN als delegierte Einträge für das CA-Computerkonto hinzugefügt.

Hinweis: Diese SPN wurden dem Dienstkonto als delegierte Einträge bei der Konfiguration des Gateway-Connectors hinzugefügt. Wenn Sie sich von der Delegierung von Dienstkonten entfernen, können diese Einträge aus der Registerkarte **Delegierung** von Dienstkonten entfernt werden.

f) Befolgen Sie den Anweisungen in der Dokumentation zu Citrix Secure Private Access, um den Citrix Secure Private Access Service einzurichten. Während der Einrichtung erkennt Citrix Cloud das Vorhandensein Ihrer Connector-Appliances und verwendet sie, um eine Verbindung zu Ihrem Ressourcenstandort herzustellen.

- Erste Schritte mit Citrix Secure Private Access
- Konfigurieren von Citrix Secure Private Access
- Connectorgerät für Cloudservices
- Anforderungen an die Internetkonnektivität.
- Unterstützung für unternehmenseigene Web-Apps

Validierung der Kerberos-Konfiguration

Wenn Sie Kerberos für Single Sign-On verwenden, können Sie auf der Administrationsseite des Connector Appliance überprüfen, ob die Konfiguration auf Ihrem Active Directory Directory-Controller korrekt ist. Mit dem Feature **Kerberos-Validierung** können Sie eine Konfiguration im Kerberos Realm-Only-Modus oder eine Konfiguration mit eingeschränkter Kerberos-Delegierung (KCD) validieren.

1. **Gehen Sie zur Administrationsseite des Connector Appliance** .
   a) Kopieren Sie von der Connector Appliance-Konsole in Ihrem Hypervisor die IP-Adresse in die Adressleiste Ihres Browsers.
   b) Geben Sie das Kennwort ein, das Sie bei der Registrierung der Connector Appliance festgelegt haben.
2. Wählen Sie im Admin-Menü oben rechts die Option **Kerberos-Validierung** aus.
3. Wählen Sie im Dialogfeld **Kerberos-Validierung** den **Kerberos-Validierungsmodus** aus.
4. Geben Sie die **Active Directory-Domäne** an oder wählen Sie sie aus.
   - Wenn Sie eine Konfiguration im Kerberos Realm-Only-Modus validieren, können Sie eine beliebige Active Directory-Domäne angeben.
   - Wenn Sie eine Konfiguration mit eingeschränkter Kerberos-Delegierung überprüfen, müssen Sie Ihre Auswahl aus einer Liste von Domänen in der verbundenen Gesamtstruktur treffen.

5. Geben Sie den **Dienst-FQDN** an. Es wird angenommen, dass der Standarddienstname lautet `http`. Wenn Sie "computer.example.com"angeben, wird dies als dasselbe wie `http/computer.example.com` angesehen.
6. Geben Sie den **Benutzernamen** an.
7. Wenn Sie eine Konfiguration im Kerberos Realm-Only-Modus validieren, geben Sie das **Kennwort** für diesen Benutzernamen an.
8. Klicken Sie auf **Kerberos testen**.

Wenn die Kerberos-Konfiguration korrekt ist, wird die Meldung angezeigt `Successfully validated Kerberos setup`. Wenn die Kerberos-Konfiguration nicht korrekt ist, wird eine Fehlermeldung angezeigt, die Informationen zum fehlgeschlagenen Validierungsfehler enthält.

Gateway Connector zur Connector-Einheit migrieren

December 27, 2023

NetScaler Gateway Connector ist veraltet. Citrix empfiehlt seinen Kunden, NetScaler Gateway Connectors in ihrer Umgebung zu verwenden, um mit der Bereitstellung der Connector Appliance für alle Secure Private Access-Anwendungsfälle zu beginnen, die zuvor vom NetScaler Gateway Connector unterstützt wurden. Dieses Thema enthält Richtlinien für die Migration von Gateway Connector zu Connector Appliance.

Allgemeine Schritte zur Migration von Gateway Connector zu Connector Appliance

1. Installieren Sie die Connector Appliances zusätzlich zu den Gateway Connectors am gleichen Ressourcenstandort.
2. Fahren Sie die Gateway Connectors herunter und testen Sie die vorhandenen Web-Apps auf Konnektivität. Überprüfen Sie, ob auf die am gleichen Ressourcenstandort gehostete Web-App zugegriffen werden kann.
3. Entfernen Sie den NetScaler Gateway Connector, sobald der Test abgeschlossen ist.

So installieren Sie das Connector

Gehen Sie wie folgt vor, um eine Connector Appliance zu installieren.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links auf dem Bildschirm die Option **Ressourcenstandorte**aus.

3. Klicken Sie auf das Plussymbol neben Connector Appliance für den Ressourcenstandort, zu dem Sie eine Connector Appliance hinzufügen möchten.
4. Wählen Sie den Hypervisor aus, und klicken Sie auf **Image herunterladen**.
5. Laden Sie die Connector Appliance herunter und installieren Sie sie auf Ihrem Hypervisor
6. Melden Sie sich bei der Web-Benutzeroberfläche an (die IP-Adresse wird auf der Konsole des Hypervisors bereitgestellt) und richten Sie bei Bedarf einen Proxy ein.
7. Klicken Sie auf die Schaltfläche **Registrieren** und rufen Sie den Funktionscode ab.
8. Fügen Sie den Kurzcode in die Citrix Cloud-Benutzeroberfläche ein, die beim Herunterladen der Connector Appliance verwendet wird (Schritt 5).

   Die Connector Appliance ist registriert.

Detaillierte Schritte finden Sie unter Connector Appliance für Cloud-Dienste.

Häufig gestellte Fragen

- Wie lade ich die Connector Appliance herunter?

  Laden Sie die Connector-Einheitherunter.
- Wie installiere ich das Connector Appliance?

  Installieren der Connector Appliance.
- Wie registriere ich die Connector Appliance?

  Die Connector Appliance wird registriert.
- Was sind die Konnektivitätsanforderungen für die Connector Appliance?

  Anforderungen an die Internetverbindung der Connector Appliance
- Was sind die Systemanforderungen für die Connector Appliance?

  Systemanforderungen für Connector Appliance.
- Wie wird Connector Appliance aktualisiert?

  Connector-Appliance-Updates

Direkter Zugriff auf Enterprise Web-Apps

June 19, 2024

Unternehmenswebanwendungen wie SharePoint, JIRA, Confluence und andere, die vom Kunden entweder on-premises oder in öffentlichen Clouds gehostet werden, können jetzt direkt von einem Client-Browser aus aufgerufen werden. Endbenutzer müssen den Zugriff auf ihre Unternehmens-Webanwendungen nicht mehr über die Citrix Workspace-Erfahrung initiieren. Diese Funktion ermöglicht Endbenutzern auch den Zugriff auf die Web-Apps, indem sie auf Links in ihren E-Mails, Tools für die Zusammenarbeit oder Browser-Lesezeichen klicken. Auf diese Weise wird den Kunden eine echte Null-Footprint-Lösung bereitgestellt.

Funktionsweise

- Fügen Sie einen neuen DNS-Eintrag hinzu oder ändern Sie einen vorhandenen DNS-Eintrag für die konfigurierten Enterprise-Webanwendungen.
- Der IT-Administrator würde einen neuen öffentlichen DNS-Eintrag hinzufügen oder einen vorhandenen öffentlichen DNS-Eintrag für den konfigurierten FQDN der Enterprise-Web-App ändern, um den Benutzer zum Citrix Secure Private Access Service umzuleiten.
- Wenn der Endbenutzer den Zugriff auf die konfigurierte Unternehmensweb-App initiiert, wird der App-Traffic zum Citrix Secure Private Access Service geleitet, der dann den Zugriff auf die App als Proxy durchführt.
- Sobald die Anforderung beim Citrix Secure Private Access Service landet, prüft sie auf Benutzerauthentifizierung und Anwendungsautorisierung, einschließlich kontextbezogener Zugriffsrichtlinienprüfungen.
- Nach erfolgreicher Validierung kommuniziert der Citrix Secure Private Access-Dienst mit Citrix Cloud Connector Appliances, die in der Kundenumgebung (entweder on-premises oder in der Cloud) bereitgestellt werden, um den Zugriff auf die konfigurierte Unternehmens-Web-App zu ermöglichen.

Konfigurieren Sie Citrix Secure Private Access für den direkten Zugriff auf Enterprise-Web-Apps

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes, damit die Anwendung konfiguriert werden kann.

- FQDN der Anwendung
- SSL-Zertifikat —Öffentliches Zertifikat für die zu konfigurierende App
- Standort der Ressource —Installieren Sie Citrix Cloud Connector Appliances
- Zugriff auf den öffentlichen DNS-Datensatz, um ihn mit dem kanonischen Namen (CNAME) zu aktualisieren, der von Citrix während der App-Konfiguration bereitgestellt wurde.

Vorgehensweise zum Konfigurieren des direkten Zugriffs auf Enterprise-Web-Apps:

> **Wichtig:**
>
> Eine vollständige End-to-End-Konfiguration einer App finden Sie unter Admin-geführter Workflow für einfaches Onboarding und Setup.

1. Klicken Sie auf der Secure Private Access-Startseite auf **Weiter.**

   > **Hinweis:**
   >
   > Die Schaltfläche **Weiter** wird nur angezeigt, wenn Sie den Assistenten zum ersten Mal verwenden. In den nachfolgenden Verwendungen können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen**klicken.

2. Richten Sie Identität und Authentifizierung ein. Einzelheiten finden Sie unter Admin-geführter Arbeitsablauf für einfaches Onboarding und Setup.
3. Fahren Sie fort, eine App hinzuzufügen. Einzelheiten finden Sie unter Hinzufügen und Verwalten von Anwendungen.
4. Wählen Sie die App aus, die Sie hinzufügen möchten, und klicken Sie auf **Überspringen.**
5. In **Wo ist die Anwendung?**, wählen Sie den Standort aus.
6. Geben Sie im Abschnitt **App-Details die folgenden Details** ein und klicken Sie auf **Weiter**.

   - **App-Typ** —Wählen Sie den App-Typ aus (HTTP oder HTTPS).
   - **Appname** —Name der Anwendung.
   - **App-Beschreibung** —Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Workspace angezeigt.
   - **App-Symbol** —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Icon-Datei muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

     Wenn Sie das App-Symbol nicht anzeigen möchten, wählen Sie Anwendungssymbol nicht für Benutzer anzeigen aus.

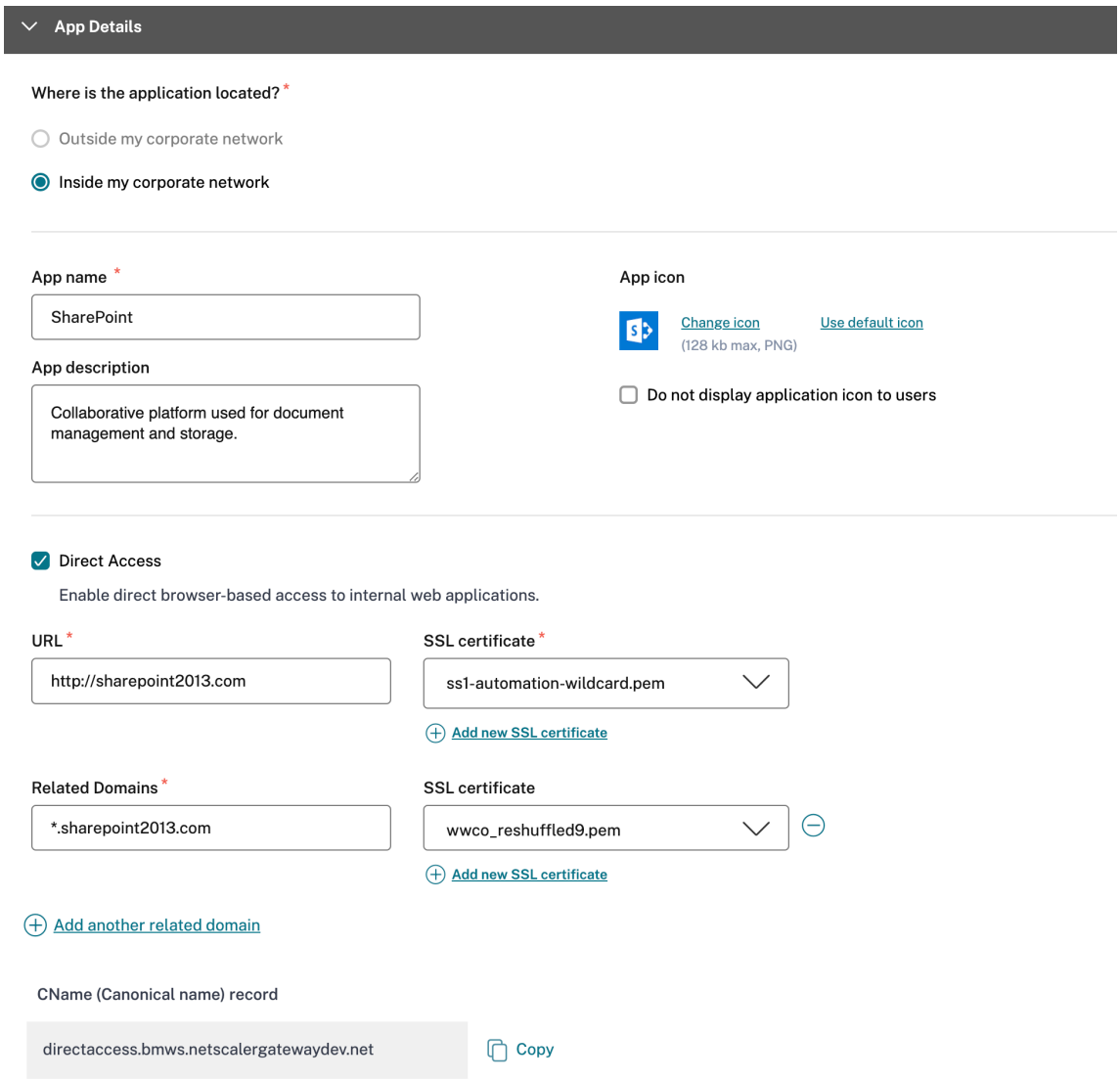
7. Wählen Sie **Direktzugriff**, damit Benutzer direkt von einem Client-Browser aus auf die App zugreifen können. Geben Sie die folgenden Details ein.

   - **URL** —URL für die Back-End-Anwendung. Die URL muss im HTTPS-Format vorliegen und ein entsprechender DNS-Eintrag muss vom Administrator hinzugefügt werden.
   - **SSL-Zertifikat** —Wählen Sie im Dropdown-Menü ein vorhandenes SSL-Zertifikat aus oder fügen Sie ein neues SSL-Zertifikat hinzu, indem Sie auf **Neues SSL-Zertifikat hinzufügen**klicken

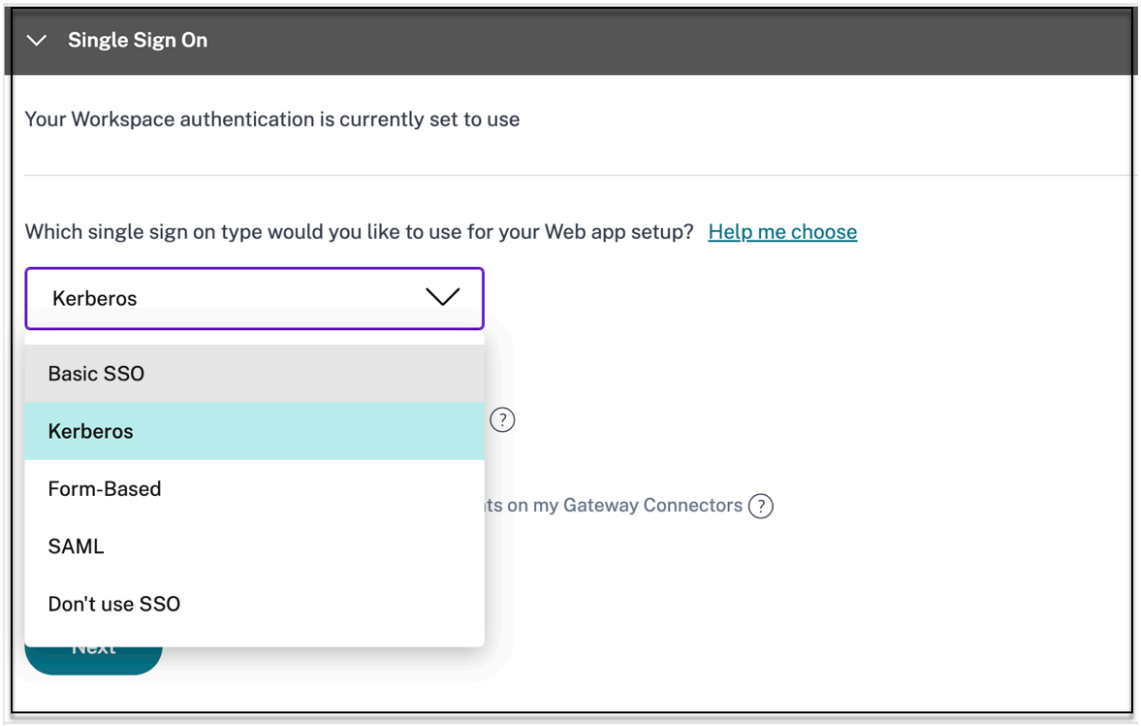
Zu beachtende Punkte:

- Es wird nur ein öffentliches oder ein vertrauenswürdiges CA-Zertifikat unterstützt. Selbstsignierte Zertifikate werden nicht unterstützt.
- Eine vollständige Kette von Zertifikaten muss hochgeladen werden.

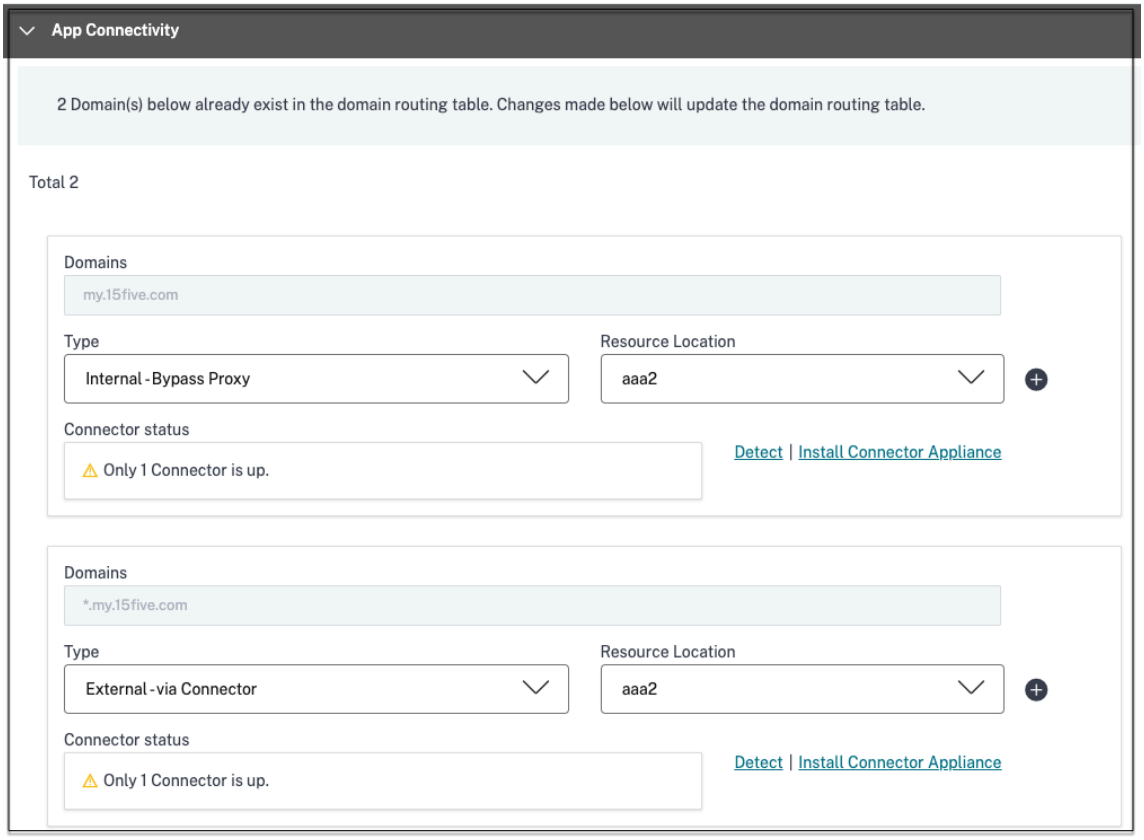
- **Verwandte Domains** —Die zugehörige Domain wird basierend auf der von Ihnen angegebenen URL automatisch ausgefüllt. Verwandte Domain hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domain hinzufügen. Sie können ein SSL-Zertifikat an jede zugehörige Domain binden, dies ist optional.
- **cName-Datensatz** —Automatisch generiert von Secure Private Access. Dies ist der Wert, der in das DNS eingegeben werden muss, um den direkten Zugriff auf die Anwendung zu ermöglichen.



8. Klicken Sie auf **Weiter.**
9. Wählen Sie im Abschnitt **Single Sign-On** Ihren bevorzugten Single Sign-On-Typ aus, der für Ihre Anwendung verwendet werden soll, und klicken Sie auf**Weiter**.



10. Im Abschnitt **App-Konnektivität** können Sie entweder einen vorhandenen Ressourcenstandort auswählen oder einen erstellen und eine neue Connector Appliance bereitstellen. Um einen vorhandenen Ressourcenstandort auszuwählen, klicken Sie in der Liste der Ressourcenstandorte auf einen der Ressourcenstandorte, z. B. Mein Ressourcenstandort, und klicken Sie auf**Weiter**. Einzelheiten finden Sie unter Weiterleiten von Tabellen zur Lösung von Konflikten, wenn die zugehörigen Domänen sowohl in SaaS als auch in Web-Apps identisch sind.



11. Klicken Sie auf **Fertigstellen**. Die App wird der Seite “Anwendungen “hinzugefügt. Sie können eine auf der Anwendungsseite bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu in einer App auf die Ellipsenschaltfläche und wählen Sie die Aktionen entsprechend aus.

    - **Anwendung bearbeiten**
    - **Löschen**

> **Wichtig:**
>
> - Um den Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps ist nur aktiviert, wenn der Anwendung eine Zugriffsrichtlinie zugeordnet ist. Einzelheiten zum Erstellen von Zugriffsrichtlinien finden Sie unter Zugriffsrichtlinien erstellen.
> - Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, kann dies zu einer widersprüchlichen Konfiguration führen. Informationen zur Vermeidung von Konfigurationskonflikten finden Sie unter Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen.

Support für Software as a Service Apps

June 19, 2024

Software as a Service (SaaS) ist ein Softwareverteilungsmodell, mit dem Software remote als webbasierter Dienst bereitgestellt wird. Häufig verwendete SaaS-Apps umfassen Salesforce, Workday, Concur, GoToMeeting usw.

Auf SaaS-Apps kann über Citrix Workspace mit dem Secure Private Access-Dienst zugegriffen werden. Der Secure Private Access-Dienst in Verbindung mit Citrix Workspace bietet eine einheitliche Benutzererfahrung für die konfigurierten SaaS-Apps, konfigurierten virtuellen Apps oder andere Arbeitsbereichsressourcen.

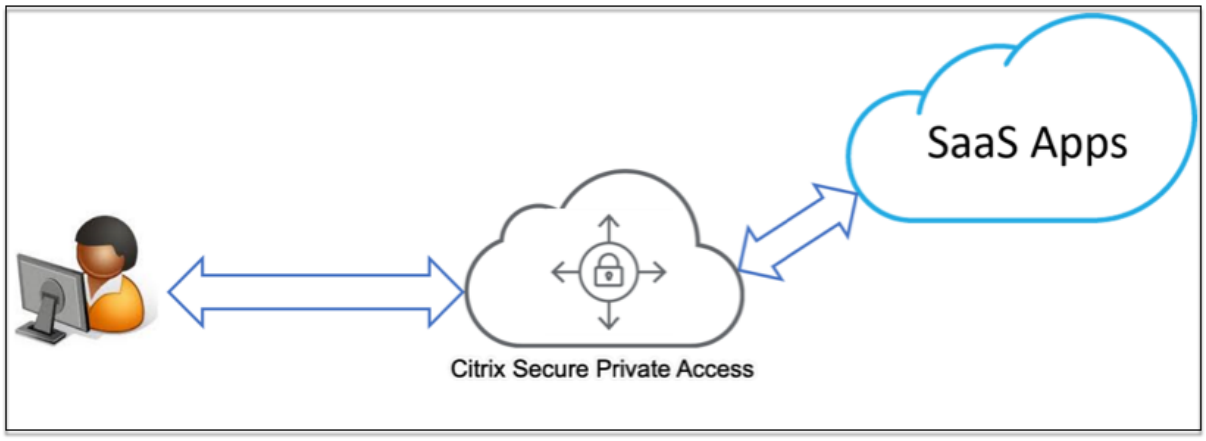
Die Bereitstellung von SaaS-Apps mithilfe des Secure Private Access Service bietet Ihnen eine einfache, sichere, robuste und skalierbare Lösung für die Verwaltung der Apps. SaaS-Apps, die in der Cloud bereitgestellt werden, bieten folgende Vorteile:

- **Einfache Konfiguration** — Einfach zu bedienen, zu aktualisieren und zu verwenden.
- **Single Sign-On** - Problemlose Anmeldung mit Single Sign-On.
- **Standardvorlage für verschiedene Apps** —Vorlagenbasierte Konfiguration beliebter Apps.

So werden SaaS-Apps mit dem Secure Private Access-Dienst unterstützt

1. Der Kundenadministrator konfiguriert SaaS-Apps mithilfe der Secure Private Access Service Access-Dienstbenutzeroberfläche.
2. Admin stellt den Benutzern die Dienst-URL für den Zugriff auf Citrix Workspace zur Verfügung.
3. Um die App zu starten, klickt ein Benutzer auf das aufgezählte SaaS-App-Symbol.
4. Die SaaS-App vertraut der SAML-Assertion, die vom Secure Private Access-Dienst bereitgestellt wird, und die App wird gestartet.

> **Hinweis:**
>
> - Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
> - Konfigurierte SaaS-Apps werden zusammen mit virtuellen Apps und anderen Ressourcen in Citrix Workspace zusammengefasst, um eine einheitliche Benutzererfahrung zu erzielen.



SaaS-App konfigurieren

Die Konfiguration einer SaaS-App umfasst die folgenden allgemeinen Schritte.

1. Konfigurieren Sie die Anwendungsdetails
2. Stellen Sie die bevorzugte Anmeldemethode ein
3. Anwendungsrouting definieren

Anwendungsdetails konfigurieren

1. Klicken Sie auf der Kachel **Secure Private Access** auf **Verwalten.**
2. Klicken Sie auf **Weiter** und dann auf **App hinzufügen.**

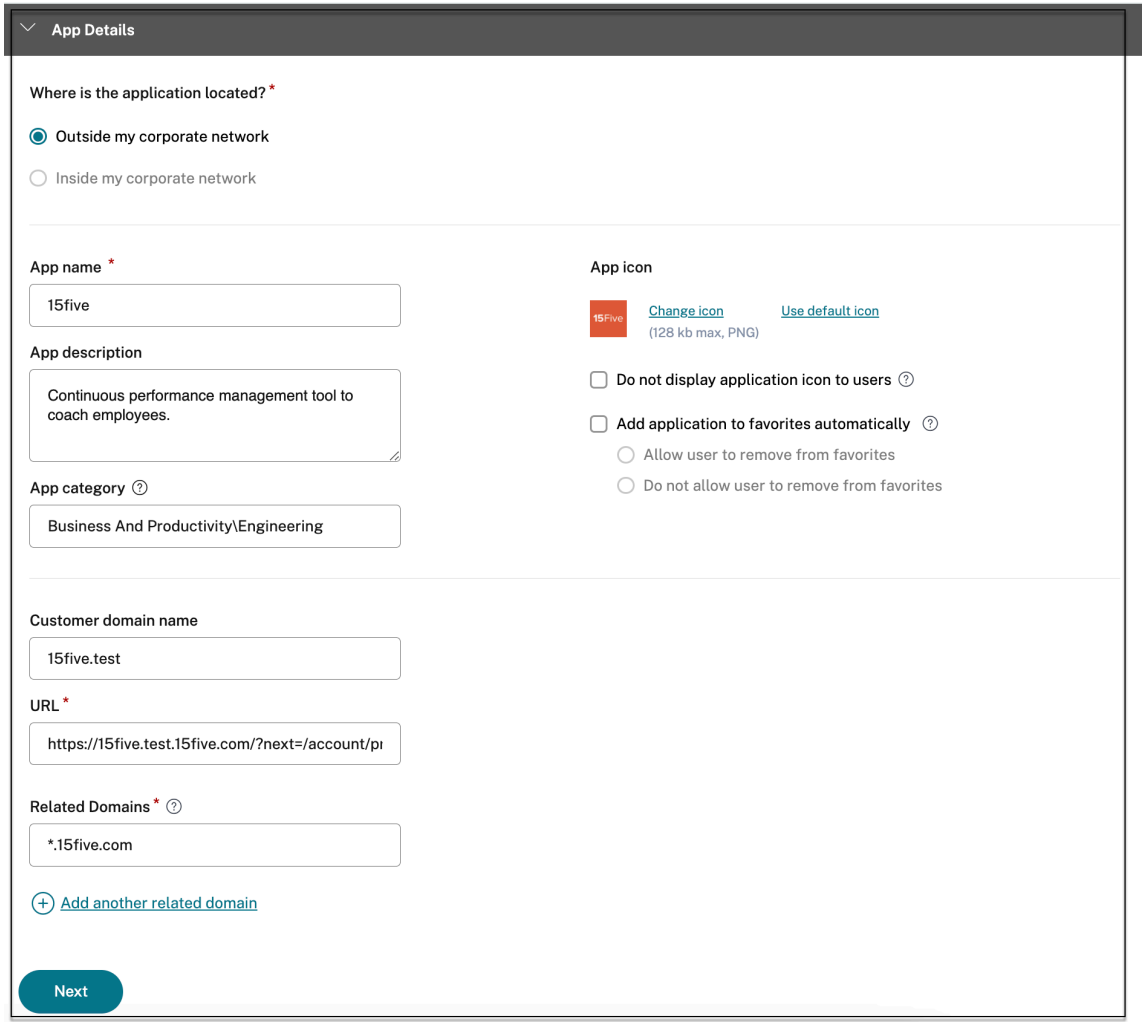
   > **Hinweis:**
   >
   > - Die Schaltfläche **Weiter** wird nur angezeigt, wenn Sie den Assistenten zum ersten Mal verwenden. Bei den nachfolgenden Verwendungen können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen**klicken.
   > - Sie können eine SaaS-App manuell hinzufügen, indem Sie die App-Details eingeben, oder eine App-Vorlage auswählen, die für eine Liste beliebter SaaS-Apps verfügbar ist. Die Vorlage enthält viele Informationen, die für die Konfiguration von Anwendungen erforderlich sind. Die für den Kunden spezifischen Informationen müssen jedoch noch zur Verfügung gestellt werden. Einzelheiten zur SaaS-App-Konfigurationsvorlage finden Sie unter SaaS-App-Server-spezifische Konfiguration.

3. Konfiguriere die App.

   - Um die App-Details manuell einzugeben, klicken Sie auf **Überspringen.**
   - Um die App mithilfe einer Vorlage zu konfigurieren, klicken Sie auf **Weiter.**

Die Option **“Außerhalb meines Unternehmensnetzwerks** “ist standardmäßig für eine SaaS-App aktiviert.

4. Geben Sie im Abschnitt **App-Details die folgenden Details** ein und klicken Sie auf **Weiter.**

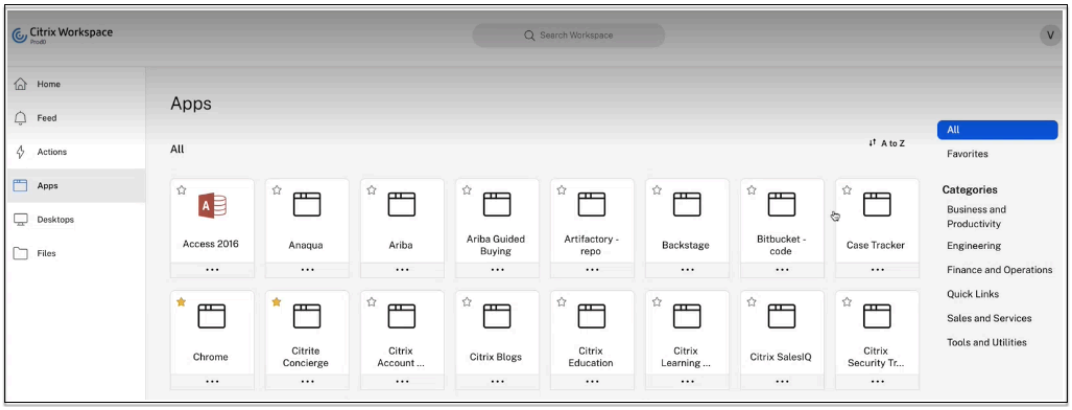


- **Appname** —Name der Anwendung.
- **App-Beschreibung** —Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Workspace angezeigt.
- **App-Kategorie** —Fügen Sie die Kategorie und den Namen der Unterkategorie (falls zutreffend) hinzu, unter denen die App, die Sie veröffentlichen, in der Citrix Workspace-Benutzeroberfläche erscheinen muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien über die Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angegeben haben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.
  - Die Kategorie/Unterkategorien sind vom Administrator konfigurierbar und Admins

können für jede App eine neue Kategorie hinzufügen.

- Das Feld **App-Kategorie** gilt für HTTP/HTTPS-Apps und ist für TCP/UDP-Apps ausgeblendet.
- Die Namen der Kategorie/Unterkategorien müssen durch einen Backslash getrennt werden. Zum Beispiel **Business And Productivity\ Engineering** . Außerdem unterscheidet dieses Feld zwischen Groß- und Kleinschreibung. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn der Name in der Citrix Workspace-Benutzeroberfläche nicht mit dem im Feld **App-Kategorie eingegebenen Kategorienamen** übereinstimmt, wird die Kategorie als neue Kategorie aufgeführt.

  Wenn Sie beispielsweise die Kategorie **Geschäft und Produktivität** falsch als **Geschäft und Produktivität** in das Feld **App-Kategorie** eingeben, wird in der Citrix Workspace Workspace-Benutzeroberfläche zusätzlich zur Kategorie **Geschäft und Produktivität** eine neue Kategorie mit dem Namen **Geschäft und Produktivität** aufgeführt.



- **App-Symbol** —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Icon-Datei muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

  Wenn Sie das App-Symbol nicht anzeigen möchten, wählen Sie Anwendungssymbol nicht für Benutzer anzeigen aus.

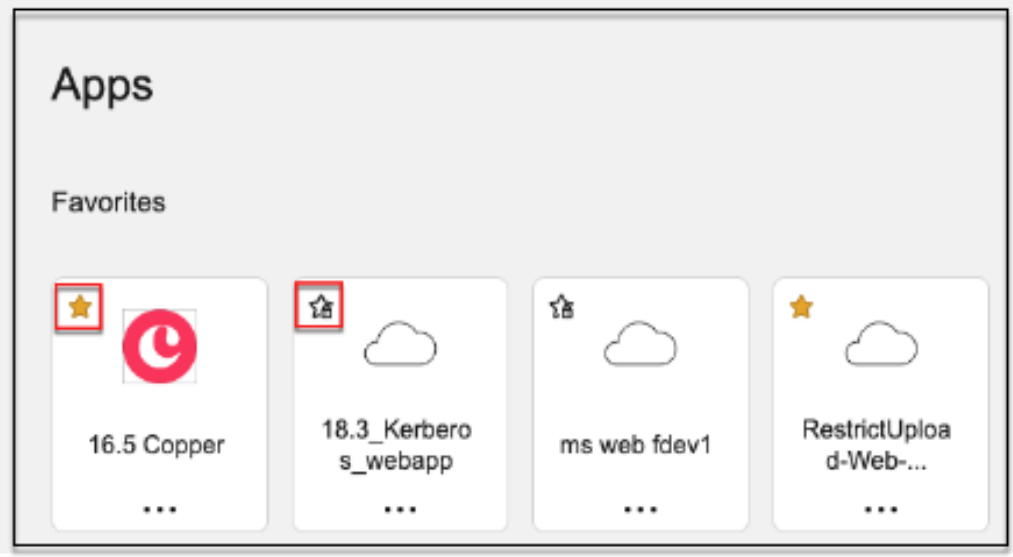
- **URL** —URL mit Ihrer Kunden-ID. Die URL muss Ihre Kunden-ID (Citrix Cloud-Kunden-ID) enthalten. Informationen zum Abrufen Ihrer Kunden-ID finden Sie unter Anmelden für Citrix Cloud. Falls SSO fehlschlägt oder Sie SSO nicht verwenden möchten, wird der Benutzer zu dieser URL umgeleitet.
- **Kundendomänenname** und **Kundendomänen-ID** - Der Domänenname und die ID des Kunden werden verwendet, um die App-URL und andere nachfolgende URLs auf der SAML-SSO-Seite zu erstellen.

  Wenn Sie beispielsweise eine Salesforce-Anwendung hinzufügen, Ihr Domänenname

`salesforceformyorg` und die ID 123754 sind, dann lautet die Anwendungs-URL `https://salesforceformyorg.my.salesforce.com/?so=123754`.

Die Felder "Kundendomänenname"und "Kunden-ID"sind spezifisch für bestimmte Apps.

- **Verwandte Domains** —Die zugehörige Domain wird basierend auf der von Ihnen angegebenen URL automatisch ausgefüllt. Verwandte Domain hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domain hinzufügen.
- Klicken Sie auf **Anwendung automatisch zu Favoriten hinzufügen**, um diese App als Lieblings-App in der Citrix Workspace-App hinzuzufügen.
  - Klicken Sie auf **Allow user to remove from favorites**, um App-Abonnenten zu ermöglichen, die App aus der Favoriten-Liste der Apps in der Citrix Workspace-App zu entfernen. Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein gelber Stern angezeigt.
  - Klicken Sie auf **Do not allow user to remove from favorites**, um zu verhindern, dass Abonnenten die App aus der Favoritenliste der Citrix Workspace-App entfernen. Wenn Sie diese Option auswählen, wird in der Citrix Workspace-App oben links in der App ein Sternsymbol mit einem Vorhängeschloss angezeigt.



Wenn Sie die als Favoriten markierten Apps aus der Secure Private Access Service-Konsole entfernen, müssen diese Apps manuell aus der Favoritenliste in Citrix Workspace entfernt werden. Die Apps werden nicht automatisch aus der Workspace-App gelöscht, wenn sie aus der Secure Private Access Service Access-Servicekonsole entfernt werden.

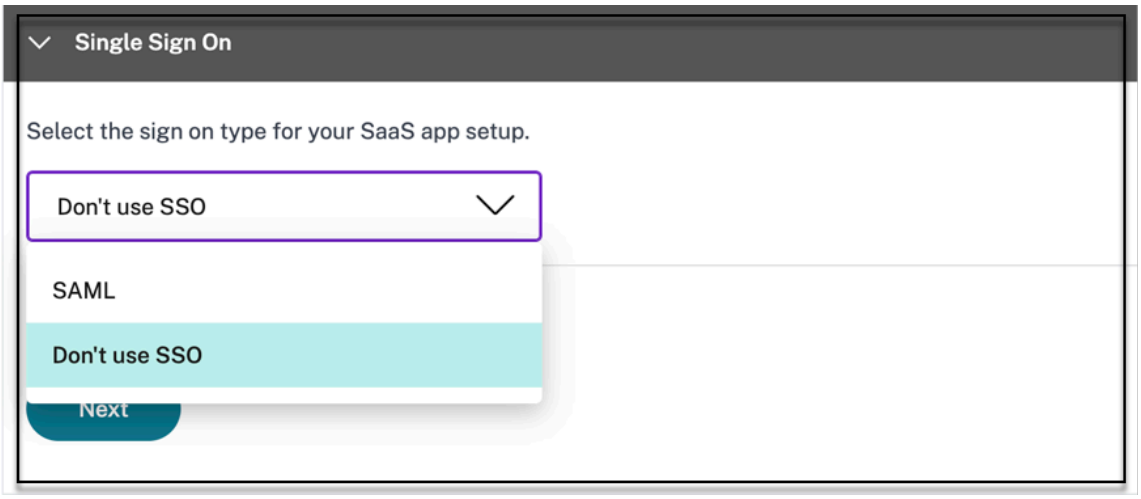
5. Klicken Sie auf **Weiter.**

Wichtig:

- Um den Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps ist nur aktiviert, wenn der Anwendung eine Zugriffsrichtlinie zugeordnet ist. Einzelheiten zum Erstellen von Zugriffsrichtlinien finden Sie unter Zugriffsrichtlinien erstellen.
- Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, kann dies zu einer widersprüchlichen Konfiguration führen. Informationen zur Vermeidung von Konfigurationskonflikten finden Sie unter Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen.

Legen Sie eine bevorzugte Anmeldemethode fest

1. Wählen Sie im Abschnitt **Single Sign On** Ihren bevorzugten Single Sign-On-Typ aus, der für Ihre Anwendung verwendet werden soll, und klicken Sie auf **Speichern**. Die folgenden Single-Sign-On-Typen sind verfügbar.



   - **SSO nicht verwenden** —Verwenden Sie die Option **SSO nicht verwenden**, wenn Sie keinen Benutzer auf dem Backend-Server authentifizieren müssen. Wenn die Option "**SSO nicht verwenden** "ausgewählt ist, wird der Benutzer zu der im Abschnitt "**App-Details** "konfigurierten URL weitergeleitet.
   - **SAML** - Wählen Sie **SAML** für SAML-basiertes SSO in Webanwendungen. Geben Sie die Konfigurationsdetails für den **SAML**-SSO-Typ ein.

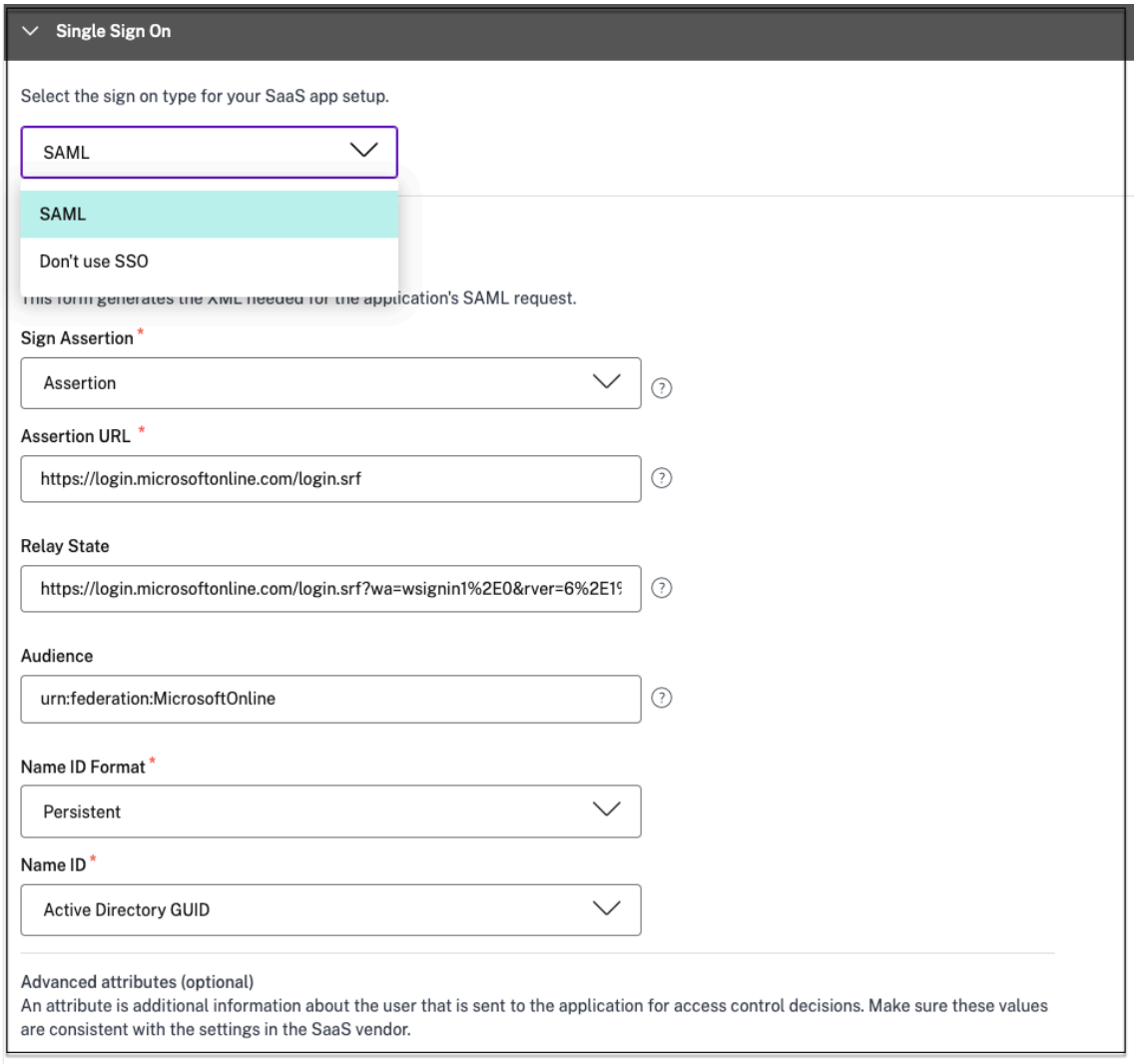
     Geben Sie die folgenden Details in den Abschnitt Anmelden ein und klicken Sie auf **Speichern**.

     - **Assertion signieren** - Das Signieren der Assertion oder Antwort gewährleistet die Integrität der Nachricht, wenn die Antwort oder Assertion an die vertrauende Partei (SP)

übermittelt wird. Sie können **Assertion, Response, Both** oder **None** auswählen.

- **Assertion-URL** —Assertion-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.
- **Relay State** —Der Relay State-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die die Benutzer zugreifen, nachdem sie angemeldet und an den Verbundserver der vertrauenden Partei weitergeleitet wurden. Relay-Status generiert eine einzelne URL für die Benutzer. Benutzer können auf diese URL klicken, um sich bei der Zielanwendung anzumelden.
- **Zielgruppe** —Die Zielgruppe wird vom Anwendungsanbieter bereitgestellt. Dieser Wert bestätigt, dass die SAML-Assertion für die richtige Anwendung generiert wurde.
- **Namens-ID-Format** —Wählen Sie das unterstützte Format für Namensbezeichner
- **Name-ID** —Wählen Sie die unterstützte Namen-ID aus.
- Wählen Sie **App mithilfe der spezifischen URL starten (SP-initiiert), um den vom Identitätsanbieter initiierten** Ablauf zu überschreiben und nur den vom Dienstanbieter initiierten Flow zu verwenden.

2. Fügen Sie unter **Erweiterte Attribute (optional)**zusätzliche Informationen über den Benutzer hinzu, die für Zugriffskontrollentscheidungen an die Anwendung gesendet werden.



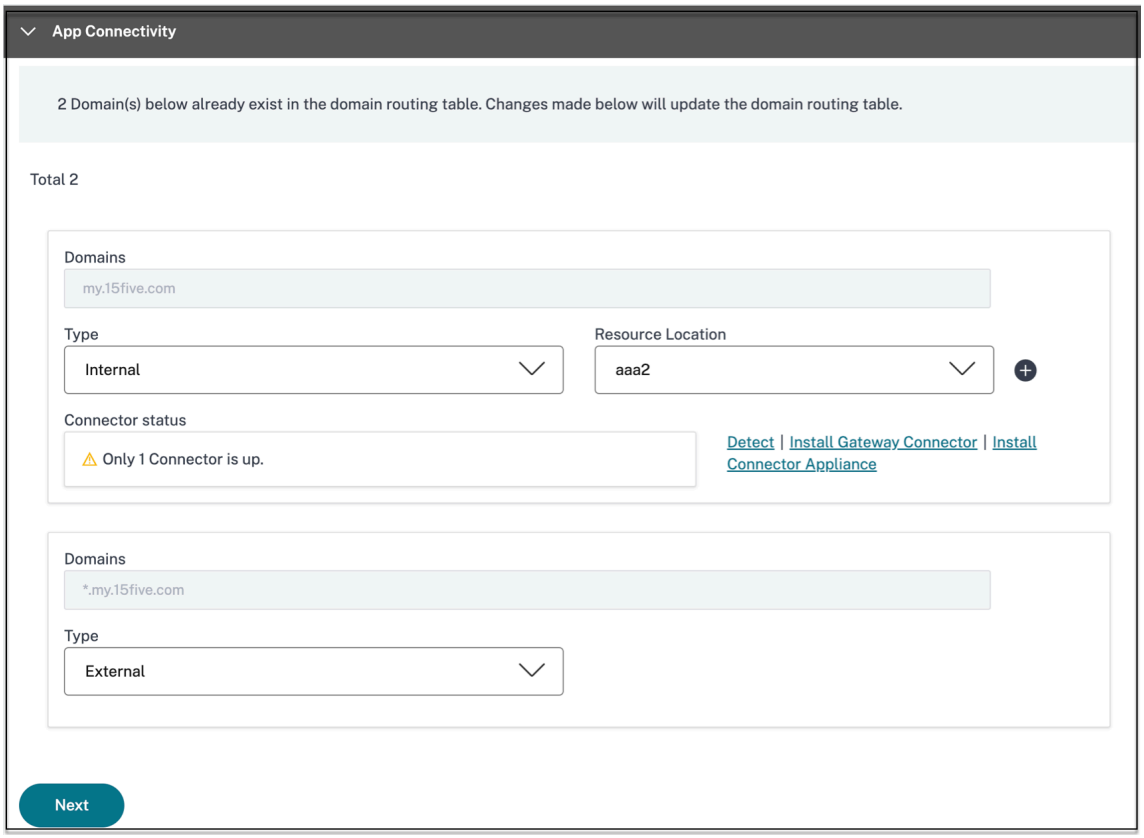
3. Laden Sie die Metadatendatei herunter, indem Sie auf den Link unter SAML-Metadaten klicken.** Verwenden Sie die heruntergeladene Metadatendatei, um SSO auf dem SaaS-Apps-Server zu konfigurieren.

   > **Hinweis:**
   >
   > - Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.
   > - Sie können das Zertifikat auch aus der **Zertifikatsliste** herunterladen und das Zertifikat verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.

