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

Citrix Secure Private Access 3

Was ist neu 6

Erste Schritte mit Citrix Secure Private Access 23

Überblick über die Secure Private Access-Servicelösung 26

Administratorgeführter Workflow für einfaches Onboarding und Einrichten 38

Optionen zur Zugriffsbeschränkung 51

Tool zur Richtlinienmodellierung 71

Konfiguration und Verwaltung von Apps 73

Unterstützung für Enterprise-Web-Apps 73

Direkter Zugriff auf Enterprise-Web-Apps 85

Unterstützung für Software-as-a-Service-Apps 93

Apps-Konfiguration über eine Vorlage 103

SaaS-App-Server-spezifische Konfiguration 108

Reservierte CIDR-Adressen für die TCP- und UDP-Server 123

DNS-Suffixe zur Auflösung von FQDNs in IP-Adressen 124

Connector-Appliance für sicheren privaten Zugriff 131

Gateway Connector zur Connector-Einheit migrieren 144

Migration von App-Sicherheitskontrollen und Zugriffsrichtlinien auf das neue Access Policy Framework 145

Starten einer konfigurierten App - Endbenutzerworkflow 148

Ermitteln Sie Domänen oder IP-Adressen, auf die Endbenutzer zugreifen 149

Bewährte Methoden für Web- und SaaS-Anwendungskonfigurationen 157

Beenden Sie aktive Benutzersitzungen und fügen Sie Benutzer zur Benutzersperrliste hinzu 163

Timeouts für Benutzersitzungen **165**

Schreibgeschützter Zugriff für Administratoren auf SaaS und Web-Apps **167**

Dashboard-Übersicht **171**

Protokollierung und Fehlerbehebung **181**

Auditprotokolle **227**

Adaptive Zugriffs- und Sicherheitskontrollen für Enterprise Web-, TCP- und SaaS-Anwendungen **229**

Routentabellen zur Lösung von Konflikten, die aus denselben verwandten Domänen resultieren **241**