4. Klicken Sie auf **Weiter.**

Anwendungsrouting definieren

1. Definieren Sie im Abschnitt **App Connectivity** das Routing für die zugehörigen Anwendungsdomänen, wenn die Domänen extern oder intern über Citrix Connector Appliances weitergeleitet werden müssen. Einzelheiten finden Sie unter Weiterleiten von Tabellen zur Lösung von Konflikten, wenn die zugehörigen Domänen sowohl in SaaS als auch in Web-Apps identisch sind.

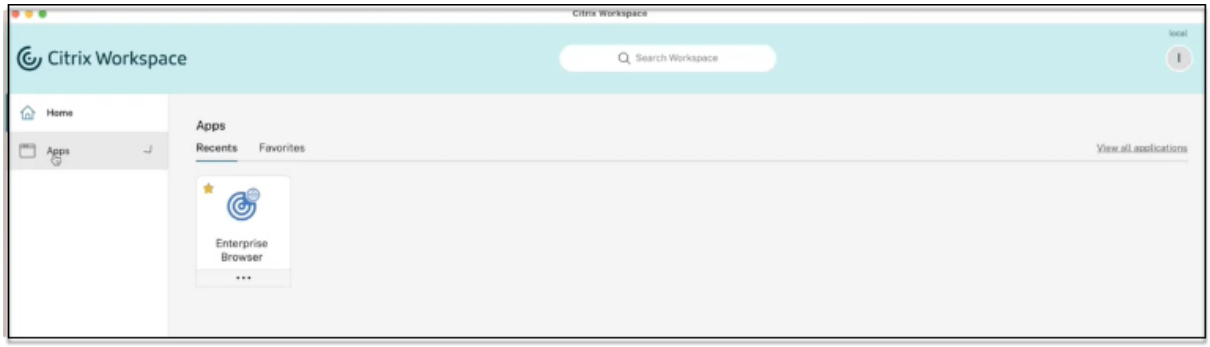


2. Klicken Sie auf **Fertig stellen.**

   Nachdem Sie auf **Fertig stellen**geklickt haben, wird die App zur Seite Anwendungen hinzugefügt. Sie können eine App auf der Seite "Anwendungen"bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu in einer App auf die Ellipsenschaltfläche und wählen Sie die Aktionen entsprechend aus.

   - **Anwendung bearbeiten**
   - **Löschen**

Wenn Sie eine Web- oder SaaS-App über den Secure Private Access Service veröffentlichen und diese App nicht ausgeblendet ist, wird die Citrix Enterprise Browser App automatisch in der Citrix Workspace-Benutzeroberfläche angezeigt. Darüber hinaus wird der Citrix Enterprise Browser standardmäßig als Lieblings-App hinzugefügt. Endbenutzer können den Workspace-Browser ohne URL starten und mit den Workspace-Browsern auf interne Websites zugreifen.



Referenzen

Eine vollständige End-to-End-Konfiguration einer App finden Sie unter Admin-geführter Workflow für einfaches Onboarding und Setup.

Unterstützung für Client-Server-Apps

February 16, 2024

Mit Citrix Secure Private Access können Sie jetzt auf alle privaten Apps zugreifen, einschließlich TCP/UDP- und HTTPS-Apps, entweder mit einem nativen Browser oder einer nativen Clientanwendung über den Citrix Secure Access-Client, der auf Ihrem Computer ausgeführt wird.

Mit der zusätzlichen Unterstützung von Client-Server-Anwendungen in Citrix Secure Private Access können Sie jetzt die Abhängigkeit von einer herkömmlichen VPN-Lösung beseitigen, um Remotebenutzern Zugriff auf alle privaten Apps zu ermöglichen.

Preview-Features

Unterstützung für DNS-Suffixe zur Auflösung von FQDNs in IP-Adressen.

Funktionsweise

Endbenutzer können problemlos auf alle ihre genehmigten privaten Apps zugreifen, indem sie einfach den Citrix Secure Access Client auf ihren Client-Geräten installieren.

- Für Windows kann die Client-Version (22.3.1.5 und höher) von https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html heruntergeladen werden.

- Für macOS kann die Client-Version (22.02.3 und höher) aus dem App Store heruntergeladen werden.

Admin-Konfiguration —Client-basierter Zugriff von Citrix Secure Access auf TCP/UDP-Apps

Voraussetzungen

Stellen Sie sicher, dass die folgenden Anforderungen für den Zugriff auf TCP/UDP-Apps erfüllt sind.

- Zugriff auf Citrix Secure Private Access in der Citrix Cloud.
- Citrix Cloud Connector —Installieren Sie eine Citrix Cloud Connector für Active Directory-Domänenkonfiguration wie in der Cloud Connector-Installationerfasst.
- Identitäts- und Zugriffsmanagement —Schließen Sie die Konfiguration ab. Einzelheiten finden Sie unter Identitäts- und Zugriffsmanagement.
- Connector-Appliance —Citrix empfiehlt, zwei Connector-Appliances in einer Hochverfügbarkeitskonfiguration an Ihrem Ressourcenstandort zu installieren Der Connector kann entweder on-premises, im Hypervisor des Rechenzentrums oder in der Public Cloud installiert werden. Weitere Informationen zur Connector-Appliance und ihrer Installation finden Sie unter Connector Appliance for Cloud Services.
- Sie müssen eine Connector Appliance für TCP/UDP-Apps verwenden.

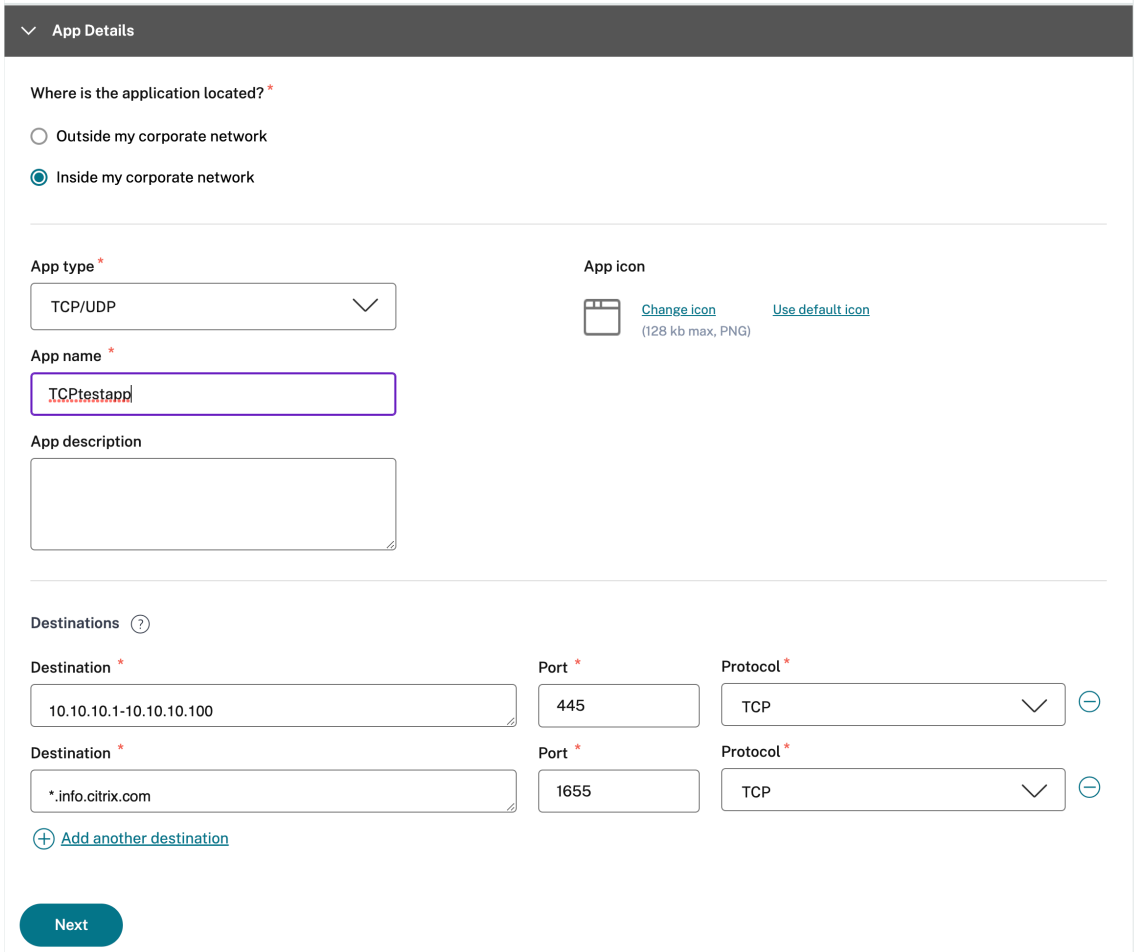
> **Wichtig:**
>
> Eine vollständige End-to-End-Konfiguration einer App finden Sie unter Admin-geführter Workflow für einfaches Onboarding und Setup.

1. Klicken Sie auf der Citrix Secure Private Access-Kachel auf **Verwalten**.
2. Klicken Sie auf **Weiter** und dann **auf App hinzufügen** .

   > **Hinweis:**
   >
   > Die Schaltfläche **Weiter** wird nur angezeigt, wenn Sie den Assistenten zum ersten Mal verwenden. Bei den nachfolgenden Verwendungen können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen** klicken.

   App ist eine logische Gruppierung von Zielen. Wir können eine App für mehrere Ziele erstellen - Jedes Ziel bedeutet verschiedene Server im Backend. Eine App kann beispielsweise einen SSH, einen RDP, einen Datenbankserver und einen Webserver haben. Sie müssen nicht eine App pro Ziel erstellen, aber eine App kann viele Ziele haben.
3. Klicken **Sie im Abschnitt Vorlage auswählen** auf **Überspringen**, um die TCP/UDP-App manuell zu konfigurieren.

4. Wählen Sie im Abschnitt **App-Details** die Option **In meinem Unternehmensnetzwerk**aus, geben Sie die folgenden Details ein und klicken Sie auf **Weiter**.



- **App-Typ** —Wählen Sie TCP/UDP aus.
- **Appname** —Name der Anwendung.
- **App-Symbol**—Ein App-Symbol wird angezeigt. Das Feld ist optional.
- **App-Beschreibung** —Beschreibung der App, die Sie hinzufügen. Das Feld ist optional.
- **Ziele** —IP-Adressen oder FQDNs der Back-End-Computer, die sich im Ressourcenstandort befinden. Ein oder mehrere Ziele können wie folgt angegeben werden.
  - **IP-Adresse v4**
  - **IP-Adressbereich** —Beispiel: 10.68.90.10-10.68.90.99
  - **CIDR** —Beispiel: 10.106.90.0/24
  - **FQDN der Maschinen oder Domänenname** —Einzel- oder Platzhalterdomäne. Beispiel: ex.destination.domain.com, *.domain.com

> **Wichtig:**
>
> Endbenutzer können über FQDN auf die Apps zugreifen, auch wenn der Administrator die Apps mithilfe der IP-Adresse konfiguriert hat. Dies ist möglich, weil der Citrix Secure Access Client einen FQDN in die echte IP-Adresse auflösen kann. Die folgende Tabelle enthält Beispiele für verschiedene Ziele und wie Sie mit diesen Zielen auf die Apps zugreifen können:

Ziel-Eingabe	So greifen Sie auf die App zu
10.10.10.1-10.10.10.100	Es wird erwartet, dass der Endbenutzer nur über IP-Adressen in diesem Bereich auf die App zugreift.
10.10.10.0/24	Es wird erwartet, dass der Endbenutzer nur über die im IP-CIDR konfigurierten IP-Adressen auf die App zugreift.
10.10.10.101	Es wird erwartet, dass der Endbenutzer nur bis 10.10.10.101 auf die App zugreift
`*.info.citrix.com`	Es wird erwartet, dass der Endbenutzer auf Unterdomänen von `info.citrix.com` und auch `info.citrix.com` (der übergeordneten Domäne) zugreift. Zum Beispiel `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Hinweis:** Der Platzhalter muss immer das Startzeichen der Domäne sein und nur ein *. ist zulässig.
info.citrix.com	Es wird erwartet, dass der Endbenutzer nur auf `info.citrix.com` und nicht auf Unterdomänen zugreift. Zum Beispiel, `sub1.info.citrix.com` ist nicht zugänglich.

- **Port** —Der Port, auf dem die App ausgeführt wird. Administratoren können mehrere Ports oder Portbereiche pro Ziel konfigurieren.

  Die folgende Tabelle enthält Beispiele für Ports, die für ein Ziel konfiguriert werden können.

Port-Eingang	Beschreibung
*	Standardmäßig ist das Port-Feld auf " * " (any port) eingestellt. Die Portnummern von 1 bis 65535 werden für das Ziel unterstützt.
1300–2400	Die Portnummern von 1300 bis 2400 werden für das Ziel unterstützt.
38389	Nur die Portnummer 38389 wird für das Ziel unterstützt.
22,345,5678	Die Ports 22, 345, 5678 werden für das Ziel unterstützt.
1300–2400, 42000-43000,22,443	Die Portnummern reichen von 1300 bis 2400, 42000—43000, und die Ports 22 und 443 werden für das Ziel unterstützt.

> **Hinweis:**
>
> Wildcard-Port (*) kann nicht mit Portnummern oder Bereichen koexistieren.

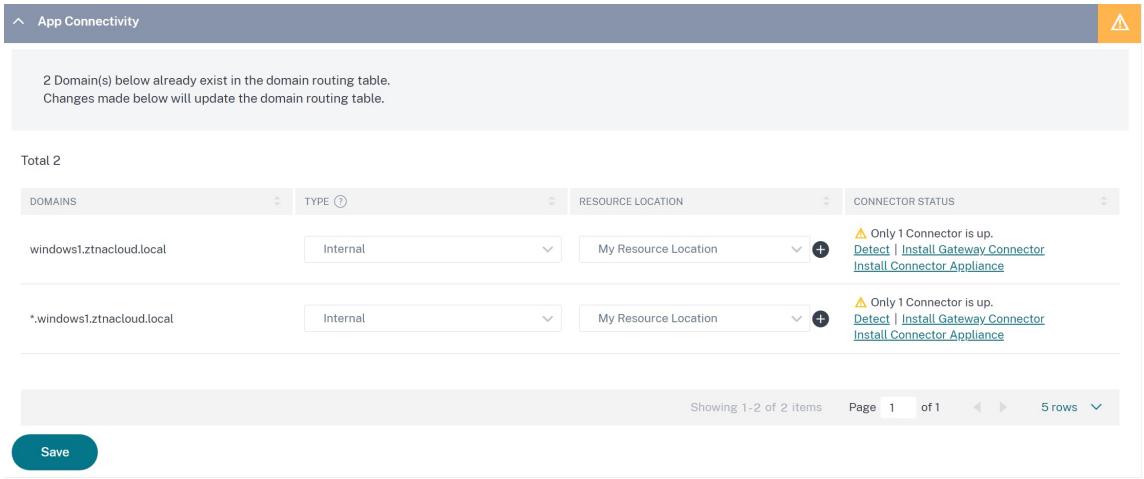
- **Protokoll** —TCP/UDP

5. Im Abschnitt **App-Konnektivität** ist eine Miniversion der Tabelle **Anwendungsdomänen** verfügbar, um die Routing-Entscheidungen zu treffen. Für jedes Ziel können Sie einen anderen oder denselben Ressourcenstandort wählen. Ziele, die im vorherigen Schritt konfiguriert wurden, werden in der Spalte **DESTINATION** aufgefüllt. Die hier hinzugefügten Ziele werden auch der Haupttabelle **Anwendungsdomänen** hinzugefügt. ****Die Tabelle Anwendungsdomänen ist die Informationsquelle für die Routing-Entscheidung, um den Verbindungsaufbau und den Datenverkehr an den richtigen Ressourcenstandort weiterzuleiten. Weitere Informationen zur Tabelle **Anwendungsdomänen** und zu möglichen IP-Konfliktszenarien finden Sie im Abschnitt *Anwendungsdomänen —IP-Adresskonfliktlösung* .
6. Wählen Sie für die folgenden Felder eine Eingabe aus dem Dropdown-Menü aus und klicken Sie auf **Weiter**.

   > **Hinweis:**
   >
   > Nur der interne Routentyp wird unterstützt.

   - **RESSOURCENSTANDORT** —Im Dropdown-Menü müssen Sie eine Verbindung zu einem Ressourcenstandort herstellen, auf dem mindestens eine Connector-Appliance installiert ist.

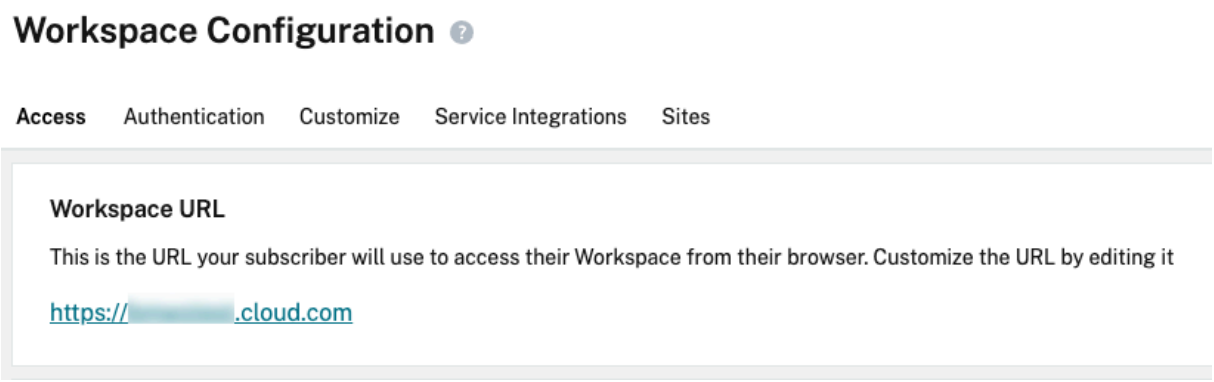
> **Hinweis:**
>
> Die Installation der Connector Appliance wird im Abschnitt App Connectivity unterstützt. Sie können es auch im Abschnitt Ressourcenstandorte im Citrix Cloud-Portal installieren. Weitere Informationen zum Erstellen eines Ressourcenstandorts finden Sie unter Einrichten von Ressourcenstandorten.



7. Klicken Sie auf **Fertig stellen**. Die App wird der Seite „**Anwendungen**“hinzugefügt. Sie können eine App auf der Seite **Anwendungen** bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu in einer App auf die Ellipsenschaltfläche und wählen Sie die Aktionen entsprechend aus.

   - **Anwendung bearbeiten**
   - **Löschen**

> **Hinweis:**
>
> - Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
> - Informationen zum Konfigurieren der für die Benutzer erforderlichen Authentifizierungsmethoden finden Sie unter Einrichten von Identität und Authentifizierung.
> - Um die Workspace-URL abzurufen, die für die Benutzer freigegeben werden soll, klicken Sie im Citrix Cloud-Menü auf **Workspace-Konfiguration** und wählen Sie die Registerkarte **Zugriff** aus.



Admin-Konfiguration —Client-basierter Zugriff von Citrix Secure Access auf HTTP/HTTPS-Apps

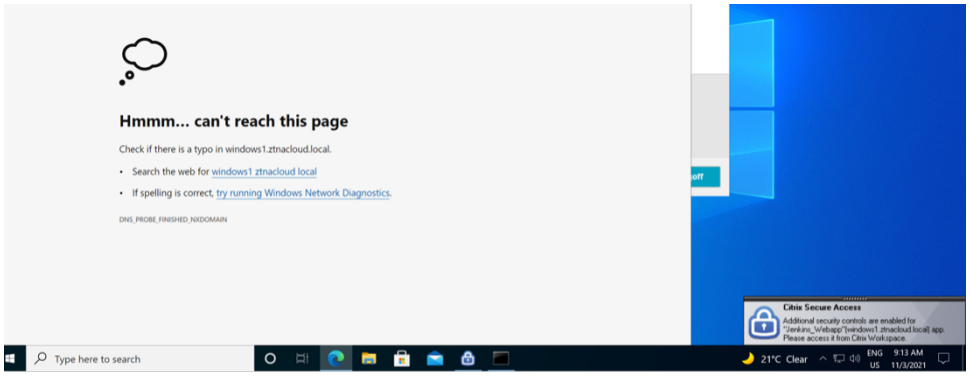
> **Hinweis:**
>
> Um mit dem Citrix Secure Access Client auf vorhandene oder neue HTTP/HTTPS-Apps zuzugreifen, müssen Sie mindestens ein Connector Appliance (zwei für hohe Verfügbarkeit empfohlen) an Ihrem Ressourcenstandort installieren. Die Connector-Appliance kann on-premises, im Datencenter-Hypervisor oder in der Public Cloud installiert werden. Einzelheiten zur Connector Appliance und ihrer Installation finden Sie unter Connector Appliance für Cloud-Dienste.

Voraussetzungen

- Zugriff auf Citrix Secure Private Access in der Citrix Cloud.

Wichtige Hinweise

- Auf interne Web-Apps, die mit erweiterten Sicherheitskontrollen durchgesetzt wurden, kann nicht über den Citrix Secure Access Client zugegriffen werden.
- Wenn Sie versuchen, auf eine HTTP(S) -Anwendung zuzugreifen, für die erweiterte Sicherheitssteuerung aktiviert ist, wird die folgende Popup-Meldung angezeigt. **Zusätzliche Sicherheitskontrollen sind für die App <"app name"(FQDN)> aktiviert. Bitte greifen Sie von Citrix Workspace darauf zu.**



- Wenn Sie die SSO-Erfahrung aktivieren möchten, greifen Sie mit der Citrix Workspace-App oder dem Webportal auf die Webanwendungen zu.

Die Schritte zum Konfigurieren von HTTP (S) -Apps bleiben dieselben wie die vorhandenen Funktionen, die unter Support for Enterprise Web Appserläutert werden.

Adaptiver Zugriff auf TCP/UDP- und HTTP (S) -Apps

Der adaptive Zugriff bietet Administratoren die Möglichkeit, den Zugriff auf geschäftskritische Apps basierend auf mehreren kontextbezogenen Faktoren wie der Überprüfung des Gerätestatus, der Geolokalisierung der Benutzer, der Benutzerrolle und der Risikobewertung des Citrix Analytics Service zu steuern.

> **Hinweis:**
>
> - Sie können den Zugriff auf TCP/UDP-Anwendungen verweigern, Administratoren erstellen Richtlinien basierend auf den Benutzern, Benutzergruppen, den Geräten, von denen aus die Benutzer auf die Anwendungen zugreifen, und dem Ort (Land), von dem aus auf eine Anwendung zugegriffen wird. Der Zugriff auf Anwendungen ist standardmäßig zulässig.
> - Das für eine App erstellte Benutzerabonnement gilt für alle TCP/UDP-App-Ziele, die für die TCP/UDP-Anwendungen konfiguriert sind.

So erstellen Sie eine Richtlinie für adaptiven Zugriff

Administratoren können den vom Administrator geleiteten Workflow-Assistenten verwenden, um den Zero-Trust-Netzwerkzugriff auf SaaS-Apps, interne Web-Apps und TCP/UDP-Apps im Secure Private Access Service zu konfigurieren.

> **Hinweis:**
>
> - Einzelheiten zum Erstellen einer Richtlinie für adaptiven Zugriff finden Sie unter Erstellen von Zugriffsrichtlinien.

> • Eine End-to-End-Konfiguration von Zero Trust Network Access auf SaaS-Apps, interne Web-Apps und TCP/UDP-Apps im Secure Private Access Service finden Sie unter Admin-gesteuerter Workflow für einfaches Onboarding und Einrichtung.

Wichtige Hinweise

- Der Zugriff auf eine vorhandene Web-App, für die erweiterte Sicherheit aktiviert ist, wird über den Secure Access-Client verweigert. Es wird eine Fehlermeldung angezeigt, die darauf hindeutet, sich mit der Citrix Workspace-App anzumelden.
- Beim Zugriff auf die App über den Secure Access Client gelten Richtlinienkonfigurationen für Web-Apps, die auf der Risikobewertung des Benutzers, der Überprüfung des Gerätestatus usw. über die Citrix Workspace-App basieren.
- Die an eine Anwendung gebundene Richtlinie gilt für alle Ziele in der Anwendung.

DNS-Auflösung

Die Connector-Appliance muss eine DNS-Serverkonfiguration für die DNS-Auflösung haben.

Schritte zur Installation des Citrix Secure Access Clients auf einer Windows-Maschine

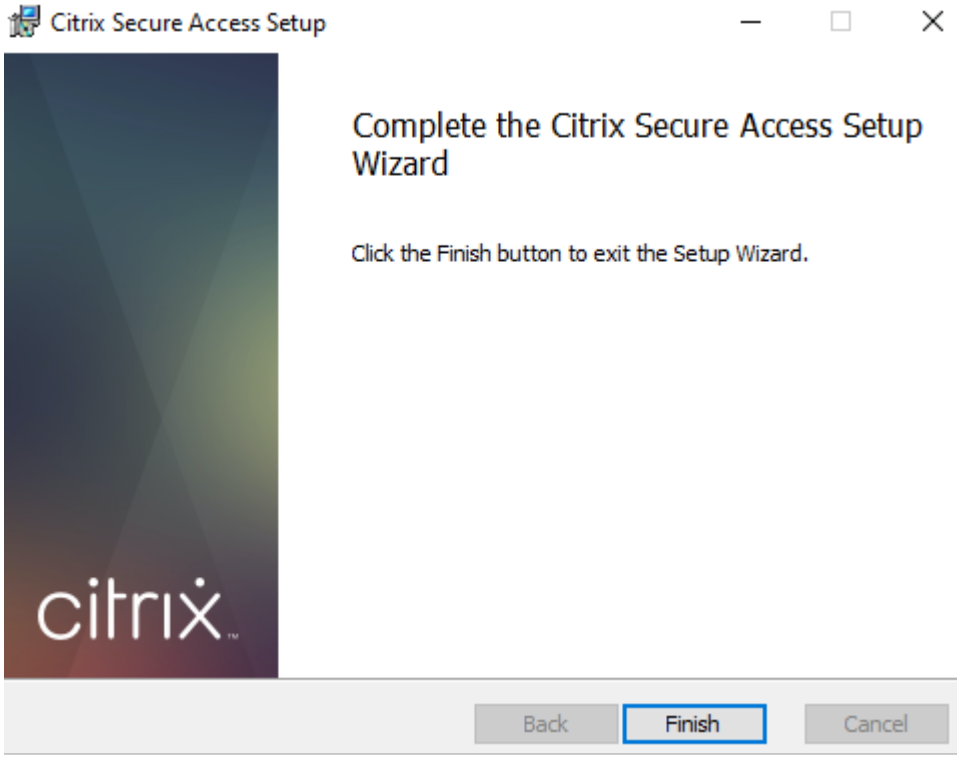
Unterstützte Betriebssystemversionen:

Windows —Windows 11, Windows 10, Windows Server 2016 und Windows Server 2019.

Im Folgenden finden Sie die Schritte, um den Citrix Secure Access Client auf einer Windows-Maschine zu installieren.

1. Laden Sie den Citrix Secure Access Client von https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html herunter.
2. Klicken Sie auf **Installieren**, um den Client auf Ihrem Windows-Computer zu installieren. Wenn Sie einen vorhandenen Citrix Gateway-Client haben, wird dieser aktualisiert.

3. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.



> **Hinweis:**
>
> Mehrbenutzersitzungen in Windows werden nicht unterstützt.

Installationsschritte für Microsoft Edge Runtime

Microsoft Edge Runtime ist jetzt für die Authentifizierungsoberfläche auf dem Secure Access-Client erforderlich.
Es ist standardmäßig auf den neuesten Windows 10- und Windows 11-Computern installiert. Führen Sie für Computer mit früheren Versionen die folgenden Schritte aus.

1. Gehen Sie zum folgenden Link, https://go.microsoft.com/fwlink/p/?LinkId=2124703.
2. Downloaden und installieren Sie Microsoft Edge. Wenn auf dem Benutzersystem die Microsoft Edge-Runtime nicht installiert ist, werden Sie vom Citrix Secure Access Client zur Installation aufgefordert, wenn Sie versuchen, eine Verbindung mit der Workspace-URL herzustellen.

> **Hinweis:**
>
> Sie können eine automatisierte Lösung wie SCCM-Software oder eine Gruppenrichtlinie verwenden, um den Citrix Secure Access Client oder Microsoft Edge Runtime auf die Client-Computer zu übertragen.

Schritte zur Installation des Citrix Secure Access Clients auf einem macOS-Computer

Voraussetzungen:

- Laden Sie den Citrix Secure Access Client für macOS aus dem App Store herunter. Diese App ist ab macOS 10.15 (Catalina) und neuer verfügbar.
- Vorschau-Builds sind in der TestFlight-App nur für macOS Monterey (12.x) verfügbar.
- Wenn Sie zwischen der App Store-App und der TestFlight-Vorschau-App wechseln, müssen Sie das Profil, das Sie mit der Citrix Secure Access-App verwenden möchten, neu erstellen. Wenn Sie beispielsweise ein Verbindungsprofil mit verwendet haben `blr.abc.company.com`, löschen Sie das VPN-Profil und erstellen Sie dasselbe Profil erneut.

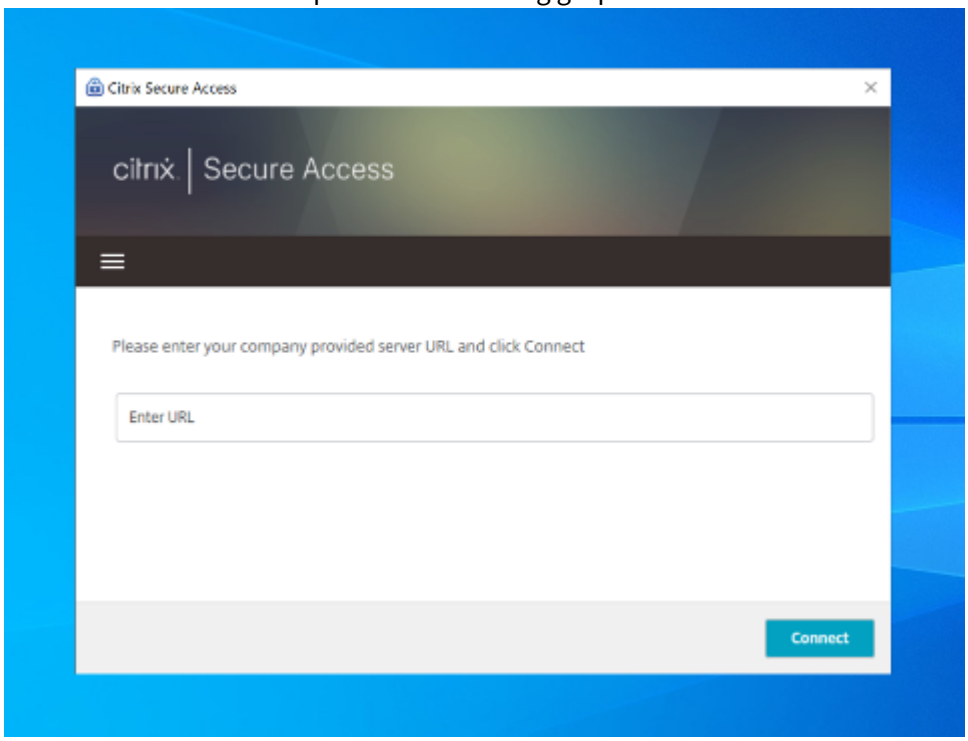
Unterstützte Betriebssystemversionen:

- macOS: 12.x (Monterey). 11.x (Big Sur) und 10.15 (Catalina) werden unterstützt.
- Mobilgeräte: iOS und Android werden nicht unterstützt.

Starten einer konfigurierten App —Endbenutzer-Fluss

1. Starten Sie den Citrix Secure Access Client auf dem Clientgerät.
2. Geben Sie die vom Kundenadministrator bereitgestellte Workspace-URL in das URL-Feld des Citrix Secure Access-Clients ein und klicken Sie auf **Verbinden**. Es ist eine einmalige Aktivität

und die URL wird für die spätere Verwendung gespeichert.



3. Der Benutzer wird basierend auf der in Citrix Cloud konfigurierten Authentifizierungsmethode zur Authentifizierung aufgefordert.
   Nach erfolgreicher Authentifizierung kann der Benutzer auf die konfigurierten privaten Apps zugreifen.

Benachrichtigungen von Benutzern

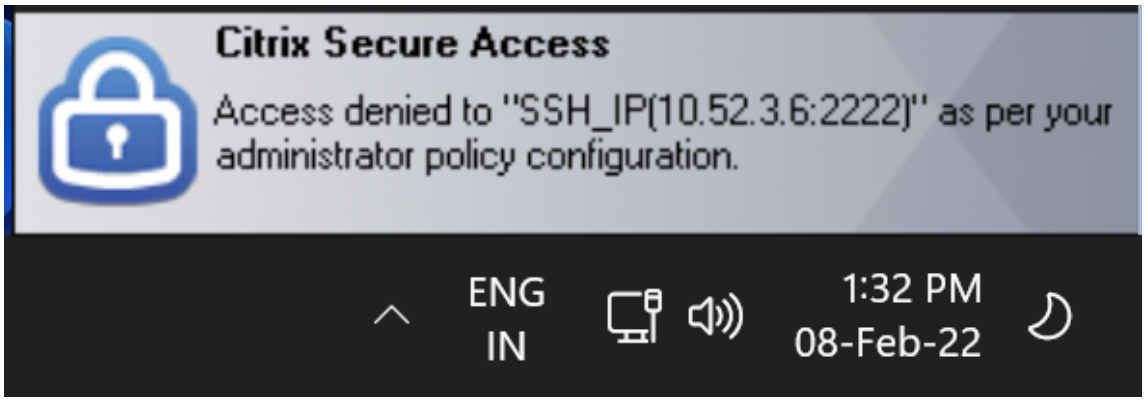
In den folgenden Szenarien wird eine Popup-Benachrichtigung angezeigt:

- Die App ist vom Administrator nicht für den Benutzer autorisiert.

  Ursache: Die Anwendung, die für die zugegriffene Ziel-IP-Adresse oder den FQDN konfiguriert ist, ist für den angemeldeten Benutzer nicht abonniert.

- Die Bewertung der Zugriffsrichtlinien führt zu einer Zugriffsverweigerung.

  Ursache: Der Zugriff auf die Ziel-IP-Adresse oder den FQDN wurde verweigert, da die an die Anwendung gebundene Richtlinie als "Zugriff verweigern"für den angemeldeten Benutzer ausgewertet wird.



- Die erweiterte Sicherheitssteuerung ist für die App aktiviert.

  Ursache: Die erweiterte Sicherheitssteuerung ist für die Anwendung für das Ziel aktiviert, auf das zugegriffen wird. Die Anwendung kann mit der Citrix Workspace App gestartet werden.

Weitere Informationen

Anwendungsdomänen —Konfliktlösung bei IP-Adressen

Ziele, die beim Erstellen einer App hinzugefügt wurden, werden zu einer Haupt-Routingtabelle hinzugefügt.
Die Routing-Tabelle ist die Informationsquelle für die Routing-Entscheidung, um den Verbindungsaufbau und den Verkehr an den richtigen Ressourcenstandort zu leiten.

- Die Ziel-IP-Adresse muss an allen Ressourcenstandorten eindeutig sein.
- Citrix empfiehlt, eine Überlappung der IP-Adressen oder Domänen in der Routingtabelle zu vermeiden. Falls Sie auf eine Überlappung stoßen, müssen Sie diese beheben.

Es folgen die Arten von Konfliktszenarien. **Complete Overlap** ist das einzige Fehlerszenario, das die Administratorkonfiguration einschränkt, bis der Konflikt gelöst ist.

Konflikte	Domäneneintrag für vorhandene	Neuer Eintrag von App Addition	Ergebnis
Teilmenge überlappen	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	Zulassen; Warnhinweise — Teilmengenüberschneidung der IP-Domäne mit vorhandenen Einträgen
Teilmenge überlappen	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	Zulassen; Warnhinweise — Teilmengenüberschneidung der IP-Domäne mit vorhandenen Einträgen
Teilweise Überlappung	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	Zulassen; Warnhinweise - Teilweise Überlappung der IP-Domäne mit vorhandenen Einträgen
Teilweise Überlappung	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	Zulassen; Warnhinweise - Teilweise Überlappung der IP-Domäne mit vorhandenen Einträgen

Konflikte	Domäneneintrag für vorhandene	Neuer Eintrag von App Addition	Ergebnis
Vollständige Überlappung	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	Fehler; <Completely overlapping IP domain's value> IP-Domäne überschneidet sich vollständig mit vorhandenen Einträgen. Bitte ändern Sie den vorhandenen Routing-IP-Eintrag oder konfigurieren Sie ein anderes Ziel
Vollständige Überlappung	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	Fehler; <Completely overlapping IP domain's value> IP-Domäne überschneidet sich vollständig mit vorhandenen Einträgen. Bitte ändern Sie den vorhandenen Routing-IP-Eintrag oder konfigurieren Sie ein anderes Ziel

Exakte Übereinstimmung	20.20.20.0/29 RL1	20.20.20.0/29	Zulassen; Domänen sind in der Domain-Routing-Tabelle vorhanden. Vorgenommene Änderungen aktualisieren die Domänen-Routingtabelle

Hinweis:

- Wenn die hinzugefügten Ziele zu einer vollständigen Überschneidung führen, wird beim Konfigurieren der App im Abschnitt **App-Details** ein Fehler angezeigt. Der Administrator muss diesen Fehler beheben, indem er die Ziele im Abschnitt **App-Konnektivität** ändert.

  Wenn im Abschnitt **App-Details** keine Fehler auftreten, kann der Administrator mit dem Speichern der App-Details fortfahren. Wenn die Ziele jedoch im Abschnitt **App-Konnektivität** eine Teilmenge aufweisen und sich teilweise miteinander oder mit vorhandenen Einträgen in der Hauptroutingtabelle überlappen, wird eine Warnmeldung angezeigt. In diesem Fall kann der Administrator entweder den Fehler beheben oder mit der Konfiguration fortfahren.

- Citrix empfiehlt, eine saubere **Anwendungsdomänentabelle** zu führen. Es ist einfacher, neue Routing-Einträge zu konfigurieren, wenn die IP-Adressdomänen ohne Überlappungen in entsprechende Chunks aufgeteilt werden.

Anmelde- und Abmeldeskriptkonfigurationsregister

Der Citrix Secure Access Client greift über die folgenden Registrierungen auf die Anmelde- und Abmeldeskriptkonfiguration zu, wenn der Citrix Secure Access Client eine Verbindung zum Citrix Secure Private Access-Clouddienst herstellt.

Registrierung: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- Anmeldeskriptpfad: SecureAccessLogInScript type REG_SZ
- Abmeldeskriptpfad: SecureAccessLogOutScript type REG_SZ

Versionshinweise

- Citrix Secure Access für Windows —Versionshinweise

- Citrix Secure Access für macOS —Versionshinweise
- Versionsinformationen zu Citrix Secure Private Access

Reservierte CIDR-Adressen für die TCP- und UDP-Server

December 27, 2023

Administratoren können reservierte CIDR-IP-Adressen für die TCP/UDP-Server konfigurieren. Diese IP-Adressen werden in der DNS-Antwort anstelle der tatsächlichen IP-Adresse während der DNS-Auflösung gemeinsam genutzt.

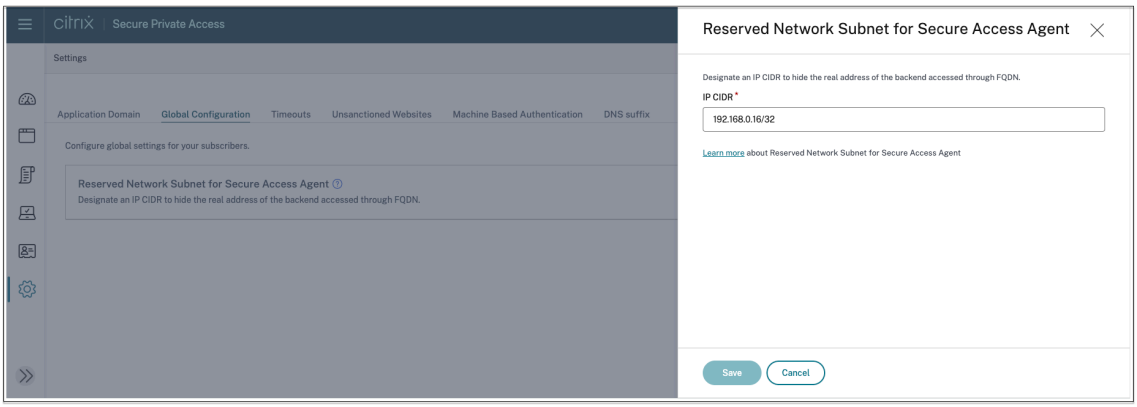
Im Folgenden sind die zulässigen reservierten CIDR-IP-Adressbereiche aufgeführt:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> **Hinweis:**
>
> Stellen Sie sicher, dass die reservierten IP-Adressen nicht mit den folgenden in Konflikt stehen:
>
> - IP-Adresse, die für TCP/UDP-Anwendungen am Ressourcenstandort des Kunden konfiguriert ist.
> - Netzwerk-Subnetz der Client-Computer.

Reservierte CIDR-IP-Adressen konfigurieren

1. Klicken Sie auf **Einstellungen**und dann auf **Globale Konfiguration**.



2. Klicken Sie unter **Reserviertes Netzwerksubnetz für Secure Access Agent**auf **Verwalten**.
3. Geben Sie **unter IP CIDR**den privaten IP-Adressbereich ein.

4. Klicken Sie auf **Speichern**.

DNS-Suffixe zur Auflösung von FQDNs in IP-Adressen

December 27, 2023

Das DNS-Suffix ist eine globale Konfiguration, die für alle Endbenutzer angewendet wird. Die DNS-Suffix-Funktion des Citrix Secure Private Access-Dienstes kann für die folgenden Anwendungsfälle verwendet werden:

- Ermöglichen Sie dem Citrix Secure Access Client, einen nicht vollständig qualifizierten Domänennamen (Hostnamen) in einen vollqualifizierten Domänennamen (FQDN) aufzulösen, indem Sie die DNS-Suffixdomäne für die Backend-Server hinzufügen.
- Ermöglichen Sie Administratoren, Anwendungen mithilfe von IP-Adressen (IP-CIDR/IP-Bereich) zu konfigurieren, sodass die Endbenutzer über den entsprechenden FQDN unter der DNS-Suffixdomäne auf die Anwendungen zugreifen können.

Wenn beispielsweise bei der Auflösung eines nicht vollständig qualifizierten Domänennamens “workday”das DNS-Suffix “citrix.net”konfiguriert ist, hängt das Betriebssystem das Suffix “citrix.net”an und löst es in “workday.citrix.net”auf.

Wenn mehrere DNS-Suffixe konfiguriert sind, werden die DNS-Suffixe nacheinander aufgelöst. Nehmen wir zum Beispiel an, dass die folgenden Suffixe hinzugefügt werden:

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

Wenn ein Endbenutzer “workday”eingibt, versucht das Betriebssystem, die FQDNs in der folgenden Reihenfolge aufzulösen. Wenn es mit einem Suffix erfolgreich ist, werden die übrigen Suffixe übersprungen.

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> **Wichtig:**
>
> - Die DNS-Suffixkonfiguration kann es dem Client nur ermöglichen, einen nicht vollständig qualifizierten Domänennamen aufzulösen, indem er der mit der DNS-Suffix-Funktion konfigurierten Domäne ein Suffix anfügt. Damit ein Endbenutzer auf einen FQDN unter der DNS-Suffixdomäne zugreifen kann, muss der Administrator eine Anwendung mit einer IP-

Adresse, einem FQDN oder einer Wildcard-Domäne konfigurieren. Einzelheiten finden Sie unter Punkt 4 unter Anwendungsbeispiel.

- Wenn zwei verschiedene Anwendungen konfiguriert sind, eine mit FQDN und eine andere mit IP-Adresse (beide entsprechen demselben Backend-Server), hat die Richtlinie der Anwendung mit IP-Adresse höhere Priorität. Einzelheiten finden Sie unter Punkt 5 unter Anwendungsbeispiel.

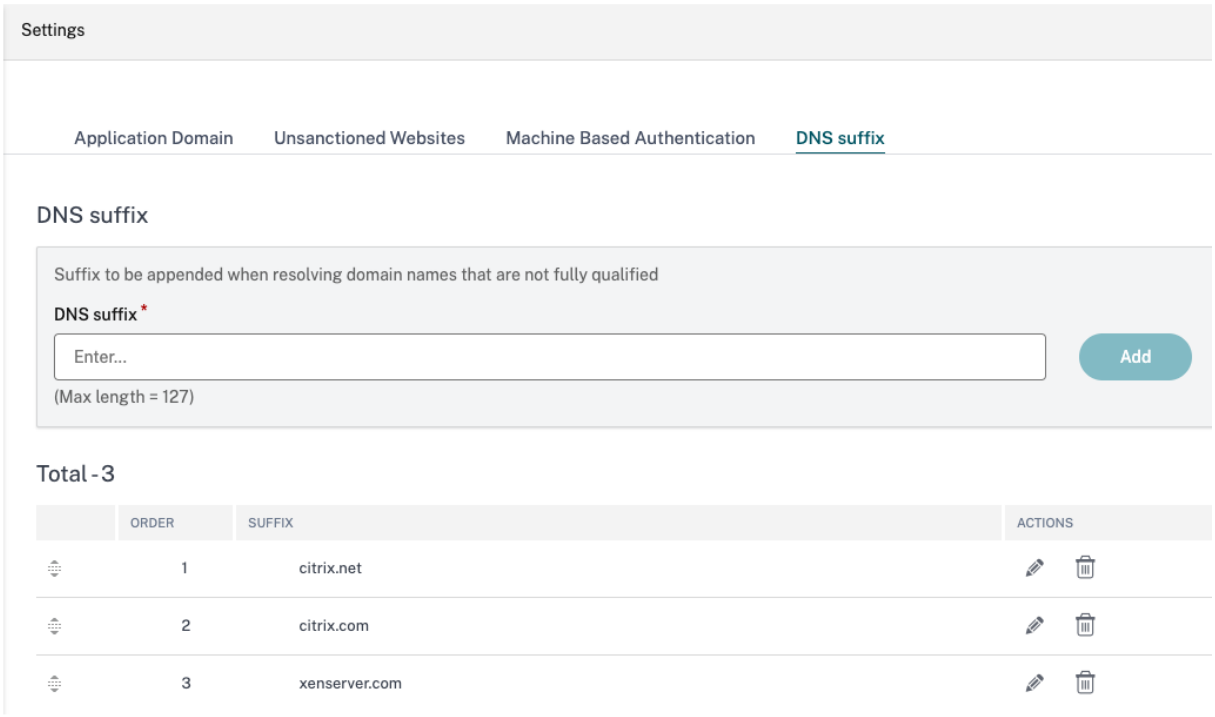
Voraussetzungen

- Kunden müssen Anspruch auf die Secure Private Access Advanced Edition haben, um die DNS-Suffix-Funktion nutzen zu können.
- Wenden Sie sich an das Citrix Product Management Team, um die Feature-Flags für das DNS-Suffix zu aktivieren.

So fügen Sie DNS-Suffixe hinzu

1. Klicken Sie auf der Kachel Secure Private Access auf **Verwalten** .
2. Klicken Sie auf der Secure Private Access-Landingpage auf **Einstellungen** und dann auf **DNS-Suffix**.
3. Geben Sie im Feld **DNS-Suffix** das Suffix ein, das angehängt werden muss, wenn ein nicht vollständig qualifizierter Name aufgelöst wird.
4. Klicken Sie auf **Hinzufügen**.

Die Suffixe werden in der Reihenfolge aufgeführt, in der sie hinzugefügt wurden. Admins können die Suffixe löschen oder ändern.



Anwendungsbeispiel

Beachten Sie Folgendes:

- Ein Administrator hat einem Computer im Kundennetzwerk die IP-Adresse 192.0.2.1 zugewiesen.
- Die FQDNs für den Computer (mit den IP-Adressen 192.0.2.1) befinden sich unter der Domäne “citrix.net”(Beispiel workday.citrix.net).

		DNS-Suffix und App-Konfiguration	Erfahrung für Endbenutzer
	1	Admin konfiguriert das DNS-Suffix als “citrix.net”und erstellt eine App mit der IP-Adresse 192.0.2.1, deren Zugriffsrichtlinie für user1 auf “allow” gesetzt ist.	Wenn Benutzer1 versucht, eine Verbindung zu “workday” herzustellen, erhält der FQDN das Suffix “citrix.net” (workday.citrix.net) und die IP-Adresse wird in 192.0.2.1 aufgelöst. Da 192.0.2.1 für Benutzer1 mit einer konfigurierten App zulässig ist, wird der Zugriff gewährt. **Hinweis:** Endbenutzer können mit 192.0.2.1 oder workday.citrix.net oder “workday”auf die Workday-App zugreifen. Ohne DNS-Suffix-Konfiguration wird der Zugriff über “workday” und “workday.citrix.net” verweigert.

		DNS-Suffix und App-Konfiguration	Erfahrung für Endbenutzer
	2	Admin konfiguriert das DNS-Suffix als “citrix.net”, erstellt eine App mit FQDN (workday.citrix.net) und legt die Zugriffsrichtlinie für user1 auf “allow”fest.	Wenn Benutzer1 versucht, eine Verbindung zu “workday” herzustellen, wird “citrix.net”an das Suffix “workday” (workday.citrix.net) angehängt. Endbenutzer können auf Workday zugreifen, da eine Anwendung mit “workday.citrix.net” konfiguriert ist und die Zugriffsrichtlinie für Benutzer1 auf “zulassen”gesetzt ist. **Hinweis:** Endbenutzer können über workday.citrix.net oder “workday”auf die Workday-App zugreifen. Der Zugriff auf 192.0.2.1 wird verweigert, da keine App mit dieser IP-Adresse konfiguriert ist.

		DNS-Suffix und App-Konfiguration	Erfahrung für Endbenutzer
	3	Der Administrator konfiguriert das DNS-Suffix als “citrix.net”, erstellt eine App mit der Platzhalterdomäne “*.citrix.net”und legt die Zugriffsrichtlinie für Benutzer1 auf “zulassen”fest.	Wenn Benutzer1 versucht, eine Verbindung zu “workday” herzustellen, wird “citrix.net”an das Suffix “workday” (workday.citrix.net) angehängt. Endbenutzer können auf Workday zugreifen, da eine Anwendung mit “*.citrix.net” konfiguriert ist und die Zugriffsrichtlinie für Benutzer1 auf “zulassen”gesetzt ist. **Hinweis:** Endbenutzer können über workday.citrix.net oder “workday”auf Workday zugreifen. Der Zugriff auf 192.0.2.1 wird verweigert, da keine App mit dieser IP-Adresse konfiguriert ist.

		DNS-Suffix und App-Konfiguration	Erfahrung für Endbenutzer
	4	Admin konfiguriert das DNS-Suffix als “citrix.net”. Für Benutzer1 mit FQDN (workday.citrix.net) oder 192.0.2.1 ist keine Anwendung konfiguriert.	Wenn Benutzer1 versucht, eine Verbindung zu “workday” herzustellen, wird “workday”vom Client mit “citrix.net”als Suffix versehen und “workday.citrix.net”in 192.0.2.1 aufgelöst. Benutzer1 kann jedoch keine Verbindung zum privaten Server (workday.citrix.net/192.0.2.1) herstellen, da keine App mit 192.0.2.1 oder workday.citrix.net oder *.citrix.net für Benutzer1 konfiguriert ist.

		DNS-Suffix und App-Konfiguration	Erfahrung für Endbenutzer
	5	Der Administrator konfiguriert das DNS-Suffix als “citrix.net”. Fügt eine App mit der IP-Adresse 192.0.2.1 hinzu und setzt die Zugriffsrichtlinie für Benutzer1 auf “Verweigern”. Fügt dann eine weitere App mit FQDN (workday.citrix.net) hinzu, die auf 192.0.2.1 auflöst und die Zugriffsrichtlinie für Benutzer1 auf “zulassen”setzt.	Wenn Benutzer1 versucht, eine Verbindung zu “workday” herzustellen, wird “citrix.net”an Workday (workday.citrix.net) angehängt und die IP-Adresse wird in 192.0.2.1 aufgelöst. Der Zugriff auf Workday wird jedoch verweigert, da die Richtlinie der mit IP 192.0.2.1 konfigurierten Anwendung Vorrang vor der mit FQDN konfigurierten App hat.

Single Sign-On am Citrix Secure Access-Client über die Citrix Workspace-App

December 27, 2023

Der Citrix Secure Access-Client unterstützt jetzt Single Sign-On für die Workspace-URL, wenn ein Benutzer bereits über die Citrix Workspace-App angemeldet ist. Diese SSO-Funktionalität verbessert die Benutzererfahrung, indem mehrere Authentifizierungen vermieden werden.

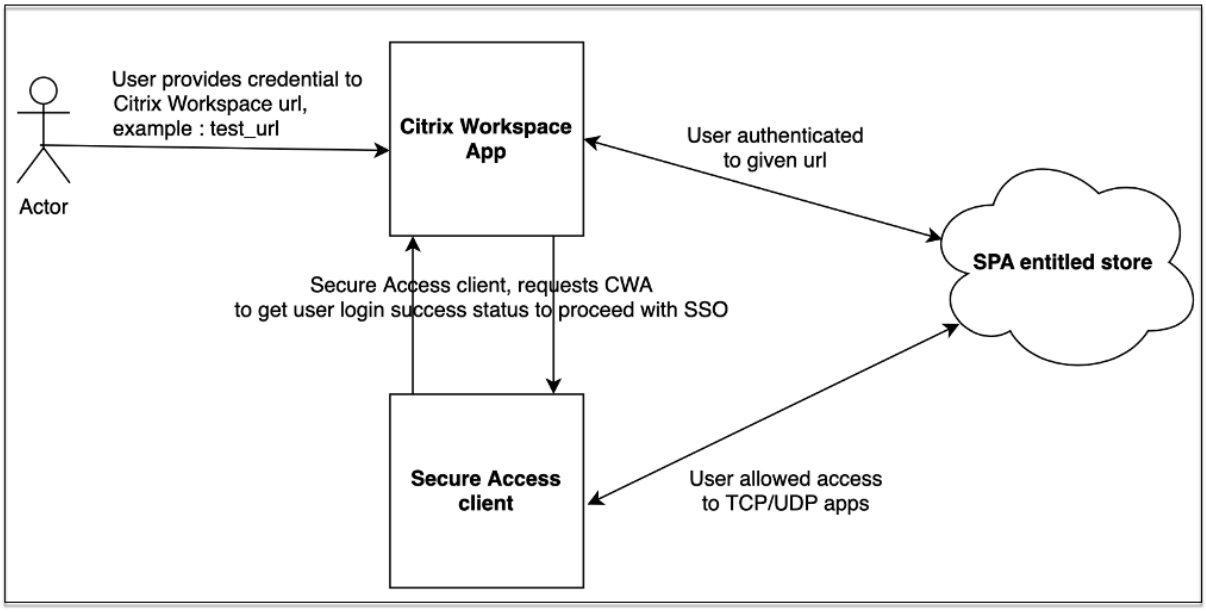
Voraussetzungen

- Sowohl die Citrix Workspace-App als auch der Secure Access-Client müssen auf dem Gerät installiert sein.

- Benutzer müssen sich zuerst bei der Citrix Workspace-App angemeldet haben, damit das automatische SSO im Citrix Secure Access-Client ausgeführt wird.

> **Hinweis:**
>
> Die Single Sign-On-Funktion wird nur für den primären Store unterstützt, der in der Citrix Workspace-App konfiguriert ist. Wenn sich der Benutzer bei einem anderen Store als dem primären Store anmeldet, findet SSO nicht statt. Der Benutzer muss sich manuell beim Citrix Secure Access-Client anmelden.

Die folgende Abbildung zeigt den SSO-Fluss zwischen der Citrix Workspace-App und dem Citrix Secure Access-Client.



Funktionsanforderungen für Windows

- Citrix Workspace-Anwendungsversion - **Citrix Workspace 22.10.5.14 (2210.5) oder höher**
- Citrix Secure Access-Version - **22.10.1.9 oder höher**
- Citrix Secure Access Windows-Registrierung —**EnableCWASSO**

Die SSO-Funktion ist standardmäßig deaktiviert. Um diese Funktion zu aktivieren, fügen Sie die folgende Registrierung auf der Endbenutzermachine hinzu.

- Name der Registrierung: EnableCWASSO
- Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Registrierungstyp: REG_DWORD
- Registrierungswert: 1

> **Wichtig:**
>
> Manchmal müssen die Endbenutzercomputer möglicherweise neu gestartet werden, um Single Sign-On mit der Citrix Workspace-App erfolgreich einzurichten.

Beenden Sie aktive Benutzersitzungen und fügen Sie Benutzer zur Liste der deaktivierten Benutzer hinzu

June 19, 2024

Administratoren können alle aktiven Endbenutzersitzungen sofort beenden und die Benutzer zur Liste der deaktivierten Benutzer hinzufügen. Das Hinzufügen eines Benutzers zu dieser Liste deaktivierter Benutzer beendet alle aktiven Secure Private Access-Anwendungssitzungen und blockiert den zukünftigen Anwendungszugriff.

Alle aktiven Anwendungssitzungen über Citrix Enterprise Browser, Direct Access, CWA für HTML5 und den Secure Access Agent werden beendet und blockiert. Alle Ressourcen, die über den Secure Access Agent verbunden sind, wie Dateifreigaben, RDP- und SSH-Sitzungen, werden ebenfalls beendet und blockiert. Blockierte Benutzer können keine neuen Anwendungen starten, bis sie aus der Liste der deaktivierten Benutzer entfernt werden.

> **Hinweis:**
>
> - Durch das Hinzufügen eines Benutzers zur Liste der deaktivierten Benutzer wird die konfigurierte Secure Private Access-Zugriffsrichtlinie nicht geändert oder bearbeitet. Die Beendigung und Sperrung des Zugriffs erfolgt unabhängig von der konfigurierten Zugriffsrichtlinie. Sobald der Benutzer aus der Liste entfernt wurde, werden die vorhandenen Secure Private Access-Zugriffsrichtlinien für den Benutzer wieder aktiviert.
> - Benutzer werden nach 7 Tagen automatisch aus der Liste der deaktivierten Benutzer entfernt.
> - Nur der Zugriff auf veröffentlichte Secure Private Access-Anwendungen wird gesperrt. Der Internetzugriff über den Citrix Enterprise Browser ist erlaubt oder verweigert, auch wenn ein Benutzer zur Sperrliste hinzugefügt wurde (basierend auf Ihrer Webfilterkonfiguration).

Anwendungsfälle

Sie können diese Funktion in den folgenden Szenarien verwenden.

- Ein Mitarbeiter verlässt die Organisation oder wird aus der Organisation gekündigt. In diesem

Fall widerruft der Administrator den gesamten Secure Private Access-App-Zugriff, indem er aktive Secure Private Access-Sitzungen beendet und jeglichen zukünftigen App-Zugriff blockiert.

- Ein Gerät ist verloren gegangen oder wurde gestohlen. In diesem Fall wird der Zugriff gesperrt und alle aktuellen Sitzungen werden beendet. Der Benutzer kann aus der Liste der deaktivierten Benutzer entfernt werden, nachdem die Situation unter Kontrolle ist.
- Ein Nutzer missbraucht den App-Zugriff. In diesem Fall kann der Zugang für den Nutzer sofort widerrufen werden. Der Zugriff ist gesperrt, bis der Benutzer zur Liste hinzugefügt wird.

Benutzer zur Liste der deaktivierten Benutzer hinzufügen

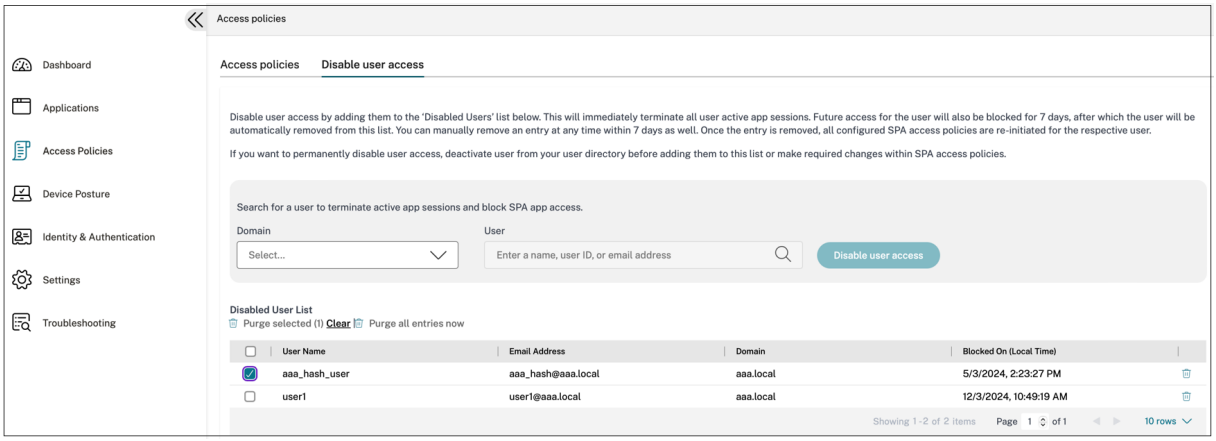
1. Navigieren Sie zu **Secure Private Access > Zugriffsrichtlinien** und klicken Sie dann auf die Registerkarte **Benutzerzugriff deaktivieren** .
2. Wählen Sie unter **Domain**die Domain aus, für die der Zugriff deaktiviert werden muss.
3. Suchen Sie unter **Benutzer**nach dem Benutzernamen, der zur Liste der deaktivierten Benutzer hinzugefügt werden muss. Alle Benutzernamen, die den Suchkriterien entsprechen, werden angezeigt. Wenn der Benutzer aus dem Verzeichnisdienst entfernt wird, erscheint dieser Benutzername nicht in der **Benutzerliste** .
4. Klicken Sie auf **Benutzerzugriff deaktivieren**.

   Der Benutzer wird zur Liste der deaktivierten Benutzer hinzugefügt. Die folgenden Aktionen werden ausgeführt, sobald der Benutzer zur Liste der deaktivierten Benutzer hinzugefügt wird:

   - Alle aktiven Secure Private Access-Sitzungen werden sofort beendet.
   - Der zukünftige Zugriff auf alle veröffentlichten Secure Private Access-Anwendungen ist gesperrt.
   - Der Internetzugriff über den Citrix Enterprise Browser ist auch dann zulässig, wenn ein Benutzer zur Liste der deaktivierten Benutzer hinzugefügt wurde. Nur der Zugriff auf veröffentlichte Secure Private Access-Anwendungen wird gesperrt.
   - Alle deaktivierten Benutzer werden nach 7 Tagen automatisch aus der Liste der deaktivierten Benutzer entfernt. Nach der Entfernung haben die Secure Private Access-Zugriffsrichtlinien Vorrang und der Zugriff wird wieder hergestellt.

Sie können die Option **Ausgewählte löschen verwenden,** um Benutzer aus der Liste der deaktivierten Benutzer zu entfernen.

Sie können die Option **Alle Einträge jetzt löschen verwenden, um alle** Benutzer aus der Liste der deaktivierten Benutzer zu entfernen.



Empfehlungen:

- Um einem Benutzer den Zugriff auf unbestimmte Zeit zu entziehen, entfernen Sie den Benutzer aus Ihrem jeweiligen Verzeichnisdienst, z. B. Active Directory, und fügen Sie ihn dann der Liste der deaktivierten Benutzer hinzu. Dadurch wird die aktive Secure Private Access-Sitzung des Benutzers beendet, der zukünftige App-Zugriff wird blockiert. Sobald der Benutzer von Workspace abgemeldet ist, kann er sich aufgrund inaktiver Verzeichnisanmeldedaten nicht erneut anmelden.
- Der Benutzer wird nach 7 Tagen automatisch aus der Liste der deaktivierten Benutzer entfernt. Danach werden die vorhandenen Secure Private Access-Zugriffsrichtlinien wieder aktiviert. Wenn Sie die Sperrung des Zugriffs verlängern möchten, fügen Sie den Benutzer nach 7 Tagen erneut zur Liste hinzu.

Timeouts für Benutzersitzungen

December 27, 2023

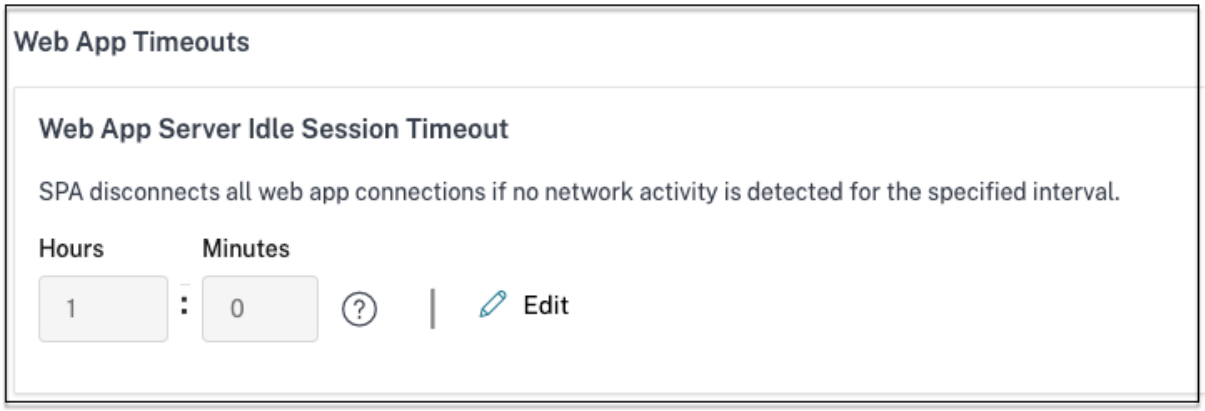
Sie können einen Timeout-Zeitraum für die Web-Apps und den Citrix Secure Access Client für Endbenutzersitzungen konfigurieren, wenn für den angegebenen Zeitraum keine Netzwerkaktivität stattfindet.

Für den Citrix Secure Access Client können Sie den Citrix Secure Access Client auch so konfigurieren, dass eine Sitzung beendet wird, wenn für den angegebenen Zeitraum keine Benutzeraktivität stattfindet. Außerdem können Sie unabhängig von der Benutzer- und Netzwerkaktivität eine erzwungene Verbindungstrennung auf dem Citrix Secure Access Client konfigurieren, sobald der konfigurierte Zeitraum abgelaufen ist.

Timeout für die Web-App-Server

1. Navigiere zu **Einstellungen > Timeouts**.
2. Wählen Sie **unter Web App Server Idle Session Timeout**die Dauer in Stunden und Minuten aus, für die die Web-App-Sitzung inaktiv sein kann. Der Secure Private Access Service beendet die Sitzung nach Ablauf dieser Zeit, wenn die Sitzung inaktiv bleibt.

   Die Mindestdauer beträgt 1 Stunde und die Höchstdauer kann 168 Stunden betragen. Der Standardwert ist 2 Stunden.

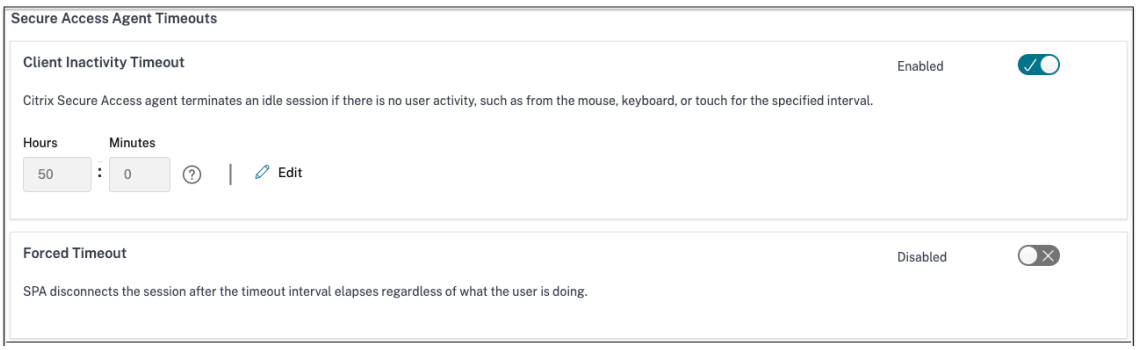


Timeouts für den Citrix Secure Access Client

Sie können die folgenden Timeouts für den Citrix Secure Access Client konfigurieren:

- Inaktivität des Kunden
- Erzwungenes Timeout

1. Navigiere zu **Einstellungen > Timeouts**.



2. Wählen Sie **unter Secure Access Agent Timeout**die Dauer in Stunden und Minuten für das Timeout aus, das Sie erzwingen möchten.

   - **Timeout für Client-Inaktivität**: Die Dauer, nach der der Citrix Secure Access Client eine Sitzung beendet, wenn für den konfigurierten Zeitraum keine Benutzeraktivität

(Maus oder Tastatur) vorhanden ist. Diese Option ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, indem Sie den Kippschalter verwenden, um den konfigurierten Timeout-Zeitraum zu erzwingen. Wenn Sie den Kippschalter jedoch deaktivieren, nachdem die Konfiguration gespeichert wurde, initiiert der Client kein Timeout.

Die Mindestdauer beträgt 5 Minuten und die Höchstdauer kann 168 Stunden betragen. Der Standardwert ist 8 Stunden.

- **Erzwungenes Timeout**: Die Dauer, nach der der Citrix Secure Access Client eine Sitzung unabhängig von der Benutzer- oder Netzwerkaktivität beendet. Diese Option ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, indem Sie den Kippschalter verwenden, um den konfigurierten Timeout-Zeitraum zu erzwingen. Wenn Sie den Kippschalter jedoch deaktivieren, nachdem die Konfiguration gespeichert wurde, initiiert der Client kein Timeout.

  Eine Benachrichtigung erscheint 15 Minuten vor Beendigung der Sitzung.

  Die Mindestdauer beträgt 1 Stunde und die Höchstdauer kann 168 Stunden betragen. Der Standardwert ist 168 Stunden.

> **Hinweis:**
>
> Wenn Sie mehr als eine dieser Einstellungen aktivieren, schließt das erste Timeout-Intervall, das abläuft, die Benutzerverbindung.

Migration von App-Sicherheitskontrollen und Zugriffsrichtlinien auf das neue Access Policy Framework

December 27, 2023

Citrix hat Änderungen an der Aktivierung des Anwendungszugriffs im Produkt vorgenommen. Bisher mussten Anwendungen für die Benutzer oder Benutzergruppen im Abschnitt **Anwendungen > App-Abonnenten** des Assistenten abonniert werden, um den Zugriff zu ermöglichen. Künftig ist mindestens eine Zugriffsrichtlinie erforderlich, um den Zugriff auf die Anwendungen zu ermöglichen. Beim Erstellen der Richtlinien ist die Bedingung **Benutzer oder Gruppen** eine obligatorische Bedingung, die erfüllt sein muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

Außerdem ist der Abschnitt **Erweiterte Sicherheit** in der Anwendungskonfiguration veraltet. Sie können jetzt detaillierte Sicherheitskontrollen wie die Einschränkung der Zwischenablage, Download-Einschränkung und Druckeinschränkungen zusätzlich zu erweiterten Optionen wie dem Öffnen einer App im Remote-Browser über Zugriffsrichtlinien durchsetzen. Mit dieser Änderung können Kunden

anpassungsfähige Sicherheit basierend auf Kontext wie Benutzer, Standort, Gerät und Risiko durchsetzen.

Um die Sicherheitskontrollen und Zugriffsrichtlinien Ihrer Apps auf das neue Framework für Zugriffsrichtlinien zu migrieren und Ausfallzeiten beim Anwendungszugriff zu vermeiden, hat Citrix die erforderlichen Änderungen vorgenommen. Infolgedessen stellen Sie möglicherweise einige Änderungen in Ihrer Richtlinienliste fest, wie zum Beispiel die folgenden:

- Neue Richtlinien erstellt
- Eine einzelne Richtlinie, die in mehrere Richtlinien aufgeteilt ist
- Richtliniennamen mit dem Präfix <System generated policy – App name>

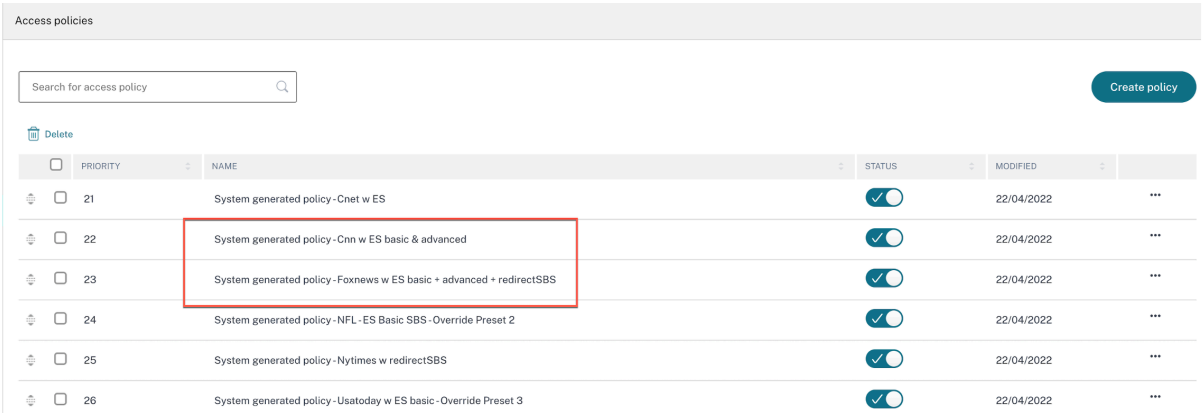
> **Hinweis:**
>
> Wenn den Apps keine Benutzer oder Gruppen hinzugefügt wurden, werden keine neuen Richtlinien erstellt.

In der folgenden Tabelle sind die Änderungen zusammengefasst.

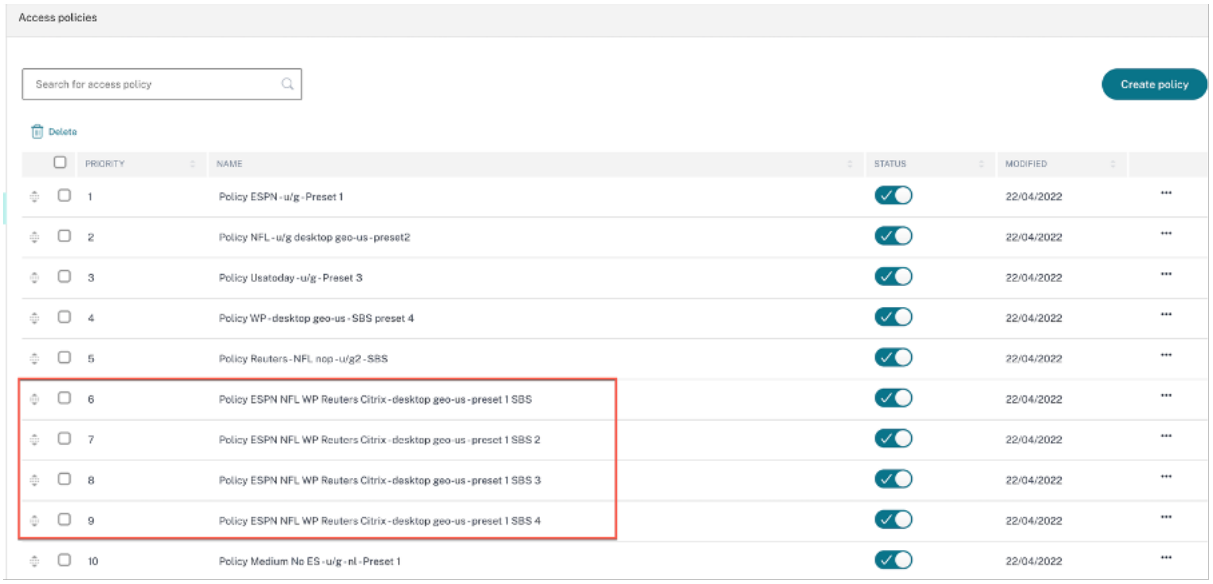
Wenn Sie eine konfiguriert hätten…	Dann…
App ohne erweiterte Sicherheitsbedingungen	Es wird eine neue Richtlinie mit Benutzern und Gruppen als obligatorische Bedingung erstellt. Die Benutzer oder Gruppen werden aus den Zugriffsrichtlinien abgeleitet. Die Aktion ist auf **Zugriff zulassen**festgelegt.
App mit verbesserten Sicherheitsbedingungen	Es wird eine neue Richtlinie mit Benutzern und Gruppen als obligatorische Bedingung erstellt. Die Benutzer oder Gruppen werden aus den Zugriffsrichtlinien abgeleitet. Die Aktion ist auf **Zulassen mit Einschränkung** gesetzt. Basierend auf der zuvor konfigurierten Sicherheitsbedingung auf App-Ebene. Die entsprechenden Sicherheitseinschränkungen werden beim Erstellen der Richtlinie ausgewählt. Den migrierten Richtlinien wird das Präfix vorangestellt <System generated policy – App name>.

Wenn Sie eine konfiguriert hätten…	Dann…
Zugriffsrichtlinie mit Voreinstellungen	Wenn für die Richtlinie bereits eine Benutzergruppenbedingung ausgewählt wurde, wird eine neue Richtlinie unverändert erstellt und die entsprechenden Sicherheitsbedingungen werden in der Zugriffsrichtlinie basierend auf den Vorgaben ausgewählt.
Zugriffsrichtlinie ohne Benutzer- oder Gruppenbedingung	Da die Benutzer oder Gruppen eine obligatorische Bedingung für den Zugriff auf die Apps sind, wird eine einzelne Richtlinie, die für mehrere Apps konfiguriert wurde, jetzt in mehrere Richtlinien aufgeteilt, da jede App unterschiedliche Benutzer oder Gruppen haben kann. Die Benutzer oder Gruppen werden aus den Zugriffsrichtlinien abgeleitet. Für jede Richtlinie werden Benutzer oder Gruppen als obligatorische Bedingung festgelegt.

Die folgende Abbildung zeigt Beispielrichtliniennamen mit dem Präfix <System generated policy - App name>.



Die folgende Abbildung zeigt ein Beispiel für eine einzelne Richtlinie, die in mehrere Richtlinien aufgeteilt ist.



Apps-Konfiguration über eine Vorlage

December 27, 2023

Die Konfiguration von SaaS-Apps mit Single Sign-On im Secure Private Access-Dienst wird durch die Bereitstellung einer Vorlagenliste für beliebte SaaS-Apps vereinfacht. Die zu konfigurierende SaaS-App kann aus der Liste ausgewählt werden.

Die Vorlage enthält viele Informationen, die für die Konfiguration von Anwendungen erforderlich sind. Die für den Kunden spezifischen Informationen müssen jedoch noch zur Verfügung gestellt werden.

> **Hinweis:**
>
> Der folgende Abschnitt enthält die Schritte, die für den Secure Private Access-Dienst zum Konfigurieren und Veröffentlichen einer App mithilfe einer Vorlage ausgeführt werden müssen. Die Konfigurationsschritte, die auf dem App-Server ausgeführt werden sollen, werden im folgenden Abschnitt dargestellt.

Apps über Vorlage konfigurieren und veröffentlichen

Klicken Sie auf der Kachel **Secure Private Access** auf **Verwalten.**

1. Klicken Sie auf **Weiter** und dann auf **App hinzufügen**.

> **Hinweis:**
>
> Die Schaltfläche **Weiter** wird nur angezeigt, wenn Sie den Assistenten zum ersten Mal verwenden. Bei den nachfolgenden Verwendungen können Sie direkt zur Seite „ **Anwendungen** “navigieren und dann auf **App hinzufügen**klicken.

2. Wählen Sie in der Liste **Vorlage auswählen** die App aus, die Sie konfigurieren möchten, und klicken Sie auf **Weiter**.
3. Geben Sie im Abschnitt **App-Details** die folgenden Details ein und klicken Sie auf **Speichern**.

   Appname —Name der Anwendung.

   Beschreibung der App —Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Workspace angezeigt.

   App-Symbol —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Icon-Datei muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

   Wenn Sie das App-Symbol nicht anzeigen möchten, wählen **Sie Anwendungssymbol für Benutzer nicht anzeigen aus.**

   URL —URL mit Ihrer Kunden-ID. Der Benutzer wird zu dieser URL weitergeleitet, wenn;
   - SSO fehlschlägt oder
   - **SSO nicht verwenden** ausgewählt ist.

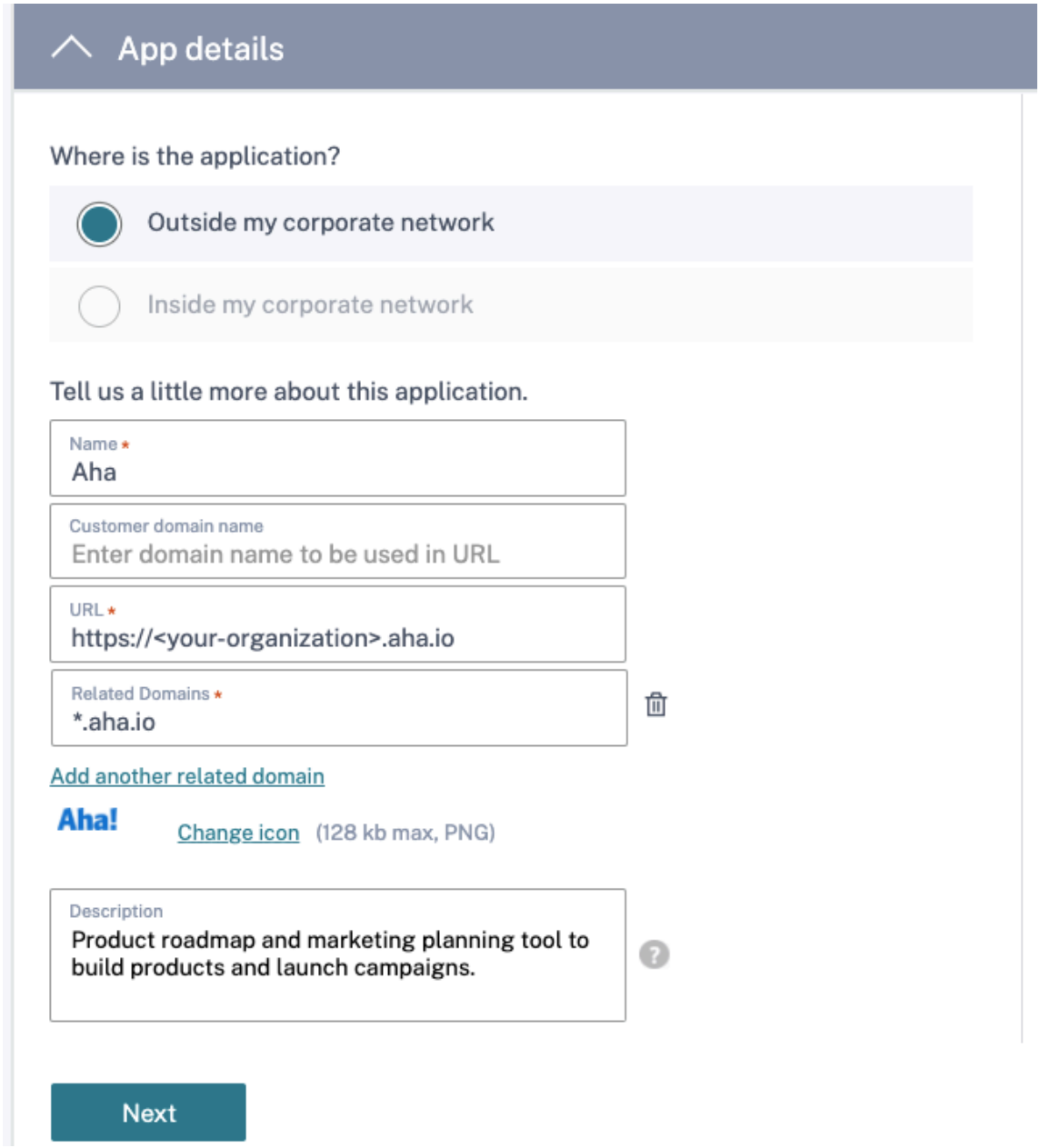
   Kundendomänenname und **Kundendomänen-ID** - Der Domänenname und die ID des Kunden werden verwendet, um eine App-URL und andere nachfolgende URLs auf der SAML-SSO-Seite zu erstellen.

   Wenn Sie beispielsweise eine Salesforce-App hinzufügen, ist Ihr Domänenname `salesforceformyorg` und die ID 123754, dann ist die App-URL `https://salesforceformyorg.my.salesforce.com/?so=123754`.

   Die Felder “Kundendomänenname”und “Kunden-ID”sind spezifisch für bestimmte Apps.

   Verwandte Domänen —Die zugehörige Domäne wird automatisch basierend auf der von Ihnen angegebenen URL ausgefüllt. Verwandte Domain hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domain hinzufügen.

   Symbol —Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Größe der Icon-Datei muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.



4. Geben Sie im Abschnitt **Single Sign On** die folgenden SAML-Konfigurationsdetails ein und klicken Sie auf **Speichern**.

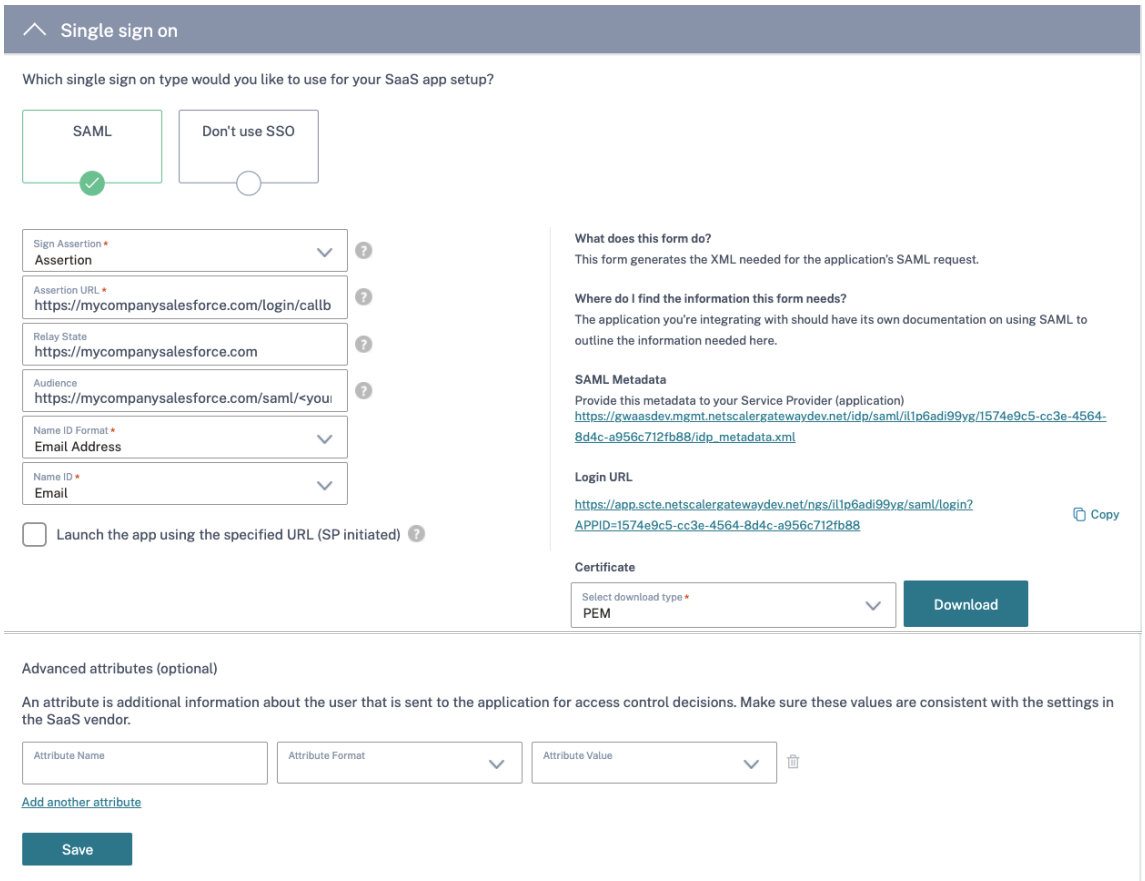
   Assertion-URL —SaaS-App-SAML-Assertion-URL, die vom Anwendungsanbieter bereitgestellt wird. Die SAML-Assertion wird an diese URL gesendet.

   Relay State —Der Relay State-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und an den Verbundserver der verweisenden Partei weitergeleitet wurden. Relay-Status generiert eine einzelne URL für die Benutzer. Benutzer können auf diese URL klicken, um sich bei der Zielanwendung anzumelden.

   Zielgruppe —Dienstleister, für den die Assertion bestimmt ist.

Namens-ID-Format —Unterstützter Formattyp des Benutzers.

Name ID —Name des Formattyps des Benutzers.



Hinweis:

Wenn die Option **SSO nicht verwenden** ausgewählt ist, wird der Benutzer zu der im Abschnitt **App-Details** konfigurierten URL umgeleitet.

5. Laden Sie die Metadatendatei herunter, indem Sie auf den Link unter **SAML-Metadaten**klicken. Verwenden Sie die heruntergeladene Metadatendatei, um SSO auf dem SaaS-Apps-Server zu konfigurieren.

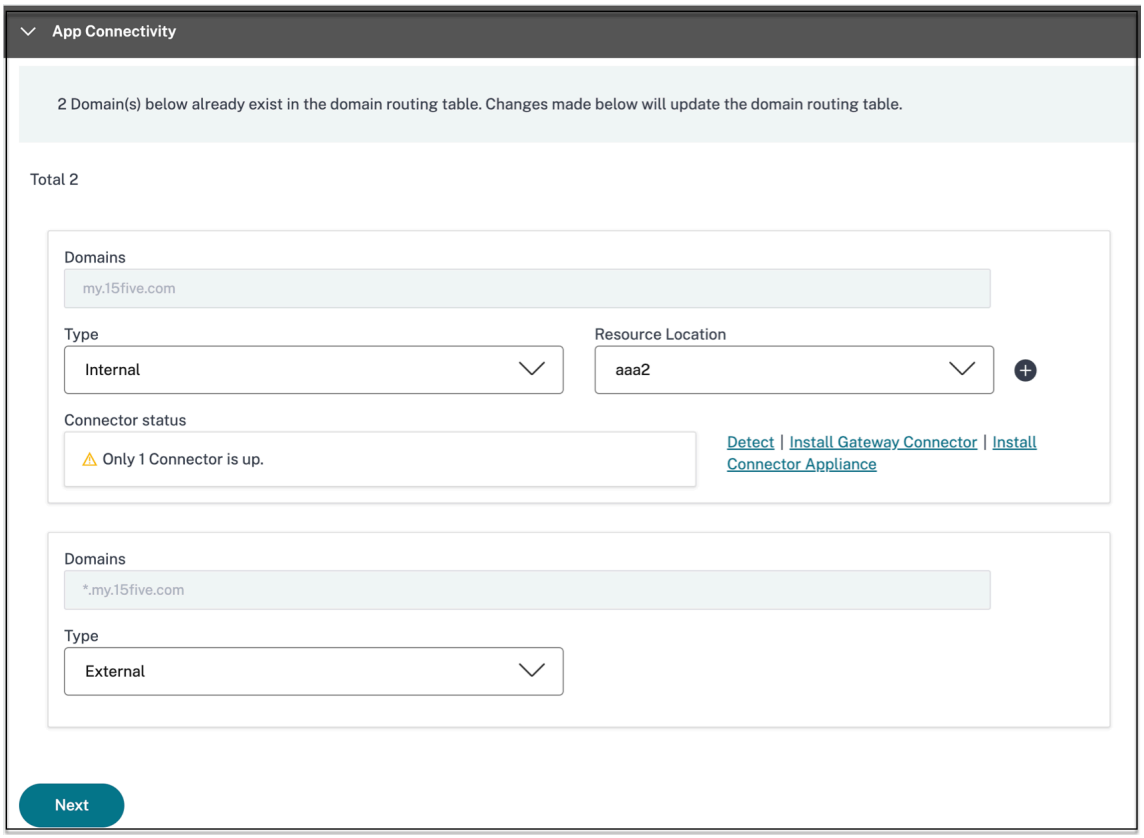
   Hinweis:

   - Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.
   - Sie können das Zertifikat auch aus der **Zertifikatsliste** herunterladen und das Zertifikat verwenden, wenn Sie SSO auf dem SaaS-Apps-Server konfigurieren.

6. Klicken Sie **auf Weiter.**

7. Definieren Sie im Abschnitt **App Connectivity** das Routing für die zugehörigen Anwendungsdomänen, wenn die Domänen extern oder intern über eine Citrix Connector Appliance weit-

ergeleitet werden müssen. Einzelheiten finden Sie unter Weiterleiten von Tabellen zur Lösung von Konflikten, wenn die zugehörigen Domänen sowohl in SaaS als auch in Web-Apps identisch sind.



8. Klicken Sie auf **Fertig stellen.**

   Nachdem Sie auf **Fertig stellen**geklickt haben, wird die App zur Seite Anwendungen hinzugefügt. Sie können eine App auf der Seite Anwendungen bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu in einer App auf die Ellipsenschaltfläche und wählen Sie die Aktionen entsprechend aus.

   - **Anwendung bearbeiten**
   - **Löschen**

> **Hinweis:**
>
> Um den Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

SaaS-App-Server-spezifische Konfiguration

December 27, 2023

Im Folgenden finden Sie die Links zu den Dokumenten, die eine Anleitung zur App-Server-spezifischen Konfiguration mit einer Vorlage enthalten. Citrix unterstützt derzeit die nachfolgend aufgeführten SaaS-Apps. Unterstützung für weitere Apps wird kontinuierlich hinzugefügt.

- 15Five - Kontinuierliches Leistungsmanagementtool zum Coaching von Mitarbeitern.
- 10000 ft - Projektmanagement-Tool zur Planung von Wachstum.
- 4me - Servicemanagement-Tool für die Zusammenarbeit zwischen internen, externen und ausgelagerten Teams.
- Abacus - Ausgabenberichterstellungssoftware in Echtzeit.
- Absorb - Lernmanagement-Tool.
- Accompa - Anforderungsmanagement-Tool zum Erstellen von Produkten.
- Adobe Captivate Prime - Lernmanagementsystem zur Bereitstellung personalisierter Lernerlebnisse auf allen Geräten.
- Aha - Produkt-Roadmap und Marketingplanungstool zum Erstellen von Produkten und zur Einführung von Kampagnen.
- AlertOps - Collaboration Incidence Response Tool zur Verwaltung von IT-Vorfällen.
- Allocadia - Marketing-Performance-Management-Tool zur Verwaltung des Marketingplanungsprozesses eines Unternehmens. ‘
- Ana-Plan - Planungstool, das Unternehmen bei der Entscheidungsfindung unterstützt, indem Daten, Personen und Pläne miteinander verbunden werden.
- &frankly - Ein Engagement-Tool, um Veränderungen am Arbeitsplatz voranzutreiben.
- Anodot - Eine KI-Plattform, die Zeitreihendaten überwacht, Anomalien erkennt und die Geschäftsleistung in Echtzeit prognostiziert.
- App Follow - Produktmanagement-Tool zur Beschleunigung des globalen App-Wachstums und zur Steigerung der Kundenbindung.
- Assembla - Versionskontrolle und Quellcode-Management-Tool für die Softwareentwicklung.
- Automox - Patch-Management-Tool zur Verfolgung, Steuerung und Verwaltung des Patching-Prozesses.
- Azendoo - Collaboration-Tool für Teams zur Unterhaltung und Zusammenarbeit.

- BambooHR - Personalmanagement-Tool zur Verwaltung von Mitarbeiterdaten.
- Bananatag - Tool zum Verfolgen und Planen von E-Mails, zum Verfolgen von Dateien und zum Erstellen von E-Mail-Vorlagen
- Base CRM - Vertriebsmanagement-Tool zur Verwaltung von E-Mails, Telefonanrufen und Notizen.
- Beekeeper - Tool zur Integration mehrerer Betriebssysteme und Kommunikationskanäle in einem Secure Hub, der von Desktop- und Mobilgeräten aus zugänglich ist.
- BitaBIZ - Abwesenheits - und Urlaubsplanung und Kommunikationstool für die Urlaubs- und Abwesenheitsverwaltung
- BlazeMeter - Testsuite.
- Blissbook - Policy Management-Tool zum Erstellen von Mitarbeiterhandbüchern.
- BlueJeans - Videokonferenzlösung.
- Bold360 - Live-Chat-Tool für Kundenbindung.
- Bonusly - Tool zur Anerkennung und Belohnung von Mitarbeitern zur Anerkennung von Teambeiträgen.
- Box - Content-Management- und Filesharing-Tool zum Verwalten, Teilen und Zugreifen auf Ihre Inhalte.
- Branch - Eine mobile Linking-Plattform, die Deep Links und Mobilgeräte versorgt.
- Brandfolder - Digitales Asset Management-Tool zum Speichern und Teilen digitaler Assets.
- Breezy HR - Recruiting-Software und Bewerber-Tracking-System.
- Buddy Punch - Zeitmanagement-Tool zur Überwachung der Anwesenheit der Mitarbeiter.
- Bugsnag - Monitoring-Tool zur Verwaltung der Anwendungsstabilität und zur Meldung von Fehlern und Diagnosedaten.
- Buildkite - Infrastruktur-Tool für die Entwicklung von Software mit kontinuierlicher Integration.
- Bullseye Locations - Ladenlokalisierungstool zum Auffinden eines Geschäfts oder Händlers auf einem Gerät.
- CA Flowdock: Tool für die Zusammenarbeit und Kommunikation im Team
- CakeHR - Personalmanagement-Tool für Anwesenheits- und Leistungsmanagement.
- Cardboard - Kollaboratives Produktplanungstool zur Verfolgung unorganisierter Informationen.
- Citrix Cedexis - Traffic-Management-Tool für große Websites zur Nutzung der Beschaffung von Rechenzentren, Cloud-Anbietern und Content-Delivery-Netzwerken durch mehrere Anbieter.

- CipherCloud - Plattform, die einen End-to-End-Datenschutz und erweiterten Bedrohungsschutz sowie umfassende Compliance-Funktionen für ein Unternehmen bietet, das Cloud-basierte Anwendungen umfasst.
- Celoxis - Projektmanagement-Tool zur Erstellung von Projektplänen, zur Automatisierung der Arbeit und zur Zusammenarbeit.
- CircleHD - Schulungs-, Lern- und Kollaborationstool zum Teilen von Videos und Folien innerhalb der Organisation.
- Circonus - Datenanalyse- und Überwachungstool zur Bereitstellung von Warnungen, Grafiken, Dashboards und Intelligenz für maschinelles Lernen.
- Cisco Umbrella - Cloud-Sicherheitsplattform, die die erste Verteidigungslinie gegen Bedrohungen im Internet bietet.
- Citrix RightSignature - Eine Lösung, um Dokumente elektronisch signieren zu lassen.
- ClearSlide - Tool für das Vertriebsengagement, mit dem Benutzer Inhalte und Verkaufsmaterial für die Kundeninteraktion austauschen können.
- Cloudability - Cloud-Kostenmanagement-Plattform zur Verbesserung der Sichtbarkeit, Optimierung und Governance in Cloud-Umgebungen.
- CloudAMQP - Message Queue-Tool zum Übermitteln von Nachrichten zwischen Prozessen und anderen Systemen.
- CloudCheckr - Tool für Kostenmanagement, Sicherheit, Berichterstellung und Analyse, mit dem Benutzer ihre AWS- und Azure-Bereitstellungen optimieren können.
- CloudMonix - Tool für die Überwachung und Automatisierung von Cloud- und on-premises Ressourcen.
- CloudPassage - Tool für Sichtbarkeit und kontinuierliche Überwachung zur Reduzierung von Cyberrisiken und zur Aufrechterhaltung der Compliance.
- CloudRanger - Tool zur Optimierung Ihrer Backups, Disaster Recovery und Serversteuerung für AWS Cloud.
- Clubhouse - Projektmanagement-Tool für die Softwareentwicklung.
- Coggle - Mind Mapping-Webanwendung, um hierarchisch strukturierte Dokumente wie einen verzweigten Baum zu erstellen.
- Comm100 - Kundendienstsoftware und Kommunikationsinstrument für Kundendienstprofis.
- Confluence: Tool für die Zusammenarbeit und den Austausch von Wissen
- ConceptShare —Proofing-Tool zur schnelleren, schnelleren und billigeren Bereitstellung von Inhalten.