Nicht genehmigte Websites **245**

ADFS-Integration mit Secure Private Access **248**

Veraltete Funktionen **257**

Citrix Secure Private Access

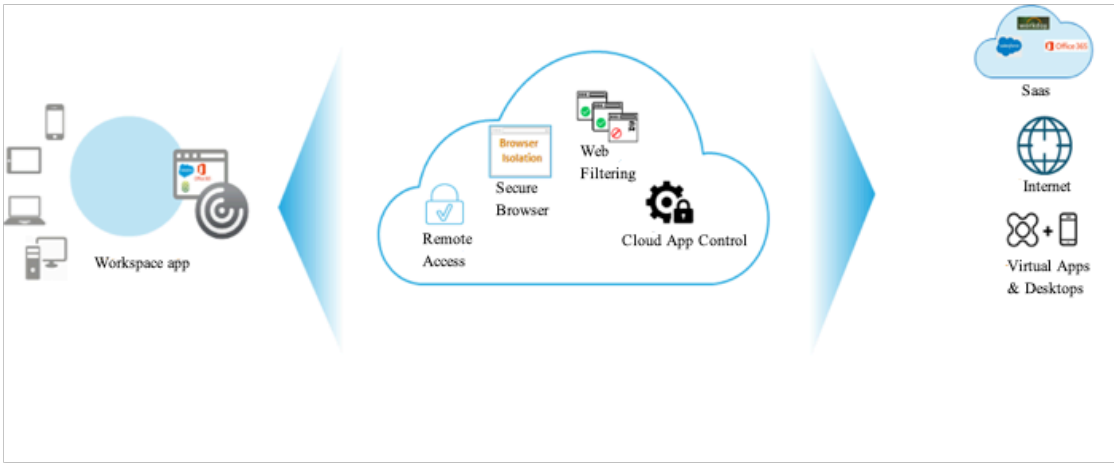
October 21, 2024

Mit dem Citrix Secure Private Access-Dienst können Administratoren eine einheitliche Erfahrung bereitstellen, indem sie Single Sign-On, Remote-Zugriff und Inhaltsprüfung in einer einzigen Lösung für eine durchgängige Zugriffskontrolle integrieren. IT-Administratoren können den Zugriff auf genehmigte SaaS-Apps mit einer vereinfachten Single-Sign-On-Erfahrung regeln. Mit dem Citrix Secure Private Access-Dienst können Administratoren außerdem das Netzwerk und die Endbenutzergeräte des Unternehmens vor Malware und Datenlecks schützen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern. Administratoren können erweiterte Zugriffssicherheitsrichtlinien für den sicheren Zugriff auf SaaS-Anwendungen durchsetzen. Nach der Authentifizierung haben Mitarbeiter von jedem Gerät aus Zugriff auf alle wichtigen Geschäftsanwendungen, unabhängig davon, ob sie sich im Büro, zu Hause oder unterwegs befinden.

Administratoren können Benutzeraktivitäten überwachen, etwa besuchte bösartige, gefährliche oder unbekannte Websites, die verbrauchte Bandbreite sowie riskante Download- und Upload-Verhaltensweisen. Mithilfe der Analyse der aufgerufenen Websites und Websitekategorien können Administratoren Korrekturmaßnahmen zum Schutz des Unternehmensnetzwerks ergreifen. Gleichzeitig bietet der Dienst Endbenutzern nahtlosen und sicheren Zugriff auf alle ihre gehosteten Apps.

Administratoren können außerdem Aktionen einschränken, wie etwa das Drucken, Downloads und den Zugriff auf die Zwischenablage (Kopieren und Einfügen).

Das folgende Diagramm ist eine visuelle Darstellung des Secure Private Access-Dienstes.



Wichtige Funktionen von Citrix Secure Workspace Access

Im Folgenden sind einige der wichtigsten Aufgaben aufgeführt, die Sie mit dem Citrix Secure Workspace Access-Dienst ausführen können:

- **SaaS-Apps mit Single Sign-On-Zugriff veröffentlichen** –Sobald der Benutzer mit einer primären Identität bei Citrix Workspace authentifiziert ist, werden nachfolgende Authentifizierungsaufforderungen für SaaS- und Web-Apps automatisch von der Single Sign-On-Funktion in der Citrix Cloud unter Verwendung von SAML-Assertionen erfüllt.

Standardmäßig kombiniert die SAML-Assertion die E-Mail-Adresse, die mit dem Active Directory-Konto des Benutzers verknüpft ist (Identitätsanbieter), mit der E-Mail-Adresse, die mit dem SaaS- oder Web-App-Konto des Benutzers verknüpft ist (Dienstanbieter).

- **Legen Sie erweiterte Sicherheitsrichtlinien für SaaS-Apps fest. (Zum Beispiel Wasserzeichen, Kopier- und Einfügebeschränkung und Download-Verhinderung.)** –Zum Schutz von Inhalten integrieren Organisationen erweiterte Sicherheitsrichtlinien in die SaaS-Anwendungen. Jede Richtlinie erzwingt eine Einschränkung des Citrix Enterprise Browsers bei Verwendung der Workspace-App für den Desktop oder des Secure Browsers bei Verwendung der Workspace-App im Web oder auf Mobilgeräten.
  - Bevorzugter Browser: Deaktiviert die Verwendung eines lokalen Browsers und verwendet die Citrix Enterprise Browser-Engine (Workspace-App –Desktop) oder den Secure Browser (Workspace-App –Mobil und Web).

  - Zugriff auf die Zwischenablage einschränken: Deaktiviert Ausschneiden/Kopieren/Einfügen-Vorgänge zwischen der Zwischenablage der App und des Endpunkts.
  - Drucken einschränken: Deaktiviert die Möglichkeit zum Drucken aus dem App-Browser heraus.
  - Downloads einschränken: Deaktiviert die Möglichkeit des Benutzers, aus der SaaS-App heraus Downloads durchzuführen.
  - Wasserzeichen anzeigen: Überlagert ein bildschirmbasiertes Wasserzeichen, das den Benutzernamen und die IP-Adresse des Endpunkts zeigt. Wenn ein Benutzer versucht, einen Screenshot zu drucken oder zu erstellen, wird das Wasserzeichen wie auf dem Bildschirm angezeigt.