- Concur - Reise- und Spesenmanagement-Tool zur Verwaltung von Ausgaben unterwegs.
- ConnectWise Control - Business-Management-Tool für Remote-Support und Fernzugriff.
- Contactzilla - Kontaktmanagement-Tool für den Zugriff auf aktuelle Kontaktinformationen.
- ContractSafe - Vertragsmanagement-Tool zur Verfolgung, Speicherung und Verwaltung von Verträgen.
- Contentful - Software für Inhalte zum Erstellen, Verwalten und Verteilen von Inhalten an jede Plattform.
- Convo - Tool für Teamkommunikation und Zusammenarbeit für interne Gespräche.
- Copper - CRM-Tool.
- Cronitor - Monitoring-Tool für Cron-Jobs.
- Crowdin - Lösung, die Entwicklern eine nahtlose und kontinuierliche Lokalisierung bietet.
- Dashlane - Kennwort-Management-Tool, das auch digitale Geldbörsen verwaltet.
- Declaree - Reise- und Spesenmanagement-Tool für Geschäftsreisen.
- Dell Boomi —Ein Integrationstool zur Verbindung von Cloud- und on-premises Anwendungen und Daten.
- Deskpro - Helpdesk-Tool zur Erleichterung des Ticketmanagements, der Selbsthilfe von Kunden und Kundenfeedback.
- Stellvertretender - Workforce-Management-Tool zur Planung und Verfolgung von Zeit, Aufgaben und Kommunikation der Mitarbeiter.
- DigiCert - Tool zur Zertifikatverwaltung und Fehlerbehebung für SSL-Zertifikate für Websites.
- Dmarcian - E-Mail-Überwachungstool zum Filtern von Spam, Malware und Phishing.
- DocuSign - Ein Online-Signatur-Tool für verschiedene Dokumente wie Versicherungen, Medizin und Immobilien.
- DOME9 ARC - Sicherheits- und Compliance-Tool zur Verwaltung öffentlicher Cloud-Umgebungen.
- Dropbox - Cloud-Speicher-Tool für sichere Dateifreigabe und Speicherung.
- Duo - Sicherheits-Tool für sicheren Zugriff auf Ihre Anwendungen.
- Dynatrace - Medizinische Labordienstleistungen.
- Easy Projects - Projektmanagement-Tool.
- EdApp - Lernmanagement-Tool für das Lernen am Workspace.
- EduBrite - Lernmanagement-Tool zum Erstellen, Bereitstellen und Verfolgen von Schulungsprogrammen.

- Ekarda - Tool zum Entwerfen elektronischer Karten.
- Envoy - Besuchermanagement-Tool zur Verwaltung von Personen und Paketen.
- Evernote - Anwendung zum Notieren, Organisieren, Aufgabenlisten und Archivieren.
- Expensify —Ausgabenmanagement-Tool für die Verwaltung von Spesenabrechnungen, die Belegverfolgung und Geschäftsreisen.
- ezeep - Druckinfrastruktur-Management-Tool, um von jedem Gerät und jedem Standort auf jeden Drucker in der Cloud zu drucken.
- EZOfficeInventory - Inventarverwaltungstool zur Verfolgung all Ihrer Vermögenswerte und Geräte.
- EZRentOut - Tool zum Verleih von Geräten zur Verfolgung der Qualität und Verfügbarkeit von Geräten.
- Fastly - Edge-Cloud-Plattform, um Anwendungen näher an den Benutzern zu bedienen und zu sichern.
- Favro - Planungs- und Kollaborationstool für den organisatorischen Ablauf
- Federated Directory - unternehmensübergreifendes Kontaktverzeichnis-Tool zum Durchsuchen der Firmenadressbücher verschiedener Unternehmen.
- Feeder
- Feedly - News-Aggregationstool zum Zusammenstellen von News-Feeds aus verschiedenen Quellen.
- FileCloud - Softwarelösung, die eine robuste und sichere Dateihosting- und Sharing-Plattform für Unternehmen bietet.
- Fivetran - Tool zur Unterstützung von Analysten bei der Replikation von Daten in ein Cloud-Warehouse.
- Flatter Files - Digitaler flacher Aktenschrank für Zeichnungen und Dokumente, um eine sichere und einfache Möglichkeit für den Zugriff auf Inhalte zu bieten.
- Float - Ressourcenplanungstool zur Projektplanung und Verwaltung der Auslastung der Teams.
- Flock —Tool für Zusammenarbeit.
- Formstack - Ein Online-Tool zum Erstellen von Formularen und zur Datenerfassung.
- FOSSA - Automatisierte Open-Source-Tools zum Scannen von Lizenzen und Schwachstellenmanagement, die nativ in CI/CD integriert sind
- Freshdesk - Kundensupport-Tool zur Unterstützung der Bedürfnisse der Kunden.
- Freshservice - IT-Helpdesk-Tool zur Vereinfachung des IT-Betriebs.

- FrontApp - Collaboration-Tool zur Verwaltung aller Konversationen an einem Ort.
- Frontify - Plattform zur Erleichterung und Rationalisierung des täglichen Branding-, Marketing- und Entwicklungsvorgangs.
- Fulcrum - Mobile Datenerfassungsplattform, mit der Sie auf einfache Weise mobile Formulare erstellen und Daten sammeln können.
- Fusebill - Abrechnungsmanagement und wiederkehrende Abrechnungssoftware.
- G-Suite - Eine Reihe intelligenter Apps, um die Menschen in Ihrem Unternehmen zu verbinden.
- GetGuru - Wissensmanagement-Software.
- GitBook - Tool zum Erstellen und Pflegen Ihrer Dokumentation.
- GitHub - Ein webbasierter Hosting-Dienst zur Versionskontrolle mit Git für Repositorys, die hinter einer Unternehmensfirewall gehostet werden.
- GitLab - Eine komplette DevOps-Plattform, die als eine einzige Anwendung bereitgestellt wird.
- GlassFrog - Software zur Holacracy-Praxis.
- GoodData - Eine eingebettete BI- und Analyseplattform, die schnelle, zuverlässige und benutzerfreundliche Analysen bietet
- GotoMeeting —Online-Meeting-Software mit HD-Videokonferenz-Funktionen.
- HackerRank - Bietet wettbewerbsfähige Programmierherausforderungen für Verbraucher und Unternehmen.
- HappyFox - Online-Helpdesk-Software und webbasiertes Support-Ticketsystem.
- Helpjuice - Wissensmanagement-Lösung zur Erstellung und Pflege von Wissensdatenbanken.
- Help Scout - Kundendienstsoftware und Wissensdatenbank-Werkzeug für Kundendienstprofis.
- Hello sign - E-Signatur-Schnittstelle, um das Signieren von überall, zu jeder Zeit und auf jedem Gerät zu ermöglichen.
- HelpDocs - Knowledge Base-Software, um Ihre Benutzer zu führen, wenn sie nicht weiterkommen.
- Honeybadger - Tool zur Überwachung des Anwendungszustands.
- Harness —Tool zur kontinuierlichen Bereitstellung und Integration für Java, .NET-Apps in AWS, GCP, Azure und Bare Metal.
- HelpDocs - Tool zum Erstellen einer maßgeblichen Knowledge Base, die Ihre Benutzer anleitet, wenn sie nicht weiterkommen.
- Helpmonks - Eine kollaborative E-Mail-Plattform für die Zusammenarbeit im Team.

- Hoshinplan - Tool zur Visualisierung Ihrer strategischen Pläne und zur Verfolgung des Status auf einer Leinwand.
- Gehosteter Graphit - Tool zur Überwachung der Leistung Ihrer Website, App, Server und Container.
- Menschlichkeit - Online-Mitarbeiterplanungssoftware zur Verwaltung von Schichten, Zeitplänen, Gehaltsabrechnungen und Zeitakten.
- Iglu - Anbieter digitaler Arbeitsplatz- und Intranet-Lösungen zur Lösung von IT-Herausforderungen in Ihrem Unternehmen.
- iLobby - Cloud-basierte Lösung zur Verwaltung der Besucherregistrierung.
- Illumio - Sicherheitssystem zur Verhinderung der Ausbreitung von Sicherheitsverletzungen in Rechenzentrums- und Cloud-Umgebungen.
- Image Relay - Software für digitales Asset Management und Markenmanagement zur sicheren Organisation und Freigabe digitaler Dateien.
- Informatica - Tool für die Integration von SaaS-Apps und eine Plattform zur Entwicklung und Bereitstellung von benutzerdefinierten Integrationsdiensten.
- Intelligent contract - Vertragsmanagement-Software.
- iMeet Central - Projektmanagement-Software für Vermarkter, Kreativagenturen und Unternehmen.
- InteractGo - Tool zur Messung von Echtzeit- und historischen Daten zur Systemleistung.
- iQualify One - Lern- und Management-Tool zur Bereitstellung authentischer Lernerfahrungen.
- InsideView - Daten- und Intelligence-Lösungen zur Lösung von Vertriebs-, Marketing- und anderen geschäftlichen Herausforderungen.
- Insightly - Ein Cloud-basiertes Customer Relationship Management (CRM) und Projektmanagement-Tools für kleine und mittlere Unternehmen.
- ITGlue - Eine Cloud-basierte IT-Dokumentationsplattform, die MSPs dabei hilft, die Dokumentation zu standardisieren, Wissensdatenbanken zu erstellen, Passwörter zu verwalten. und Geräte zu verfolgen.
- Jitbit - Helpdesk-Software und Ticketsystem zur Verwaltung und Verfolgung eingehender Supportanfrage-E-Mails und der zugehörigen Tickets.

JupiterOne - Softwareplattform zur Erstellung und Verwaltung Ihres gesamten Sicherheitsprozesses.

- Kanbanize - Ein Online-Portfolio Kanban-Software für Lean-Management.

- Klipfolio - Eine Online-Dashboard-Plattform zum Erstellen leistungsstarker Business-Dashboards in Echtzeit für Ihr Team oder Ihre Kunden.
- Jira - Tool zum Planen, Verfolgen und Verwalten Ihrer Probleme und Projekte.
- Kanban Tool - Visuelle Managementsoftware zur Verbesserung der Teamleistung und Steigerung der Produktivität.
- Keeper Security - Kennwortmanager und Sicherheitssoftware zum Schutz Ihrer Passwörter und privaten Informationen.
- Kentik - Tool zur Anwendung von Big Data für die Netzwerk- und Leistungsüberwachung, den DDoS-Schutz und die Echtzeit-Ad-hoc-Netzwerkflussanalyse.
- Kissflow - Workflow-Tool und Workflow-Management-Software für Geschäftsprozesse zur Automatisierung Ihres Workflow-Prozesses.
- KnowBe4 - Tool zur Bereitstellung von Schulungen zum Sicherheitsbewusstsein und simuliertes Phishing.
- KnowledgeOwl - Wissensdatenbank und Autorentool.
- Kudos - Einzelhandels-, Job-, Projekt- und Fulfillment-Prozesssysteme.
- LaunchDarkly - Feature-Management-Plattform, mit der Entwicklungs- und Operationsteams den Feature-Lebenszyklus steuern können.
- Lifesize —Videokonferenzlösung.
- Litmos - Lernmanagementsystem für Mitarbeiterschulungen, Kundenschulungen, Compliance-Schulungen und Partnerschulungen.
- LiquidPlanner - Online-Projektmanagement-Software für Ihr Unternehmen.
- LeanKit - Lean-basierte Unternehmensprozess- und Arbeitsmanagement-Software, mit der Unternehmen ihre Arbeit visualisieren, Prozesse optimieren und schneller liefern können.
- LiveChat - Live-Chat- und Helpdesk-Software für Unternehmen.
- LogDNA - Tool zum Sammeln, Überwachen, Analysieren und Analysieren von Protokollen aus allen Quellen in einem zentralen Protokollierungstool.
- Mango - Team-Collaboration-Software zur Konsolidierung und Rationalisierung von Einzelanwendungen auf einer einzigen Plattform.
- Manuskript - Ein Schreibwerkzeug, mit dem Sie Ihre Arbeit planen, bearbeiten und teilen können.
- Marketo - Automatisierungssoftware, die Marketingteams hilft, die Kunst und Wissenschaft des digitalen Marketings zu beherrschen.

- Matomo - Eine Webanalyseplattform, die die gesamte User-Journey aller Personen bewertet, die die Website besuchen.
- Meisterplan - Software, die Unternehmen bei der Erstellung von Projektportfolios unterstützt.
- Mingle - Ein agiles Projektmanagement- und Collaboration-Tool, um dem gesamten Team einen kombinierten Arbeitsplatz zu bieten.
- MojoHelpdesk - Helpdesk-Software und Ticketsystem.
- Monday - Teammanagement-Software, mit der Sie Ihre gesamte Arbeit in einem Tool planen, verfolgen und zusammenarbeiten können.
- Mixpanel - System zur Verfolgung von Benutzerinteraktionen mit Web und Mobilgeräten.
- MuleSoft - Integrationssoftware zur Verbindung von SaaS und Unternehmensanwendungen in der Cloud und on-premises.
- MyWebTimesheets - Online-Zeiterfassungssystem zur Verfolgung der für verschiedene Projekte/Jobs/Aktivitäten aufgewendeten Zeit.
- New Edge - Sicherer Netzwerkdienst für Anwendungen für Hybrid IT.
- NextTravel - Softwaretool für Unternehmensreisemanagement.
- N2F - Tool zur Verwaltung von Spesenabrechnungen zur Verwaltung Ihrer Geschäfts- und Reisekosten.
- New Relic - Digitale Intelligenzplattform zur Messung und Überwachung der Leistung von Anwendungen und Infrastruktur.
- Nmbrs - Cloud HR- und Gehaltsabrechnungssoftware für Unternehmen.
- Nuclino - Collaboration-Software zur Zusammenarbeit und zum Austausch von Informationen in Echtzeit.
- Office365 —Microsofts Cloud-basierter Abonnementdienst.
- OfficeSpace —Cloud-basierte Plattform, die Unternehmen bei der Zuweisung von Workspace unterstützt.
- OneDesk - Projektmanagement- und Helpdesk-Software, um mit Ihren Kunden in Kontakt zu treten und sie zu unterstützen.
- OpsGenie - Eine Incident-Management-Plattform für DevOps- und IT-Ops-Teams zur Rationalisierung von Warnungen und Prozessen zur Behebung von Vorfällen.
- Orginio - Ein Online-Tool zur Erstellung von Organigrammen zur Visualisierung der Organisationsstruktur.
- Oomnitza - IT Asset Management-Plattformlösung zur Nachverfolgung und Verwaltung von Assets.

- OpenEye - Mobile App zum Anzeigen von Live- und aufgezeichneten Videos auf dem Apex-Rekorder.
- Oracle ERP Cloud - Cloud-basierte Software-Anwendungs-Suite zur Verwaltung von Unternehmensfunktionen.
- Pacific Timesheet - Webbasiertes Stundenzettel-Tool für Gehaltsabrechnung, Projektstunden und Ausgaben.
- PagerDuty - Digitales Betriebsmanagementsystem.
- PandaDoc - Eine mobile App für iPhone-Nutzer, die direkt auf ihren Mobiltelefonen auf ihre Dokumente, Analysen und ihr Dashboard zugreifen können.
- Panopta - Infrastruktur-Monitoring-Tool.
- Panorama9 - Cloud-basierte IT-Management-Plattform für die Überwachung von Unternehmensnetzwerken.
- Papyrs - Redakteur zum Entwerfen eigener Intranet-Seiten.
- ParkMyCloud - Einzweck-SaaS-Tool zur Verbindung mit AWS, Azure Services oder GCP.
- Peakon - Tool zur Messung und Verbesserung des Mitarbeiterengagements.
- People HR - HR-Softwaresystem für alle wichtigen HR-Funktionen.
- Pingboard - Tool zum Erstellen von Organigrammen für die Organisation von Teams und die Personalplanung.
- Pigeonhole Live - Interaktive Q&A-Plattform.
- Pipedrive - Vertriebs-CRM und Pipeline-Management-Software.
- PlanMyLeave - Leave Managementsystem zur Verwaltung und Verfolgung der Beurlaubung von Mitarbeitern.
- PlayVox - Tool zur Überwachung der Qualität des Kundendienstes.
- Podbean - Podcast-Dienstleister.
- Podio - Ein webbasiertes Tool zur Organisation von Teamkommunikation, Geschäftsprozessen, Daten und Inhalten in Projektmanagement-Arbeitsbereichen.
- POPin - Crowd-Solving-Plattform und mobile App, die das Teamengagement zur Problemlösung operationalisiert
- Postbote - API-Entwicklungsumgebung.
- Prescreen - Bewerber-Tracking-Tool zur Online-und Offline-Veröffentlichung von Stellenangeboten.
- ProductBoard —Produktmanagement-Tool.

- ProdPad - Produktmanagement-Software zur Entwicklung von Produktstrategien.
- Proto.io - Anwendungsprototyping-Plattform zur Erstellung vollständig interaktiver High-Fidelity-Prototypen.
- Proxyclick - Cloud-basierte Besuchermanagementlösung zur Verwaltung von Besuchern, zum Aufbau ihres Markenimages und zur Gewährleistung der Sicherheit.
- Pulumi - Native Cloud-Entwicklungsplattform für Container, Serverless, Infrastruktur und Kubernetes.
- PurelyHR - Leave Management Tool für den Zugriff auf Urlaubsdaten von Mitarbeitern.
- Promapp: Tool für Business Process Management (BPM)
- Prescreen - Cloud-basiertes Bewerber-Tracking-System zur Online-und Offline-Veröffentlichung von Stellenangeboten.
- QAComplete - Softwaretest-Management-Tool.
- Qualaroo - Feedback-Tool, um Erkenntnisse von Kunden zu gewinnen.
- Quality Built, LLC: Qualitätssicherungslösungen für die Versicherungs-, Finanz- und Bauindustrie
- Qubole —Self-Service-Plattform für Big-Data-Analysen auf Amazon.
- Questetra BPM Suite - Webbasierte Geschäftsprozessplattform für Routine-Workflows.
- QuestionPro - Online-Umfragesoftware zur Erstellung von Umfragen und Fragebögen.
- Quandora - Frage-und-Antwort-basierte Wissensmanagement-Lösung.
- Quip - Kollaborative Produktivitäts-Softwaresuite für Mobilgeräte und das Web.
- Rackspace - Managed Cloud Computing-Dienste.
- ReadCube - Tool für Web-, Desktop- und Mobile-Referenzverwaltung.
- RealtimeBoard - Whiteboard Collaboration Tool für Unternehmen zur Zusammenarbeit über Formate, Tools, Standorte und Zeitzonen hinaus.
- Rezeptiv - Tool, um Feedback von Kunden, Teams und dem Markt an einem Ort zu sammeln.
- Remedyforce - IT-Servicemanagement und Helpdesk-System.
- Retrace - Ein Tool zur Anwendungsleistung, das Fehlerverfolgung, Datenaggregation und automatische Warnungen bietet.
- Robin - Tools für Arbeitsplatzerfahrungen zur Planung von Konferenzräumen und Schreibtischbuchungen.
- Rollbar - Tools zur Fehlerwarnung und Fehlerbehebung in Echtzeit für Entwickler.

- Really Simple Systems - Cloud-basierte CRM-Software für kleine Unternehmen zur Verwaltung ihres Vertriebs und Marketings.
- Reamaze - Kundensupport-Software zur Unterstützung, Bindung und Konvertierung von Kunden mit Chat, Social Media, SMS, FAQ und E-Mail auf einer einzigen Plattform.
- Resource Guru - Ressourcenverwaltungssoftware zur Planung von Personen, Ausrüstung und anderen Ressourcen.
- Retrace - Anwendungsleistungsmanagement zur Integration von Codeprofilerstellung, Fehlerverfolgung, Anwendungsprotokollen und Metriken.
- Roadmunk - Produkt-Roadmap-Software und Roadmap-Tool zur Erstellung von Produkt-Roadmaps.
- Runscope - Tool zum Erstellen, Verwalten und Ausführen von funktionalen API-Tests und Monitoren.
- Salesforce —CRM-Tool zur Verwaltung von Kundenkontaktinformationen, zur Integration sozialer Medien und zur Erleichterung der Zusammenarbeit mit Kunden in Echtzeit.
- SalesLoft - Vertriebsplattform für effiziente und umsatzsteigernde Verkäufe
- Salsify - Plattform für Produkterfahrungsmanagement (PXM).
- Samanage - Tool für das IT-Servicemanagement.
- Samepage - Collaboration-Software zur Verwaltung von Online-Projekten.
- Screencast-O-Matic —Tool zum Screencast und Bearbeiten von Videos.
- ScreenSteps —Tools zum Erstellen visueller Dokumente, die auf Bildschirmaufnahmen zentriert sind.
- SendSafely —Verschlüsselungsplattform für den sicheren Austausch von Dateien und E-Mails.
- Sentry - Open-Source-Software zur Fehlerverfolgung.
- ServiceDesk Plus —Tool für IT-Servicedesk.
- ServiceNow - Cloud-Plattform zur Erstellung digitaler Workflows.
- SharePoint: Plattform für Zusammenarbeit, Dokumentenverwaltung und -speicherung
- Shufflrr - Präsentationsmanagement-Tool zum Erstellen, Aktualisieren, Teilen und Übertragen von Präsentationen.
- Sigma Computing —Ein Analytics-Tool zur Untersuchung, Analyse und Visualisierung von Daten.
- Signavio —Ein Tool zur Modellierung von Geschäftsprozessen.
- Skeddly —Tool zur Automatisierung von AWS-Ressourcen.

- Skills Base - Talentmanagement-Tool zur Verfolgung und Dokumentation der Leistung und Fähigkeiten der Mitarbeiter.
- Skyprep - Lernmanagementsystem (LMS) zur Schulung von Kunden und Mitarbeitern.
- Slack - Collaboration-Tool zur Kommunikation und zum Austausch von Informationen.
- Slemma - Datenanalyse-Tool zum Erstellen von Datenberichten aus mehreren Datensätzen.
- Sli.do - Interaktionstool für Meetings, Veranstaltungen und Konferenzen.
- SmartDraw - Diagramm-Tool zum Erstellen von Flussdiagrammen, Organigrammen, Mindmaps, Projektdiagrammen und anderen Geschäftsvisuals.
- SmarterU - Lernmanagementsystem (LMS) zur Schulung von Kunden und Mitarbeitern.
- Smartsheet - Collaboration Tool zum Zuweisen von Aufgaben, Nachverfolgen von Projektprozessen, Verwalten von Kalendern und Teilen von Dokumenten.
- SparkPost - E-Mail-Zustelldienst.
- Split - Antrag auf Bill Splitting.
- Spoke - Service Desk Tool zum Ablegen von Servicetickets.
- Spotinst - Eine SaaS-Optimierungsplattform, die Unternehmen beim Kauf und der Verwaltung von Cloud-Infrastrukturkapazitäten unterstützt.
- SproutVideo - Plattform zum Hosten von Geschäftsvideos.
- Stackify - Tool zur Fehlerbehebung, das Unterstützung mit einer Reihe von Tools wie Präfix und Retrace bietet.
- StatusCast - Gehostete Seite, um Ihre Mitarbeiter und Kunden über Ausfallzeiten und Website-Wartung auf dem Laufenden zu halten.
- StatusDashboard - Kommunikationsplattform zum Hosten von Status-Dashboards und zur Übertragung von Vorfallsbenachrichtigungen an Kunden.
- Status Hero - Tool zur Verfolgung von Statusaktualisierungen und täglichen Zielen Ihres Teams.
- StatusHub —Plattform zum Hosten der Service-Status-Seite.
- Statuspage - Tool zur Kommunikation von Status und Vorfällen.
- SugarCRM - CRM-Tool für Salesforce-Automatisierung, Marketingkampagnen, Kundensupport, Zusammenarbeit, Mobile CRM, Social CRM und Berichterstattung.
- Sumo Logic - Datenanalyse-Software, die sich auf Sicherheit, Betrieb und BI-Anwendungsfälle konzentriert.
- Supermood - HR-Plattform, um das Feedback der Mitarbeiter in Echtzeit zu sammeln.
- Syncplicity - Tool zum Teilen und Synchronisieren von Dateien.

- Tableau - Tool zum Erstellen interaktiver Datenvisualisierung.
- TalentLMS - Lernmanagementsystem (LMS) zur Erleichterung von Online-Seminaren, Kursen und anderen Schulungsprogrammen.
- Tallie —Tool zum Erfassen und Hochladen von Belegen, zur Erstellung von Spesenabrechnungen und zum Anpassen von Ausgabendetails.
- Targetprocess - Agile Projektmanagement-Software für Scrum, Kanban, SAFe und so weiter.
- Teamphoria - Software zur Bereitstellung von Kennzahlen zur Mitarbeiterbindung in Echtzeit, Mitarbeiterbewertungen und Anerkennung.
- TeamViewer - Proprietäre Softwareanwendung für Fernsteuerung, Desktop-Sharing, Online-Meetings, Webkonferenzen und Dateiübertragung zwischen Computern.
- Tenable.io - Tool, das Daten zur Identifizierung, Untersuchung und Priorisierung der Behebung von Schwachstellen und Fehlkonfigurationen in Ihrer IT-Umgebung bereitstellt.
- Testable - Tool zur Erstellung von Verhaltensexperimenten und Umfragen.
- TestingBot - Tool zur Bereitstellung verschiedener Browserversionen für Live- und automatisierte Tests.
- TestFairy - Mobile Testplattform, um Unternehmen Videoaufnahmen, Protokolle und Absturzberichte von mobilen Sitzungen zur Verfügung zu stellen.
- TextExpander - Kommunikationstool zum Einfügen von Textausschnitten aus einem Repository von E-Mails und anderen Inhalten während der Eingabe.
- TextMagic - Messaging-Dienst, um mit Kunden in Kontakt zu treten.
- ThousandEyes - Tool zur Überwachung der Netzwerkinfrastruktur, zur Fehlerbehebung bei der Anwendungsbereitstellung und zur Abbildung der Internetleistung.
- Thycotic Secret Server - Kontoverwaltungs-Softwaretool zur Verwaltung von Passwörtern.
- TimeLive —Tool zur Bereitstellung von Arbeitszeittabellen und zum Nachverfolgen der Zeit.
- Tinfoil Security - Software für Sicherheitslösungen zur Suche nach Schwachstellen.
- Trisotech - Tool, mit dem Kunden ihr digitales Unternehmen entdecken, modellieren und analysieren können.
- Trumba - Tool zur Veröffentlichung interaktiver Online-Veranstaltungskalender.
- TwentyThree - Video-Marketing-Plattform zum Integrieren und Hinzufügen von Videos zum Marketing-Stack.
- Twilio - Eine Entwicklerplattform für Kommunikation.
- Ubersmith - Unternehmensverwaltungssoftware für nutzungsbasierte Abrechnungs-, Angebots-, Auftragsmanagement-, Infrastrukturmanagement- und Helpdesk-Ticketing-Lösungen.

- UniFi - Kommunikations- und Kollaborationssoftware mit Sprach-, Web- und Videokonferenzfunktionen.
- UPTRENDS —Website-Überwachungslösung zur Verfolgung der Verfügbarkeit und Leistung der Website.
- UserEcho - Community-Forum-Tool, mit dem Unternehmen Kundenfeedback verwalten können.
- UserVoice - Produktfeedback-Management-Software, mit der Unternehmen datengesteuerte Produktentscheidungen treffen können.
- VALIMAIL - E-Mail-Authentifizierungssoftware zur Authentifizierung legitimer E-Mails und zur Blockierung von Phishing-Angriffen.
- Veracode - Quellcode-Analysator und Code-Scanner schützen Unternehmen vor Cyber-Bedrohungen und Anwendungs-Hintertüren.
- Velpic - Lernmanagementsystem (LMS) zur Rationalisierung der Schulung am Arbeitsplatz.
- VictorOps - Incident-Management-Software zur Bereitstellung von DevOps Beobachtbarkeit, Zusammenarbeit und Echtzeit-Alarmierung.
- VIDIZMO - Live- und On-Demand-Videostreaming-Software für Unternehmen.
- Visual Paradigm - Online-Plattform für visuelle Modellierung und Diagramme für die Zusammenarbeit im Team.
- Vtiger - CRM-Tool, mit dem Vertriebs-, Support- und Marketingteams organisieren und zusammenarbeiten können.
- WaveMaker —Software zum Erstellen und Ausführen von benutzerdefinierten Apps.
- Weekdone - Tool zur Erstellung des Dashboards- und Teammanagement-Service von Managern für Unternehmen.
- Wepow - Tool zur Verbindung von Personalvermittlern, Bewerbern und Arbeitgebern durch mobile und Video-Interview-Lösungen.
- When I Work - Tool zur Mitarbeiterplanung und Zeiterfassung.
- WhosOnLocation —Tool zur Verfolgung des Personenflusses durch Standorte und Zonen.
- Workable - Bewerber-Tracking-System.
- Workday - Tool für Finanzmanagement, Personalwesen und Planung.
- Workpath - Tool zur Verwaltung der Ziele und Leistungen der Organisation.
- Arbeitsplatz - Collaboration-Tool von Facebook, das Mitarbeitern hilft, über eine vertraute Oberfläche zu kommunizieren.
- Workstars - Plattform für soziale und Peer-Mitarbeiter-Anerkennungsprogramme.

- Workteam - Tool zur Verfolgung von Zeit und Anwesenheit von Mitarbeitern.
- Wrike - Software für soziales Projektmanagement und Zusammenarbeit.
- XaitPorter - Co-Authoring-Software für Dokumente für Angebote und Vorschläge und andere Geschäftsdokumente.
- Ximble - Tool zur Mitarbeiterplanung und Zeiterfassung.
- XMatters - Collaboration-Plattform mit einer Warnsoftware, die sich in andere Tools integrieren lässt und einen nahtlosen Prozess und eine effektive Kommunikation ermöglicht.
- Yodeck - Tool zur Remote-Verwaltung von Bildschirmen, über das Web oder Handy.
- Zendesk - Software zur Anforderung des Kundendienstes und zur Protokollierung von Support-Tickets.
- Ziflow - Tool für kreative Produktionsteams.
- Zillable —Collaboration-Plattform mit Kommunikationsmöglichkeiten.
- Zing tree - Ein Toolkit zum Erstellen interaktiver Entscheidungsbäume und Troubleshooter.
- ZIVVER - Tool, das eine sichere E-Mail- und Dateiübertragung von Ihrem vertrauten E-Mail-Programm ermöglicht.
- Zoho —Business-Anwendungs-Suite.
- Zoom - Kommunikations- und Kollaborationssoftware mit Sprach-, Web- und Videokonferenzfunktionen.
- Zuora - Eine abonnementbasierte Software, die es einem Unternehmen ermöglicht, ein Abonnementgeschäft zu starten, zu verwalten und in ein Abonnementgeschäft umzuwandeln.

Starten einer konfigurierten App - Endbenutzerworkflow

December 27, 2023

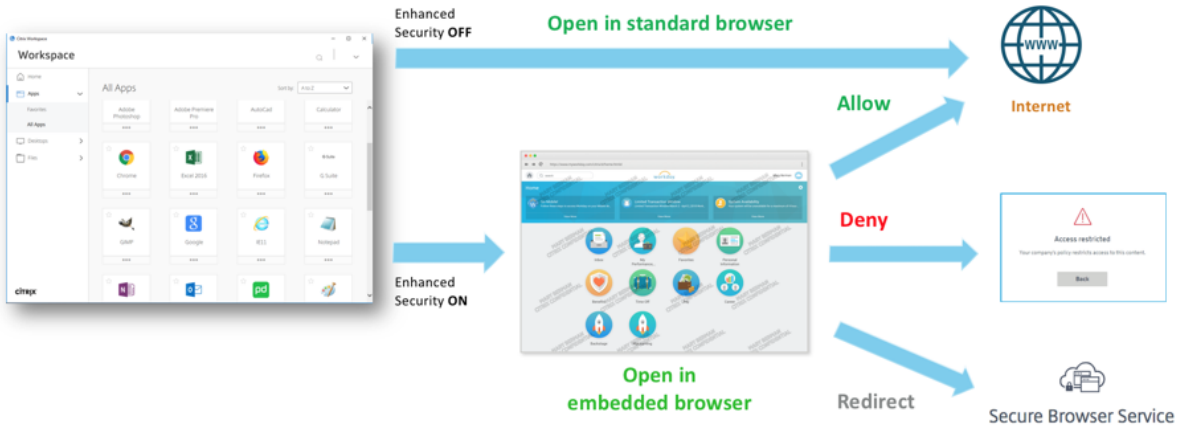
Führen Sie als Endbenutzer folgende Schritte aus:

1. Laden Sie die Citrix Workspace-App von https://www.citrix.com/downloads herunter. Wählen Sie unter **Find Downloads** die **Citrix Workspace-App**.
2. Melden Sie sich an und suchen Sie nach Ihren SaaS-Anwendungen. Klicken Sie auf die App, um sie zu starten.

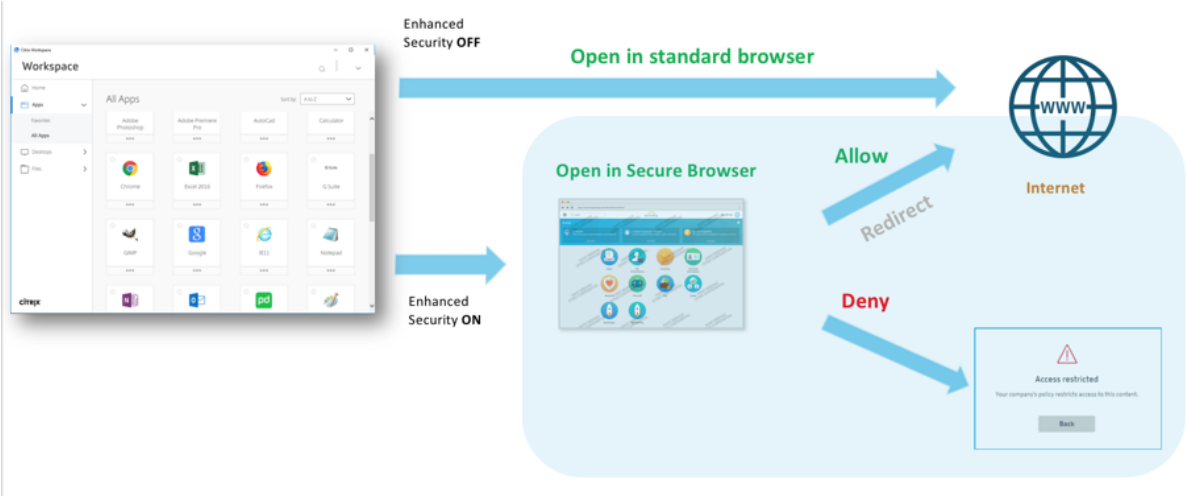
Sie können nun die SaaS-Anwendung in der Citrix Workspace-App oder im Citrix Workspace-Webportal verwenden.

Je nach den vom Administrator konfigurierten Einstellungen werden Ihre SaaS-Anwendungen per Browser-Engine in der Workspace-App geöffnet oder Sie werden zu einem sicheren Browser umgeleitet.

Das folgende Diagramm zeigt die allgemeine Verwendung der Citrix Workspace-App.



Das folgende Diagramm die allgemeine Verwendung des Citrix Workspace-Webportals.



Schreibgeschützter Zugriff für Administratoren auf SaaS und Web-Apps

December 27, 2023

Organisationen bestehen in der Regel aus mehreren Administratoren und Administratoren müssen unterschiedliche Zugriffsberechtigungen erhalten. Sicherheitsadministratorteams, die den Secure Private Access-Dienst verwenden, können detaillierte Kontrollen bereitstellen, z. B. schreibgeschützten Zugriff für Administratoren. Administratoren, die eine App nicht hinzufügen oder

ändern, können mit Lesezugriff versehen werden, um die App-Details anzuzeigen. Secure Private Access-Dienstadministratoren mit schreibgeschütztem Zugriff können die folgenden Aufgaben nicht ausführen.

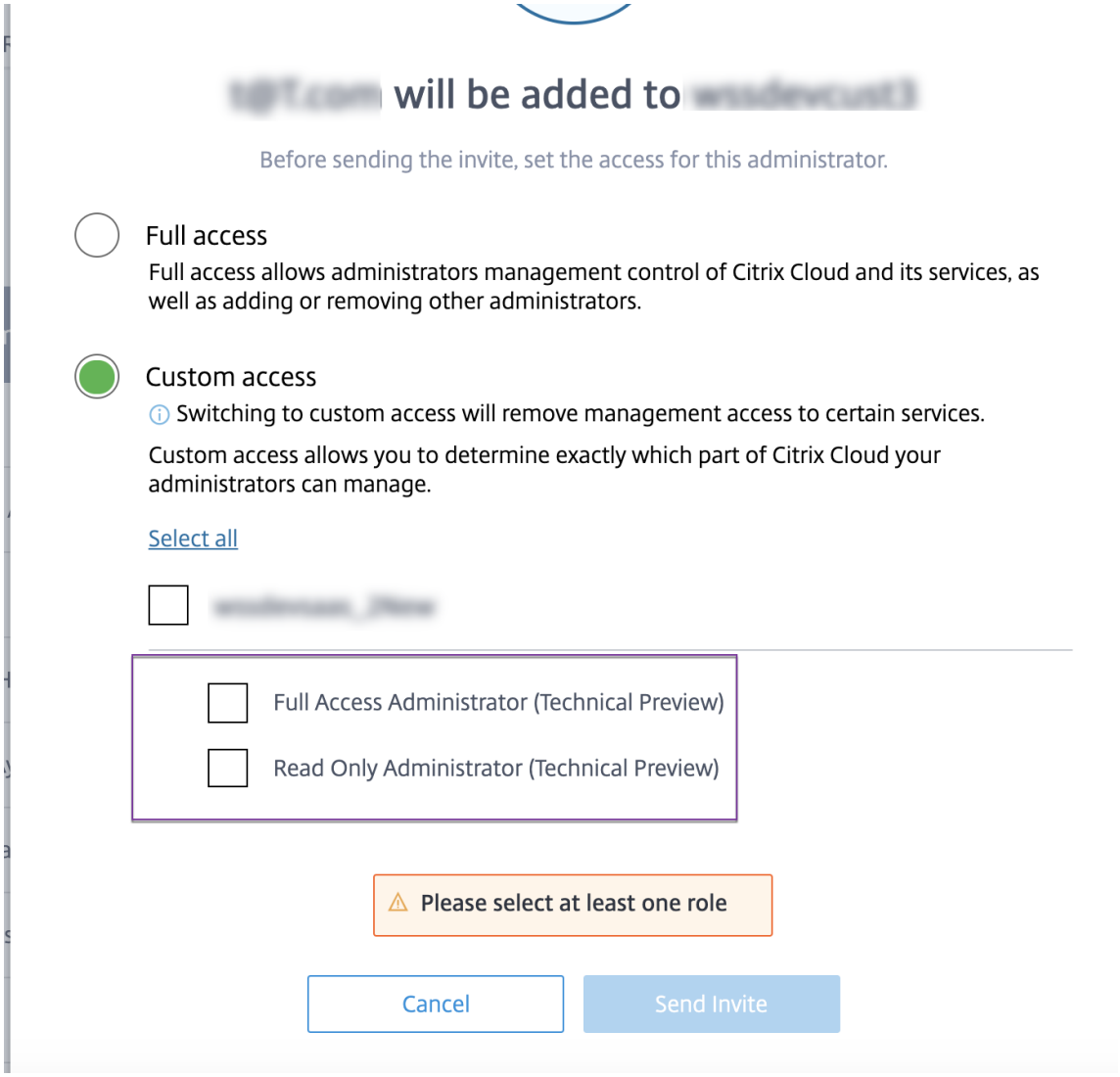
- Fügen Sie Enterprise Web- oder SaaS-Apps hinzu.
- Fügen Sie neue Connector-Appliances an bestehenden oder neuen Ressourcenstandorten hinzu.

So gewähren Sie Administratoren nur Lesezugriff

Nach dem Anmelden bei Citrix Cloud wählen Sie im Menü **Identitäts- und Zugriffsverwaltung**. Klicken Sie auf der Seite Identitäts- und Zugriffsmanagement auf **Administratoren**. In der Konsole werden alle aktuellen Administratoren im Konto angezeigt.

Einen Administrator mit schreibgeschütztem Zugriff hinzufügen

1. Wählen **Sie unter Administratoren hinzufügen**den Identitätsanbieter aus, von dem Sie den Administrator auswählen möchten. Manchmal fordert Citrix Cloud Sie möglicherweise auf, sich zuerst beim Identitätsanbieter anzumelden (z. B. Azure Active Directory).
2. Wenn **Citrix Identity** ausgewählt ist, geben Sie die E-Mail-Adresse des Benutzers ein und klicken Sie dann auf **Einladen**.
3. Bei Auswahl von Azure Active Directory geben Sie den Namen des Benutzers ein, den Sie hinzufügen möchten, und klicken Sie auf Einladen.
4. Wählen Sie **Benutzerdefinierter Zugriff**. Die folgenden Optionen werden angezeigt:
    - **Wählen Sie Full Access Administrator (Technical Preview)** —Bietet vollen Zugriff.
    - **Schreibgeschützter Administrator (Technical Preview)** —Bietet schreibgeschützten Zugriff.
5. Wählen Sie **Read Only Administrator (Technical Preview)** aus.



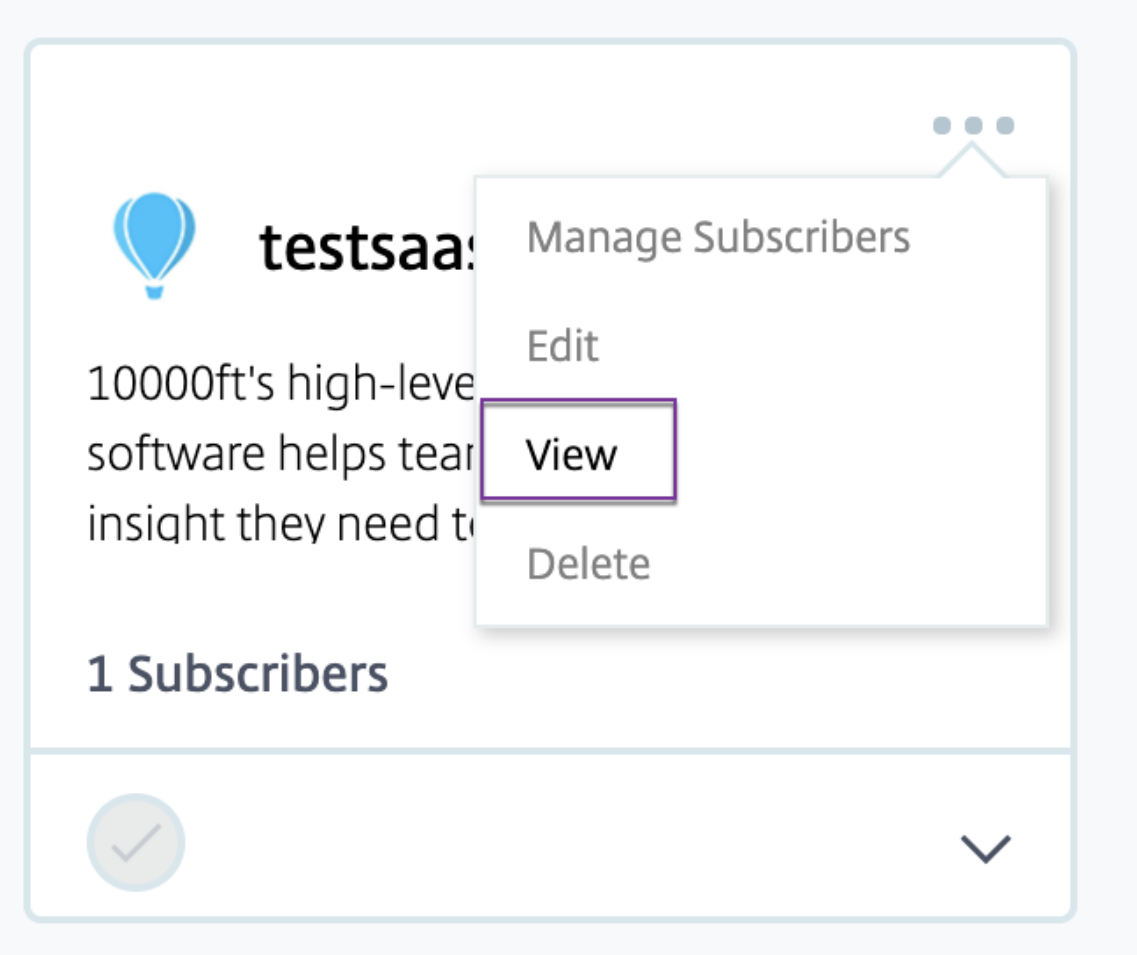
6. Klicken Sie auf **Einladung senden**.

> **Wichtig:**
>
> - Wenn Sie Citrix Gateway **Service-Administratoren nur Lese-Administratorzugriff** gewähren, müssen Sie die **Bibliothek** auch in der Liste der **allgemeinen Verwaltung** für diese Administratoren aktivieren. Nur dann ist die Option **Anzeigen** für die Apps für die Administratoren aktiviert.
> - Die Schaltfläche **Web-/SaaS-App hinzufügen** ist für Benutzer mit **Nur-Lese-Administratorzugriff** deaktiviert.

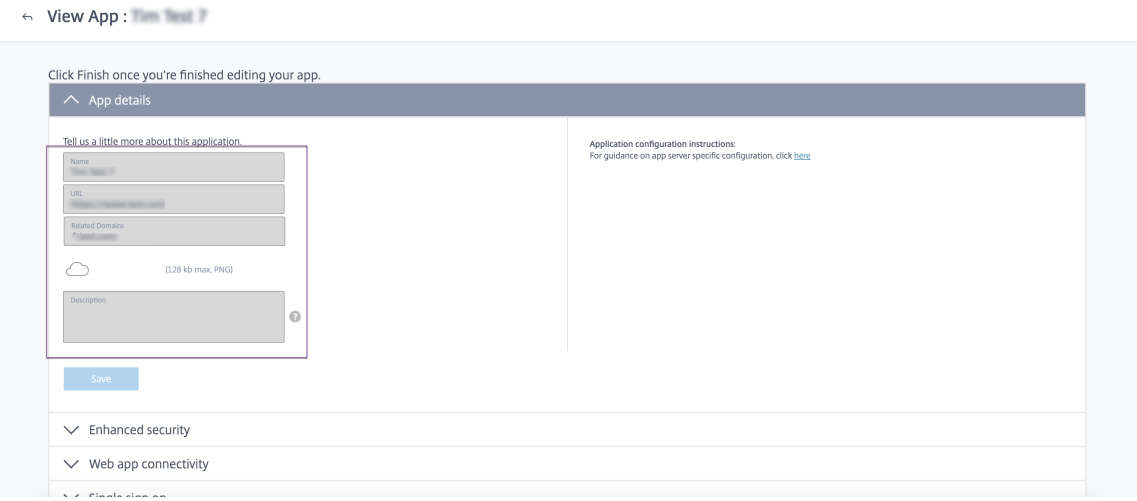
So zeigen Sie die App-Details an, wenn Administratoren nur Lesezugriff haben

1. Nachdem Sie sich bei Citrix Cloud angemeldet haben, wählen Sie im Menü die Option **Bibliothek** aus.

2. Wählen Sie die App aus, in der Sie die Details anzeigen möchten, und klicken Sie auf die **Ellipse**. Nur die Option "**Ansicht** "ist aktiviert. Alle anderen Optionen sind deaktiviert.



3. Klicken Sie auf **Ansicht**.



Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen

June 19, 2024

Der Anwendungszugriff für veröffentlichte und unveröffentlichte Apps hängt von den Anwendungen und Zugriffsrichtlinien ab, die im Secure Private Access Service konfiguriert sind.

Anwendungszugriff innerhalb von Secure Private Access für veröffentlichte und unveröffentlichte Apps

- **Zugriff auf veröffentlichte Webanwendungen und verwandte Domains:**
  - Wenn ein Endbenutzer auf einen FQDN zugreift, der einer veröffentlichten Web-App zugeordnet ist, ist der Zugriff nur zulässig, wenn eine Zugriffsrichtlinie explizit mit der Aktion **Zulassen oder Zulassenmit Einschränkungen** für den Benutzer konfiguriert wurde.

    > **Hinweis:**
    >
    > Es wird empfohlen, nicht mehrere Anwendungen dieselbe Anwendungs-URL-Domain oder verwandte Domänen zu verwenden, um eine genaue Übereinstimmung zu erzielen. Wenn mehrere Apps dieselbe Anwendungs-URL-Domain oder verwandte Domänen verwenden, erfolgt der Zugriff auf der Grundlage der exakten FQDN-Übereinstimmung und der Richtlinienpriorisierung. Einzelheiten finden Sie unter Abstimmung und Priorisierung von Zugriffsrichtlinien.

  - Wenn keine Zugriffsrichtlinie mit der veröffentlichten App übereinstimmt oder wenn eine App keiner Zugriffsrichtlinie zugeordnet ist, wird der Zugriff auf die App standardmäßig verweigert. Einzelheiten zu Zugriffsrichtlinien finden Sie unter Zugriffsrichtlinien.
- **Zugriff auf unveröffentlichte interne Webanwendungen und externe Internet-URLs:**

  Um Zero-Trust zu ermöglichen, verweigert Secure Private Access den Zugriff auf interne Webanwendungen oder Intranet-URLs, die keiner Anwendung zugeordnet sind und für die keine Zugriffsrichtlinie konfiguriert ist. Um bestimmten Benutzern den Zugriff zu ermöglichen, stellen Sie sicher, dass Sie eine Zugriffsrichtlinie für Ihre Intranet-Webanwendungen konfiguriert haben.

  Für jede URL, die nicht als Anwendung in Secure Private Access konfiguriert ist, fließt der Datenverkehr direkt ins Internet.

  - In solchen Fällen wird der Zugriff auf URL-Domänen der Intranet-Webanwendung direkt weitergeleitet und somit der Zugriff verweigert (es sei denn, der Benutzer befindet sich bereits im Intranet).

- Für unveröffentlichte Internet-URLs basiert der Zugriff auf die Regeln, die für nicht genehmigte Apps konfiguriert wurden, sofern diese aktiviert sind. Standardmäßig ist dieser Zugriff innerhalb von Secure Private Access zulässig. Einzelheiten finden Sie unter Regeln für nicht sanktionierte Websites konfigurieren.

Abstimmung und Priorisierung von Zugriffsrichtlinien

Secure Private Access geht beim Zuordnen einer Zugriffsanwendung wie folgt vor:

1. Ordnen Sie die Domain, auf die zugegriffen wird, der Domain der Anwendungs-URL oder verwandten Domains zu, um eine exakte Übereinstimmung zu erhalten.
2. Wenn eine Secure Private Access-Anwendung gefunden wird, die mit einer exakten FQDN-Übereinstimmung konfiguriert ist, bewertet Secure Private Access alle für diese Anwendung konfigurierten Richtlinien.
   - Richtlinien werden in einer Prioritätsreihenfolge bewertet, bis der Benutzerkontext übereinstimmt. Die Aktion (erlauben/verweigern) wird gemäß der ersten Richtlinie angewendet, die in der Prioritätsreihenfolge übereinstimmt.
   - Wenn keine Richtlinie zutrifft, wird der Zugriff standardmäßig verweigert.
3. Wenn keine exakte FQDN-Übereinstimmung gefunden wird, vergleicht Secure Private Access die Domain anhand der längsten Übereinstimmung (z. B. eine Platzhalterübereinstimmung), um Anwendungen und entsprechende Richtlinien zu finden.

   Beispiel 1: Betrachten Sie die folgenden App- und Richtlinienkonfigurationen:

Anwendung	Anwendungs-URL	Verwandte Domain
Intranet	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

Richtlinienname	Priorität	Benutzer und zugehörige Apps
Richtlinie A	Hoch	Eng-User5 (Intranet)
Richtlinie B	Niedrig	HR-Benutzer4 (Wiki)

Bei `HR-User4` Zugriffen `app.intranet.local`passiert Folgendes:

a) Secure Private Access durchsucht in diesem Fall alle Richtlinien nach einer exakten Übereinstimmung mit der Domain, `app.intranet.local` auf die zugegriffen wird.
b) Secure Private Access findet und prüft `PolicyA`, ob die Bedingungen erfüllt sind.
c) Da die Bedingungen nicht übereinstimmen, stoppt Secure Private Access hier und überprüft nicht weiter die Platzhalter-Treffer, obwohl sie mit der zugehörigen Domain der `*.intranet.local`Wiki-App übereinstimmen und Zugriff gewährt worden `PolicyB`wäre. `app.intranet.local`
d) Daher `HR-User4` wird der Zugriff auf die Wiki-App verweigert.

Beispiel 2: Betrachten Sie die folgenden Apps und Richtlinienkonfigurationen, bei denen dieselbe Domain in mehreren Anwendungen verwendet wird:

Anwendung	Anwendungs-URL	Verwandte Domain
App 1	xyz.com	app.intranet.local
App 2	app.intranet.local	-

Richtlinienname	Priorität	Benutzer und zugehörige Apps
Richtlinie A	Hoch	Eng-User5 (App1)
Richtlinie B	Niedrig	HR-User7 (App 2)

Wenn der Benutzer `Eng-User5` zugreift `app.intranet.local`, stimmen App1 und App2 auf der Grundlage der exakten FQDN-Übereinstimmung überein, sodass der `Eng-User5` Benutzer Zugriff über erhält. `PolicyA`

Hätte App1 jedoch stattdessen eine `*.intranet.local` verwandte Domain, dann `Eng-User5` wäre der Zugriff für verweigert worden, da genau gepasst `app.intranet.local` hätte `PolicyB`, für die der Benutzer, `Eng-User5`, keinen Zugriff hat.

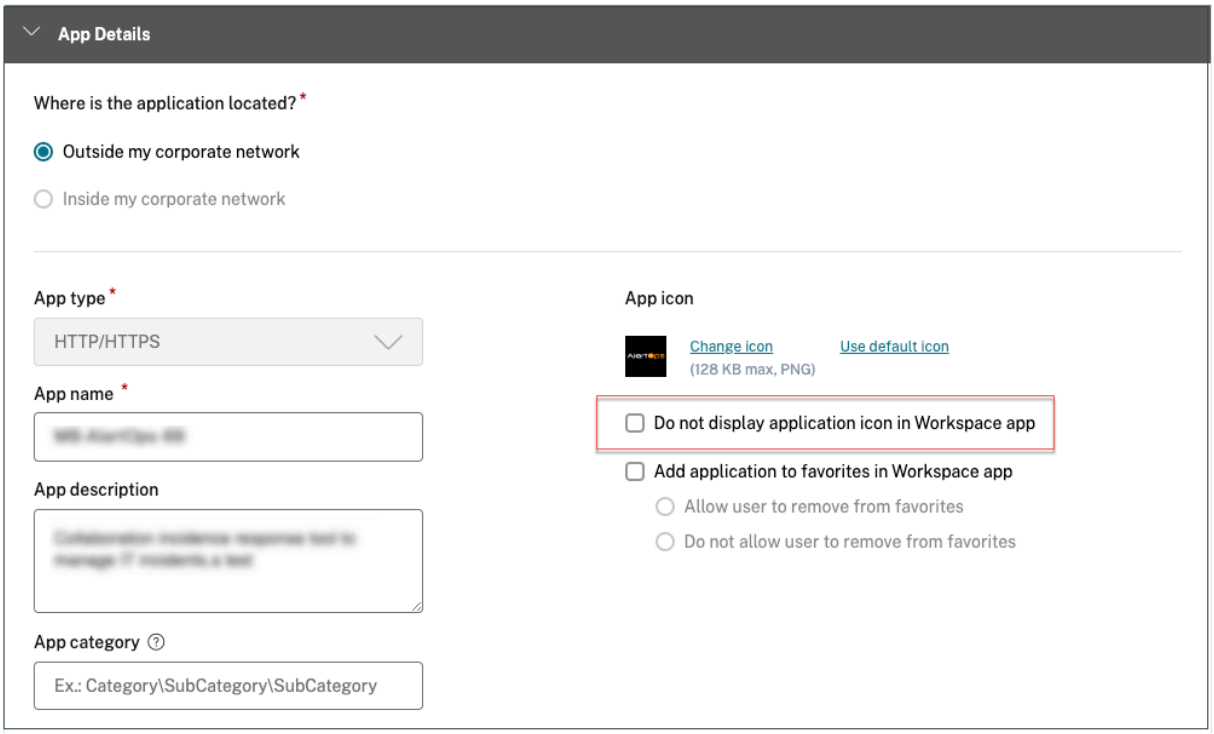
Bewährte Methoden zur App-Konfiguration

IDP-Domains müssen über eine eigene Anwendung verfügen

Anstatt IDP-Domains als verwandte Domains in Ihren Intranet-App-Konfigurationen hinzuzufügen, empfehlen wir Folgendes:

- Erstellen Sie separate Anwendungen für alle IDP-Domänen.
- Erstellen Sie eine Richtlinie, um allen Benutzern den Zugriff auf die IDP-Authentifizierungsseite zu ermöglichen, und behalten Sie die Richtlinie mit der höchsten Priorität bei.

- Blenden Sie diese App in der App-Konfiguration aus (indem **Sie die Option Anwendungssymbol den Benutzern nicht anzeigen** auswählen), damit sie nicht im Workspace aufgeführt wird. Weitere Informationen finden Sie unter Anwendungsdetails konfigurieren.



> **Hinweis:**
>
> Diese App-Konfiguration ermöglicht nur den Zugriff auf die IDP-Authentifizierungsseite. Der weitere Zugriff auf einzelne Anwendungen hängt immer noch von den einzelnen App-Konfigurationen und ihren jeweiligen Zugriffsrichtlinien ab.

Beispielkonfiguration:

1. Konfigurieren Sie alle gängigen FQDNs in ihren eigenen Apps und gruppieren Sie sie gegebenenfalls.

   Wenn Sie beispielsweise einige Apps haben, die Azure AD als IdP verwenden, und Sie weitere verwandte Domänen (`*.msauth.net`) konfigurieren `login.microsoftonline.com` müssen, gehen Sie wie folgt vor:

   - Erstellen Sie eine einzige gemeinsame Anwendung mit `https://login.microsoftonline.com` als Anwendungs-URL `*.login.microsoftonline.com` und `*.msauth.net` als zugehörigen Domänen.

2. Wählen Sie bei der Konfiguration der App **die Option Anwendungssymbol den Benutzern nicht anzeigen** . Einzelheiten finden Sie unter Anwendungsdetails konfigurieren.

3. Erstellen Sie eine Zugriffsrichtlinie für die gemeinsame Anwendung und ermöglichen Sie den Zugriff für alle Benutzer. Einzelheiten finden Sie unter Konfigurieren einer Zugriffsrichtlinie.
4. Weisen Sie der Zugriffsrichtlinie die höchste Priorität zu. Einzelheiten finden Sie unter Prioritätsreihenfolge.
5. Überprüfen Sie die Diagnoseprotokolle, um sicherzustellen, dass der FQDN mit der App übereinstimmt und dass die Richtlinie erwartungsgemäß durchgesetzt wird.

Dieselben verwandten Domains dürfen nicht Teil mehrerer Anwendungen sein

Die zugehörige Domain muss für eine App eindeutig sein. Widersprüchliche Konfigurationen können zu Problemen mit dem App-Zugriff führen. Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, treten möglicherweise die folgenden Probleme auf:

- Die Websites werden nicht mehr geladen oder es wird möglicherweise eine leere Seite angezeigt.
- Die Seite **Blockierter Zugriff wird** möglicherweise angezeigt, wenn Sie auf eine URL zugreifen.
- Die Anmeldeseite wird möglicherweise nicht geladen.

Daher empfehlen wir, eine eindeutige verwandte Domain zu verwenden, die in einer einzigen App konfiguriert werden kann.

Beispiele für falsche Konfigurationen:

- **Beispiel: Duplizieren verwandter Domains in mehreren Anwendungen**

  Angenommen, Sie haben 2 Apps, bei denen beide Zugriff auf Okta benötigen (example.okta.com):

App	Anwendungs-URL-Domäne	Verwandte Domain
App 1	`https://code.example.net`	beispiel.okta.com
App 2	`https://info.example.net`	beispiel.okta.com

Richtlinienname	Priorität	Benutzer und zugehörige Apps
App1 der Personalabteilung verweigern	Hoch	Benutzergruppe HR für App1

Richtlinienname	Priorität	Benutzer und zugehörige Apps
Jedem Zugriff auf App1 gewähren	Medium	Zugriff auf die Benutzergruppe Everyone to App1 aktivieren
Jedem Zugriff auf App2 gewähren	Niedrig	Zugriff auf die Benutzergruppe “Jeder“auf App2 aktivieren

Problem mit der Konfiguration: Obwohl beabsichtigt war, allen Benutzern Zugriff auf App2 zu gewähren, kann die Benutzergruppe HR nicht auf App2 zugreifen. Die Benutzergruppe HR wird zu Okta umgeleitet, hängt aber aufgrund der ersten Richtlinie fest, die den Zugriff auf App1 verweigerte (die auch dieselbe verwandte Domain `example.okta.com` wie App2 hat).

Dieses Szenario ist bei Identitätsanbietern wie Okta sehr verbreitet, kann aber auch bei anderen eng integrierten Apps mit gemeinsamen verwandten Domänen auftreten. Einzelheiten zum Abgleich und zur Priorisierung von Richtlinien finden Sie unter Abgleich und Priorisierung von Zugriffsrichtlinien.

Empfehlung für die obige Konfiguration:

1. Entfernen Sie example.okta.com als verwandte Domain aus allen Apps.
2. Erstellen Sie eine neue App nur für Okta (mit der Anwendungs-URL `https://example.okta.com` und einer zugehörigen Domain von `*.okta.com`).
3. Verstecke diese App im Workspace.
4. Weisen Sie der Richtlinie die höchste Priorität zu, um Konflikte zu beseitigen.

Bewährtes Verfahren:

- Die verwandten Domains einer App dürfen sich nicht mit den verwandten Domains einer anderen App überschneiden.
- In diesem Fall muss eine neue veröffentlichte App erstellt werden, die die gemeinsame verwandte Domain abdeckt, und dann sollte der Zugriff entsprechend eingerichtet werden.
- Administratoren müssen prüfen, ob diese gemeinsame verwandte Domain als tatsächliche App in Workspace angezeigt werden muss.
- Wenn die App nicht in Workspace erscheinen darf, wählen Sie beim Veröffentlichen der App die Option **Anwendungssymbol den Benutzern nicht anzeigen,** um sie in Workspace auszublenden.

Deep-Link-URLs

Für Deep-Link-URLs muss die URL-Domain der Intranetanwendung als zugehörige Domain hinzugefügt werden:

Beispiel:

Die URL der Intranet-App ist `https://example.okta.com/deep-link-app-1` als Hauptanwendungs-URL-Domäne konfiguriert, und die zugehörige Domäne hat die URL-Domäne der Intranetanwendung, d. h. `*.issues.example.net`

Erstellen Sie in diesem Fall separat eine IdP-App mit URL `https://example.okta.com` und dann der zugehörigen Domain als `*.example.okta.com`.

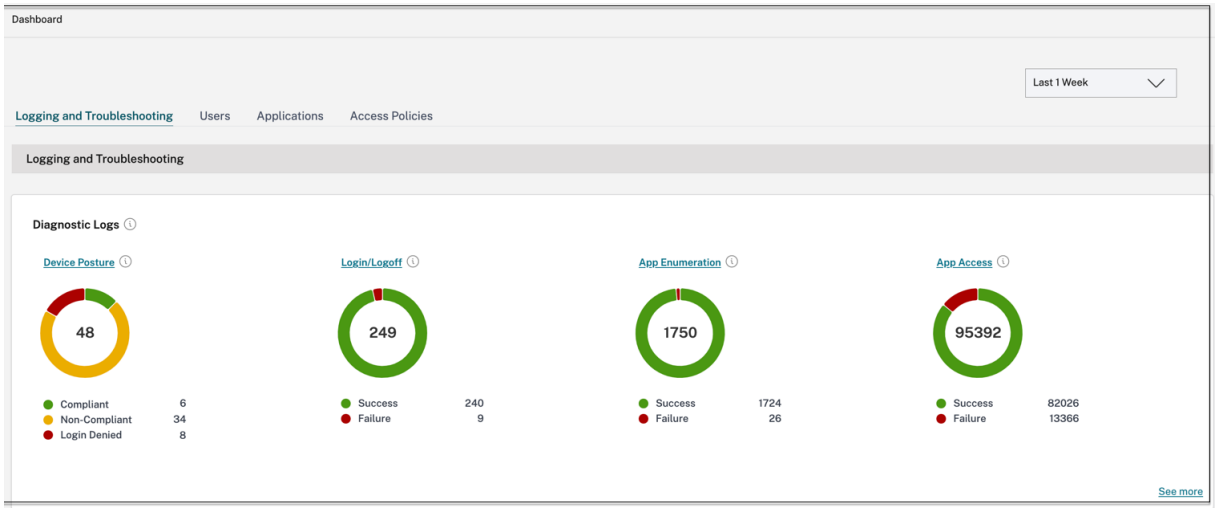
Diagnoseprotokolle

June 19, 2024

Das Secure Private Access Service Access-Dienst-Dashboard zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Verwenden Sie das Diagramm mit den **Diagnoseprotokollen**, um die Protokolle zur Authentifizierung, zum Anwendungsstart, zur App-Aufzählung sowie zur Geräteposition anzuzeigen. Sie können auf den Link **Weitere Informationen** klicken, um die Details der Protokolle anzuzeigen. Die Details werden in einem tabellarischen Format dargestellt. Sie können die Protokolle für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitleiste anzeigen. Sie können dem Diagramm Spalten hinzufügen, indem Sie auf das Pluszeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerprotokolle in das CSV-Format exportieren.

- Mit der Option **Filter hinzufügen** können Sie Ihre Suche anhand der verschiedenen Kriterien wie App-Typ, Kategorie und Beschreibung verfeinern. Beispielsweise können Sie im Suchfeld auf und geben Sie Folgendes ein `Transaction ID= (equals to some value)`, um nach allen Protokollen zu suchen `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`, die sich auf diese Transaktions-ID beziehen. Einzelheiten zu Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.
- **Protokolle zum Gerätestatus:** Sie können Ihre Suche anhand der Richtlinienergebnisse verfeinern (**konform, nicht konform und Anmeldung verweigert**). Einzelheiten zum Gerätestatus finden Sie unter Gerätestatus.

> **Hinweis:**
>
> - Jedem Fehlerereignis im Dashboard der Secure Private Access-Diagnoseprotokolle ist ein Infocode zugeordnet. Einzelheiten finden Sie unter Infocode.
> - Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanfrage. Einzelheiten finden Sie unter Transaktions-ID.



Hinweis:

- Standardmäßig werden auf der Seite "**Diagnoseprotokolle** "die Daten der aktuellen Woche und nur die letzten 10.000 Datensätze angezeigt. Verwenden Sie die benutzerdefinierte Datumssuche und Filter, um Ihre Suchergebnisse weiter zu verfeinern.

Auditprotokolle

February 16, 2024

Ereignisse im Zusammenhang mit dem Secure Private Access Service werden jetzt in **Citrix Cloud > Systemprotokoll** erfasst. Alle Ereignisse, die ein Administrator im Citrix Secure Private Access Service ausführt, werden an Citrix Cloud gesendet und in den Systemprotokollen erfasst. Bei den Admin-Ereignissen kann es sich um Folgendes handeln, sind aber nicht darauf beschränkt:

- Konfigurieren einer Web- oder SaaS-App
- Eine App abonnieren
- Eine App löschen
- Konfiguration einer adaptiven Zugriffsrichtlinie

Die folgende Abbildung zeigt die Ereignisse im Zusammenhang mit Secure Private Access im **Systemprotokoll**. Einzelheiten wie das Exportieren von Ereignissen, das Abrufen von Ereignissen für einen bestimmten Zeitraum, das Weiterleiten von Protokollereignissen und die Datenaufbewahrung finden Sie unter Systemprotokoll.

Adaptive Zugriffs- und Sicherheitskontrollen für Enterprise Web-, TCP- und SaaS-Anwendungen

June 19, 2024

In den sich ständig ändernden Situationen von heute ist Anwendungssicherheit für jedes Unternehmen von entscheidender Bedeutung. Kontextbezogene Sicherheitsentscheidungen zu treffen und dann den Zugriff auf die Anwendungen zu ermöglichen, reduziert die damit verbundenen Risiken und ermöglicht gleichzeitig den Zugriff für Benutzer.

Die Funktion für den adaptiven Zugriff des Citrix Secure Private Access-Dienstes bietet einen umfassenden Zero-Trust-Zugriffsansatz, der sicheren Zugriff auf die Anwendungen ermöglicht. Durch den adaptiven Zugriff können Administratoren granularen Zugriff auf die Apps gewähren, auf die Benutzer basierend auf dem Kontext zugreifen können. Der Begriff "Kontext"bezieht sich hier auf:

- Benutzer und Gruppen (Benutzer und Benutzergruppen)
- Geräte (Desktop- oder Mobilgeräte)
- Standort (Geolocation oder Netzwerkstandort)
- Gerätestatus (Gerätestatusprüfung)
- Risiko (Benutzerrisikobewertung)

Die Funktion für adaptiven Zugriff wendet adaptive Richtlinien auf die Anwendungen an, auf die zugegriffen wird. Diese Richtlinien bestimmen die Risiken auf der Grundlage des Kontextes und treffen dynamische Zugriffsentscheidungen, um den Zugriff auf die Enterprise Web-, SaaS-, TCP- und UDP-Apps zu gewähren oder zu verweigern.

Funktionsweise

Um den Zugriff auf Anwendungen zu gewähren oder zu verweigern, erstellen Administratoren Richtlinien basierend auf den Benutzern, Benutzergruppen, den Geräten, von denen aus die Benutzer auf die Anwendungen zugreifen, dem Standort (Land oder Netzwerkstandort), von dem aus der Benutzer auf die Anwendung zugreift, und dem Benutzerrisikowert.

Die Richtlinien für den adaptiven Zugriff haben Vorrang vor den anwendungsspezifischen Sicherheitsrichtlinien, die beim Hinzufügen von SaaS oder einer Web-App im Secure Private Access-Dienst konfiguriert werden. Die Sicherheitskontrollen auf App-Ebene werden durch die adaptiven Zugriffsrichtlinien überschrieben.

Die adaptiven Zugriffsrichtlinien werden in drei Szenarien bewertet:

- Während einer Web-, TCP- oder SaaS-App-Aufzählung vom Secure Private Access-Dienst — Wenn diesem Benutzer der Anwendungszugriff verweigert wird, kann der Benutzer diese

Anwendung nicht im Workspace sehen.

- Beim Starten der Anwendung —Nachdem Sie die App aufgelistet haben und die adaptive Richtlinie geändert wurde, um den Zugriff zu verweigern, können Benutzer die App nicht starten, obwohl die App zuvor aufgelistet wurde.
- Wenn die App in einem Citrix Enterprise Browser oder einem Remote Browser Isolation Service geöffnet wird, setzt der Citrix Enterprise Browser einige Sicherheitskontrollen durch. Diese Kontrollen werden vom Kunden durchgesetzt. Wenn der Citrix Enterprise Browser gestartet wird, wertet der Server die adaptiven Richtlinien für den Benutzer aus und gibt diese Richtlinien an den Client zurück. Der Client setzt die Richtlinien dann lokal im Citrix Enterprise Browser durch.

Erstellen Sie eine adaptive Zugriffsrichtlinie mit mehreren Regeln

Sie können mehrere Zugriffsregeln erstellen und verschiedene Zugriffsbedingungen für verschiedene Benutzer oder Benutzergruppen innerhalb einer einzigen Richtlinie konfigurieren. Diese Regeln können getrennt für HTTP/HTTPS- und TCP/UDP-Anwendungen angewendet werden, und das alles innerhalb einer einzigen Richtlinie.

Mit den Zugriffsrichtlinien in Secure Private Access können Sie den Zugriff auf die Apps je nach Kontext des Benutzers oder Benutzergeräts aktivieren oder deaktivieren. Darüber hinaus können Sie den eingeschränkten Zugriff auf die Apps aktivieren, indem Sie die folgenden Sicherheitseinschränkungen hinzufügen:

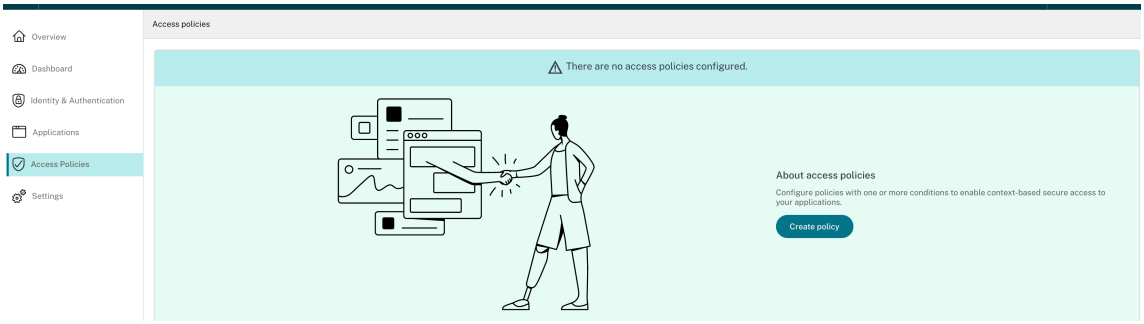
- Zugriff auf Zwischenablage einschränken
- Drucken einschränken
- Downloads einschränken
- Uploads einschränken
- Wasserzeichen anzeigen
- Schlüsselprotokollierung einschränken
- Bildschirmaufnahme einschränken

Weitere Informationen zu diesen Einschränkungen finden Sie unter Verfügbare Zugriffsbeschränkungsoptionen.

Stellen Sie sicher, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie eine Zugriffsrichtlinie konfigurieren.

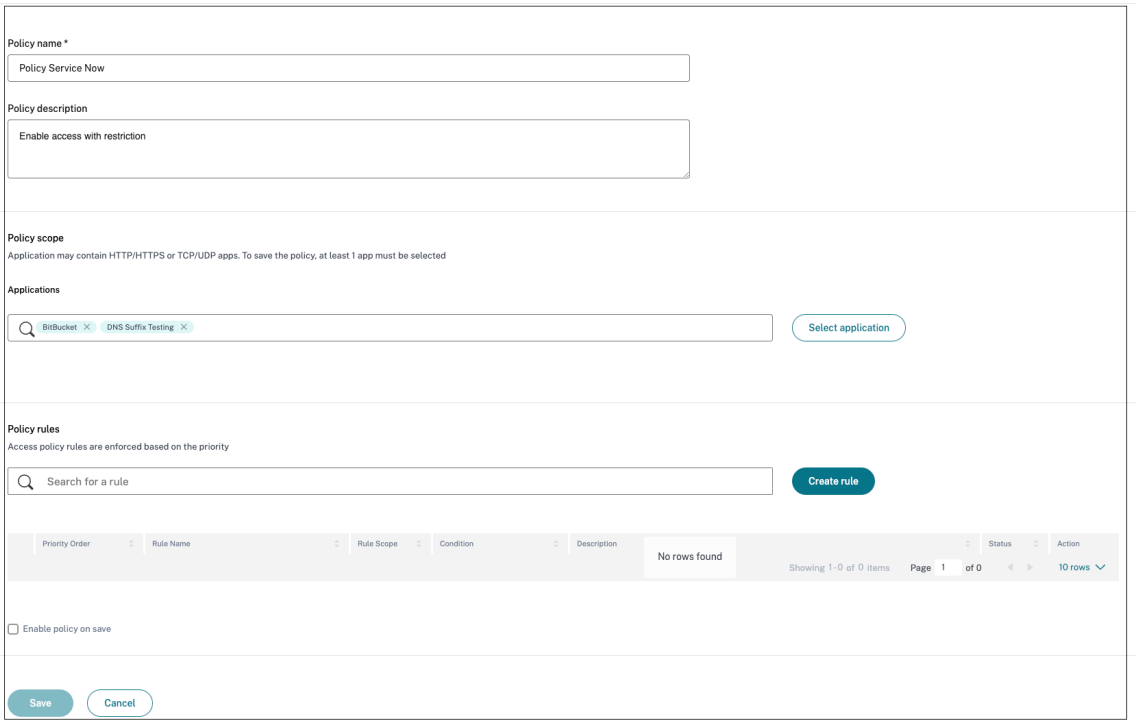
- Identität und Authentifizierung einrichten
- Konfigurierte Anwendungen

1. Klicken Sie im Navigationsbereich auf **Zugriffsrichtlinien** und dann auf **Richtlinie erstellen**.

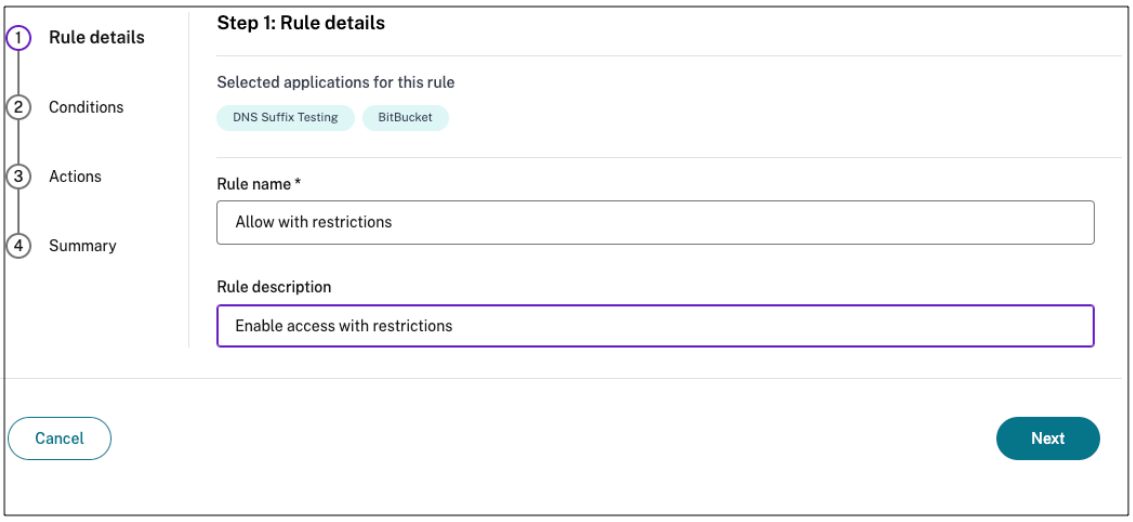


Für Erstbenutzer werden **auf der Zielseite Zugriffsrichtlinien** keine Richtlinien angezeigt. Sobald Sie eine Richtlinie erstellt haben, können Sie sie hier sehen.

2. Geben Sie den Richtliniennamen und die Beschreibung der Richtlinie ein.
3. Wählen Sie unter **Anwendungen** die App oder die Gruppe von Apps aus, für die diese Richtlinie durchgesetzt werden muss.
4. Klicken Sie auf **Regel erstellen**, um Regeln für die Richtlinie zu erstellen.

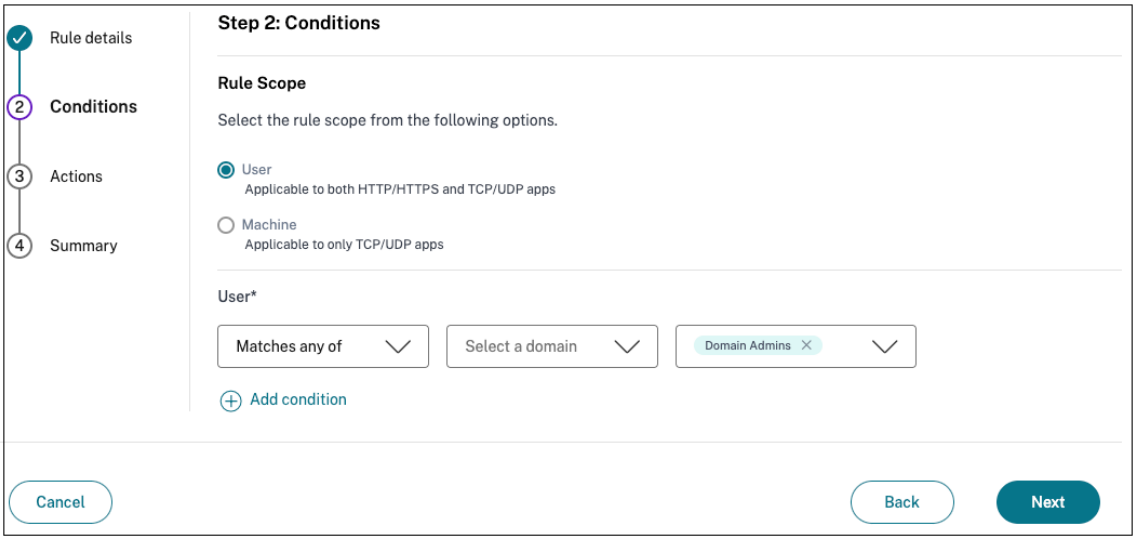


5. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein, und klicken Sie dann auf **Weiter**.



6. Wählen Sie die Bedingungen der Benutzer aus. Die **Benutzerbedingung** ist eine zwingende Voraussetzung, die erfüllt sein muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren. Wählen Sie eine Option aus:

   - **Entspricht einem von** —Nur die Benutzer oder Gruppen, die mit einem der im Feld aufgeführten Namen übereinstimmen und zur ausgewählten Domäne gehören, haben Zugriff.
   - **Entspricht keinem** — Alle Benutzer oder Gruppen mit Ausnahme der im Feld aufgeführten Benutzer oder Gruppen, die zur ausgewählten Domäne gehören, sind berechtigt, darauf zuzugreifen.



7. (Optional) Klicken Sie auf +, um je nach Kontext mehrere Bedingungen hinzuzufügen.

   Wenn Sie Bedingungen hinzufügen, die auf einem Kontext basieren, wird eine UND-Operation auf die Bedingungen angewendet, wobei die Richtlinie nur dann ausgewertet wird, wenn die **Benutzer*** und die optionalen kontextbezogenen Bedingungen erfüllt sind. Sie können die folgenden Bedingungen je nach Kontext anwenden.

- **Desktop** oder **Mobilgerät** —Wählen Sie das Gerät aus, für das Sie den Zugriff auf die Apps aktivieren möchten.
- **Geografischer Standort** —Wählen Sie die Bedingung und den geografischen Standort aus, von dem aus die Benutzer auf die Apps zugreifen.
- **Netzwerkstandort** —Wählen Sie die Bedingung und das Netzwerk aus, über das die Benutzer auf die Apps zugreifen.
- **Gerätestatusprüfung** —Wählen Sie die Bedingungen aus, die das Benutzergerät für den Zugriff auf die Anwendung erfüllen muss.
- **Risikobewertung für Benutzer** —Wählen Sie die Risikobewertungskategorien aus, auf deren Grundlage die Benutzer Zugriff auf die Anwendung erhalten müssen.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie die Aktionen aus, die auf der Grundlage der Zustandsbewertung angewendet werden müssen.

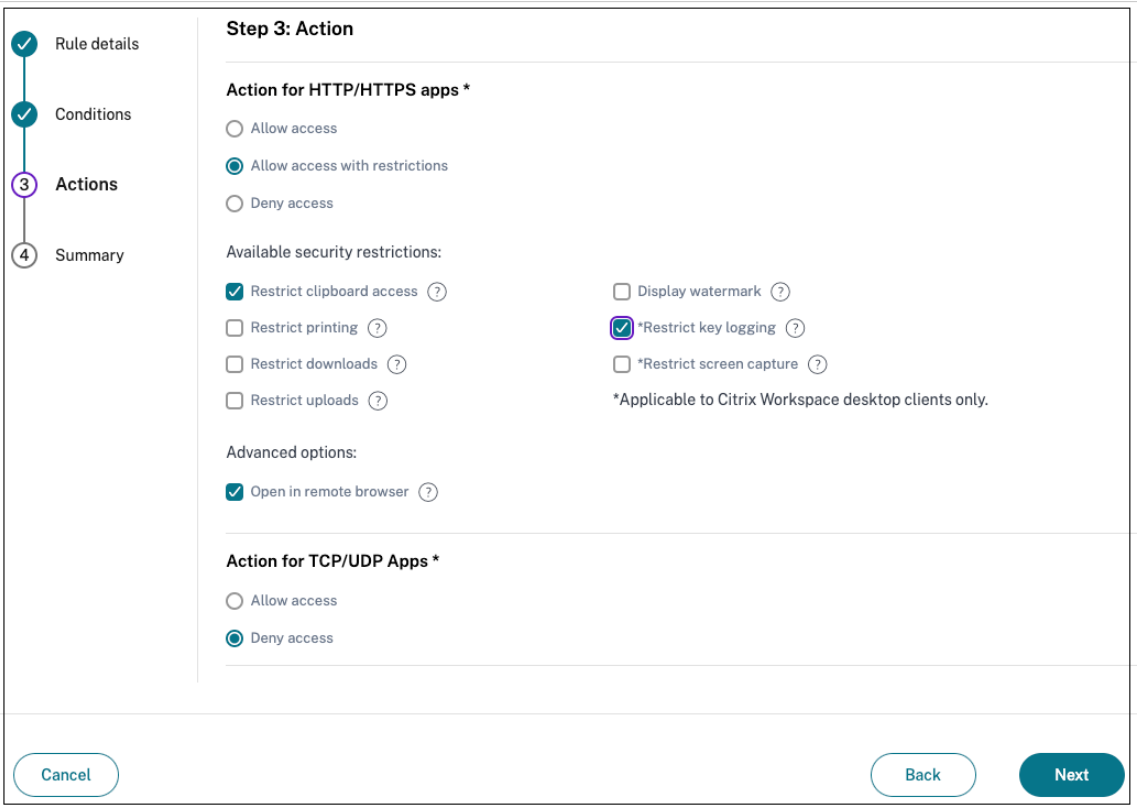
    - Für HTTP/HTTPS-Apps können Sie Folgendes auswählen:

        - **Zugriff erlauben**
        - **Zugriff mit Einschränkungen zulassen**
        - **Zugriff verweigern**

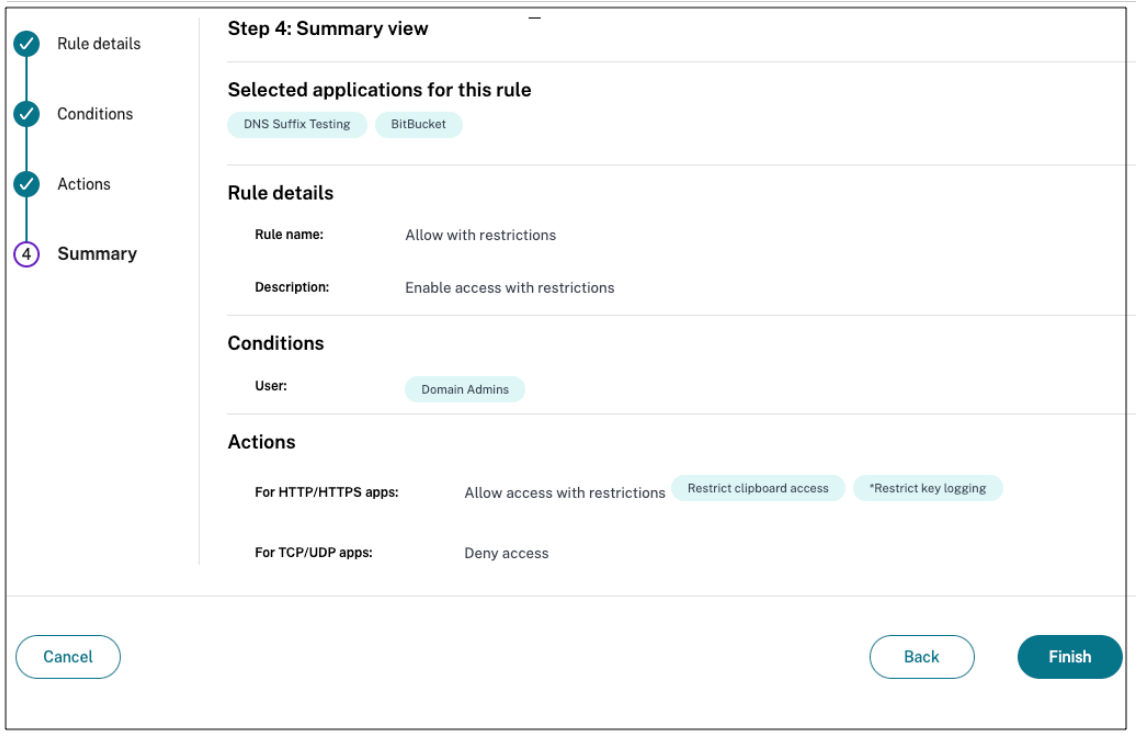
        > **Hinweis:**
        >
        > Wenn Sie **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie die Einschränkungen auswählen, die Sie für die Apps erzwingen möchten. Einzelheiten zu den Einschränkungen finden Sie unter Verfügbare Optionen für Zugriffsbeschränkungen . Sie können auch angeben, ob die App in einem Remote-Browser oder im Citrix Secure Browser geöffnet werden soll.

    - Für den TCP/UDP-Zugriff können Sie Folgendes auswählen:

        - **Zugriff erlauben**
        - **Zugriff verweigern**



10. Klicken Sie auf **Weiter**. Auf der Übersichtsseite werden die Richtliniendetails angezeigt.
11. Sie können die Details überprüfen und auf **Fertig stellen**klicken.



Punkte, die Sie sich nach der Erstellung einer Richtlinie merken sollten

- Die von Ihnen erstellte Richtlinie wird im Abschnitt Richtlinienregeln angezeigt und ist standardmäßig aktiviert. Sie können die Regeln bei Bedarf deaktivieren. Stellen Sie jedoch sicher, dass mindestens eine Regel aktiviert ist, damit die Richtlinie aktiv ist.
- Der Richtlinie ist standardmäßig eine Prioritätsreihenfolge zugewiesen. Die Priorität mit einem niedrigeren Wert hat die höchste Präferenz. Die Regel mit der niedrigsten Prioritätsnummer wird zuerst bewertet. Wenn die Regel (n) nicht den definierten Bedingungen entspricht, wird die nächste Regel (n+1) ausgewertet und so weiter.

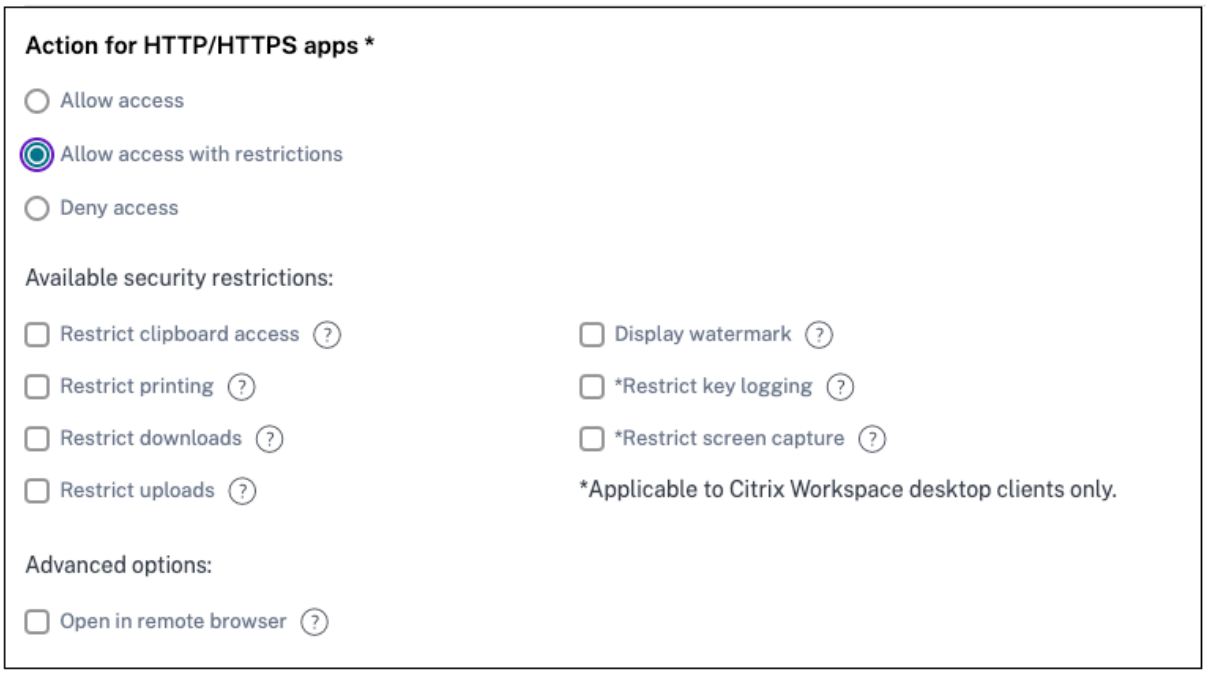
Beispiel für die Bewertung von Regeln mit Prioritätsreihenfolge:

Nehmen wir an, Sie haben zwei Regeln erstellt, Regel 1 und Regel 2.
Regel 1 wird Benutzer A zugewiesen und Regel 2 wird Benutzer B zugewiesen, dann werden beide Regeln ausgewertet.
Gehen Sie davon aus, dass beide Regeln, Regel 1 und Regel 2, dem Benutzer A zugewiesen sind. In diesem Fall hat Regel 1 die höhere Priorität. Wenn die Bedingung in Regel 1 erfüllt ist, wird Regel 1 angewendet und Regel 2 wird übersprungen. Andernfalls, wenn die Bedingung in Regel 1 nicht erfüllt ist, wird Regel 2 auf Benutzer A angewendet.

> **Hinweis:**
>
> Wenn keine der Regeln ausgewertet wird, wird die App für die Benutzer nicht aufgeführt.

Verfügbare Optionen für Zugriffsbeschränkungen

Wenn Sie die Aktion **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie mindestens eine der Sicherheitseinschränkungen auswählen. Diese Sicherheitseinschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen. Die folgenden Sicherheitseinschränkungen können für die Anwendung aktiviert werden.



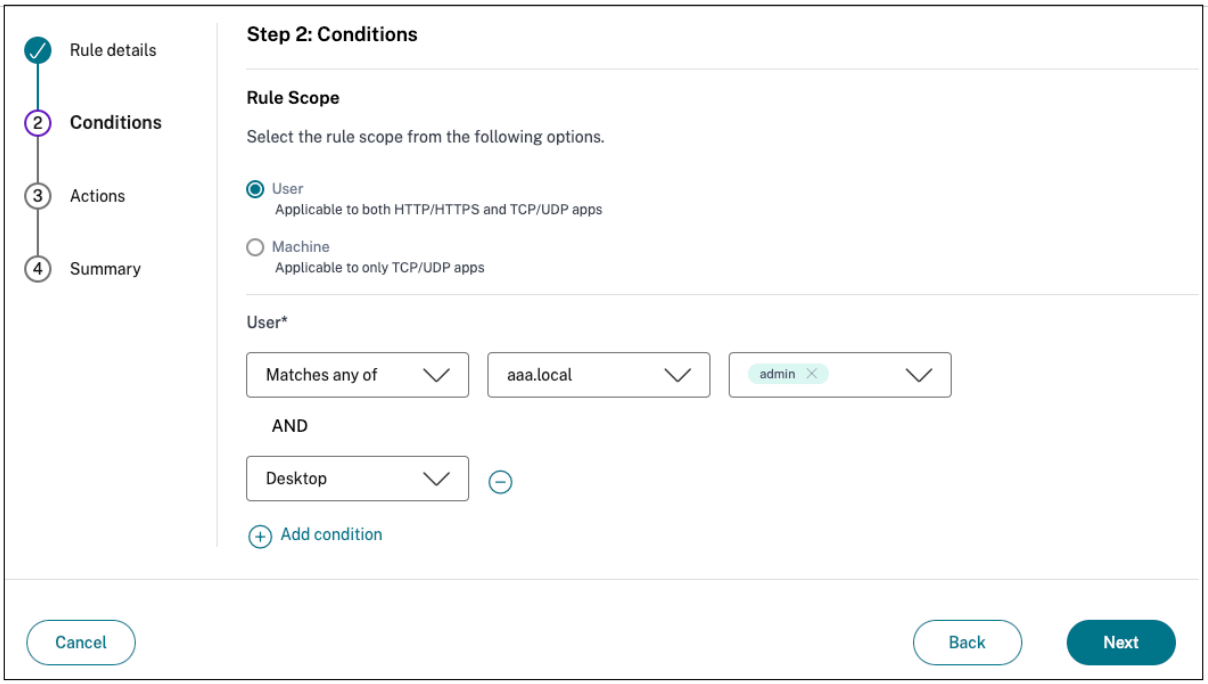
- **Zugriff auf die Zwischenablage einschränken:**Deaktiviert Ausschneiden/Kopieren/Einfügen zwischen der App und der Systemzwischenablage.
- **Drucken einschränken:**Deaktiviert die Möglichkeit, im Citrix Enterprise Browser zu drucken.
- **Downloads einschränken:**Deaktiviert die Fähigkeit des Benutzers, von der App aus herunterzuladen.
- **Uploads einschränken:**Deaktiviert die Fähigkeit des Benutzers, innerhalb der App hochzuladen.
- **Wasserzeichen anzeigen:**Zeigt auf dem Bildschirm des Benutzers ein Wasserzeichen an, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt.
- **Key-Logging einschränken:**Schützt vor Keyloggern. Wenn ein Benutzer versucht, sich mit dem Benutzernamen und dem Kennwort bei der App anzumelden, werden alle Schlüssel auf den Keyloggern verschlüsselt. Außerdem sind alle Aktivitäten, die der Benutzer in der App ausführt, vor Key-Logging geschützt. Wenn beispielsweise App-Schutzrichtlinien für Office 365 aktiviert sind und der Benutzer ein Office 365-Word-Dokument bearbeitet, werden alle Tastenanschläge auf Keyloggern verschlüsselt.
- **Bildschirmaufnahme einschränken:**Deaktiviert die Möglichkeit, die Bildschirme mit einem der Bildschirmaufnahmeprogramme oder Apps aufzunehmen. Wenn ein Benutzer versucht,

den Bildschirm zu erfassen, wird ein leerer Bildschirm aufgenommen.

Adaptiver Zugriff basierend auf Geräten

Um eine adaptive Zugriffsrichtlinie auf der Grundlage der Plattform (Mobilgerät oder Desktop-Computer) zu konfigurieren, von der aus der Benutzer auf die Anwendung zugreift, verwenden Sie das Verfahren Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen**.
- Wählen Sie **Desktop** oder **Mobilgerät**aus.
- Schließen Sie die Konfiguration der Richtlinie ab.



Adaptiver Zugriff basierend auf dem Standort

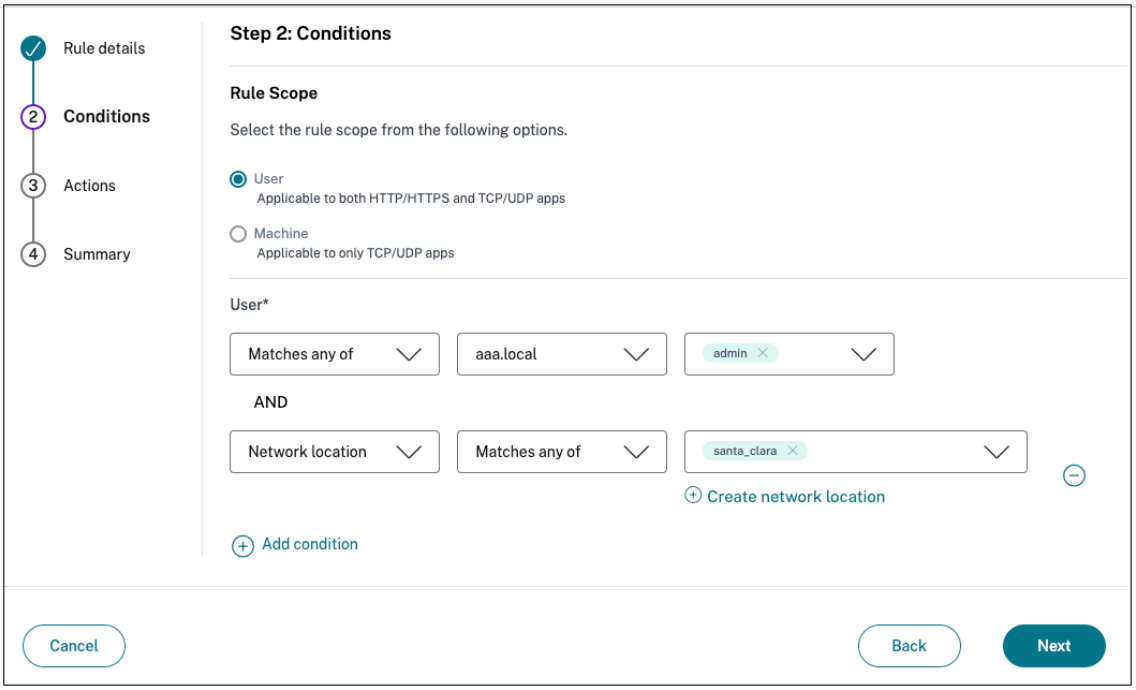
Ein Administrator kann die Richtlinie für den adaptiven Zugriff basierend auf dem Standort konfigurieren, von dem aus der Benutzer auf die Anwendung zugreift. Der Standort kann das Land sein, von dem aus der Benutzer auf die Anwendung zugreift, oder der Netzwerkstandort des Benutzers. Der Netzwerkstandort wird mithilfe eines IP-Adressbereichs oder Subnetzadressen definiert.