- **Kontextbezogenen Zugriff bereitstellen** –Obwohl eine autorisierte SaaS-App als sicher gilt, kann der Inhalt der SaaS-App tatsächlich gefährlich sein und ein Sicherheitsrisiko darstellen. Wenn ein Benutzer in einer SaaS-App auf einen Hyperlink klickt, wird der Datenverkehr durch die Webfilterfunktion geleitet, die eine Risikobewertung für den Hyperlink bereitstellt. Basierend auf der Risikobewertung des Hyperlinks und der benutzerdefinierten Liste der URL-Kategorien lässt die Webfilterfunktion die Hyperlink-Anforderung des Benutzers zu, lehnt sie ab oder leitet sie wie folgt um:

  - Genehmigt: Der Hyperlink gilt als sicher und der Citrix Enterprise Browser greift innerhalb der Workspace-App auf den Hyperlink zu.
  - Abgelehnt: Der Hyperlink wird als gefährlich eingestuft und der Zugriff wird verweigert.
  - Umgeleitet: Die Hyperlink-Anforderung wird an den Secure Browser-Dienst umgeleitet, wo die Internet-Browsing-Aktivitäten des Benutzers vom Endpunktgerät, dem Unternehmensnetzwerk und der SaaS-App isoliert werden.

- **Sicherheits- und Leistungsanalysen** –Benutzer greifen ausnahmslos auf SaaS-Apps zu, die über eine verbesserte Sicherheit verfügen. Die Workspace-App, der Secure Workspace Access-Dienst und der Secure Browser-Dienst liefern dem Security Analytics-Dienst Informationen zu den folgenden Benutzer- und Anwendungsverhalten. Diese Analysen wirken sich auf die Gesamtrisikobewertung des Benutzers aus:

  - Startzeit der App
  - App-Endzeit
  - Druckaktion
  - Zugriff auf die Zwischenablage
  - URL-Zugriff
  - Datenupload
  - Datendownload

- **Webfilterung:** Die Webfilterfunktion bewertet das Risiko jedes innerhalb der SaaS-Anwendung ausgewählten Hyperlinks. Der Zugriff auf diese Sites und die Überwachung von Änderungen

im Benutzerverhalten erhöht die Gesamtrisikobewertung des Benutzers, da dies ein Zeichen dafür ist, dass das Endgerät kompromittiert wurde und begonnen hat, Daten zu infizieren oder zu verschlüsseln, oder dass der Benutzer und das Gerät geistiges Eigentum stehlen.

- **Integration mit Security Information and Event Management (SIEM)** –Die Secure Private Access-Protokolle können über Kafka in SIEM wie Splunk, Sentinel und Elastic exportiert werden. Durch das Exportieren von Protokollen nach SIEM werden die Sicherheitsfunktionen verbessert und die Effektivität der Reaktion auf Vorfälle gesteigert. Einzelheiten finden Sie unter Secure Private Access-Ereignisse.

Was ist neu

October 21, 2024

23. September 2024

- **Unterstützung für kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten**

  Die dynamische Domänenrouting-Konfiguration in der Zugriffsrichtlinie ermöglicht Administratoren jetzt, den internen Routing-Typ pro URL basierend auf dem Benutzerkontext zu bearbeiten. Administratoren können die Ressourcenstandorte so ändern, dass die Benutzeranforderungen an das optimale Rechenzentrum weitergeleitet werden. Auf diese Weise wird sichergestellt, dass Benutzeranforderungen effizient bearbeitet und die Leistung optimiert werden. Weitere Einzelheiten finden Sie unter Kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten.

15. August 2024

- **Option zum Konfigurieren einer Zeitdauer zum Löschen der Einträge in der Liste blockierter Benutzer**

  Administratoren können jetzt eine bestimmte Dauer (1 bis 99 Tage) für die Löschung der Einträge in der Liste gesperrter Benutzer festlegen. Einzelheiten hierzu finden Sie unter Beenden aktiver Benutzersitzungen und Hinzufügen von Benutzern zur Benutzersperrliste.

- **Zusätzliche Sicherheitskontrollen**

  Zum Einschränken des Anwendungszugriffs stehen jetzt die folgenden zusätzlichen Sicherheitskontrollen zur Verfügung.

  - Mikrofon

  - Webcam
  - Benachrichtigungen
  - Popups
  - Unsicherer Inhalt

  Einzelheiten finden Sie unter Zugriffsbeschränkungsoptionen.

- **Verbesserungen der Funktion für nicht genehmigte Websites (Webfilterung)**

  Mit der Funktion für nicht genehmigte Websites (Webfilterung) können Administratoren den Zugriff auf den gesamten nicht genehmigten Datenverkehr standardmäßig blockieren oder ihn über den Citrix Enterprise Browser standardmäßig zulassen. Einzelheiten finden Sie unter Nicht genehmigte Websites.

16. Juli 2024

- **Zusätzliche Sicherheitskontrollen**

  Zum Einschränken des Anwendungszugriffs stehen die folgenden zusätzlichen Sicherheitskontrollen zur Verfügung.

  - Downloadbeschränkung nach Dateityp
  - Uploadbeschränkung nach Dateityp
  - Maskierung personenbezogener Daten
  - Druckerverwaltung
  - Zwischenablagebeschränkung für Sicherheitsgruppen

  Einzelheiten finden Sie unter Zugriffsbeschränkungsoptionen.

- **Anzeige eingebetteter Domänen auf der App-Entdeckungsseite**

  Mit der App-Erkennungsfunktion können Administratoren neue Anwendungen erstellen oder diese Domänen zu einer vorhandenen Anwendung hinzufügen, wenn einer Anwendung keine Hauptdomäne oder eingebettete Domäne (HTTP/HTTPS) oder die Ziel-IP-Adresse (TCP/UDP) zugeordnet ist. Auf der Seite **App-Erkennung** werden sowohl die Hauptdomäne als auch die darunter liegenden eingebetteten Domänen in einer Baumstruktur angezeigt. Weitere Einzelheiten finden Sie unter Ermitteln von Domänen oder IP-Adressen, auf die Endbenutzer zugreifen.

11. Juni 2024

- **Tool zur Richtlinienmodellierung**

Das Tool zur Richtlinienmodellierung (**Zugriffsrichtlinien > Richtlinienmodellierung**) unterstützt Administratoren bei der Analyse und Behebung von Konfigurationsproblemen innerhalb der Administratorkonsole. Einzelheiten finden Sie unter Richtlinienmodellierungstool.

- **Unterstützung für Filter im Diagramm „Diagnoseprotokolle“**

  Mithilfe der Filteroption im Diagramm „ **Diagnoseprotokolle** “können Administratoren die Suche anhand verschiedener Kriterien wie App-Typ, Kategorie und Beschreibung verfeinern, um die Protokollanalyse und Fehlerbehebung zu vereinfachen. Einzelheiten finden Sie unter Diagnoseprotokolle.

13. März 2024

- **Unterstützt das Beenden aktiver Benutzersitzungen und das Hinzufügen von Benutzern zur Liste deaktivierter Benutzer**

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

12. Februar 2024

- **Allgemeine Verfügbarkeit des Browsers und Antivirenscans**

  Die vom Device Posture-Dienst unterstützten Browser- und Antivirenscans sind jetzt allgemein verfügbar. Einzelheiten finden Sie unter Durch die Gerätehaltung unterstützte Scans.

23. Januar 2024

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

  Die Gerätezertifikatsprüfung mit dem Device Posture-Dienst ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Gerätezertifikatsprüfung mit dem Device Posture-Dienst.

20. Dezember 2023

- **Allgemeine Verfügbarkeit von Secure Private Access vor Ort**

  Citrix Secure Private Access für den lokalen Einsatz ist jetzt allgemein verfügbar. Weitere Einzelheiten finden Sie unter Neuigkeiten.