Um eine adaptive Zugriffsrichtlinie basierend auf dem Standort zu konfigurieren, verwenden Sie das Verfahren [Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen**.
- Wählen Sie **Geolocation** oder **Netzwerkstandort**.
- Wenn Sie mehrere Geo-Locations oder Netzwerkstandorte konfiguriert haben, wählen Sie je nach Anforderung eine der folgenden Optionen aus.
  - **Entspricht einem von** —Die geografischen Standorte oder Netzwerkstandorte stimmen mit einem der in der Datenbank konfigurierten geografischen Standorte oder Netzwerkstandorte überein.
  - **Stimmt mit keinem überein** —Die geografischen Standorte oder Netzwerkstandorte stimmen nicht mit den in der Datenbank konfigurierten geografischen oder Netzwerkstandorten überein.

Hinweis:

- Wenn Sie **Geo-Location**auswählen, wird die Quell-IP-Adresse des Benutzers mit der IP-Adresse der Länderdatenbank ausgewertet. Wenn die IP-Adresse des Benutzers dem Land in der Richtlinie zugeordnet ist, wird die Richtlinie angewendet. Wenn das Land nicht übereinstimmt, wird diese adaptive Richtlinie übersprungen und die nächste adaptive Richtlinie wird bewertet.
- Für **Netzwerkstandort**können Sie einen vorhandenen Netzwerkstandort auswählen oder einen Netzwerkstandort erstellen. Um einen neuen Netzwerkstandort zu erstellen, klicken Sie auf **Netzwerkstandort erstellen**.
- Stellen Sie sicher, dass Sie Adaptive Access über **Citrix Cloud > Citrix Workspace > Access > Adaptive Access** aktiviert haben. Wenn nicht, können Sie die Standort-Tags nicht hinzufügen. Einzelheiten finden Sie unter Adaptiven Zugriff aktivieren.
- Sie können auch über die Citrix Cloud-Konsole einen Netzwerkstandort erstellen. Einzelheiten finden Sie unter Konfiguration des Citrix Cloud-Netzwerkstandorts.



- Schließen Sie die Konfiguration der Richtlinie ab.

Adaptiver Zugriff basierend auf der Gerätehaltung

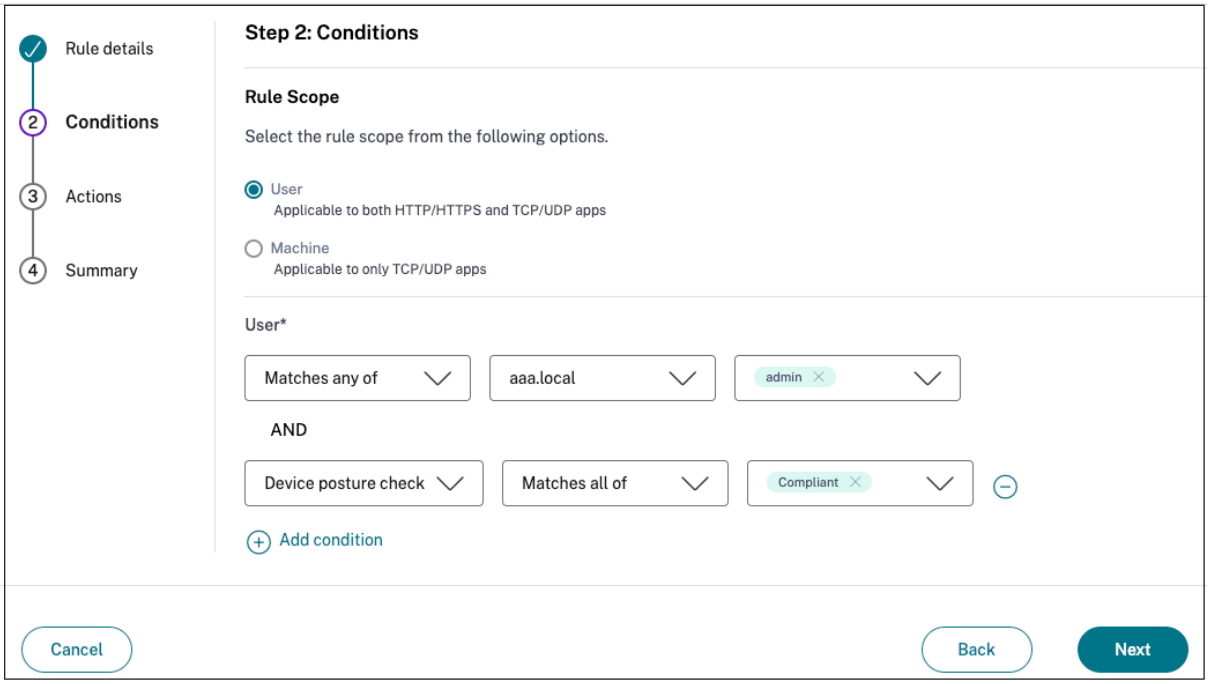
Sie können den Secure Private Access Service so konfigurieren, dass er die Zugriffskontrolle mithilfe von Device Posture Tags erzwingt. Nachdem sich ein Gerät nach der Überprüfung der Gerätehaltung anmelden darf, kann das Gerät als konform oder nicht konform eingestuft werden. Diese Informationen sind als Tags für den Citrix DaaS-Dienst und den Citrix Secure Private Access-Dienst verfügbar und werden verwendet, um kontextbezogenen Zugriff auf der Grundlage des Gerätestatus bereitzustellen.

Vollständige Informationen zum Device Posture Service finden Sie unter Device Posture.

Um eine adaptive Zugriffsrichtlinie auf der Grundlage des Gerätezustands zu konfigurieren, verwenden Sie das Verfahren "Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen "mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen**.
- Wählen Sie **Device Posture Check** und den logischen Ausdruck aus dem Drop-down-Menü aus.
- Geben Sie einen der folgenden Werte in benutzerdefinierte Tags ein:
  - **Konform** —Für konforme Geräte
  - **Nicht konform** —Für Geräte, die nicht konform sind

> **Hinweis:**
>
> Die Syntax für die Geräteklassifizierungs-Tags muss auf dieselbe Weise eingegeben werden, wie sie zuvor erfasst wurde, d. h. in Großbuchstaben (konform und nicht konform). Andernfalls funktionieren die Gerätestatusrichtlinien nicht wie vorgesehen.



Adaptiver Zugriff basierend auf der Risikobewertung des Benutzers

> **Wichtig:**
>
> Diese Funktion steht den Kunden nur zur Verfügung, wenn sie über die Berechtigung Security Analytics verfügen.

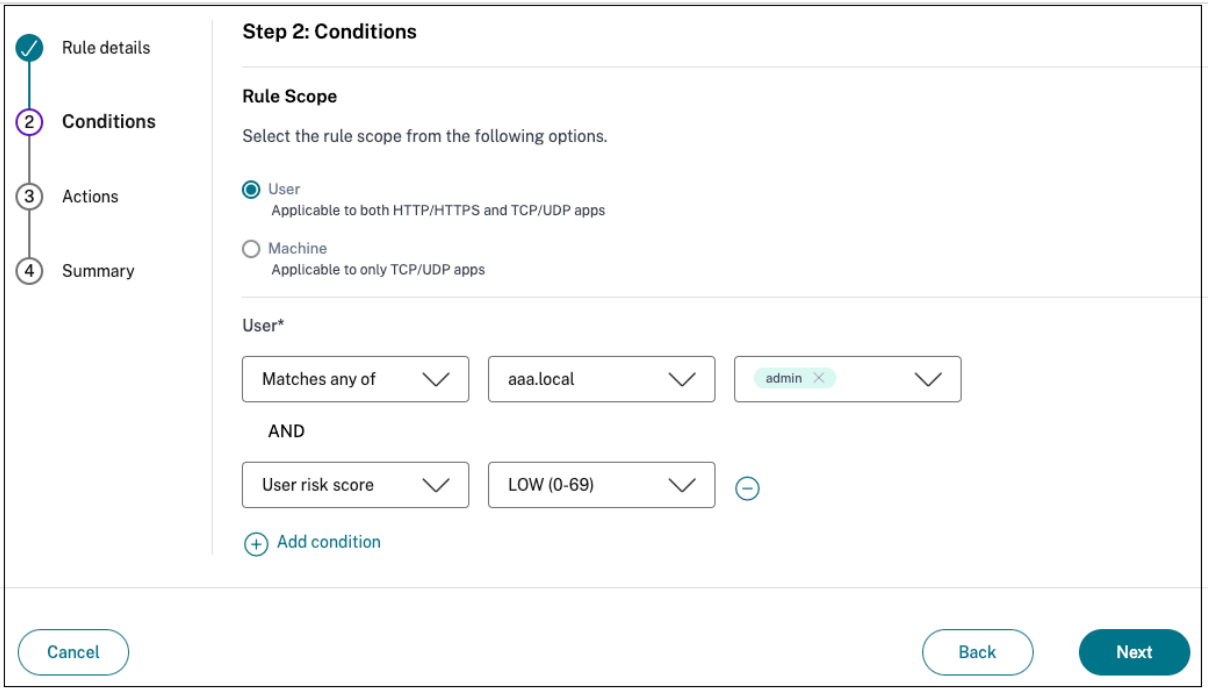
Die Benutzerrisikobewertung ist ein Bewertungssystem zur Bestimmung der Risiken, die mit den Benutzeraktivitäten in Ihrem Unternehmen verbunden sind. Risikoindikatoren werden Benutzeraktivitäten zugewiesen, die verdächtig aussehen oder eine Sicherheitsbedrohung für Ihr Unternehmen darstellen können. Die Risikoindikatoren werden ausgelöst, wenn das Verhalten des Benutzers vom Normalwert abweicht. Jeder Risikoindikator kann einen oder mehrere Risikofaktoren aufweisen. Diese Risikofaktoren helfen Ihnen, die Art der Anomalien in den Benutzerereignissen zu bestimmen. Die Risikoindikatoren und die damit verbundenen Risikofaktoren bestimmen den Risiko-Score eines Nutzers. Die Risikobewertung wird regelmäßig berechnet und es gibt eine Verzögerung zwischen der Aktion und der Aktualisierung der Risikobewertung. Einzelheiten finden Sie unter Risikoindikatoren für Benutzer von Citrix.

Um eine adaptive Zugriffsrichtlinie mit Risikobewertung zu konfigurieren, verwenden Sie das Verfahren "Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen "mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen**.
- Wählen Sie **Benutzerrisikobewertung** und dann die Risikobedingung aus.
  - Voreingestellte Tags, die vom CAS-Service abgerufen wurden
    - **NIEDRIG** 1—69
    - **MITTEL** 70—89
    - **HOCH** 90—100

    > **Hinweis:**
    >
    > Ein Risiko-Score von 0 wird nicht als Risikoniveau "Niedrig"angesehen.

  - Schwellenwert-Typen
    - **Größer oder gleich**
    - **Kleiner oder gleich**
  - Ein Nummernkreis
    - **Reichweite**



Routing-Tabellen zur Lösung von Konflikten, die sich aus denselben verwandten Domänen ergeben

December 27, 2023

Die Funktion Anwendungsdomänen des Citrix Secure Private Access-Dienstes ermöglicht es Kunden, Routing-Entscheidungen zu treffen, die es ermöglichen, verwandte Anwendungsdomänen extern oder intern über Connector Appliances zu leiten.

Bedenken Sie, dass der Kunde dieselben verwandten Domänen sowohl innerhalb einer SaaS-App als auch in einer internen Webanwendung konfiguriert hat.
Wenn Okta beispielsweise der SAML-IdP für Salesforce (SaaS-App) und Jira (interne Web-App) ist, kann der Administrator in der Konfiguration beider Apps `*.okta.com` als verwandte Domäne konfigurieren. Dies führt zu einem Konflikt und der Endbenutzer erfährt inkonsistentes Verhalten. In diesem Szenario kann der Administrator Regeln definieren, um diese Anwendungen je nach Anforderung entweder extern oder intern über die Connector Appliances weiterzuleiten.

Die Funktion Anwendungsdomänen ermöglicht es Administratoren außerdem, die Connector Appliances so zu konfigurieren, dass sie die Web-Proxyserver des Kunden Bypass, um die internen Webserver zu erreichen. Diese Bypass-Richtlinien wurden zuvor manuell konfiguriert, indem die NSCLI-Befehle auf der Connector Appliance ausgeführt wurden.

So funktioniert die Routentabelle

Die Administratoren können den Routentyp für die Apps als Extern, Intern oder Extern über die Connector Appliance definieren, je nachdem, wie sie den Verkehrsfluss definieren möchten.

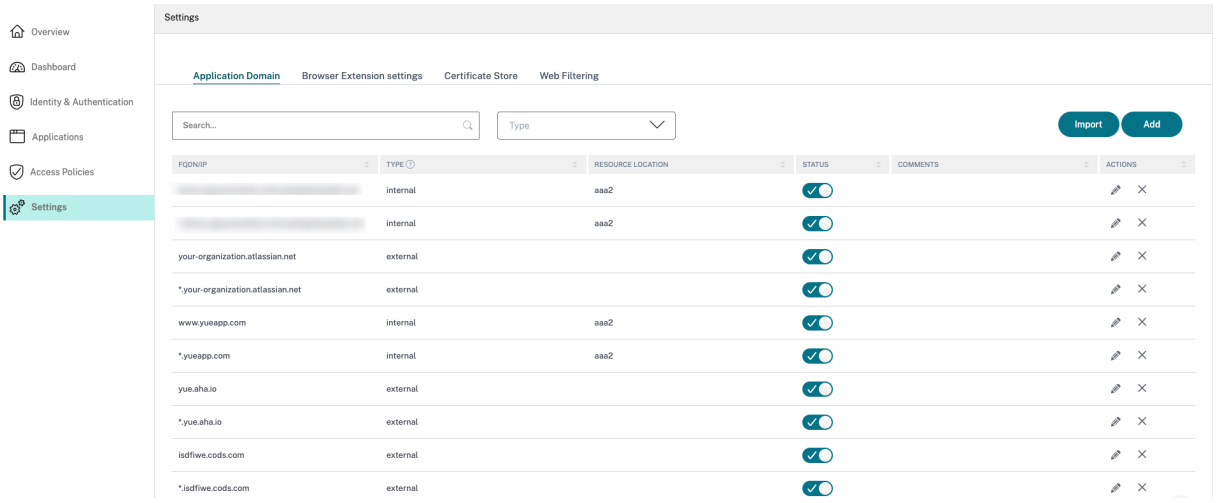
- **Extern** —Der Verkehr fließt direkt ins Internet.
- **Intern** —Der Datenverkehr fließt über die Connector Appliance.
  - Für eine Web-App fließt der Verkehr innerhalb des Rechenzentrums.
  - Bei einer SaaS-App wird der Datenverkehr über die Connector Appliance außerhalb des Netzwerks weitergeleitet.
- **Intern** —**Bypass-Proxy** —Der Domain-Verkehr wird über Citrix CloudConnector Appliances geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
- **Extern über Connector** —Die Apps sind extern, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.

> **Hinweis:**
>
> - Routeneinträge wirken sich nicht auf die Sicherheitsrichtlinien aus, die in den Apps konfiguriert sind.
> - Wenn Administratoren nicht beabsichtigen, einen Eintrag in der Routing-Tabelle zu verwenden, oder wenn die entsprechenden Apps nicht wie vorgesehen funktionieren, können Administratoren den Eintrag einfach deaktivieren, anstatt ihn zu löschen.
> - Alle Connector Appliances für einen bestimmten Kunden, unabhängig vom App-Typ, erhalten die SSO-Einstellungen. Zuvor war die SSO-Einstellung für eine bestimmte App an einen Ressourcenstandort gebunden.

Hauptrouten-Tabelle

Auf die Hauptroutentabelle kann über die Kachel **Secure Private Access zugegriffen** werden.

1. Melden Sie sich beim Citrix Cloud-Konto an.
2. Klicken Sie auf der Kachel Secure Private Access auf **Verwalten** .
3. Klicken Sie im Navigationsbereich auf **Einstellungen.** Die Seite **Anwendungsdomänen** wird angezeigt.



Die Hauptrouten-Tabelle zeigt die folgenden Spalten an.

- **FQDN/IP:** FQDN oder die IP-Adresse, für die die Art der Verkehrsweiterleitung konfiguriert werden soll.
- **Typ**: App-Typ. **Intern**, **Extern**oder **Extern über Connector**, wie beim Hinzufügen der App ausgewählt.

> **Wichtig:**
>
> Bei Konflikten wird ein Warnsymbol für die entsprechende Zeile in der Tabelle angezeigt. Um den Konflikt zu lösen, müssen Administratoren auf das Dreieckssymbol klicken und den App-Typ in der Haupttabelle ändern.

- **Ressourcenstandort:** Ressourcenstandort für Routing vom Typ **Intern**. Wenn kein Ressourcenstandort zugewiesen wird, wird in der Spalte **Ressourcenstandort** für die jeweilige App ein dreieckiges Symbol angezeigt. Wenn Sie mit der Maus auf das Symbol fahren, wird die folgende Meldung angezeigt.

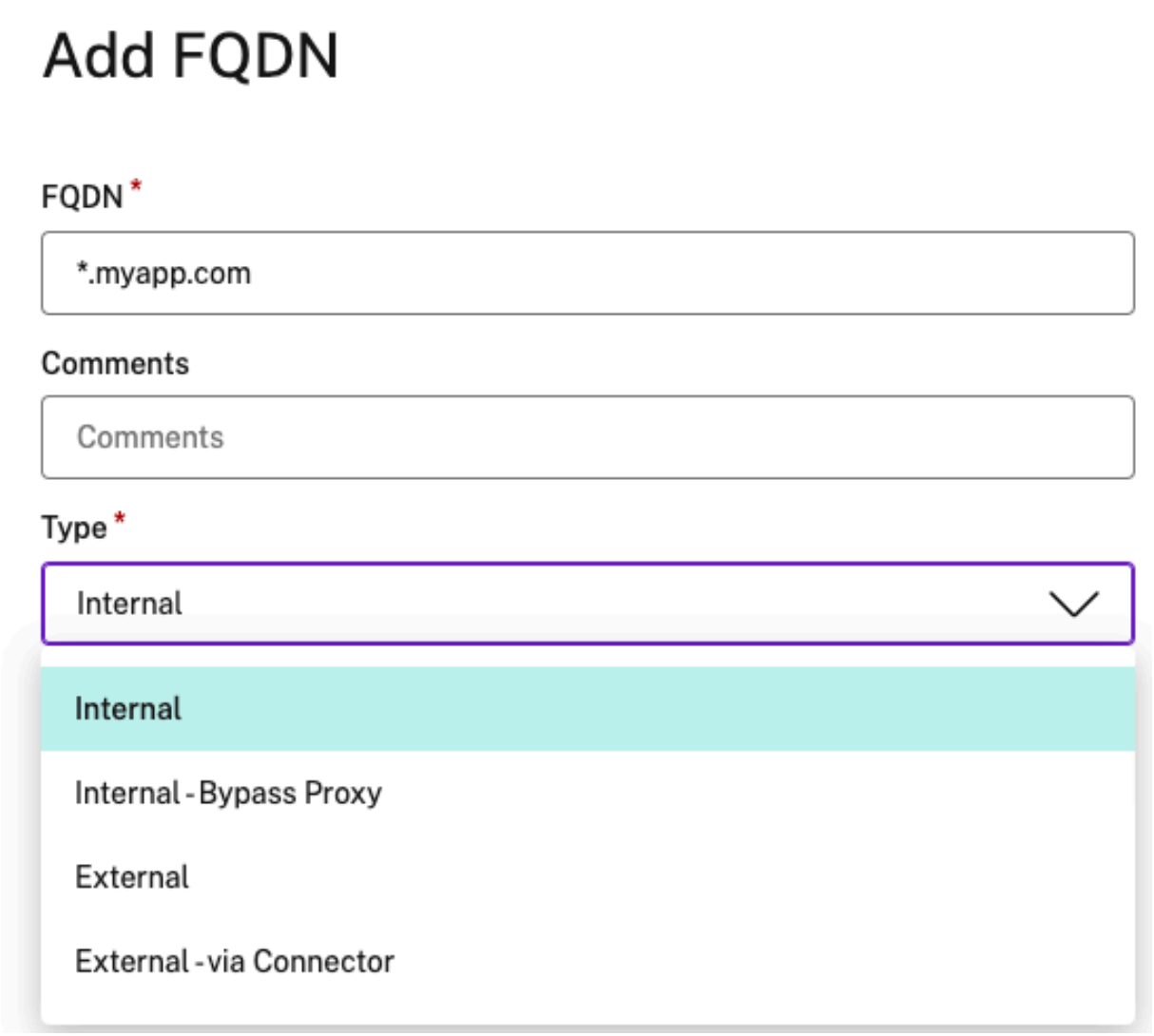
  Fehlender Ressourcenstandort Stellen Sie sicher, dass diesem FQDN ein Ressourcenstandort zugeordnet ist.

- **Status:** Der Kippschalter in der Spalte **Status** kann verwendet werden, um die Route für einen Routeneintrag zu deaktivieren, ohne die App zu löschen. Wenn der Kippschalter ausgeschaltet ist, wird die Routeneingabe nicht wirksam. Wenn FQDNs mit exakter Übereinstimmung existieren, können Administratoren die Route auswählen, die aktiviert oder deaktiviert werden soll.
- **Kommentare:** Zeigt ggf. Kommentare an.
- **Aktionen:** Das Bearbeitungssymbol wird verwendet, um einen Ressourcenstandort hinzuzufügen oder den Typ des Routeneintrags zu ändern. Das Löschsymbol wird verwendet, um die Route zu löschen.

Fügen Sie der Tabelle Anwendungsdomänen einen FQDN hinzu

Administratoren können einen FQDN zur Tabelle Anwendungsdomänen hinzufügen und den entsprechenden Routingtyp dafür auswählen.

1. Klicken Sie auf der Seite Anwendungsdomäne auf **Hinzufügen** .
2. Geben Sie den FQDN-Namen ein und wählen Sie den entsprechenden Routingtyp für den FQDN aus.



Mini-Routing-Tabelle

Eine Mini-Version der Tabelle Anwendungsdomänen ist verfügbar, um die Routing-Entscheidungen während der App-Konfiguration zu treffen. Die Mini-Routing-Tabelle, die im Abschnitt **App Connectivity** auf der Benutzeroberfläche des Citrix Secure Private Access-Dienstes verfügbar ist.

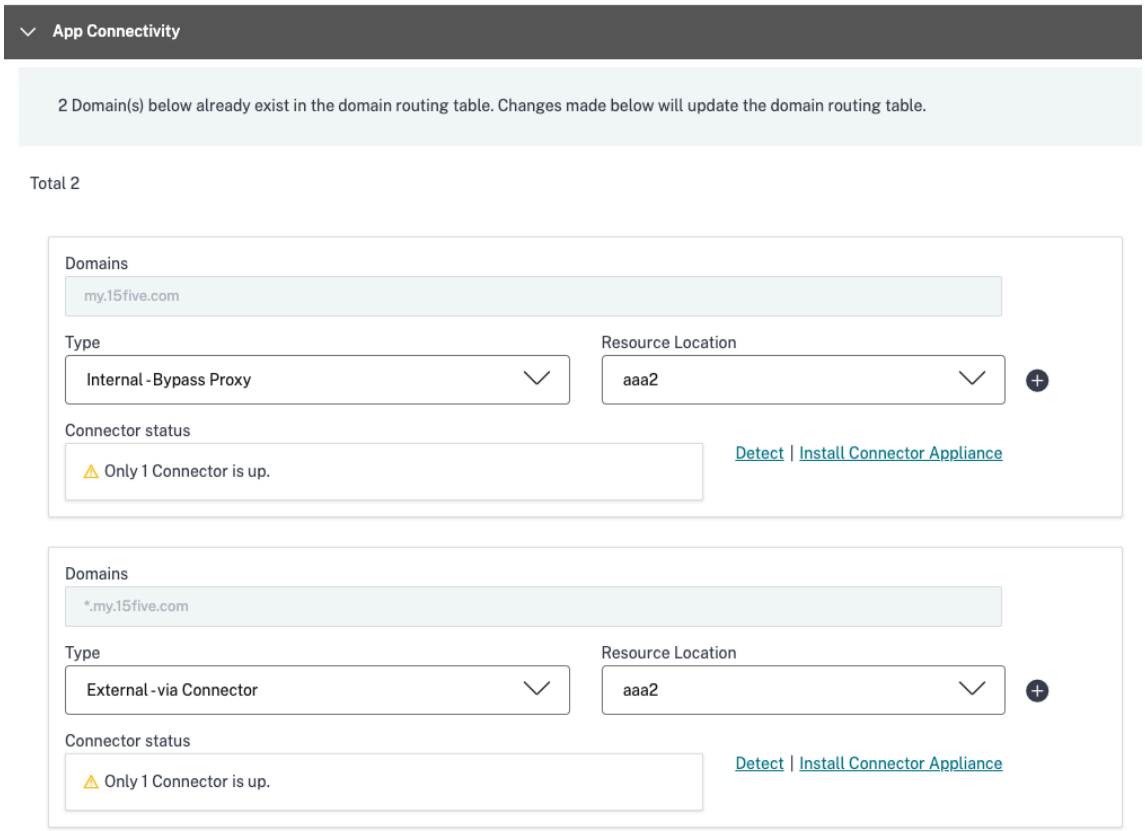
So fügen Sie der Mini-Routentabelle Routen hinzu

Die Schritte zum Hinzufügen einer App zum Citrix Secure Private Access-Dienst bleiben dieselben wie in den Themen Support für Software-as-a-Service-Apps und Support für Enterprise-Web-Apps beschrieben, mit Ausnahme der folgenden zwei Änderungen:

1. Führen Sie hierzu die folgenden Schritte aus:

- Wähle eine Vorlage aus.
- Gib App-Details ein.
- Wählen Sie soweit zutreffend erweiterte Sicherheitsdetails.
- Wählen Sie nach Belieben die Methode für einmaliges Anmelden aus.

2. Klicken Sie auf **App Connectivity**. - Eine Mini-Version der Tabelle Anwendungsdomänen ist verfügbar, um die Routing-Entscheidungen während der App-Konfiguration zu treffen.



- **Domänen:** In der Spalte Domänen werden eine oder mehrere Zeilen für eine bestimmte App angezeigt. In der ersten Zeile wird die tatsächliche App-URL angezeigt, die der Administrator beim Hinzufügen der App-Details eingegeben hat. Die anderen Zeilen sind alle verwandten Domänen, die beim Hinzufügen der App-Details eingegeben werden. Wenn die App-URL und die zugehörigen Domains identisch sind, werden sie in einer Zeile angezeigt.

Eine Zeile zeigt die SAML-Assertion-URL an, wenn SAML SSO ausgewählt ist.

- **Typ:** Wählen Sie eine der folgenden Optionen aus.
  - **Extern** —Der Verkehr fließt direkt ins Internet.
  - **Intern** —Der Datenverkehr fließt über die Connector Appliance und die App wird als Web-App behandelt.
    * Für eine Web-App fließt der Verkehr innerhalb des Rechenzentrums.

    * Bei einer SaaS-App wird der Datenverkehr über die Connector Appliance außerhalb des Netzwerks weitergeleitet.
  - **Intern —Bypass-Proxy** —Der Domain-Verkehr wird über Citrix Cloud Connector Appliances geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
  - **Extern über Connector** —Die Apps sind extern, aber der Datenverkehr muss über die Connector Appliance an das externe Netzwerk fließen.
- **Ressourcenstandort:** Wird automatisch ausgefüllt, wenn Sie den Typ Intern für eine App auswählen. Ändern Sie es, wenn ein anderer Ressourcenstandort gewünscht wird
- **Status der Connector Appliance:** Wird zusammen mit dem Ressourcenstandort automatisch ausgefüllt, wenn Sie den Typ Intern für eine App auswählen.

Nicht genehmigte Websites

June 19, 2024

Anwendungen (Intranet oder Internet), die nicht in Secure Private Access konfiguriert sind, werden als "nicht genehmigte Websites"betrachtet. Standardmäßig verweigert Secure Private Access den Zugriff auf alle Intranet-Webanwendungen, wenn für diese Anwendungen keine Anwendungen und Zugriffsrichtlinien konfiguriert sind.

Für alle anderen Internet-URLs oder SaaS-Anwendungen, für die keine App konfiguriert ist, können Administratoren den Tab **Einstellungen > Unsanktionierte Websites** in der Admin-Konsole verwenden, um den Zugriff über den Citrix Enterprise Browser zuzulassen oder zu verweigern. Administratoren können den Zugriff auch auf eine Remote Browser Isolated (RBI) -Umgebung umleiten, um browserbasierte Angriffe zu verhindern. Wenn ein Administrator die Umleitung von URLs zu RBI konfiguriert hat, werden die folgenden Aktionen ausgeführt.

1. Secure Private Access konvertiert die Domains.
2. Citrix Enterprise Browser sendet diese URLs dann zurück an Secure Private Access.
3. Secure Private Access leitet diese URLs an den Remote Browser Isolation-Dienst weiter.

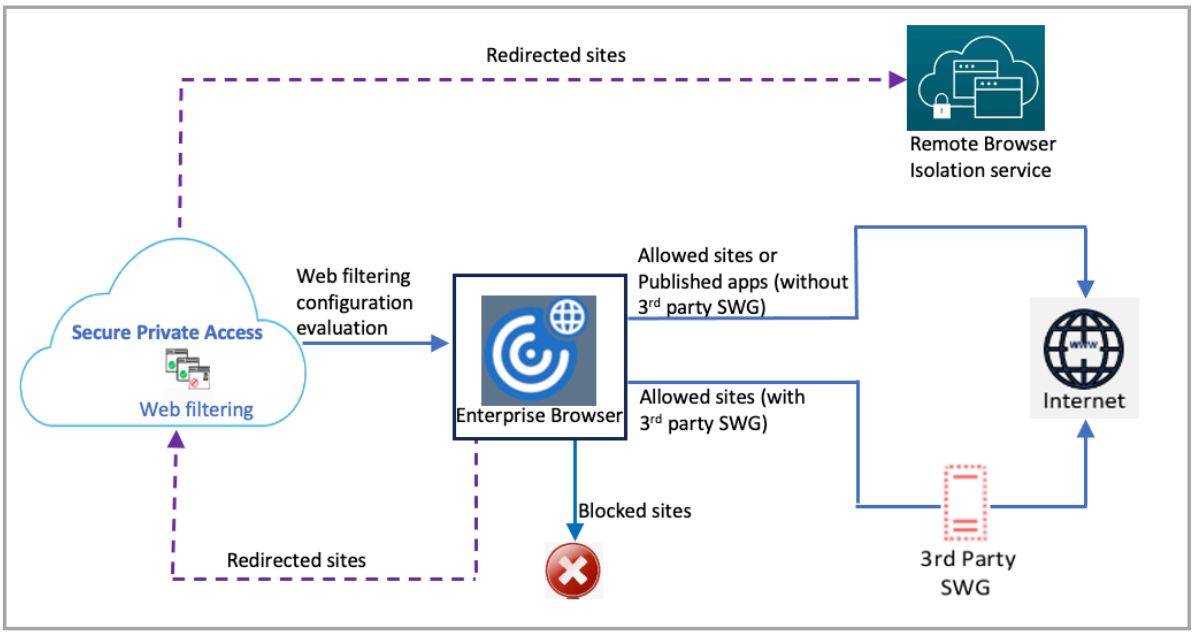
Sie können Platzhalter verwenden `*.example.com`, um z. B. den Zugriff auf alle Domains dieser Website und alle Seiten innerhalb dieser Domain zu kontrollieren.

> **Hinweis:**
>
> Standardmäßig sind die Einstellungen so konfiguriert, dass der Zugriff auf alle Internet-URLs oder SaaS-Apps über den Citrix Enterprise Browser ZUGELASSEN wird.

So funktionieren nicht genehmigte Websites

1. Die URL-Analyse wird durchgeführt, um festzustellen, ob die URL eine Citrix Dienst-URL ist.
2. Die URL wird dann überprüft, um festzustellen, ob es sich um eine Enterprise Web- oder SaaS-App-URL handelt.
3. Die URL wird dann überprüft, um festzustellen, ob sie als blockierte URL identifiziert wurde oder ob sie zu einer sicheren Browsersitzung umgeleitet werden muss oder ob der Zugriff auf die URL zulässig ist.

Die folgende Abbildung erläutert den Datenfluss für Endbenutzer.

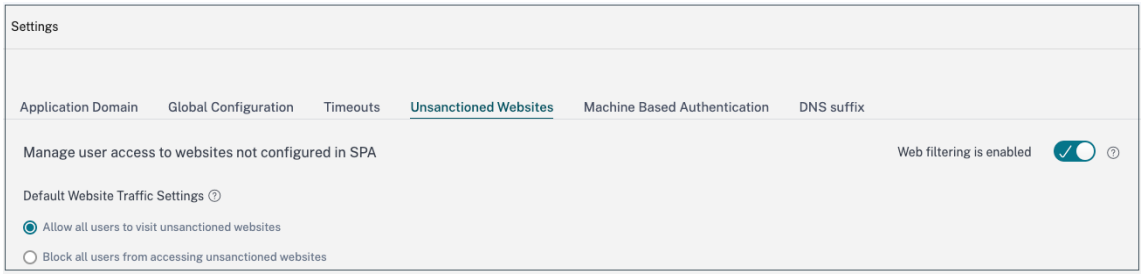


Nach dem Empfang einer Anfrage werden folgende Prüfungen und zugehörige Aktionen ausgeführt:

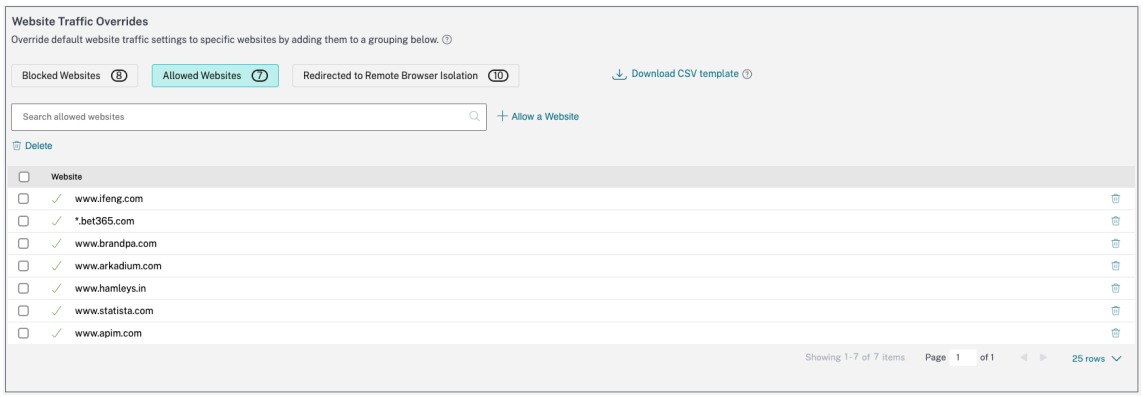
1. Stimmt die Anfrage mit der Liste global zugelassener Sites überein?
   a) Wenn ja, kann der Benutzer auf die angeforderte Website zugreifen.
   b) Wenn nicht, werden Websitelisten überprüft.
2. Stimmt die Anfrage mit der konfigurierten Websiteliste überein?
   a) Wenn ja, wird die Aktion durch folgende Sequenz festgelegt.
      i. Blockieren
      ii. Umleiten
      iii. Allow
   b) Wenn nicht, wird die Standardaktion (ZULASSEN) angewendet. Die Standardaktion kann nicht geändert werden.

Regeln für nicht genehmigte Websites konfigurieren

1. Klicken Sie in der Secure Private Access-Konsole auf **Einstellungen > Nicht genehmigte Websites**.



> **Hinweis:**
>
> - Die Webfilterfunktion ist standardmäßig aktiviert und der Zugriff auf alle nicht genehmigten Internet-URLs ist zulässig.
> - Sie können die Einstellung auf **Blockieren aller Benutzer am Zugriff auf nicht genehmigte Websites** ändern, um den Zugriff auf jede Internet-URL über den Citrix Enterprise Browser für alle Benutzer zu blockieren.



Sie können auch die Einstellungen für bestimmte URLs ändern, indem Sie sie zu blockierten Websites oder erlaubten Websites hinzufügen oder zur Remote-Browser-Isolationsliste umleiten.

Wenn Sie beispielsweise standardmäßig den Zugriff auf alle nicht sanktionierten URLs blockiert haben und den Zugriff auf nur einige bestimmte Internet-URLs zulassen möchten, können Sie dies tun, indem Sie die folgenden Schritte ausführen:

a) Klicken Sie auf den Tab **Zulässige Websites** und dann auf **Website zulassen**.

b) Fügen Sie die Adresse der Website hinzu, der der Zugriff gewährt werden muss. Sie können die Website-Adresse entweder manuell hinzufügen oder eine CSV-Datei mit der Website-Adresse per Drag-and-Drop ziehen.

c) Klicken **Sie auf URL hinzufügen** und dann auf **Speichern**.

Die URL wird zur Liste der erlaubten Websites hinzugefügt.

> **Hinweis:**
>
> Ein kostenpflichtiger Kunde (Organisation) des Remote Browser Isolation Standard-Service erhält standardmäßig 5.000 Nutzungsstunden pro Jahr. Für weitere Stunden müssen sie die sicheren Browser-Add-On-Pakete kaufen. Sie können die Nutzung des Remote Browser Isolation-Dienstes verfolgen. Weitere Informationen finden Sie in den folgenden Artikeln:
>
> - Isolierte Remotebrowser verwalten und überwachen
> - Remote-Browser-Isolierung.

ADFS-Integration mit Secure Private Access

December 27, 2023

Anspruchsregeln sind notwendig, um den Fluss von Ansprüchen durch die Anspruchspipeline zu steuern. Anspruchsregeln können auch verwendet werden, um den Anspruchsablauf während des Ausführungsprozesses für Anspruchsregeln anzupassen. Weitere Informationen zu Ansprüchen finden Sie in der Microsoft-Dokumentation.

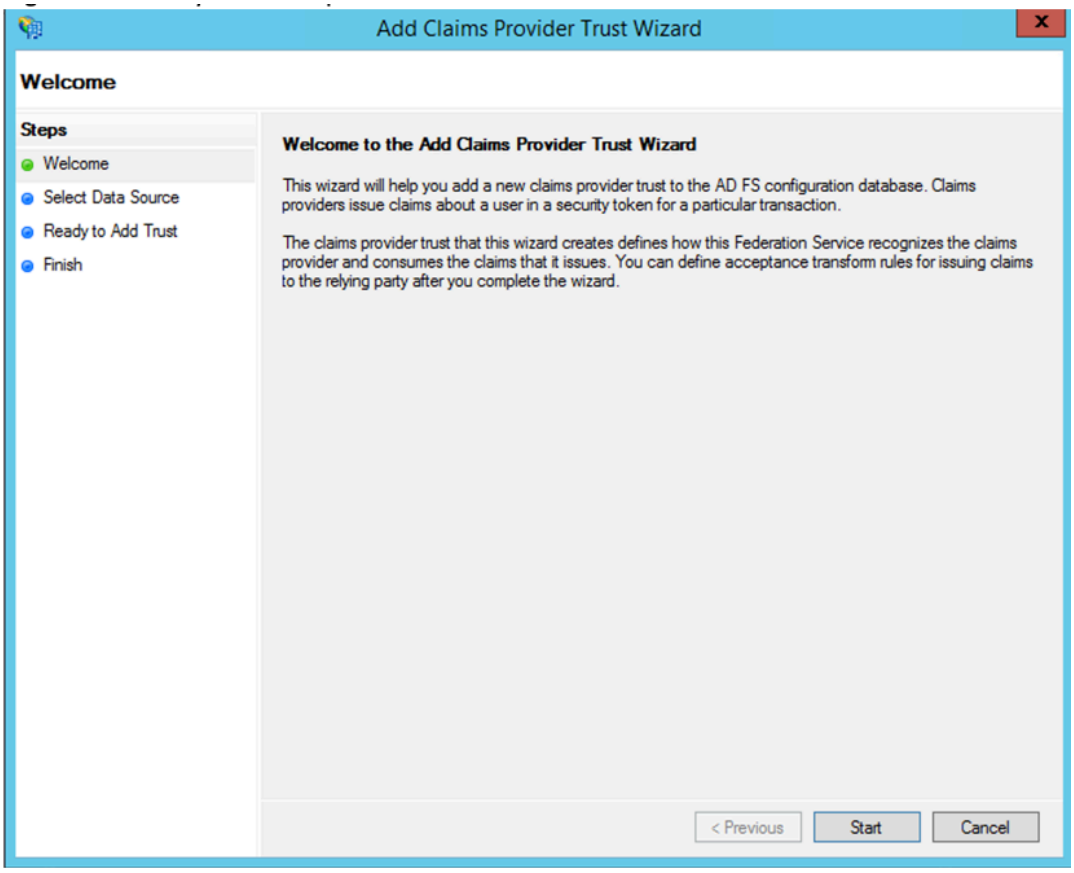
Um ADFS so einzurichten, dass Ansprüche von Citrix Secure Private Access akzeptiert werden, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie Vertrauen von Anspruchsanbietern in ADFS hinzu
2. Vervollständigen Sie die App-Konfiguration auf Citrix Secure Private Access.

Vertrauen des Antragsanbieters in ADFS hinzufügen

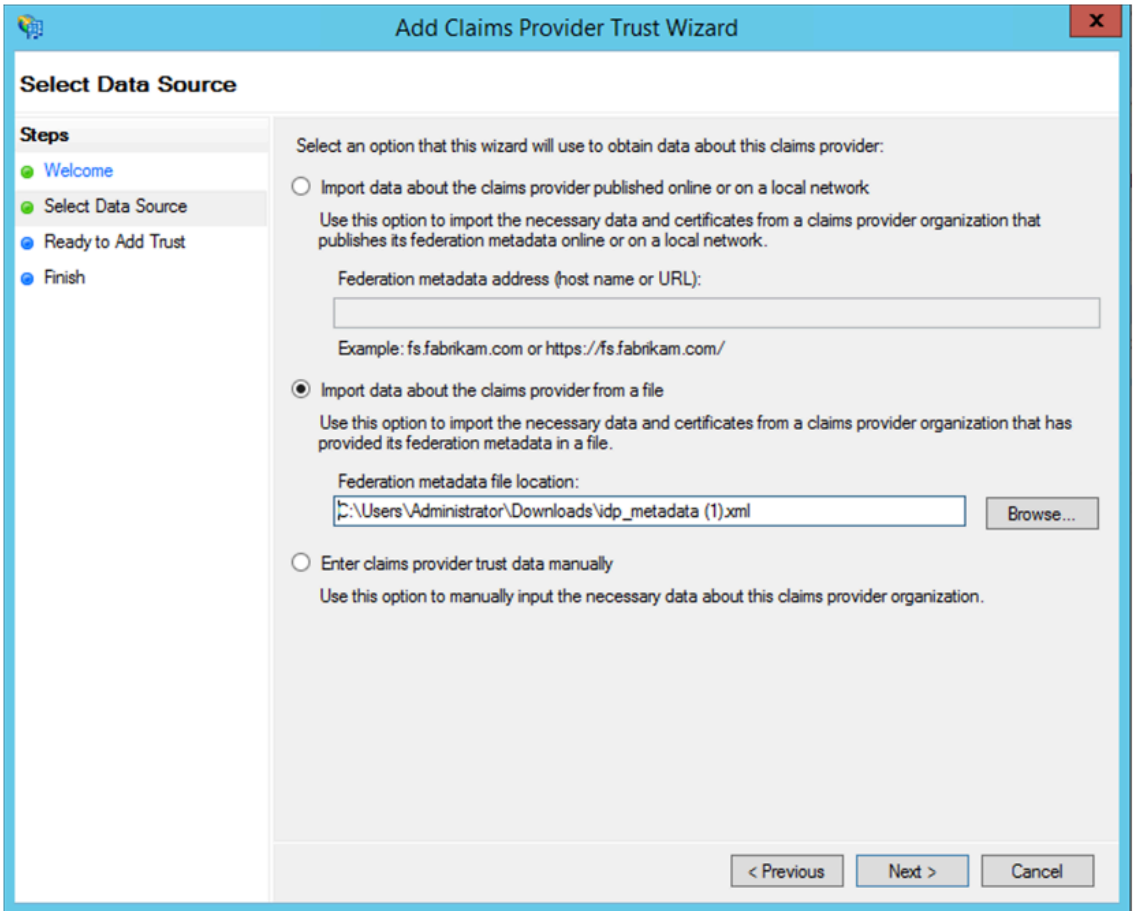
1. Öffnen Sie die ADFS-Managementkonsole. Gehen Sie zu **ADFS > Trust Beziehung > Claim Provider Trust**.

   a) Klicken Sie mit der rechten Maustaste und **wählen Sie Vertrauensstellung**für

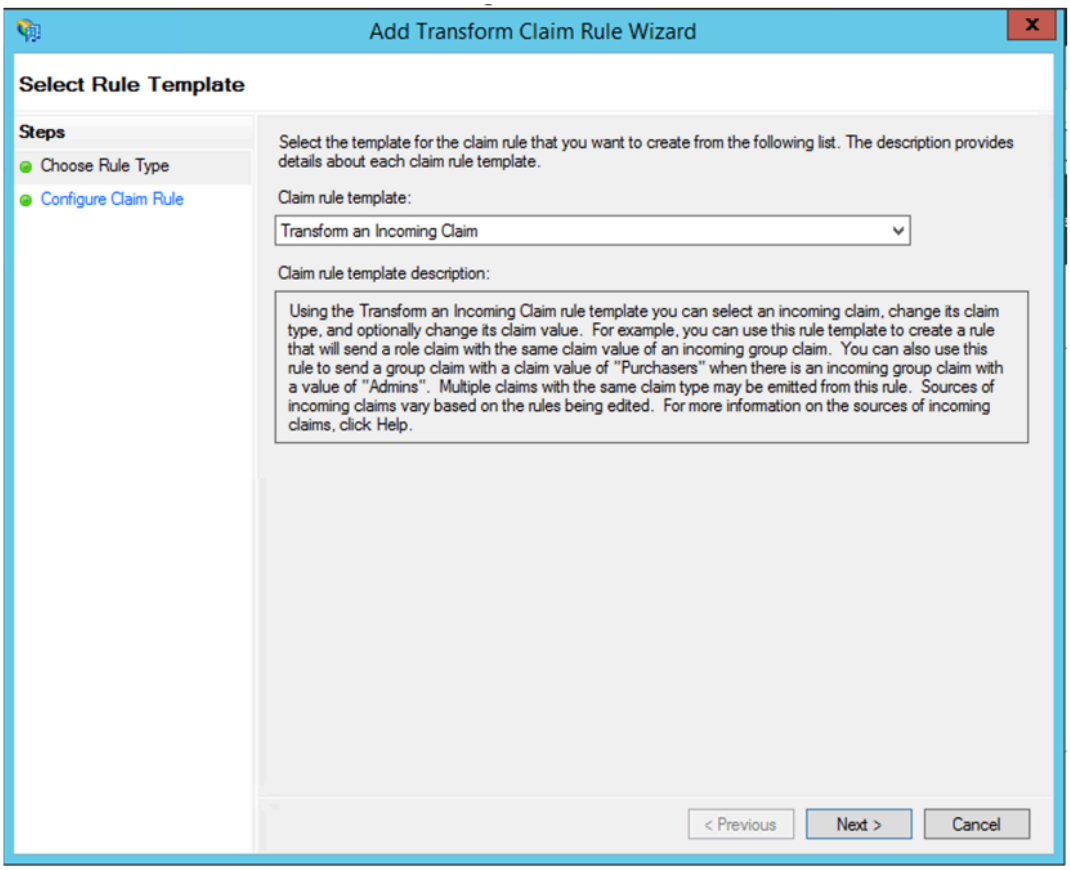


b) Fügen Sie in Secure Private Access eine App hinzu, die für die Verbindung zu ADFS verwendet wird. Einzelheiten finden Sie unter App-Konfiguration auf Citrix Secure Private Access.