16. Oktober 2023

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

  Die lokale Lösung Secure Private Access bietet jetzt Folgendes:

  - Admin-Benutzeroberfläche für die Ersteinrichtung.
  - Administrator-Benutzeroberfläche zum Konfigurieren der Anwendungen und Zugriffsrichtlinien.
  - Dashboard „Protokolle“.

  Weitere Einzelheiten finden Sie unter Sicherer privater Zugriff vor Ort.

- **Vorschaufunktionen des Device Posture-Dienstes**

  Der Device Posture-Dienst unterstützt jetzt die folgenden Prüfungen:

  - Der Device Posture-Dienst wird jetzt auf den IGEL-Plattformen unterstützt.
  - Der Device Posture-Dienst unterstützt jetzt Geolokalisierungs- 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. Weitere Einzelheiten finden Sie unter Microsoft Intune-Integration mit Device Posture.

30. August 2023

- **Verwalten des Citrix Endpoint Analysis Client für den Device Posture-Dienst**

  Der EPA-Client kann zusammen mit NetScaler und Device Posture verwendet werden. Bei Verwendung mit NetScaler und Device Posture sind einige Konfigurationsänderungen erforderlich, um den EPA-Client zu verwalten. Einzelheiten finden Sie unter Citrix Endpoint Analysis Client für den Device Posture-Dienst verwalten.

28. August 2023

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

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

Dieses Feature ist als Preview verfügbar.

22. August 2023

- **Gerätezertifikatsprüfung mit dem Citrix Device Posture-Dienst**

  Der Citrix Device Posture-Dienst kann jetzt den kontextbezogenen Zugriff (Smart Access) auf Citrix DaaS- und Secure Private Access-Ressourcen ermöglichen, indem er das Zertifikat des Endgeräts mit einer Unternehmenszertifizierungsstelle vergleicht, um festzustellen, ob das Endgerät vertrauenswürdig ist. Einzelheiten finden Sie unter Gerätezertifikatsprüfung mit dem Device Posture-Dienst.

  Dieses Feature ist als Preview verfügbar.

17. August 2023

- **Device Posture-Ereignisse im Citrix DaaS Monitor**

  Device Posture-Dienstereignisse und Überwachungsprotokolle können jetzt im DaaS Monitor durchsucht werden. Weitere Einzelheiten finden Sie unter Gerätestatusereignisse im Citrix DaaS Monitor.

07. Juni 2023

- **Tool zum Konfigurieren von Secure Workspace Access vor Ort**

  Zum Konfigurieren der Secure Private Access-Lösung vor Ort steht jetzt eine vereinfachte Benutzeroberfläche zur Verfügung. 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 mit diesem Tool Anwendungsbeschränkungen, Verkehrsrouting und NetScaler Gateway-Einstellungen festlegen. Weitere 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 innerhalb einer einzigen Richtlinie unterschiedliche Zugriffsbedingungen für verschiedene Benutzer oder Benutzergruppen konfigurieren. Diese Regeln können separat für HTTP/HTTPS- und TCP/UDP-Anwendungen angewendet

werden, alles innerhalb einer einzigen Richtlinie. Einzelheiten finden Sie unter Konfigurieren einer Zugriffsrichtlinie mit mehreren Regeln.

[SPA-746]

10. April 2023

- **Anwendungserkennung**

  Mithilfe der Anwendungserkennungsfunktion erhält ein Administrator Einblick in die internen privaten Anwendungen wie Webanwendungen und Client-Server-Anwendungen (TCP- und UDP-basierte Anwendungen) in seiner Organisation und in die Benutzer, die auf diese Anwendungen zugreifen. Administratoren können die Apps ermitteln, indem sie den Umfang der Domänen (Platzhalterdomänen) oder IP-Subnetze angeben. Einzelheiten finden Sie unter Anwendungserkennung.

  [ACS-2325]

29. März 2023

- **Secure Private Access-Lösung für lokale Bereitstellungen**

  Als Citrix StoreFront- und NetScaler Gateway-Kunde können Sie jetzt mit der Citrix Secure Private Access-Lösung für lokale Bereitstellungen nahtlos auf die Web- und SaaS-Apps sowie auf Citrix Virtual Apps und virtuelle Desktops zugreifen. Weitere Einzelheiten finden Sie unter Sicherer privater Zugriff vor Ort.

  [SPAOP-1]

07. März 2023

- **Konfigurieren von DNS-Suffixen**

  Die DNS-Suffixfunktion des Citrix Secure Workspace Access-Dienstes kann für die folgenden Anwendungsfälle verwendet werden:

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

Einzelheiten finden Sie unter DNS-Suffixe zum Auflösen von FQDNs in IP-Adressen.

[ACS-2490]

23. Januar 2023

- **Gerätehaltungsdienst**

  Der Citrix Device Posture-Dienst ist eine Cloud-basierte Lösung, die Administratoren dabei hilft, bestimmte Anforderungen durchzusetzen, 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]

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

  Zusätzlich zu den nativen Scans, die der Device Posture-Dienst bietet, kann der Device Posture-Dienst auch in andere Lösungen von Drittanbietern integriert werden. Device Posture ist in Microsoft Endpoint Manager (MEM) unter Windows und macOS integriert. Weitere Einzelheiten finden Sie unter Microsoft Endpoint Manager-Integration 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 Sie bereits über die Citrix Workspace-App angemeldet sind. Diese SSO-Funktionalität verbessert das Benutzererlebnis, indem sie mehrfache Authentifizierungen vermeidet. Einzelheiten finden Sie unter Single Sign-On-Unterstützung für die Workspace-URL.

  [ACS-1888]

- **Aktivieren des Zugriffs auf Apps mithilfe von Zugriffsrichtlinien**

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

  [ACS-3018]

03. Oktober 2022

- **Zugriffsrichtlinien zum Gewähren des Zugriffs auf die Apps**

  Die Konfigurationsoption „App-Abonnenten“wird aus dem Abschnitt „Anwendungen“im Konfigurationsassistenten 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-Dienst unterstützt jetzt den Zugriff auf UDP-Apps. Einzelheiten finden Sie unter Vorschaufunktionen.

  [ACS-1430]

09. September 2022

- **Adaptiver Zugriff basierend auf dem Benutzerrisiko-Score**

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

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

  [ACS-99]

- **Verbesserter Builder für adaptive Zugriffsrichtlinien**

  Der Zugriff auf die Apps wird nun erst aktiviert, wenn die konfigurierten Bedingungen erfüllt sind. Durch das App-Abonnement allein erhalten Ihre Kunden keinen Zugriff auf die Anwendungen. Administratoren müssen Zugriffsrichtlinien hinzufügen, um zusätzlich zum App-Abonnement Zugriff auf die Apps zu gewähren. Darüber hinaus sind Benutzer oder Gruppen eine obligatorische Bedingung in den Zugriffsrichtlinien, die für den Zugriff auf die Apps erfüllt sein muss. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.

  [ACS-1850]

- **Beschränken Sie das Hochladen von Dateien 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, am häufigsten aufgerufene Apps, Diagnoseprotokolle usw. Einzelheiten finden Sie unter Dashboard.

  [ACS-2480]

- **Veraltete Bibliothek**

  Die Secure Private Access-Anwendungen sind jetzt in der Citrix Cloud-Bibliothek nicht sichtbar. Alle für Secure Private Access konfigurierten Anwendungen befinden sich im Anwendungsbereich innerhalb der Secure Private Access-Dienstkachel. Dies erleichtert Administratoren die Navigation sowie die Bearbeitung und Konfiguration der Anwendungen.

  [ACS-1546]

- **Prüfprotokolle für Secure Workspace Access**

  Die mit dem Citrix Secure Private Access-Dienst verbundenen Ereignisse 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 Citrix Secure Private Access-Ereignisse sind jetzt in Citrix Analytics integriert. Citrix Analytics bietet einen öffentlichen Endpunkt, der Administratoren den Zugriff auf die Ereignisse und deren Download ermöglicht. Auf diese Ereignisse kann über ein PowerShell-Skript zugegriffen werden. Weitere Einzelheiten finden Sie unter Diagnoseprotokolle für den Zugriff auf Enterprise-Web- und SaaS-Apps.