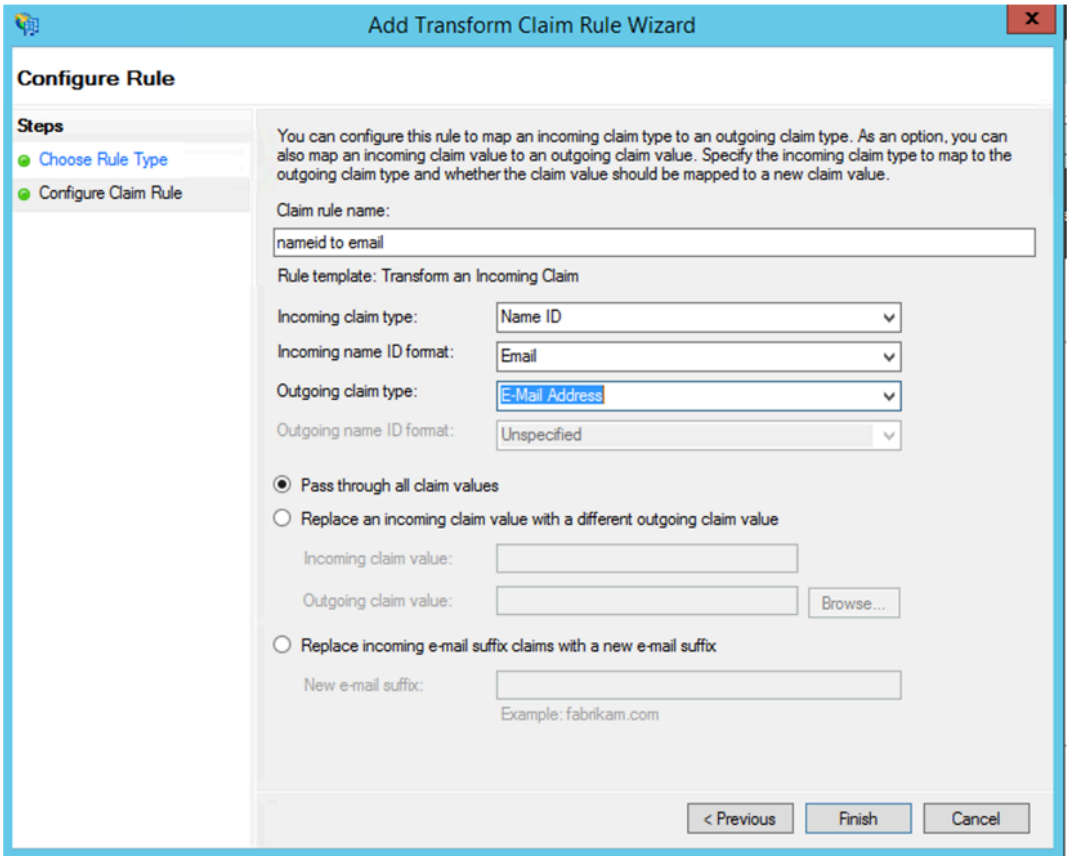
> **Hinweis:**
>
> Fügen Sie zuerst die App hinzu und aus dem SSO-Konfigurationsbereich der App können Sie die SAML-Metadatendatei herunterladen und dann die Metadatendatei in ADFS importieren.



a) Führen Sie die Schritte aus, um das Hinzufügen des Anspruchsanbietervertrauens abzuschließen Nachdem Sie die Vertrauensstellung des Antragsanbieters hinzugefügt haben, wird ein Fenster zur Bearbeitung der Anspruchsregel angezeigt.
b) Fügen Sie eine Anspruchsregel mit **Eingehenden Anspruch transformieren** hinzu



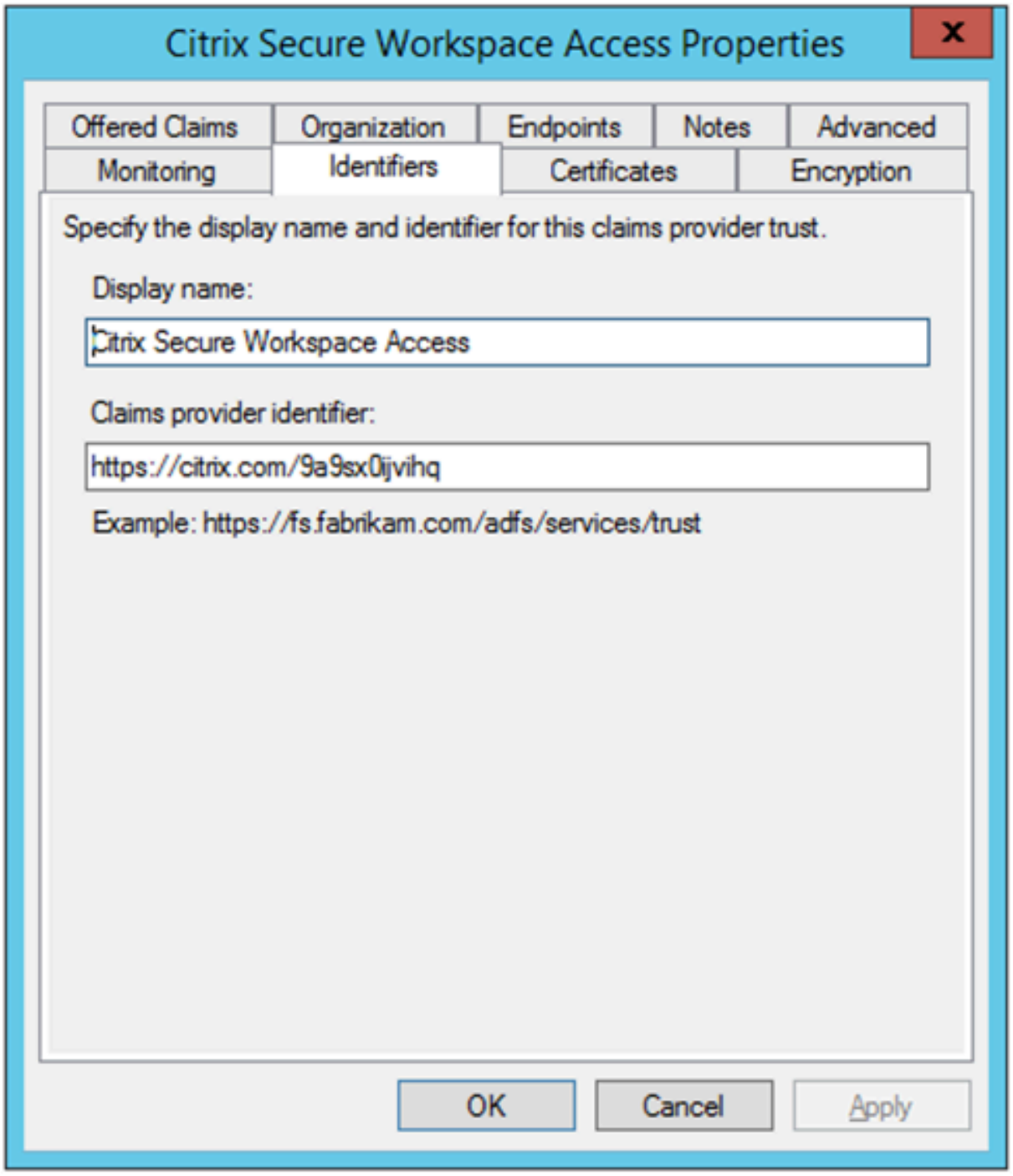
c) Vervollständigen Sie die Einstellungen wie in der folgenden Abbildung gezeigt. Wenn Ihr ADFS andere Ansprüche akzeptiert, verwenden Sie diese Ansprüche und konfigurieren Sie SSO in Secure Private Access ebenfalls entsprechend.



Sie haben jetzt die Anspruchsanbietervertrauensstellung konfiguriert, die bestätigt, dass ADFS jetzt Citrix Secure Private Access for SAML vertraut.

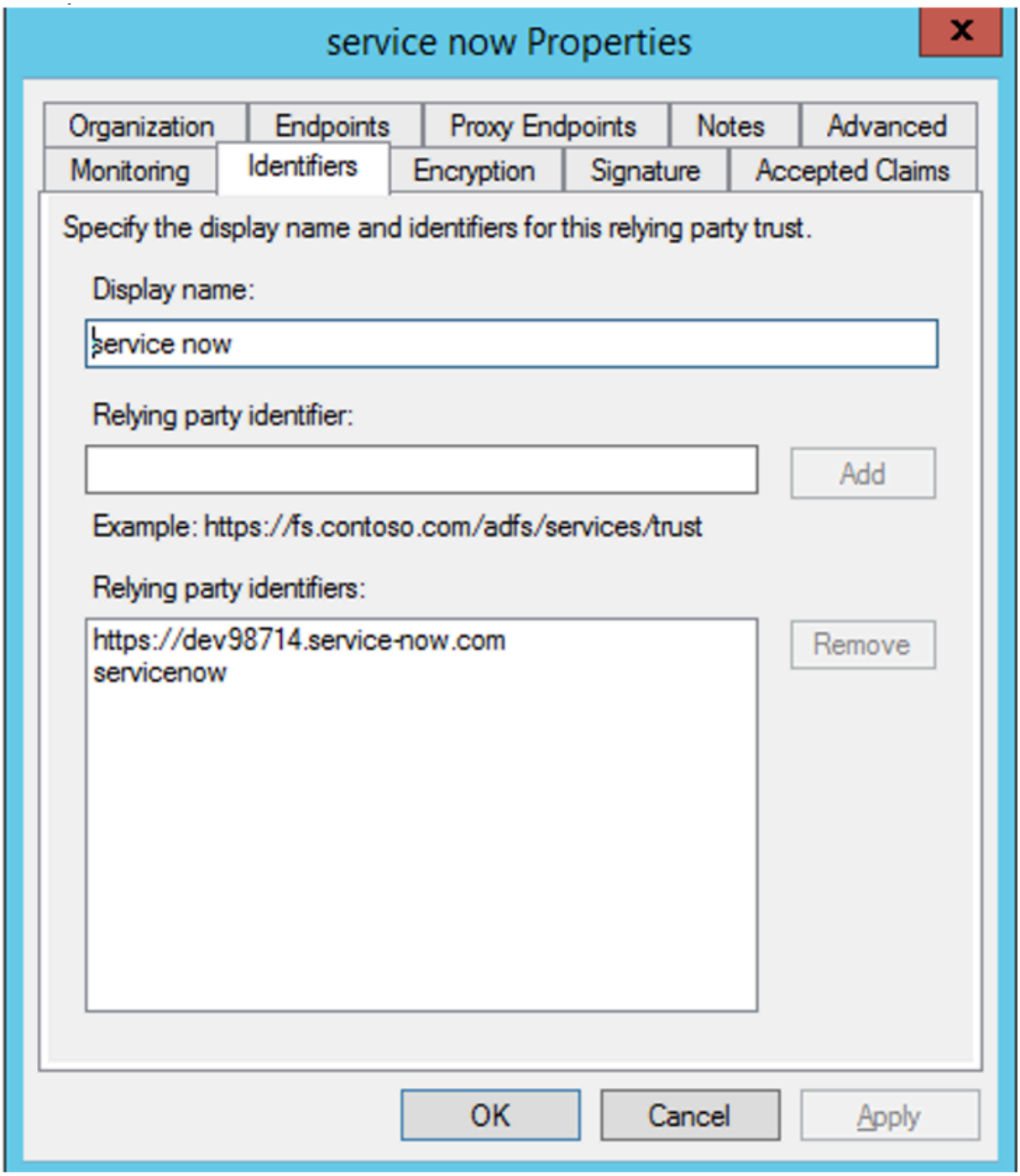
Vertrauensnummer des Anbieters

Notieren Sie sich die Vertrauensnummer des Anspruchsanbieters, die Sie hinzugefügt haben Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.



Partei-Identifikator weiterleiten

Wenn Ihre SaaS-App bereits mithilfe von ADFS authentifiziert wurde, müssen Sie bereits die Vertrauensstellung der Relaying-Partei für diese App hinzugefügt haben. Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.



Aktivieren des Relay-Status im IdP-initiierten Flow

RelayState ist ein Parameter des SAML-Protokolls, der verwendet wird, um die spezifische Ressource zu identifizieren, auf die die Benutzer zugreifen, nachdem sie angemeldet und an den Federation Server der vertrauenden Partei weitergeleitet wurden. Wenn RelayState in ADFS nicht aktiviert ist, wird Benutzern ein Fehler angezeigt, nachdem sie sich bei den Ressourcenanbietern authentifiziert

haben, die ihn benötigen.

Für ADFS 2.0 müssen Sie das Update KB2681584 (Update Rollup 2) oder KB2790338 (Update Rollup 3) installieren, um RelayState-Unterstützung zu bieten. ADFS 3.0 hat RelayState Unterstützung eingebaut. In beiden Fällen muss RelayState noch aktiviert werden.

So aktivieren Sie den RelayState-Parameter auf Ihren ADFS-Servern

1. Öffne die Datei.
   - Für ADFS 2.0 geben Sie die folgende Datei in Notepad ein: %systemroot%\inetpub\adfs\ls\web.config
   - Geben Sie für ADFS 3.0 die folgende Datei in Notepad ein: %systemroot%\ADFS\Microsoft.IdentityServe
2. Fügen Sie im Abschnitt Microsoft.IdentityServer.web eine Zeile für useRelyStateForIdpInitiatedSignOn wie folgt hinzu, und speichern Sie die Änderung:
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - Führen Sie für ADFS 2.0 aus, `IISReset` um IIS neu zu starten.
3. Starten Sie für beide Plattformen die Active Directory Federation Services neu (`adfssrv`) `service`.
   Hinweis: Wenn Sie Windows 2016 oder Windows 10 haben, verwenden Sie den folgenden PowerShell-Befehl, um es zu aktivieren.
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

Link zu den Befehlen - https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

App-Konfiguration auf Citrix Secure Private Access

Sie können entweder den IdP-initiierten Flow oder den von SP initiierten Flow konfigurieren. Die Schritte zum Konfigurieren des IdP- oder SP-initiierten Flusses in Citrix Secure Private Access sind dieselben, mit der Ausnahme, dass Sie für SP-initiierten Flow **das Kontrollkästchen App mit der angegebenen URL starten (SP-initiiert)** in der Benutzeroberfläche aktivieren müssen.

IdP initiierter Flow

1. Konfigurieren Sie beim Einrichten des IdP-initiierten Flows Folgendes.
   - **App-URL** —Verwenden Sie das folgende Format für die App-URL.
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```


- **ADFS FQDN** —FQDN Ihres ADFS-Setups.
- **RP-ID** —RP-ID ist die ID, die Sie von Ihrem vertrauenswürdigen Parteivertrauen erhalten können. Es ist das gleiche wie der Relaying Party Identifier. Wenn es sich um eine URL handelt, erfolgt die URL-Codierung.
- **IDP-ID** —IdP-ID ist die gleiche wie die Vertrauensnummer des Anspruchsanbieters. Wenn es sich um eine URL handelt, erfolgt die URL-Codierung.

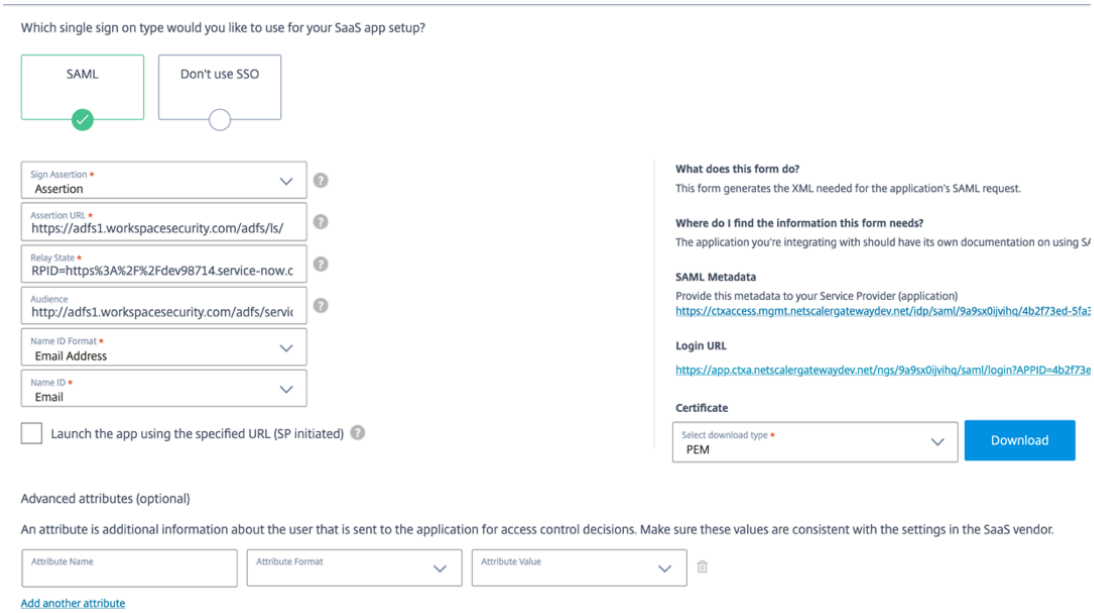
  Beispiel: https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. SAML SSO-Konfiguration

   Im Folgenden sind die Standardwerte des ADFS-Servers aufgeführt. Wenn einer der Werte geändert wird, holen Sie sich die richtigen Werte aus den Metadaten des ADFS-Servers. Federation-Metadaten des ADFS-Servers können von seinem Federation-Metadaten-Endpunkt heruntergeladen werden, dessen Endpunkt unter **ADFS > Service > Endpoints bekannt sein kann.**

   - **Behauptung URL** —`https://<adfs fqdn>/adfs/ls/`
   - **Relay State** —Der Relay-Status ist wichtig für den IdP-initiierten Flow. Folgen Sie diesem Link, um es richtig zu konstruieren - `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     Beispiel: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev9871
     now.com%2F
   - **Zielgruppe** —`http://<adfsfqdn>/adfs/services/trust`
   - Informationen zu den anderen SAML SSO-Konfigurationseinstellungen finden Sie in der folgenden Abbildung. Weitere Einzelheiten finden Sie unter https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html



3. Speichern und abonnieren Sie die App für den Benutzer.

SP initiierte Flow

Konfigurieren Sie für einen von SP initiierten Flow die Einstellungen wie im Abschnitt **IDP initiated Flow** erfasst. Aktivieren Sie außerdem das Kontrollkästchen **App mit der angegebenen URL (SP initiiert) starten**.

Problembehandlung für Secure Private Access

June 21, 2024

Verwenden Sie dieses Thema, um einige Probleme im Zusammenhang mit der App-Konfiguration, Authentifizierung und SSO oder dem App-Zugriff zu beheben. Kopieren Sie den Infocode aus der Spalte “Infocode“in den Secure Private Access-Diagnoseprotokollen und suchen Sie dann auf dieser Seite nach diesem Code, um die entsprechenden Schritte zur Fehlerbehebung zu finden. Im Folgenden finden Sie einige häufig gestellte Fragen, die Ihnen helfen sollen, dieses Thema besser zu nutzen.

Häufig gestellte Fragen?

Was sind Secure Private Access-Diagnoseprotokolle?

Wo finde ich Secure Private Access-Logs?

Welche Details kann ich in den Secure Private Access-Diagnoseprotokollen finden?

Welche Ereignisse werden in den Secure Private Access-Diagnoseprotokollen erfasst?

Wie verwende ich das Thema zur Fehlerbehebung bei Secure Private Access, um einen Fehler zu beheben, auf den ich gestoßen bin?

Was ist ein Infocode? Wo finde ich sie?

Was ist eine Transaktions-ID? Wie verwende ich es?

Was sind all die PoP-Standorte mit sicherem privaten Zugriff?

Was mache ich, wenn ich meinen Fehler nicht mithilfe des Infocodes und der Fehlernachschlagetabelle beheben kann?

Tabelle zum Nachschlagen von Infocodes

Die folgende Tabelle zur Fehlersuche bietet einen umfassenden Überblick über die verschiedenen Fehler, auf die Benutzer bei der Verwendung des Secure Private Access Services möglicherweise stoßen können.

Informationscode	Beschreibung	Auflösung
0 x 180006, 0 x 1800B7	Der App-Start ist fehlgeschlagen, weil die Länge des App-FQDN überschritten wurde	Der App-Start ist fehlgeschlagen, weil die FQDN-Länge der App überschritten wurde
0x180022	Der Start der App ist fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist	Der Start der App ist fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist
0x180001, 0x18001A, 0x18001B, 0x18008A 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0 0x1800B1, 0x1800B2, 0x1800B3, 0x180048	Single Sign-On-Fehler, Verbindungsaufbau zwischen Citrix Cloud und on-premises Connectors, SAML-SSO-Fehler, Ungültiger App-FQDN	App-Zugriff wurde verweigert
0 x 1800EF	Problem beim Herstellen einer Verbindung zum Connector Appliance	Problem beim Herstellen einer Verbindung zum Connector Appliance

Informationscode	Beschreibung	Auflösung
0X18009D	DNS-Suche/Verbindung fehlgeschlagen	Secure Browser Service — DNS-Suche/Verbindungsfehler
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5 0x1800A6, 0x1800A7	Der Start der Web-App ist fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt	Der Start der Web-App ist fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt
0x1800BC, 0x1800BF	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App zuzugreifen	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App zuzugreifen
0x1800BD	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App für DirectAccess zuzugreifen	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App für DirectAccess zuzugreifen
0x1800D0	Der Sitzungsstart des Citrix Secure Access Agent ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen	Der Sitzungsstart des Citrix Secure Access Agent ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Der Sitzungsstart des Citrix Secure Access Agents ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen, der Start der Citrix Secure Access Agent-App ist bei der Richtlinienbewertung fehlgeschlagen, der Start der Citrix Secure Access Agent-App ist fehlgeschlagen	Fehlformatierte Kundenanfragen
0X1800DE	Der Start der Citrix Secure Access Agent-App ist während der Richtlinienbewertung fehlgeschlagen	Der Start der Citrix Secure Access Agent-App ist während der Richtlinienbewertung fehlgeschlagen

Informationscode	Beschreibung	Auflösung
0 x 180055, 0 x 1800DF, 0 x 1800E3	Apps, die durch kontextuelle Richtlinien eingeschränkt sind, Zugriff aufgrund der Richtlinienkonfiguration verweigert	Eine oder mehrere Apps, die nicht im Benutzer-Dashboard aufgeführt sind
0 x 1800EB	Der Start der Citrix Secure Access Agent-App ist fehlgeschlagen, da IPv6 nicht unterstützt wird	Der Start der Citrix Secure Access Agent-App ist fehlgeschlagen, da IPv6 nicht unterstützt wird
0x1800EC, 0x1800ED	Der Start der Citrix Secure Access Agent-App ist aufgrund einer ungültigen IP-Adresse fehlgeschlagen	Der Start der Citrix Secure Access Agent-App ist aufgrund einer ungültigen IP-Adresse fehlgeschlagen
0x10000001, 0x10000002, 0x10000003, 0x10000004	Anmeldefehler beim Citrix Secure Access Client aufgrund eines Netzwerkproblems	Problem mit der Erreichbarkeit der Netzwerkkonnektivität mit dem Citrix Secure Access-Client
0x10000006	Anmeldefehler beim Citrix Secure Access Client aufgrund eines Proxys in der Mitte	Proxyserver stört die Client-Konnektivität mit dem Dienst
0x10000007	Anmeldefehler beim Citrix Secure Access Client aufgrund einer nicht vertrauenswürdigen Zertifizierungsstelle	Es wurde ein Problem mit dem Zertifikat eines nicht vertrauenswürdigen Servers beobachtet
0x10000008	Anmeldefehler beim Citrix Secure Access Client aufgrund eines ungültigen Zertifikats	Es wurde ein Problem mit einem ungültigen Serverzertifikat beobachtet
0 x 1000000A	Anmeldefehler beim Citrix Secure Access-Client aufgrund eines Konfigurationsproblems	Die Anmeldung ist fehlgeschlagen, da die Konfiguration für den Benutzer leer ist
0 x 1000000B	Anmeldefehler beim Citrix Secure Access-Client aufgrund eines Verbindungsfehlers	Verbindung wurde vom Netzwerk oder vom Endbenutzer beendet

Informationscode	Beschreibung	Auflösung
0x10000010	Anmeldefehler beim Citrix Secure Access-Client aufgrund einer abgelaufenen Sitzung	Das Herunterladen der Konfiguration ist fehlgeschlagen, da die Sitzung abgelaufen ist
0x10000013	Anmeldefehler beim Citrix Secure Access-Client aufgrund einer riesigen Konfigurationsliste	Der Citrix Secure Access-Client konnte sich nicht anmelden
0x11000003	Anmeldefehler beim Citrix Secure Access-Client aufgrund eines Fehlers bei der Erstellung des Kontrollkanals	Die Einrichtung des Kontrollkanals ist fehlgeschlagen, da die Sitzung abgelaufen ist
0x11000004	Fehler bei der Citrix Secure Access-Clientanmeldung aufgrund eines Fehlers bei der Erstellung des Kontrollkanals	Der Aufbau des Kontrollkanals ist fehlgeschlagen
0x11000005	Fehler bei der Citrix Secure Access-Clientanmeldung aufgrund eines Fehlers bei der Erstellung des Kontrollkanals	Der Aufbau des Kontrollkanals ist fehlgeschlagen
0x11000006	Fehler bei der Citrix Secure Access-Clientanmeldung aufgrund eines Fehlers bei der Erstellung des Kontrollkanals	Die Einrichtung des Kontrollkanals ist aufgrund eines Netzwerkproblems fehlgeschlagen
0x12000001	Abmeldefehler beim Citrix Secure Access Client, da die Sitzung bereits abgelaufen ist	Abmeldung nicht möglich, da die Sitzung beendet ist
0x12000002	Abmeldefehler beim Citrix Secure Access Client wegen Sitzungstimeout	Sitzung wurde gewaltsam beendet
0x13000001	Der App-Zugriff ist fehlgeschlagen, da die Sitzung abgelaufen ist	Der Anwendungsstart ist fehlgeschlagen, da die Sitzung abgelaufen ist
0x13000002	Der Zugriff auf die App ist aufgrund unzureichender Lizenz fehlgeschlagen	Der Anwendungsstart ist aufgrund eines Lizenzproblems fehlgeschlagen

Informationscode	Beschreibung	Auflösung
0x13000003, 0x13000008, 0x001800DF	Der App-Zugriff ist fehlgeschlagen, da der Zugriff verboten ist. Der TCP/UDP-App-Start wird gemäß der Richtlinie verweigert	Der Start der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde
0x13000004, 0x13000005	Der Zugriff auf die App ist fehlgeschlagen, da der Server nicht verfügbar ist	Der Anwendungsstart ist fehlgeschlagen, da der Client den Dienst nicht erreichen kann
0x13000007	Der App-Zugriff ist fehlgeschlagen, da die Zugriffsrichtlinie deaktiviert ist oder der Benutzer nicht abonniert ist	Der Anwendungsstart ist fehlgeschlagen, da die Richtlinienauswertung und die Konfigurationsüberprüfung fehlgeschlagen sind
0x13000009	Der App-Zugriff ist fehlgeschlagen, da der Routing-Eintrag fehlt	Der Anwendungsstart ist aufgrund von Problemen in der Anwendungsdomänentabelle fehlgeschlagen
0X 1300000B	Der Client hat die Verbindung geschlossen	Der Client hat die Verbindung mit dem Secure Private Access Service geschlossen
0x1300000C	Die FQDN-Auflösung über ZTNA ist fehlgeschlagen	Der FQDN kann vom DNS-Server nicht aufgelöst werden
0X001800D3	Fehler beim Herunterladen der Anwendungskonfiguration bei der Anmeldung	Die Liste der konfigurierten Anwendungsziele konnte nicht abgerufen werden
0x001800D9, 0x001800DA	Der Start der TCP/UDP-App ist beim Analysieren der Antwort zur Richtlinienbewertung fehlgeschlagen. Der Start der TCP/UDP-App ist mit einem ungültigen Ergebnis bei der Richtlinienbewertung fehlgeschlagen	Problem mit der Anwendungskonfiguration

Informationscode	Beschreibung	Auflösung
0x001800DB	Der Start der TCP/UDP-App ist mit einer ungültigen Konfiguration des Ressourcenstandorts fehlgeschlagen	Problem mit dem Standort der Ressource
0 x 13000006, 0 x 001800DC, 0 x 001800DD	Der TCP-App-Start ist fehlgeschlagen, weil die für die App konfigurierte erweiterte Sicherheitsrichtlinie nicht unterstützt wurde. Der TCP-App-Start ist aufgrund einer nicht unterstützten Secure Browser Browserdienst-Umleitung fehlgeschlagen, die für die TCP-App konfiguriert wurde	Die erweiterte Sicherheitsrichtlinie ist an die HTTP-Anwendung gebunden
0X001800DE	Der Start der TCP/UDP-App ist fehlgeschlagen, da für das Ziel keine Anwendungskonfiguration gefunden wurde	Die Anwendung kann nicht gefunden werden
0X001800EA	Der Start der TCP-App ist fehlgeschlagen, weil der Ziel-FQDN zu lang ist	Die Länge des Hostnamens überschreitet 256 Zeichen
0X001800ED	Der Start der TCP-App ist aufgrund einer ungültigen Ziel-IP fehlgeschlagen	Ungültige IP-Adresse
0X001800EF	Der Start der TCP-App ist beim Verbindungsaufbau zum privaten TCP-Server fehlgeschlagen	Es konnte keine Ende-zu-Ende-Verbindung hergestellt werden
0X001800F5	Der Start der UDP-App ist aufgrund der IPV6-Adresse fehlgeschlagen	IPv6 wurde in der App-Anfrage empfangen

Informationscode	Beschreibung	Auflösung
0x001800F9	UDP-Verkehr konnte nicht übermittelt werden, da die Client-Verbindung unterbrochen wurde	UDP-Verkehr konnte nicht übermittelt werden
0X001800FF	Die Übertragung des UDP-Datenverkehrs ist fehlgeschlagen	Die Übertragung des UDP-Datenverkehrs ist fehlgeschlagen
0x10000401	Die Wahl des Citrix Rendezvous-Servers ist fehlgeschlagen	Der Anwendungsstart ist aufgrund von Netzwerkverbindungsproblemen fehlgeschlagen
0x10000402, 0x1000040C	Das Connector Appliance kann nicht registriert werden, Fehler bei der Initialisierung der UDP-Netzwerkverbindung	Connector-Appliance konnte sich nicht beim Secure Private Access Service registrieren
0x10000403, 0x10000404, 0x10000407, 0x1000040A 0x1000040B, 0x1000040F, 0x10000410	Verbindungsfehler, Fehler bei der Übertragung des Steuerungspakets, Fehler beim Lesen des Gateway-Dienstes,	Verbindungsproblem mit Connector Appliance
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412	Fehler beim Analysieren des Steuerungspakets, Fehler beim Schreiben des Gateway-Dienstes,	Verbindungsprobleme mit Connector Appliance und privaten TCP/UDP-Servern im Back-End
0x10000406	DNS-Auflösung ist fehlgeschlagen	Connector-Appliance kann DNS für FQDNs nicht auflösen
0x10000411	Der Gateway-Dienst hat die Verbindung geschlossen	Private Serververbindung wurde beendet
0x10000413	Fehler bei der Bestimmung des Grundes für den Verbindungsabbruch	Es konnten keine Verbindung zur privaten Dienst-IP oder zum FQDN hergestellt oder Daten gesendet werden
0x100508	Der Benutzerkontext entspricht nicht den Bedingungen der Zugriffsregel	Keine übereinstimmende politische Bedingung
0x100509	Zugriffsrichtlinie, die nicht mit der Anwendung verknüpft ist	Der Anwendung ist keine Zugriffsrichtlinie zugeordnet

Informationscode	Beschreibung	Auflösung
0x10050C	Ergebnisse der politischen Bewertung mehrerer Anwendungen, auf die der Benutzer möglicherweise Anspruch hat	Informationen zur App-Aufzählung
0x00180101	Der Start der TCP/UDP-App ist fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt	Der Start der TCP/UDP-App ist fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt
0x00180102	Der Start der TCP/UDP-App ist fehlgeschlagen, da die Konnektoren nicht fehlerfrei sind	Der Start der TCP/UDP-App ist fehlgeschlagen, da die Konnektoren nicht fehlerfrei sind
0x00180103	UDP/DNS-Anfrage ist fehlgeschlagen, da Connector nicht erreichbar ist	UDP/DNS-Anfrage ist fehlgeschlagen, da Connector nicht erreichbar ist
0x20580001	Die Seite konnte nicht geladen werden, da das NGS-Cookie abgelaufen ist	Die Seite konnte nicht geladen werden, da das NGS-Cookie abgelaufen ist
0x20580002	Das Abrufen der Zugriffsrichtlinie ist aufgrund eines Netzwerkfehlers fehlgeschlagen	Das Abrufen der Zugriffsrichtlinie ist aufgrund eines Netzwerkfehlers fehlgeschlagen
0x20580003	Fehler beim Abrufen der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens	Fehler beim Abrufen der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens
0x20580004	Netzwerkfehler beim Abrufen der Zugriffsrichtliniendetails	Netzwerkfehler beim Abrufen der Zugriffsrichtliniendetails
0x20580005	Fehler beim Abrufen der Richtlinie beim Abrufen des öffentlichen Zertifikats	Fehler beim Abrufen der Richtlinie beim Abrufen des öffentlichen Zertifikats
0x20580007	Fehler beim Abrufen der Richtlinie beim Überprüfen der Signatur von JWT	Fehler beim Abrufen der Richtlinie beim Überprüfen der Signatur von JWT

Informationscode	Beschreibung	Auflösung
0x20580008	Fehler beim Abrufen der Richtlinie beim Überprüfen des öffentlichen Zertifikats	Fehler beim Abrufen der Richtlinie beim Überprüfen des öffentlichen Zertifikats
0x2058000A	Die Speicherumgebung zur Bildung einer Richtlinien-URL konnte nicht bestimmt werden	Die Speicherumgebung zur Bildung einer Richtlinien-URL konnte nicht bestimmt werden
0x2058000B	Antwort auf die Abrufanforderung der Zugriffsrichtlinie konnte nicht abgerufen werden	Antwort auf die Abrufanforderung der Zugriffsrichtlinie konnte nicht abgerufen werden
0x2058000C	Der Abruf der Zugriffsrichtlinie ist aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens fehlgeschlagen	Der Abruf der Zugriffsrichtlinie ist aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens fehlgeschlagen
0x10200002	Connector-Appliance ist nicht registriert	Connector-Appliance ist nicht registriert
0x10200003	Es kann keine Verbindung zur Connector-Appliance hergestellt werden	Es kann keine Verbindung zur Connector-Appliance hergestellt werden
0x10000301	Die Verbindung zum Citrix SPA-Dienst ist fehlgeschlagen	Die Verbindung zum Citrix Secure Private Access Service ist fehlgeschlagen
0x10000303, 0x10000304	Der Proxyserver ist nicht erreichbar	Proxyserver ist nicht erreichbar
0x10000305	Die Proxy-Server-Authentifizierung ist fehlgeschlagen	Die Proxy-Server-Authentifizierung ist fehlgeschlagen
0x10000306	Konfigurierte Proxyserver sind nicht erreichbar	Konfigurierte Proxyserver sind nicht erreichbar
0x10000307	Fehlerantwort vom Backend-Server erhalten	Fehlerantwort vom Backend-Server erhalten
0x10000005	Anfrage kann nicht an die Ziel-URL gesendet werden	Anfrage kann nicht an die Ziel-URL gesendet werden

Informationscode	Beschreibung	Auflösung
0x10000107	SSO konnte nicht verarbeitet werden	SSO konnte nicht verarbeitet werden
0x10000108, 0x1000010B	SSO konnte nicht verarbeitet werden, SSO-Einstellungen konnten nicht ermittelt werden	SSO konnte nicht verarbeitet werden, SSO-Einstellungen konnten nicht ermittelt werden
0x10000101, 0x10000102, 0x10000103, 0x10000104	FormFill SSO ist fehlgeschlagen, falsche Konfiguration der Formular-App	FormFill SSO ist fehlgeschlagen, falsche Konfiguration der Formular-App
0x1000010A	FormFill SSO ist fehlgeschlagen, falsche Konfiguration der Formular-App	FormFill SSO ist fehlgeschlagen, falsche Konfiguration der Formular-App
0x10000202	Kerberos SSO ist fehlgeschlagen	Kerberos SSO ist fehlgeschlagen
0x10000203	SSO für den Authentifizierungstyp konnte nicht verarbeitet werden	SSO für den Authentifizierungstyp konnte nicht verarbeitet werden
0x10000204	Kerberos SSO ist fehlgeschlagen, fällt aber auf NTLM zurück	Kerberos SSO ist fehlgeschlagen, fällt aber auf NTLM zurück
0x14000001	In der Citrix Workspace Workspace-Anwendung sind mehrere ZTNA-berechtigte Konten konfiguriert	In der Citrix Workspace Workspace-Anwendung sind mehrere ZTNA-berechtigte Konten konfiguriert

Schritte zur Lösung

Die folgenden Abschnitte enthalten Lösungsschritte für die meisten Infocodes. Für die Codes, für die die Lösungsschritte nicht erfasst wurden, wenden Sie sich an den Citrix Support.

Eine oder mehrere Apps, die nicht im Benutzer-Dashboard aufgeführt sind

Infocode: 0x180055, 0x1800DF, 0x1800E3

Aufgrund der kontextbezogenen Richtlinieneinstellungen werden Apps für einige Benutzer oder Geräte möglicherweise nicht angezeigt. Parameter wie Vertrauensfaktoren (Gerätestatus oder

Risikobewertung) können die Zugänglichkeit der Anwendungen beeinflussen.

1. Kopieren Sie die Transaktions-ID aus der Spalte `reasons` für den Fehlercode `0x18005C` in der CSV-Datei Diagnostic Logs.
2. Ändern Sie den Filter für die Spalte `prod` in der CSV-Datei, um Ereignisse aus der Komponente `SWA.PSE` oder `SWA.PSE.EVENTS` anzuzeigen. Dieser Filter zeigt nur Protokolle, die sich auf die Richtlinienauswertung beziehen
3. Suchen Sie in der Spalte `reason` nach der ausgewerteten Policy-Nutzlast. Diese Payload zeigt die ausgewertete Richtlinie für den Benutzerkontext für alle Apps, die der Benutzer abonniert hat.
4. Wenn die Richtlinienbewertung ergibt, dass die App für den Benutzer verweigert wurde, kann dies folgende Gründe haben:

    - Falsche Übereinstimmungsbedingungen in der Richtlinie —Überprüfen Sie die Konfiguration der App-Richtlinie in Citrix Cloud
    - Falsche Übereinstimmungsregeln in der Richtlinie —Überprüfen Sie die Konfiguration der App-Richtlinie in Citrix Cloud
    - Falsche übereinstimmende Standardregel in der Richtlinie - dies ist ein Fall-Through-Fall. Passen Sie die Bedingungen entsprechend an.

Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App zuzugreifen

Infocode: 0x1800BC, 0x1800BF

Der Benutzer hat möglicherweise auf den App-Link geklickt, für den der Benutzer möglicherweise kein Abonnement hat.

Stellen Sie sicher, dass der Benutzer ein Abonnement für die Anwendungen hat.

1. Gehen Sie zur Anwendung im Management-Portal.
2. Bearbeiten Sie die App und gehen Sie zur Registerkarte **Abonnement**.
3. Stellen Sie sicher, dass der Zielbenutzer einen Eintrag in der Abonnementliste hat.

Langsame Leistung von Back-End-App

Infocode:0x18000F

Es gibt Fälle, in denen das Kundennetzwerk aufgrund der Connectors an einem Ressourcenstandort, die ausgefallen sein können, unzuverlässig ist oder der Backend-Server selbst möglicherweise nicht reagiert.

1. Stellen Sie sicher, dass sich die Connector-Appliance geografisch in der Nähe des Back-End-Servers befindet, um Netzwerklatenzen auszuschließen.

2. Überprüfen Sie, ob die Firewall des Backend-Servers die Connector-Appliance nicht blockiert.
3. Überprüfen Sie, ob der Client eine Verbindung zum nächstgelegenen Cloud-POP herstellt.

   Zum Beispiel, `nslookup nssvc.dnsdiag.net` auf dem Client, der kanonische Name in der Antwort zeigt den geospezifischen Server an, beispielsweise `aws-us-w.g.nssvc.net`.

Der App-Start ist fehlgeschlagen, weil die Länge des App-FQDN überschritten wurde

Infocode: 0x180006, 0x1800B7

App-FQDNs dürfen eine Länge von 512 Zeichen nicht überschreiten. Überprüfen Sie den FQDN der Anwendung auf der App-Konfigurationsseite. Stellen Sie sicher, dass die Länge 512 Byte nicht überschreitet.

1. Gehen Sie in der Verwaltungskonsole zur Registerkarte **Anwendungen**.
2. Suchen Sie nach der Anwendung, deren FQDN 512 Zeichen überschreitet.
3. Bearbeiten Sie die Anwendung und korrigieren Sie die FQDN-Länge der App.

App-Detaillänge überschritten

Infocode: 0x18000E

Überprüfen Sie die Richtlinien, ob sie den App-Zugriff blockieren.

1. Gehen Sie zu **Zugriffsrichtlinien**.
2. Suchen Sie nach den Richtlinien, für die die App eine Berechtigung hat.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

App-Zugriff wurde verweigert

Infocode: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

Dies bezieht sich auf kontextuelle Richtlinien, bei denen Richtlinien die App für einen bestimmten Benutzer verweigern.

Überprüfen Sie die Richtlinien, ob sie den App-Zugriff blockieren

1. Gehen Sie zu **Zugriffsrichtlinien**.
2. Suchen Sie nach den Richtlinien, für die die App eine Berechtigung hat.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

Anwendungen sind nicht aufgeführt

Anwendungen können aufgrund von Richtlinienverweigerungen oder wenn die Secure Private Access-Integration nicht aktiviert ist, in der aufgezählten Liste fehlen.

- Wenn der Zugriff für einige Apps aktiviert werden muss, Sie aber keine Apps sehen, versuchen Sie, die Secure Private Access-Integration zu aktivieren.
  - Melden Sie sich bei Citrix Cloud an.
  - Wählen Sie im Hamburger-Menü die Option **Workspace-Konfiguration** aus und klicken Sie dann auf **Service Integrations.**
  - Klicken Sie in Secure Private Access auf die Ellipsenschaltfläche und dann auf **Aktivieren**.
- Wenn die Secure Private Access-Integration bereits aktiviert ist, deaktivieren Sie sie und aktivieren Sie sie dann erneut, um zu sehen, ob Sie über Apps verfügen.

Problem beim Herstellen einer Verbindung zum Connector Appliance

Infocode: 0x1800EF

App-Routing schlägt fehl, weil TCP-Verbindungen mit on-premises Connectors nicht verfügbar sind.

Ereignisse aus der Controller-Komponente überprüfen

1. Suchen Sie in der CSV-Datei mit den Diagnoseprotokollen die `transaction ID` für Fehlercode `0x1800EF`.
2. Filtert alle Ereignisse, die der Transaktions-ID in der CSV-Datei entsprechen.
3. Filtern Sie auch die Spalte `prod` in der CSV-Datei die mit `SWA.GOCTRL` übereinstimmt.

   Wenn Sie Ereignisse mit der Meldung `connectType multiconnect::success`? sehen:

   - Dies zeigt an, dass die Anforderung zur Tunneleinrichtung erfolgreich an den Controller weitergeleitet wurde.
   - Überprüfen Sie, ob `Resource Location` in der Protokollmeldung korrekt ist. Wenn es falsch ist, korrigieren Sie den Ressourcenstandort im Abschnitt zur App-Konfiguration im Citrix Verwaltungsportal.
   - Überprüfen Sie, ob `VDA Ip and Port` in der Protokollmeldung korrekt ist. Die VDA-IP und der Port geben die IP-Adresse und den Port der Back-End-Anwendung an. Wenn es falsch ist, korrigieren Sie den FQDN oder die IP-Adresse der App im Abschnitt zur App-Konfiguration im Citrix Verwaltungsportal.
   - Fahren Sie mit der Überprüfung der Connector-Ereignisse fort, wenn Sie keine zuvor genannten Probleme finden.

Wenn Sie Ereignisse mit der Meldung `connectType`, `connect::failure` oder `multiconnect::success` sehen;

- Überprüfen Sie, ob der empfohlene Fix für diese Protokollmeldung lautet - `Check if connector is still connected to same pop`. Dies weist darauf hin, dass der Konnektor am Ressourcenstandort möglicherweise ausgefallen ist. Fahren Sie mit der Überprüfung der Connector-Ereignissefort
- Wenden Sie sich an den Citrix Kundensupport, wenn die zuvor genannten Meldungen nicht angezeigt werden.

Wenn Ereignisse mit der Meldung `connectType IntraAll::failure` angezeigt werden, wenden Sie sich an den Citrix Customer Support.

Ereignisse aus der Konnektorkomponente überprüfen

1. Suchen Sie in der CSV-Datei mit den Diagnoseprotokollen die `transaction ID` für Fehlercode `0x1800EF`.
2. Filtert alle Ereignisse, die der Transaktions-ID in der CSV-Datei entsprechen.
3. Filtern Sie die Spalte `prod` in der CSV-Datei die mit `SWA.ConnectorAppliance.WebApps` übereinstimmt.
4. Wenn Sie Ereignisse mit `status failure` sehen:
   - Überprüfen Sie die `reason`-Meldung für jedes dieser Fehlerereignisse.
   - `UnableToRegister` gibt an, dass sich der Connector nicht erfolgreich bei Citrix Cloud registrieren konnte. Wenden Sie sich an Citrix Support
   - `IsProxyRequiredCheckError` oder `ProxyDialFailed` oder `ProxyConnectionFailed` oder `ProxyAuthenticationFailure` oder `ProxiesUnReachable` gibt an, dass der Connector die Back-End-URL nicht über die Proxykonfiguration auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Richtigkeit.
   - Weitere Informationen zum Debuggen finden Sie unter Connector-SSO-Ereignisse.

Single Sign-On-Fehler

Bei Single Sign-On werden verschiedene SSO-Attribute aus der App-Konfiguration extrahiert und beim Start der App angewendet. Wenn dieser bestimmte Benutzer nicht über die Attribute verfügt oder wenn die Attribute falsch sind, schlägt das Single Sign-On möglicherweise fehl. Stellen Sie sicher, dass die Konfiguration korrekt aussieht.

1. Gehen Sie zu **Zugriffsrichtlinien.**
2. Suchen Sie nach den Richtlinien, für die die App eine Berechtigung hat.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

SSO-Methoden wie Form SSO, Kerberos und NTLM werden vom on-premises Connector ausgeführt. Überprüfen Sie die folgenden Diagnoseprotokolle vom Connector.

SSO-Ereignisse von der Konnektorkomponente abfragen

1. Filtern Sie `component name`, der `SWA.ConnectorAppliance.WebApps` in der CSV-Datei übereinstimmt.
2. Sehen Sie Ereignisse mit Status "Fehler"?
    - Überprüfen Sie die Meldung für jedes dieser Fehlerereignisse.
    - `IsProxyRequiredCheckError` oder `ProxyDialFailed` oder `ProxyConnectionFailed` oder `ProxyAuthenticationFailure` oder `ProxiesUnReachable` gibt an, dass der Connector die Back-End-URL nicht über die Proxykonfiguration auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Richtigkeit.
    - `FailedToReadRequest` oder `RequestReceivedForNonSecureBrowse` oder `UnableToRetrieveUserCredentials` oder `CCSPolicyIsNotLoaded` oder `FailedToLoadBaseClient` oder `ProcessConnectionFailure` oder `WebAppUnSupportedAuthType` weist auf einen Tunnelausfall hin. Wenden Sie sich an Citrix Support
    - `UnableToConnectTargetServer` gibt an, dass der Backend-Server vom Connector aus nicht erreichbar ist. Überprüfen Sie die Backend-Konfiguration erneut.
    - `IncorrectFormAppConfiguration` oder `NoLoginFormFound` oder `FailedToConstructF` oder `FailedToLoginViaFormBasedAuth` weist auf einen formularbasierten Authentifizierungsfehler hin. Überprüfen Sie den Abschnitt SSO-Konfiguration des Formulars unter App-Konfiguration im Citrix Verwaltungsportal.
    - `NTLMAuthNotFound` weist auf einen NTLM-basierten Authentifizierungsfehler hin. Überprüfen Sie den Abschnitt NTLM-SSO-Konfiguration in der App-Konfiguration im Citrix Management-Portal.
    - Weitere Informationen zum Debuggen finden Sie unter Connector-Ereignisse.

Der Start der App ist fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist

Infocode: 0x180022

Secure Private Access ermöglicht es Administratoren, einen Authentifizierungsdienst eines Drittanbieters wie das herkömmliche Active Directory, AAD, Okta oder SAML zu konfigurieren. Ausfälle bei diesen Authentifizierungsdiensten können dieses Problem verursachen.

Überprüfen Sie, ob die Server von Drittanbietern betriebsbereit und erreichbar sind.

SAML-SSO-Fehler

Infocode: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Benutzer haben beim Start der App einen Authentifizierungsfehler, wenn sie IdP-initiiert wird, oder es werden möglicherweise unzugängliche Links angezeigt, wenn sie SP-initiiert wird. Überprüfen Sie auch die SAML-App-Konfiguration auf der Secure Private Access Service-Seite und die Konfiguration des Dienstanbieters.

Secure Private Access-Konfiguration:

1. Gehen Sie zur Registerkarte **Anwendungen**.
2. Suchen Sie nach der problematischen SAML-App.
3. Bearbeiten Sie die Anwendung und wechseln Sie zur Registerkarte **Single Sign On**.
4. Überprüfen Sie die folgenden Felder.
    - Assertion-URL
    - Relay-Status
    - Zielgruppe
    - Namen-ID-Format, Namen-ID und andere Attribute

Konfiguration des Dienstanbieters:

1. Melden Sie sich beim Dienstanbieter an.
2. Gehen Sie zu den **SAML-Einstellungen**.
3. Überprüfen Sie das IdP-Zertifikat, die Zielgruppe und die IdP-Anmelde-URL.

Wenn die Konfiguration korrekt aussieht, wenden Sie sich an den Citrix Support.

Ungültige App-FQDN

Infocode: 0x180048

Der Kundenadministrator hat möglicherweise einen ungültigen FQDN oder einen FQDN angegeben, bei dem die DNS-Auflösung auf dem Backend-Server fehlschlägt.

In diesem Fall sieht der Endbenutzer einen Fehler auf der Webseite. Überprüfen Sie die Anwendungseinstellungen.

SaaS-App-Validierung Prüfen Sie, ob über das Netzwerk auf die App zugegriffen werden kann.

Web-App-Validierung

1. Gehen Sie zur Registerkarte **Anwendungen**.
2. Bearbeiten Sie die problematische Anwendung.
3. Gehen Sie zur Seite **App-Details**.
4. Prüfen Sie die URL. Die URL muss entweder im Intranet oder im Internet zugänglich sein.

Secure Browser Service —DNS-Suche/Verbindung fehlgeschlagen

Infocode: 0x18009D

Fehlerhaftes Surferlebnis über den Remote Browser Isolation-Dienst. Überprüfen Sie den Backend-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte.

1. Gehen Sie zum Backend-Server und überprüfen Sie, ob er läuft und die Anfragen empfangen kann.
2. Suchen Sie nach den Proxy-Einstellungen, wenn die Verbindung zum Backend-Server unterbrochen wird.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser Service bekannt.

CWA Web —DNS-Suche/Verbindungsfehler für Web-Apps

Infocode: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Fehlerhaftes Surferlebnis von Webanwendungen, die in einem Unternehmensnetzwerk ausgeführt werden.

1. Filtern Sie die Diagnoseprotokolle nach FQDNs, die nicht auflösbar sind.
2. Prüfen Sie, ob der Backend-Server innerhalb des Unternehmensnetzwerks erreichbar ist.
3. Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector daran gehindert ist, den Backend-Server zu erreichen.

Direktzugriff —falsch konfiguriert als Web-App

Da der Web-App-Datenverkehr immer über den Connector geleitet wird, führt die Konfiguration des direkten Zugriffs auf sie zu einem App-Zugriffsfehler.

Überprüfen Sie auf die widersprüchliche Konfiguration zwischen der Routingdomänentabelle und der App-Konfiguration.

1. Gehen Sie zur Anwendung im Management-Portal.

2. Bearbeiten Sie die App und prüfen Sie, ob der Direktzugriff aktiviert ist.
3. Überprüfen Sie den App-FQDN in der Routingdomänentabelle, ob er als intern markiert wurde.

Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App für DirectAccess zuzugreifen

Infocode: 0x1800BD

Die App-Konfiguration deaktiviert den direkten Zugriff für Datenverkehr, der von browserbasierten Clients stammt.

Stellen Sie sicher, dass der Benutzer ein Abonnement für die Anwendungen hat.

1. Gehen Sie zur Anwendung im Management-Portal.
2. Bearbeiten Sie die App und überprüfen Sie die Konfiguration für den agentenlosen Zugriff.

Verbesserte Sicherheitsrichtlinien —Fehlkonfiguration des Secure Browser Service

Infocode: 0x1800C3

Falsches Verhalten als in den Richtlinienregeln beabsichtigt. Überprüfen Sie die kontextbezogenen Zugriffsrichtlinien.

1. Gehen Sie zur Registerkarte **Richtlinien**.
2. Überprüfen Sie die mit der Anwendung verknüpften Richtlinien.
3. Überprüfen Sie die Regeln für diese Richtlinien.

Verbesserte Sicherheitsrichtlinien —Fehlkonfiguration der Richtlinien

Falsches Verhalten als in den Richtlinienregeln beabsichtigt. Überprüfen Sie die erweiterten Sicherheitseinstellungen.

1. Gehen Sie zur Anwendung.
2. Klicken Sie auf die Registerkarte **Zugriffsrichtlinien**.
3. Überprüfen Sie die Einstellungen im Abschnitt **Verfügbare Sicherheitseinschränkungen**.

Der Sitzungsstart des Citrix Secure Access Agent ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen

Infocode: 0x1800D0

Die Citrix Secure Access-App kann nicht erfolgreich einen vollständigen Tunnel zur Citrix Cloud einrichten.

1. Überprüfen Sie die Konfiguration der Routingdomäne für die TCP/UDP-Apps.
2. Stellen Sie sicher, dass die maximale Anzahl von Einträgen deutlich innerhalb der 16.000 Einträge liegt.

TCP/UDP-Apps —Fehlformatierte Clientanfragen

Infocode: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

Entweder ist der VPN-Tunnel nicht eingerichtet oder bestimmte FQDNs wurden möglicherweise nicht getunnelt.

1. Stellen Sie sicher, dass die Anfragen nicht von zwischengeschriebenen Proxys manipuliert oder rekonstruiert werden.
2. Mutmaßliche Man-in-Middle-Angriffe.

TCP/UDP-Apps - Fehlkonfiguration der Umleitung des sicheren Browserdienstes

Infocode: 0x1800DD

Umleitungen des Remote-Browserisolationsdienstes können nur für Web-Apps und nicht für TCP/UDP-Apps angewendet werden. Überprüfen Sie die App-Konfiguration in der Secure Private Access Service-GUI.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser Service bekannt.

Der Start der Citrix Secure Access Agent-App ist während der Richtlinienbewertung fehlgeschlagen

Infocode: 0x1800DE

Stellen Sie sicher, dass alle internen FQDNs, die vom Citrix Secure Access-Client getunnelt werden sollen, einen entsprechenden Eintrag in der Routingdomänentabelle haben.

Der Start der Citrix Secure Access Agent-App ist fehlgeschlagen, da IPv6 nicht unterstützt wird

Infocode: 0x1800EB

Überprüfen Sie die Einträge der Routingdomäne Stellen Sie sicher, dass die Tabelle keine IPV6-Einträge enthält.

Der Start der Citrix Secure Access Agent-App ist aufgrund einer ungültigen IP-Adresse fehlgeschlagen

Infocode:0x1800EC, 0x1800ED

Überprüfen Sie die Einträge der Routingdomäne Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Backend verweisen.

Problem mit der Erreichbarkeit der Netzwerkkonnektivität mit dem Citrix Secure Access-Client

Informationscode: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Prüfen Sie, ob das Netzwerk des Client-Computers erreichbar ist. Wenn das Netzwerk erreichbar ist, wenden Sie sich mit den Client-Debug-Protokollen an den Citrix Support.
2. Prüfen Sie, ob der Proxy oder die Firewall das Netzwerk blockiert.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Proxyserver stört die Client-Konnektivität mit dem Dienst

Infocode: 0x10000006

1. Prüfen Sie, ob das Netzwerk des Client-Computers erreichbar ist.
2. Prüfen Sie, ob der Proxy im Client korrekt konfiguriert ist.
3. Wenn bei beiden keine Probleme auftreten, wenden Sie sich mit den Client-Debug-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Es wurde ein Problem mit dem Zertifikat eines nicht vertrauenswürdigen Servers beobachtet

Infocode: 0x10000007

Wenden Sie sich an den Citrix Support, um zu überprüfen, ob das Serverzertifikat von einer gültigen CA korrekt generiert wurde.

Es wurde ein Problem mit einem ungültigen Serverzertifikat beobachtet

Infocode: 0x10000008

Wenden Sie sich an den Citrix Support, um zu überprüfen, ob das Serverzertifikat selbstsigniert ist, abgelaufen ist oder von einer nicht vertrauenswürdigen Quelle stammt.

Die Anmeldung ist fehlgeschlagen, da die Konfiguration für den Benutzer leer ist

Infocode: 0x1000000A

1. Stellen Sie sicher, dass mindestens eine TCP/UDP/HTTP-App konfiguriert ist. Einzelheiten finden Sie unter Anwendungen hinzufügen und verwalten.
2. Stellen Sie sicher, dass die Anwendungsdomänentabelle (**Secure Private Access > Einstellungen > Anwendungsdomäne**) nicht leer ist oder dass nicht alle Einträge deaktiviert sind. Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden automatisch zu dieser Tabelle hinzugefügt.

Es wird empfohlen, die Ziele oder die URL einer aktiven TCP/UDP/HTTP-Anwendung nicht zu löschen oder zu deaktivieren.

Verbindung wurde vom Netzwerk und/oder vom Endbenutzer beendet

Informationscode: 0x1000000B

Prüfen Sie, ob das Netzwerk unterbrochen ist oder ob der Endbenutzer die Verbindung während der ZTNA-Sitzungsverbindung unterbrochen hat.

Das Herunterladen der Konfiguration ist fehlgeschlagen, da die Sitzung abgelaufen ist

Informationscode: 0x10000010

Die VPN-Sitzung ist möglicherweise während der Download-Anfrage für die ZTNA-Sitzungskonfiguration abgelaufen. Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Der Citrix Secure Access-Client konnte sich nicht anmelden

Informationscode: 0x10000013

Der Citrix Secure Access-Client konnte sich nicht anmelden, da die Konfigurationsgröße das maximale Konfigurationslimit überschreitet.

1. Überprüfen Sie die Routingdomänenkonfiguration für die TCP/UDP-Apps unter **Secure Private Access > Einstellungen > Anwendungsdomäne**
2. Stellen Sie sicher, dass die Anzahl der Einträge nicht groß ist. Wenn die Liste der Einträge sehr umfangreich ist, deaktivieren oder entfernen Sie ungenutzte Ziele.

   Wenn die Zielliste voraussichtlich mehr als 1000 Sekunden lang sein wird, versuchen Sie, die maximale Downloadgröße für die Konfiguration zu erhöhen, indem Sie den ConfigSize-Registrierungsschlüssel aktualisieren. Einzelheiten finden Sie unter Registrierungsschlüssel für den Citrix Gateway VPN-Client.

Die Einrichtung des Kontrollkanals ist fehlgeschlagen, da die Sitzung abgelaufen ist

Informationscode: 0x11000003

Der Steuerkanal für die Einrichtung der DNS-Anfrage ist fehlgeschlagen, da die Sitzung abgelaufen ist.

Die ZTNA-Sitzung ist möglicherweise während der Einrichtung des Steuerkanals abgelaufen.

Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Der Aufbau des Kontrollkanals ist fehlgeschlagen

Informationscode: 0x11000004

Der Kontrollkanal für die Einrichtung von DNS-Anfragen ist fehlgeschlagen.

- **Sorgen Sie dafür, dass der Ressourcenstandort intakt bleibt:**

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie im Hamburger-Menü auf **Ressourcenstandort** .
3. Führen Sie eine Zustandsprüfung für die Connector-Appliances am jeweiligen Ressourcenstandort durch.
4. Wenn das Problem dadurch nicht behoben wird, versuchen Sie, die virtuelle Connector-Maschine neu zu starten.

- **Pflegen Sie die HA-Connector-Appliance:**

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie im Hamburger-Menü auf **Ressourcenstandort** .
3. Stellen Sie sicher, dass der erwartete Ressourcenstandort über mindestens zwei Connector-Appliances verfügt.

Stellen Sie dabei Folgendes sicher:

- Das LAN des Ressourcenstandorts ist funktionsfähig.
- In der Mitte befindet sich keine Firewall oder kein Proxy, der die Verbindung zwischen dem Connector Appliance und dem Dienst oder den Backend-Servern blockiert.
- Das Client-Netzwerk ist intakt.
- Die privaten Backend-Server sind in Betrieb.
- Die DNS-Server sind in Betrieb.
- FQDNs sind auflösbar.

Wenn Sie die obigen Empfehlungen erfüllen, gehen Sie wie folgt vor.

1. Ruft die Transaktions-ID für diesen Fehler aus dem Diagnoseprotokoll ab.

2. Filtern Sie alle Ereignisse, die der Transaktions-ID im Secure Private Access-Dashboard entsprechen.
3. Prüfen Sie, ob in den Diagnoseprotokollen des Clients, der Connector Appliance oder des Dienstes ein Fehler aufgetreten ist, der mit der Transaktions-ID übereinstimmt. Ergreifen Sie dann die entsprechenden Maßnahmen.
4. Überprüfen Sie, ob der Ressourcenstandort für das Ziel in der Anwendungsdomänentabelle richtig ausgewählt wurde (**Secure Private Access > Einstellungen > Anwendungsdomäne**).
5. Überprüfen Sie, ob die Anwendung mit dem richtigen Port, den richtigen IP-Bereichen und Domänen konfiguriert ist. Einzelheiten finden Sie unter Anwendungen hinzufügen und verwalten.

Wenn Sie das Problem immer noch nicht lösen können, wenden Sie sich an den Citrix Support und geben Sie den Fehlercode für die Transaktions-ID und die Client-Logs an.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Der Aufbau des Kontrollkanals ist fehlgeschlagen

Informationscode: 0x11000005

Die Einrichtung des Kontrollkanals (für DNS-Anfragen) ist fehlgeschlagen.

1. Überprüfen Sie die Lizenzberechtigung für den Secure Private Access-Dienst.
2. Wenn Sie nicht berechtigt sind, wenden Sie sich an den Citrix Support, um die Lizenz zu überprüfen.

Einzelheiten finden Sie unter https://www.citrix.com/buy/licensing/product.html.

Die Einrichtung des Kontrollkanals ist aufgrund eines Netzwerkproblems fehlgeschlagen

Informationscode: 0x11000006

Die Einrichtung des Kontrollkanals (für DNS-Anfragen) ist aufgrund eines Netzwerkproblems fehlgeschlagen.

1. Prüfen Sie, ob der Secure Private Access Service erreichbar ist.
2. Wenn nicht erreichbar, wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Die Einrichtung des Kontrollkanals schlug aufgrund unzureichender IIPs fehl

Informationscode: 0x11000007

Die Einrichtung des Kontrollkanals (für DNS-Anfragen) ist aufgrund unzureichender IIPs fehlgeschlagen.

Wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Abmeldung nicht möglich, da die Sitzung beendet ist

Dieses Problem ist möglicherweise aufgetreten, weil der Client-Computer (Tastatur oder Maus) länger als den konfigurierten Timeout-Zeitraum inaktiv war.

Informationscode: 0x12000001

Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Sitzung wurde gewaltsam beendet

Die Sitzung wird zwangsweise beendet, wenn das konfigurierte Force-Timeout erreicht ist.

Informationscode: 0x12000002

Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Der Anwendungsstart ist fehlgeschlagen, da die Sitzung abgelaufen ist

Informationscode: 0x13000001

1. Die ZTNA-Sitzung ist während des App-Starts abgelaufen.
2. Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Der Anwendungsstart ist aufgrund eines Lizenzproblems fehlgeschlagen

Informationscode: 0x13000002

1. Prüfen Sie, ob die Secure Private Access-Dienstlizenz berechtigt ist.
2. Wenn Sie nicht berechtigt sind, wenden Sie sich an den Citrix Support, um die Lizenz zu überprüfen.

Einzelheiten finden Sie unter https://www.citrix.com/buy/licensing/product.html.

Der Start der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde

Informationscode: 0x13000003, 0x13000008, 0x001800DF

Der Anwendungsstart wird gemäß der Richtlinienkonfiguration für den Benutzer und die Anwendung verweigert.

Stellen Sie Folgendes sicher.

- Dieselben Ziele werden nicht in mehreren Anwendungen verwendet (HTTP, HTTPS, TCP, UDP)
- In mehreren Anwendungen gibt es keine überlappenden Ziele.
- Zugriffsrichtlinien sind an die Anwendungen gebunden.

Überprüfen Sie auch die Bedingungen und Aktionen der Richtlinien, die für die abgelehnte Anwendung konfiguriert wurden. Überprüfen Sie dann die politischen Bedingungen und Maßnahmen.

Einzelheiten finden Sie unter Zugriffsrichtlinien.

Der Anwendungsstart ist fehlgeschlagen, da der Client den Dienst nicht erreichen kann

Informationscode: 0x13000004, 0x13000005

1. Prüfen Sie, ob der Secure Private Access Service erreichbar ist.
2. Starten Sie die App erneut.
3. Wenn die App längere Zeit nicht erreichbar ist, wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Der Anwendungsstart ist fehlgeschlagen, da die Richtlinienauswertung und die Konfigurationsüberprüfung fehlgeschlagen sind

Informationscode: 0x13000007

Der Anwendungsstart ist fehlgeschlagen, da die Überprüfung der Richtlinien und Konfiguration durch den Secure Private Access Service fehlgeschlagen ist.

DieAnwendung für das aufgerufene Ziel konnte nichterkannt werden.

DerStart der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde.

Der Anwendungsstart ist aufgrund von Problemen in der Anwendungsdomänentabelle fehlgeschlagen

Informationscode: 0x13000009

Der Anwendungsstart ist fehlgeschlagen, da die Anwendungsdomänentabelle keinen Eintrag für das Ziel enthält, auf das zugegriffen wurde.

Überprüfen Sie, ob der Routeneintrag für die Anwendung unter **Secure Private Access > Einstellungen > Anwendungsdomäne**korrekt konfiguriert ist.

Der Client hat die Verbindung mit dem Secure Private Access Service geschlossen

Informationscode: 0x1300000B

1. Prüfen Sie, ob der Endbenutzer die Verbindung manuell geschlossen hat.
2. Wenn nicht, wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

Der FQDN kann vom DNS-Server nicht aufgelöst werden

Informationscode: 0x1300000C

Dieses Problem tritt auf, wenn das Connector Appliance DNS für FQDNs nicht auflösen kann.

1. Überprüfen Sie den DNS-Eintrag für den jeweiligen App-FQDN auf dem DNS-Server.
2. Stellen Sie sicher, dass in den Connector Appliances ein geeigneter DNS-Server konfiguriert ist. Einzelheiten finden Sie unter Konfiguration der Netzwerkeinstellungen auf der Administrationsseite der Connector Appliance.

Die Anwendung kann nicht gefunden werden

Informationscode: 0x001800DE

Möglicherweise können Sie die Anwendung für das Ziel, auf das der Benutzer zugegriffen hat, nicht finden. Dies kann vorkommen, wenn die Zuordnung zwischen Ziel und Ressourcenstandort in der Tabelle der Anwendungsdomäne fehlt.

- Stellen Sie sicher, dass die TCP/UDP- oder HTTP-Anwendung für das aufgerufene Ziel konfiguriert ist.
- Stellen Sie sicher, dass der Benutzer ein Abonnement für die Anwendung für das aufgerufene Ziel hat.

1. Gehen Sie zur Anwendung im Management-Portal.
2. Bearbeiten Sie die App und gehen Sie zur Registerkarte **Abonnement**.
3. Stellen Sie sicher, dass der Zielbenutzer einen Eintrag in der Abonnementliste hat.

4. Stellen Sie sicher, dass die Tabelle der **Anwendungsdomäne** das Ziel und den entsprechenden Ressourcenstandort enthält.

Die Liste der konfigurierten Anwendungsziele konnte nicht abgerufen werden

Informationscode: 0x001800D3

- Stellen Sie sicher, dass mindestens eine TCP/UDP/HTTP-App konfiguriert ist. Einzelheiten finden Sie unter Anwendungen hinzufügen und verwalten.
- Stellen Sie sicher, dass die Seite der Anwendungsdomänentabelle (**Secure Private Access > Einstellungen > Anwendungsdomäne**) nicht leer ist oder dass nicht alle Einträge deaktiviert sind. Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden automatisch zu dieser Tabelle hinzugefügt. Es wird empfohlen, die Ziele oder URLs der aktiven TCP/UDP/HTTP-Anwendung in der Tabelle Anwendungsdomäne nicht zu löschen oder zu deaktivieren.

Problem mit der Anwendungskonfiguration

Die Anwendungskonfiguration enthält ein Sonderzeichen oder ein Problem mit der Richtlinienkonfiguration.

Infocode: 0x001800D9, 0x001800DA

Stellen Sie dabei Folgendes sicher:

- Die App-Konfiguration enthält keine Zeichen, die nicht unterstützt werden.
- Die Ziel-IP-Adresse oder der IP-Adressbereich oder die IP-CIDR sind gültig.
- Das Anwendungsziel ist in der Anwendungsdomänentabelle aktiviert (**Secure Private Access > Einstellungen > Anwendungsdomäne**).
- Die Richtlinien sind konfiguriert und an die jeweilige Anwendung gebunden.
- Die Konfiguration der Zugriffsrichtlinien ist korrekt.

Problem mit dem Standort der Ressource

Informationscode: 0x001800DB

- Stellen Sie sicher, dass ein Ressourcenstandort konfiguriert ist.

    1. Wählen Sie im Citrix Cloud-Hamburger-Menü die Option **Resource Location**aus.
    2. Stellen Sie sicher, dass der erwartete Ressourcenstandort konfiguriert ist und sich der Ressourcenstandort im aktiven Status befindet.

- Stellen Sie sicher, dass in der Tabelle der Anwendungsdomäne (**Secure Private Access > Einstellungen > Anwendungsdomäne**) ein korrekter Ressourcenstandort für das Ziel ausgewählt ist.

Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden automatisch zu dieser Tabelle hinzugefügt. Es wird empfohlen, die Ziele oder URLs der aktiven TCP/UDP/HTTP-Anwendung in der Anwendungsdomänentabelle nicht zu löschen oder zu deaktivieren.

Die erweiterte Sicherheitsrichtlinie ist an die HTTP-Anwendung gebunden

Infocode: 0x001800DC, 0x001800DD, 0x13000006

Auf die HTTP-Anwendung, an die eine erweiterte Sicherheitsrichtlinie gebunden ist, wird über den Citrix Secure Access-Client zugegriffen.

- Stellen Sie sicher, dass nicht dasselbe Ziel für TCP/UDP- und HTTP-Anwendungen verwendet wird.
- Wenn die erweiterte Sicherheitsrichtlinie für die HTTP/HTTPS-Anwendung aktiviert ist, wird empfohlen, nur über die Citrix Workspace-App oder den Citrix Remote Browser Isolation Service auf die App zuzugreifen.
- Deaktivieren Sie die erweiterte Sicherheitskontrolle für HTTP/HTTPS-Anwendungen, um über den Citrix Secure Access Client auf die App zuzugreifen.
  - Gehen Sie zum Secure Private Access-Administrationsportal.
  - Klicken Sie auf die Registerkarte **Anwendungen** und suchen Sie nach dem Richtliniennamen für die HTTP/HTTPS-Zielanwendung, auf die zugegriffen wurde.
  - Klicken Sie auf die Registerkarte **Zugriffsrichtlinien** und suchen Sie nach dem zuvor angegebenen Richtliniennamen.
  - Wählen Sie die Richtlinie aus und klicken Sie auf **Bearbeiten**.
  - Ändern Sie die Aktion von **Zugriff mit Einschränkungenzulassen in Zugriff zulassen.**

Einzelheiten zur Konfiguration finden Sie unter Anwendungen hinzufügen und verwalten.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser Service bekannt.

Die Länge des Hostnamens überschreitet 256 Zeichen

Informationscode: 0x001800EA

Der in der Anwendungsstartanforderung erhaltene Hostname ist länger als 256 Zeichen.

Es wird empfohlen, dass die FDQN-Zeichen 256 Zeichen nicht überschreiten.

Ungültige IP-Adresse

Informationscode: 0x001800ED

Die in der Anwendungsstartanfrage empfangene IP-Adresse ist ungültig.

Es wird empfohlen, von den Clients nur auf eine gültige private IP-Adresse zuzugreifen.

Es konnte keine Ende-zu-Ende-Verbindung hergestellt werden

Informationscode: 0x001800EF

Es konnte keine durchgängige Verbindung zwischen dem Client und dem am Ressourcenstandort konfigurierten Server hergestellt werden.

- Stellen Sie sicher, dass sich der Ressourcenstandort im aktiven Status befindet.
  - Wählen Sie im Citrix Cloud-Hamburger-Menü die Option **Resource Location**aus.
  - Führen Sie eine Integritätsprüfung für die Connector-Appliances am jeweiligen Ressourcenstandort durch.
  - Wenn das Problem dadurch nicht behoben wird, starten Sie die virtuelle Connector-Maschine neu.
- Pflegen Sie eine Connector Appliance mit hoher Verfügbarkeit
  - Wählen Sie im Citrix Cloud-Hamburger-Menü die Option **Resource Location**aus.
  - Stellen Sie sicher, dass der Ressourcenstandort über mindestens zwei Connector-Appliances verfügt.
- Stellen Sie dabei Folgendes sicher:
  - Das LAN für den Ressourcenstandort funktioniert.
  - Keine Firewalls oder Proxys in der Mitte blockieren das Connector Appliance für den Dienst oder die Backend-Server.
  - Das Client-Netzwerk ist gesund.
  - Private Backend-Server sind fehlerfrei.
  - DNS-Server sind fehlerfrei.
  - FQDNs sind auflösbar.

Wenn damit keine Probleme auftreten, gehen Sie wie folgt vor:

1. Ruft die Transaktions-ID für diesen Fehler aus den Diagnoseprotokollen ab.
2. Filtern Sie alle Ereignisse, die der Transaktions-ID im Secure Private Access Service Access-Dienst-Dashboard entsprechen.

3. Überprüfen Sie die Diagnoseprotokolle, die der Transaktions-ID entsprechen, im Secure Private Access Service Access-Dienst-Dashboard und ergreifen Sie dann die entsprechenden Maßnahmen.
4. Vergewissern Sie sich, dass in der Tabelle der Anwendungsdomäne ein korrekter Ressourcenstandort als Ziel ausgewählt ist (**Secure Private Access > Einstellungen > Anwendungsdomäne**).
5. Überprüfen Sie, ob die Anwendung mit der richtigen IP-Adresse, dem richtigen Port und dem richtigen FQDN konfiguriert ist (**Secure Private Access > Applications**).

Wenn keiner dieser Schritte das Problem behebt, wenden Sie sich an den Citrix Support und geben Sie den Fehlercode für die Transaktions-ID an und sammeln Sie die Client-Logs.

Informationen zum Sammeln von Client-Debug-Logs finden Sie unter So sammeln Sie Client-Logs.

IPv6 wurde in der App-Anfrage empfangen

Informationscode: 0x001800F5

In der App-Anfrage wird eine IPv6-Anfrage empfangen, die nicht unterstützt wird. Derzeit wird nur IPv4 unterstützt.

Bearbeiten Sie die Anwendung, um das Problem mit der IP-Adresse der Anwendung zu beheben.

1. Gehen Sie zum Secure Private Access-Administrationsportal.
2. Klicken Sie auf die Registerkarte **Anwendungen**.
3. Suchen Sie nach der App und klicken Sie auf **Bearbeiten**.

Einzelheiten finden Sie unter Apps hinzufügen und verwalten.

UDP-Verkehr konnte nicht übermittelt werden

Informationscode: 0x001800F9

Der UDP-Verkehr konnte nicht übermittelt werden, da die Client-Verbindung unterbrochen wurde

1. Prüfen Sie, ob die Client-Sitzung aktiv ist.
2. Loggen Sie sich ab und melden Sie sich dann erneut an.

Die Übertragung des UDP-Datenverkehrs ist fehlgeschlagen

Informationscode: 0x001800FF

- Suchen Sie nach der Transaktions-ID für den Fehlercode und filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Secure Private Access Service Access-Dienst-Dashboard.

- Prüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Wenn ein Problem in anderen Komponenten festgestellt wird, ergreifen Sie entsprechende Maßnahmen.
- Wenn das Problem dadurch nicht behoben wird, wenden Sie sich mit dem Fehlercode und der entsprechenden Transaktions-ID an den Citrix Support.

Der Start der Anwendung ist aufgrund von Netzwerkverbindungsproblemen fehlgeschlagen

Informationscode: 0x10000401

Fehler beim Starten der Anwendung aufgrund von Netzwerkverbindungsproblemen zwischen Connector Appliance und Secure Private Access Service

1. Überprüfen Sie die öffentliche Internetverbindung der Connector Appliance.
2. Prüfen Sie, ob irgendwelche Proxy- oder Firewallregeln die Verbindung blockieren.
3. Wenn ein Proxy das Problem verursacht, Bypass Sie den Proxy und versuchen Sie erneut, die App zu starten.
4. Überprüfen Sie den Systemstatus der Connector Appliance (**Citrix Cloud > Ressourcenstandort**).

Einzelheiten zu den Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Connector Appliance konnte sich nicht beim Secure Private Access Service registrieren

Infocode: 0x10000402, 0x1000040C

1. Gehen Sie zur Admin-Seite von Connector Appliances und überprüfen Sie die Connector-Zusammenfassung.
2. Wenn der Connector-Status nicht gut ist, wechseln Sie zur Ressourcenposition im Management-Portal.
3. Führen Sie eine Integritätsprüfung für die Connector-Appliances am jeweiligen Ressourcenstandort durch.
4. Wenn die Integritätsprüfung fehlschlägt, starten Sie die virtuelle Connector-Maschine neu.
5. Überprüfen Sie die Connector-Zusammenfassung und führen Sie die Integritätsprüfung erneut aus.

Einzelheiten zu den Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Verbindungsproblem mit Connector Appliance

Informationscode: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Suchen Sie in der Transaktions-ID nach dem Fehlercode.
- Filtern Sie alle Ereignisse, die der Transaktions-ID im Secure Private Access-Dashboard entsprechen.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist, falls gefunden, führen Sie die entsprechende Problemumgehung durch, die mit diesem Fehlercode übereinstimmt.
- Wenn in anderen Komponenten kein Fehler gefunden wird, gehen Sie wie folgt vor:
  - Gehen Sie zur Admin-Seite von Connector Appliances.
  - Laden Sie den Diagnosebericht herunter. Einzelheiten finden Sie unter Generieren eines Diagnoseberichts.
  - Erfassen Sie den Paket-Trace. Einzelheiten finden Sie unter Überprüfen Sie Ihre Netzwerkverbindung.
- Wenden Sie sich mit diesem Diagnosebericht und der Paketverfolgung zusammen mit dem Fehlercode und der Transaktions-ID an den Citrix Support.

Verbindungsprobleme mit Connector Appliance und privaten TCP/UDP-Servern im Back-End

Informationscode: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Die Connector Appliance hat ein Verbindungsproblem mit den privaten TCP/UDP-Servern im Back-End.

- Prüfen Sie, ob der Backend-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, betriebsbereit ist und die Anfragen empfangen kann.
- Überprüfen Sie die Erreichbarkeit der Backend-Server innerhalb des Unternehmensnetzwerks.
- Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector daran gehindert ist, den Backend-Server zu erreichen.
- Wenn es sich um eine FQDN-basierte App handelt, überprüfen Sie den DNS-Eintrag für die entsprechende App auf dem DNS-Server.

Connector Appliance kann DNS für FQDNs nicht auflösen

Informationscode: 0x10000406

- Überprüfen Sie den DNS-Eintrag für den jeweiligen App-FQDN auf dem DNS-Server.
- Stellen Sie sicher, dass in den Connector Appliances ein geeigneter DNS-Server konfiguriert ist. Einzelheiten finden Sie unter Konfiguration der Netzwerkeinstellungen auf der Administrationsseite der Connector Appliance.

Private Serververbindung wurde beendet

Informationscode: 0x10000411

Die Verbindung zum privaten Server wird vom Client oder vom Secure Private Access Service beendet.

1. Prüfen Sie, ob der Endbenutzer die Anwendung geschlossen hat.
2. Prüfen Sie andere Diagnoseprotokolle, die mit der Transaktions-ID dieses Protokolls übereinstimmen, und ergreifen Sie die entsprechenden Maßnahmen.
3. Starten Sie die App erneut.
4. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich mit dem Fehlercode und der Transaktions-ID an den Citrix Support.

Es konnten keine Verbindung zur privaten Dienst-IP oder zum FQDN hergestellt oder Daten gesendet werden

Informationscode: 0x10000413

- Private Serververbindung wurde beendet
- [Verbindungsprobleme mit Connector Appliance und privaten TCP/UDP-Servern im Backend] (/en-us/citrix-secure-private-access/service/secure-private-access-troubleshooting. html #connectivity -problees-with-connector-appliance and-backend-private-tcpudp-Servern).
  Überprüfen Sie die Einträge der Routingdomäne Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Backend verweisen.

Keine übereinstimmende politische Bedingung

Informationscode: 0x100508

Der Benutzerkontext entspricht nicht den Bedingungen der Zugriffsregeln, die in den der App zugewiesenen Richtlinien definiert sind.

Aktualisieren Sie die Richtlinienkonfiguration so, dass sie dem Kontext des Benutzers entspricht.

Der Anwendung ist keine Zugriffsrichtlinie zugeordnet

Informationscode: 0x100509

1. Klicken Sie in der Benutzeroberfläche des Citrix Secure Private Access-Dienstes im linken Navigationsbereich auf **Zugriffsrichtlinien**.
2. Stellen Sie sicher, dass der jeweiligen App eine Zugriffsrichtlinie zugeordnet ist.
3. Wenn der App keine Zugriffsrichtlinie zugeordnet ist, erstellen Sie eine Zugriffsrichtlinie für die App. Einzelheiten finden Sie unter Zugriffsrichtlinien erstellen.
4. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Keine Anwendungskonfiguration für den FQDN oder die IP-Adresse gefunden

Info code: 0x10050A

Für den eingehenden FQDN oder die IP-Adressanforderung wurde keine passende Anwendung gefunden. Daher wird die App als unveröffentlichte Anwendung eingestuft. Wenn dies nicht erwartet wird, gehen Sie wie folgt vor.

1. Gehen Sie zum Administratorportal für den Secure Private Access Service.
2. Klicken Sie in der linken Navigationsleiste auf **Anwendungen**.
3. Suchen Sie nach der App und klicken Sie auf **Bearbeiten**.
4. Fügen Sie der Anwendung einen FQDN oder die IP-Adresse hinzu. Sie können die genaue Domain, IP-Adresse oder eine Wildcard-Domain hinzufügen.

   Hinweis: Das Hinzufügen eines FQDN oder einer IP-Adresse unter **Secure Private Access > Einstellungen > Anwendungsdomäne** löst dieses Problem nicht. Es muss als Teil der Anwendungskonfiguration hinzugefügt werden.

Informationen zur App-Aufzählung

Informationscode: 0x10050C

Dieser Code erfasst die Ergebnisse der Richtlinienbewertung mehrerer Anwendungen, für die der Benutzer möglicherweise berechtigt ist. Der Zugriff auf die App kann aus den folgenden Gründen verweigert werden:

- Der Benutzerkontext entspricht nicht den Bedingungen der Zugriffsregel, die in den der App zugewiesenen Richtlinien definiert sind. Einzelheiten finden Sie unter Keine übereinstimmende Richtlinienbedingung.

- Der Anwendung ist keine Zugriffsrichtlinie zugeordnet —Einzelheiten finden Sie unter Keine mit der Anwendung verknüpfte Zugriffsrichtlinie.
- Eine der Anwendung zugeordnete Richtlinie ist so konfiguriert, dass sie den Zugriff verweigert. In diesem Fall ist keine Aktion erforderlich, da dies beabsichtigt ist.
- Unerwarteter interner Fehler bei der Durchsetzung der Zugriffsrichtlinie. Weitere Informationen erhalten Sie vom Citrix Support.

Der Start der TCP/UDP-App ist fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt

Infocode: 0x00180101

Dieses Problem kann auftreten, wenn die Anwendungskonfiguration vorhanden ist, der Routing-Eintrag jedoch fehlt oder zuvor gelöscht wurde.

Fügen Sie einen Routing-Eintrag (**Secure Private Access > Einstellungen > Anwendungsdomäne**) für das Ziel hinzu, auf das zugegriffen wird.

Der Start der TCP/UDP-App ist fehlgeschlagen, da die Konnektoren nicht fehlerfrei sind

Infocode: 0x00180102

Dieses Problem kann auftreten, wenn keiner der Konnektoren auf die neue Verbindung funktioniert oder reagiert.

Führen Sie eine Integritätsprüfung für die Connector-Appliances am jeweiligen Ressourcenstandort durch.

Die UDP/DNS-Anfrage ist fehlgeschlagen, da der Connector nicht erreichbar ist

Infocode: 0x00180103

Dieses Problem kann auftreten, wenn der UDP/DNS-Verkehr den Connector nicht erreichen kann.

Führen Sie eine Integritätsprüfung für die Connector-Appliances am jeweiligen Ressourcenstandort durch.

Die Seite konnte nicht geladen werden, da das NGS-Cookie abgelaufen ist

Infocode: 0x20580001

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Das Abrufen der Zugriffsrichtlinie ist aufgrund eines Netzwerkausfalls fehlgeschlagen

Infocode: 0x20580002

1. Überprüfen Sie die URL und die Netzwerkverbindung.
2. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Fehler beim Abrufen der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens

Infocode:0x20580003

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Netzwerkfehler beim Abrufen der Zugriffsrichtlinien-Details

Infocode:0x20580004

1. Prüfen Sie, ob die Zugriffsrichtlinie aktiviert ist.
2. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Fehler beim Abrufen der Richtlinie beim Abrufen des öffentlichen Zertifikats

Infocode: 0x20580005

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Fehler beim Abrufen der Richtlinie beim Überprüfen der Signatur des JSON-Web-Tokens

Infocode: 0x20580007

1. Prüfen Sie, ob die Netzwerkzeit und die Uhrzeit des Benutzergeräts synchron sind.
2. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Fehler beim Abrufen der Richtlinie beim Überprüfen des öffentlichen Zertifikats

Infocode: 0x20580008

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Die Store-Umgebung für die Bildung einer Richtlinien-URL konnte nicht bestimmt werden

Infocode: 0x2058000A

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Es konnte keine Antwort auf die Abrufanforderung der Zugriffsrichtlinie abgerufen werden

Infocode: 0x2058000B

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Der Abruf der Zugriffsrichtlinie ist aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens fehlgeschlagen

Infocode: 0x2058000C

1. Starten Sie den Browser neu und versuchen Sie erneut, die App zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Connector Appliance ist nicht registriert

Infocode: 0x10200002

Überprüfen Sie die Registrierung des Connector Appliance.

Einzelheiten finden Sie unter Registrieren Sie Ihr Connector Appliance bei Citrix Cloud.

Es konnte keine Verbindung zum Connector Appliance hergestellt werden

Infocode: 0x10200003

Das Connector Appliance kann nicht zwischen Citrix Cloud und Ressourcenstandorten kommunizieren.

Überprüfen Sie die Connector-Registrierung.

Einzelheiten finden Sie unter Registrieren Sie Ihr Connector Appliance bei Citrix Cloud.

Die Verbindung zum Citrix Secure Private Access Service ist fehlgeschlagen

Infocode: 0x10000301

Überprüfen Sie die Netzwerkeinstellungen des Connector Appliance. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Proxyserver ist nicht erreichbar

Infocode: 0x10000303, 0x10000304

Überprüfen Sie die Proxy-Servereinstellungen und stellen Sie sicher, dass sie für das Connector Appliance erreichbar sind. Einzelheiten finden Sie unter Registrieren Sie Ihr Connector Appliance bei Citrix Cloud.

Die Proxy-Server-Authentifizierung ist fehlgeschlagen

Infocode: 0x10000305

Überprüfen Sie die Anmeldeinformationen für den Proxyserver und stellen Sie sicher, dass sie im Connector Appliance richtig konfiguriert sind. Einzelheiten finden Sie unter Nach der Registrierung Ihres Connector Appliance.

Konfigurierte Proxyserver sind nicht erreichbar

Infocode: 0x10000306

Überprüfen Sie die Netzwerkeinstellungen, Firewalleinstellungen oder Proxyservereinstellungen des Connector Appliance. Einzelheiten finden Sie in den folgenden Themen:

- Netzwerkeinstellungen für Ihre Connector Appliance
- Connector Appliance bei Citrix Cloud registrieren
- Kommunikation der Connector Appliance

Fehlerantwort vom Backend-Server erhalten

Infocode: 0x10000307

Überprüfen Sie den HTTP-Statuscode des Backend-Webservers, falls es sich nicht um einen erwarteten Code handelt.

Anfrage kann nicht an die Ziel-URL gesendet werden

Infocode: 0x10000005

Überprüfen Sie die Ziel-URL oder überprüfen Sie die Netzwerkeinstellungen des Connector Appliance. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

SSO konnte nicht verarbeitet werden

Infocode: 0x10000107

Fehler beim Abrufen der App-Konfigurationsdaten aus Citrix Cloud.

Überprüfen Sie die Netzwerkeinstellungen des Connector Appliance und stellen Sie sicher, dass der NTP-Server konfiguriert ist und keine Timestrip-Probleme vorliegen. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Die Verbindung zum Citrix Secure Private Access Service ist fehlgeschlagen

Infocode: 0x10000108, 0x1000010B

Überprüfen Sie die Netzwerkeinstellungen des Connector Appliance. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

SSO konnte nicht verarbeitet werden, SSO-Einstellungen konnten nicht ermittelt werden

Infocode: 0x1000010A

Überprüfen Sie die SSO-Konfiguration und stellen Sie sicher, dass der Server für das Connector Appliance erreichbar ist.

FormFill SSO ist fehlgeschlagen, falsche Konfiguration der Formular-App

Infocode: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Überprüfen Sie die Konfiguration der SSO-Formular-App und stellen Sie sicher, dass die Felder Benutzername, Kennwort, Aktion und Anmelde-URL in den App-Einstellungen korrekt konfiguriert sind.

Kerberos SSO ist fehlgeschlagen

Infocode: 0x10000202

Überprüfen Sie die Kerberos-SSO-Einstellungen auf dem Backend-Server und dem Domänencontroller. Überprüfen Sie auch die NTLM-Fallback-Authentifizierungseinstellungen.

Informationen zu Kerberos-SSO-Einstellungen finden Sie unter Überprüfen Ihrer Kerberos-Konfiguration.

SSO für den Authentifizierungstyp konnte nicht verarbeitet werden

Infocode: 0x10000203

Überprüfen Sie die SSO-Einstellungen im Secure Private Access Service und auf dem Backend-Server. Informationen zum Secure Private Access Service finden Sie unter Bevorzugte Anmeldemethode festlegen.

Kerberos SSO ist fehlgeschlagen, fällt aber auf NTLM zurück

Infocode: 0x10000204

Das Abrufen des Kerberos-Tickets vom Domänencontroller ist fehlgeschlagen. Als sekundäre Authentifizierung hat Connector Appliance die NTLM-Fallbackauthentifizierung versucht.

Um eine erfolgreiche Kerberos-Authentifizierung zu aktivieren, überprüfen Sie die Kerberos-SSO-Einstellungen auf dem Backend-Server und dem Domänencontroller.

Einzelheiten finden Sie unter Überprüfen Ihrer Kerberos-Konfiguration.

In der Citrix Workspace Workspace-Anwendung sind mehrere ZTNA-berechtigte Konten konfiguriert

Infocode: 0x14000001

Konfigurieren Sie in der Citrix Workspace Workspace-Anwendung nur ein ZTNA-berechtigtes Konto.

So sammeln Sie Kundenprotokolle

- **Windows-Client:**
  1. Öffnen Sie die App und stellen Sie sicher, dass die Protokollierung aktiviert ist.
  2. Stellen Sie nun eine Verbindung zum Secure Private Access Service her und duplizieren Sie das Problem, mit dem Sie konfrontiert sind.

3. Gehen Sie in der App zu **Logging** und klicken Sie auf **Logfiles sammeln**. Dadurch wird die Logdatei generiert.
4. Speichern Sie die Protokolldatei auf dem Desktop des Client-Computers.

- **Mac-Client:**

1. Öffne die App und gehe zu **Logs > Verbose.**
2. Löschen Sie die Protokolle und fahren Sie mit der Reproduktion des Problems fort.
3. Gehen Sie zurück zu **Protokolle > Protokolle exportieren**. Dadurch wird eine Zip-Datei erstellt, die Protokolldateien enthält.

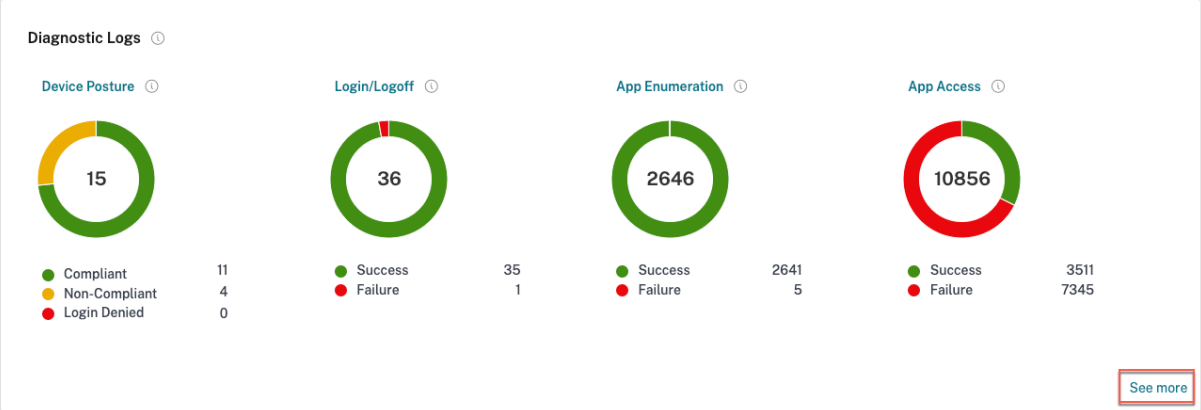
Antworten auf häufig gestellte Fragen

Was sind Secure Private Access-Diagnoseprotokolle?

Secure Private Access-Diagnoseprotokolle erfassen alle Ereignisse, die auftreten, wenn ein Benutzer auf eine Anwendung zugreift (Web/SaaS/TCP/UDP). Diese Protokolle erfassen den Gerätestatus, die App-Authentifizierung, die App-Aufzählung und die App-Zugriffsprotokolle.

Wo finde ich Secure Private Access-Logs?

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Secure Private Access Service Access-Dienstkachel auf **Verwalten**.
3. Klicken Sie in der linken Navigationsleiste der Admin-Benutzeroberfläche auf **Dashboard**.
4. Klicken Sie in der Tabelle **Diagnoseprotokolle** auf den Link **Weitere anzeigen**.



Welche Details kann ich in den Secure Private Access-Diagnoseprotokollen finden?

Das Secure Private Access-Benutzerprotokoll-Dashboard enthält standardmäßig die folgenden Details.

- **Zeitstempel** —Uhrzeit des Ereignisses in UTC.
- **Benutzername** —**Benutzername** des Endbenutzers, der auf die App zugreift.
- **App-Name** —Name der App/Apps, auf die zugegriffen wurde.
- **Richtlinieninformationen** —Zeigt den Namen der Zugriffsrichtlinie oder Richtlinien an, die während des Ereignisses ausgelöst wurden.
- **Status** —Zeigt den Status des Ereignisses, des Erfolgs oder Fehlers an.
- **Infocode** —Weitere Informationen finden Sie unter dem Infocode.
- **Beschreibung** —Zeigt den Grund für den Fehler oder weitere Details zum Ereignis an.
- **APP FQDN**: FQDN der aufgerufenen Anwendung
- **Ereignistyp** —Zeigt den Ereignistyp an, der dem ausgeführten Vorgang zugeordnet ist.
- **Vorgangstyp** —Zeigt den Vorgang an, für den das Protokoll generiert wurde.
- **Kategorie** —Je nach Art des Ereignisses sind drei Kategorien verfügbar. Das ist App-Authentifizierung, App-Aufzählung oder App-Zugriff. Diese Optionen sind auch als Filteroptionen verfügbar. Sie können diese Optionen verwenden, um Protokolle je nach Art des Problems zu filtern, mit dem Sie konfrontiert sind.
- **Transaktions-ID** —Erfahren Sie, wie Sie eine Transaktions-ID verwenden
  . Die folgenden Details können abgerufen werden, indem Sie auf die Schaltfläche + ganz rechts im Dashboard klicken:
- **SPA-PoP-Standort** —Zeigt den Namen/die ID des PoP-Standorts des Secure Private Access-Dienstes an, der beim App-Zugriff verwendet wurde. Siehe Secure Private Access PoP Locations

Welche Ereignisse werden in den Secure Private Access-Diagnoseprotokollen erfasst?

Die Secure Private Access-Diagnoseprotokolle erfassen die folgenden Ereignisse:

- **Gerätestatus:** Gerätestatus des Endbenutzers. Diese Protokolle erfassen Informationen über die Ergebnisse der Gerätehaltung. Ob das Gerät aufgrund Ihrer Gerätezustandsrichtlinie als konform oder nicht konform eingestuft wurde oder ob der Zugriff verweigert wurde.
- **Anmeldung/Abmeldung**: Ereignisse zum Anmelde- oder Abmeldestatus von Endbenutzern am Citrix Secure Access-Client und zur Authentifizierung bei Workspace (interne oder externe Anbieter).
- **App-Enumeration**: Im Secure Private Access Service entscheiden von Administratoren konfigurierte Zugriffsrichtlinien darüber, welcher Benutzer auf welche App zugreifen darf. Abgelehnte Anwendungen sind für Endbenutzer in der Citrix Workspace App nicht sichtbar (nicht aufgeführt). Anhand dieser Ereignisse können Sie feststellen, welchen Anwendungen der Zugriff für einen Benutzer auf der Grundlage der im Secure Private Access-Dienst konfigurierten Zugriffsrichtlinien gewährt oder verweigert wurde.
- **App-Zugriff**: Ereignisse des Anwendungs-/Endpunktzugriffs des Endbenutzers, des Zulassen/Verweigerns, des Single Sign-On-Status und des Konnektivitätsstatus gemäß den konfigurierten Zugriffsrichtlinien für das ausgewählte Zeitintervall.

Wie verwende ich das Thema zur Fehlerbehebung bei Secure Private Access, um einen Fehler zu beheben, auf den ich gestoßen bin?

1. Rufen Sie den Infocode für den Fehler ab, den Sie beheben möchten.
2. Suchen Sie den Infocode in der Fehlersuchtabelle.
3. Folgen Sie den für diesen Infocode angegebenen Lösungsschritten.

Was ist ein Infocode? Wo finde ich sie?

Einigen Protokollierungsereignissen, wie z. B. Ausfällen, ist ein Infocode zugeordnet. Suchen Sie in der Fehler-Suchtabelle nach diesem Infocode, um die Lösungsschritte oder weitere Informationen zu diesem Ereignis zu finden.

Was ist eine Transaktions-ID? Wie verwende ich es?

Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanfrage. Für eine App-Zugriffsanforderung können mehrere Protokolle generiert werden, angefangen mit der Authentifizierung, dann der App-Aufzählung innerhalb der Workspace-App und dann dem App-Zugriff selbst. All diese Ereignisse generieren ihre eigenen Protokolle. Die Transaktions-ID wird verwendet, um all diese Protokolle zu korrelieren. Sie können die Diagnoseprotokolle anhand der Transaktions-ID filtern, um alle Protokolle zu finden, die sich auf eine bestimmte App-Zugriffsanforderung beziehen.

Was sind all die PoP-Standorte mit sicherem privaten Zugriff?

Im Folgenden finden Sie die Liste der PoP-Standorte von Secure Private Access.

PoP-Name	Zone	Region
az-us-e	Azure East US	Virginia
az-us-w	Azure West US	Kalifornien
az-us-sc	Azure South Central US	Texas
az-aus-e	Azure Australien Ost	New South Wales
az-eu-n	Azure Nordeuropa	Irland
az-eu-w	Azure Westeuropa	Niederlande
az-jp-e	Azure Japan Ost	Tokio, Saitama
az-bz-s	Azure Brazil South	Sao Paulo State
az-asia-se	Azure southeastasia	Singapur

PoP-Name	Zone	Region
az-uae-n	Azure uaenorth	Dubai
az-in-s	Azure southindia	Chennai
az-asia-hk	Azure eastasia	Hongkong

Was mache ich, wenn ich meinen Fehler nicht mithilfe des Infocodes und der Fehlernachschlagetabelle beheben kann?

Wenden Sie sich an Citrix Support

Referenzen

- **Eine Web-App hinzufügen**
  - Unterstützung für unternehmenseigene Web-Apps
  - Direkter Zugriff auf Web-Apps konfigurieren
- **Eine SaaS-App hinzufügen**
  - Unterstützung für Software as a Service App
  - Serverspezifische Konfiguration für SaaS App
- **Client-Server-Apps konfigurieren**
  - Unterstützung für Client-Server-Apps
- **Zugriffsrichtlinien erstellen**
  - Zugriffsrichtlinien erstellen
- **Routentabellen**
  - Routentabellen