  [ACS-805]

- **Anleitung zur Fehlerbehebung**

  Mithilfe des Leitfadens zur Fehlerbehebung können die Administratoren konfigurationsbezogene Probleme beheben. Weitere Einzelheiten finden Sie unter Fehlerbehebung bei App-bezogenen Problemen.

  [ACS-2719]

15. Juli 2022

- **Aktivieren Sie den Zugriff auf eine Anwendung nur, wenn eine Zugriffsrichtlinie konfiguriert ist.**

  Der Zugriff auf die Apps wird 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 adaptive Sicherheit kontextbasiert wie Benutzer, Standort, Gerät und Risiko erzwingen. Administratoren müssen die vorhandenen App-Sicherheitskontrollen und Zugriffsrichtlinien auf das neue Zugriffsrichtlinien-Framework migrieren. Einzelheiten finden Sie unter Migration von App-Sicherheitskontrollen und Zugriffsrichtlinien.

  [ACS-1850]

01. Juni 2022

- **Adaptive Authentifizierung**

  Adaptive Authentifizierung ist jetzt allgemein verfügbar (GA). Ausführliche Informationen zur adaptiven Authentifizierung finden Sie unter Adaptiver Authentifizierungsdienst.

  [CGS-6510]

04. April 2022

- **Änderungen beim Rebranding**

  Der Citrix Secure Workspace Access-Dienst wurde jetzt in Citrix Secure Private Access-Dienst umbenannt.

  [ACS-2322]

- **Vom Administrator geleiteter Workflow für einfaches Onboarding und Einrichten**

  Secure Private Access bietet jetzt eine neue optimierte Administratorerfahrung mit einem schrittweisen Prozess zum Konfigurieren des Zero Trust Network Access auf SaaS-Apps, interne Web-Apps und TCP-Apps. Es umfasst die Konfiguration der adaptiven Authentifizierung, von Anwendungen wie Benutzerabonnements, adaptiven Zugriffsrichtlinien und mehr innerhalb einer einzigen Administratorkonsole. Weitere Einzelheiten finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichten.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

  [ACS-1102]

- **Dashboard „Sicherer privater Zugriff“**

  Über das Secure Private Access-Dashboard haben Administratoren an einem einzigen Ort vollständige Einblicke in ihre Top-Apps, Top-Benutzer, den Integritätsstatus von Konnektoren und die Bandbreitennutzung. 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 Enterprise-Web-Apps.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

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

  Citrix-Kunden können jetzt Zero Trust Network Access (ZTNA) für alle Client-Server-Anwendungen und IP-/Port-basierten Ressourcen sowie für interne 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 gewährleistet. Mit adaptivem Zugriff können Administratoren den Benutzerzugriff auf Apps je nach Kontext präzise und detailliert anpassen. 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 Workspace Access**

  Die mit dem Citrix Secure Private Access-Dienst verbundenen Ereignisse 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 Citrix Secure Private Access-Ereignisse sind jetzt in Citrix Analytics integriert. Citrix Analytics bietet einen öffentlichen Endpunkt, der Administratoren den Zugriff auf die Ereignisse und deren Download ermöglicht. Auf diese Ereignisse kann über ein PowerShell-Skript zugegriffen werden. Weitere 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 Citrix Virtual Apps und Desktops eine adaptive Authentifizierung bereitzustellen. 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-Dienst ist ein von Citrix verwalteter und von Citrix Cloud gehosteter ADC. Einzelheiten finden Sie unter Adaptiver Authentifizierungsdienst.

  Dieses Feature ist als Preview verfügbar.

  [CGS-6510]

16. Februar 2022

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

  Weitere Einzelheiten finden Sie unter Unterstützung für Client-Server-Apps –Vorschau

  [ACS-870]

11. Oktober 2021

- **Zusammenführung der Citrix Gateway-Dienstkachel zu einem einzigen Secure Private Access in Citrix Cloud**

Die Citrix Gateway-Dienstkachel wird jetzt in Citrix Cloud zu einem einzigen Secure Private Access 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 und kontextbezogenen Richtlinien sowie Webfilterrichtlinien verwenden.
- Alle Citrix DaaS-Kunden können den Citrix Gateway-Dienst weiterhin als HDX-Proxy in der Workspace-Konfiguration aktivieren. Allerdings wurde die Verknüpfung zum Aktivieren des Citrix Gateway-Dienstes über die Kachel des Gateway-Dienstes entfernt. Sie können den Citrix Gateway-Dienst unter **Arbeitsbereichskonfiguration > Zugriff > Externe Konnektivität**aktivieren. Einzelheiten finden Sie unter Externe Konnektivität. Sonst ändert sich die Funktionalität nicht.

[NGSWS-16761]

30. Juli 2021

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

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

  [ACS-833]

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

  Administratoren können jetzt eine bestimmte Web- oder SaaS-App aus dem Citrix Workspace-Portal ausblenden. Wenn eine App im Citrix Workspace-Portal ausgeblendet ist, gibt der Citrix Gateway-Dienst 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 zum Weiterleiten des App-Datenverkehrs**

  Administratoren können jetzt die Routentabelle verwenden, um die Regeln für die Weiterleitung des App-Datenverkehrs direkt ins Internet oder über den Citrix 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 May 2021

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

  Die kontextbezogene Zugriffsfunktion des Citrix Secure Private Access-Dienstes bietet einen umfassenden Zero-Trust-Zugriffsansatz, der sicheren Zugriff auf die Anwendungen gewährleistet. Durch den kontextbezogenen Zugriff können Administratoren einen granularen Zugriff auf die Apps gewähren, auf die Benutzer kontextabhängig 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 Citrix Gateway Connector-Benutzeroberfläche**

  Die Benutzeroberfläche des Citrix Cloud Gateway Connectors wird gemäß den Citrix-Markenrichtlinien umbenannt.

  [NGSWS-17100]

01 May 2021

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

  Kundendaten, einschließlich Backups, werden 90 Tage nach Ablauf der Serviceberechtigung aus dem Datenspeicher des Citrix Secure Private Access-Dienstes gelöscht.

  [ACS-388]

- **Vereinfachte Schritte zum Föderieren einer Domäne von Azure AD zu Citrix Workspace**

  Die Schritte zum Föderieren einer Domäne von Azure AD zur Citrix Workspace-App sind jetzt vereinfacht, um ein schnelleres Onboarding in Citrix Workspace zu ermöglichen. Die Domänenföderation kann jetzt in der Benutzeroberfläche des Citrix Gateway-Dienstes auf der Seite „Single Sign-On“durchgeführt werden.

  [ACS-351]

- **Erweiterung des Konnektivitätstest-Tools**

  Das Konnektivitätstesttool im Citrix Gateway Connector wurde erweitert, um Timeout-Fehler zu verarbeiten und die erforderlichen Protokolle zu generieren.

[NGSWS-17212]

15. März 2021

- **Plattformverbesserungen**

  Es wurden verschiedene Plattformverbesserungen vorgenommen, um die Zuverlässigkeit bei der Übertragung der Administratorkonfigurationen des Kunden an die Citrix Gateway Connectors zu erhöhen.

  [ACS-85]

- **Verbesserte Leistung von Web-Apps**

  Die Leistung der Web-Apps wurde verbessert, wenn über den Systembrowser mithilfe eines clientlosen VPN auf die Web-Anwendungen zugegriffen wird.

  [NGSWS-16469]

- **Aktivieren des Citrix Gateway Connectors zur Verwendung von TLS1.2 Grade A oder höher-Verschlüsselungssammlungen**

  Der Citrix Gateway Connector verwendet jetzt TLS1.2 mit Verschlüsselungssammlungen der Klasse A oder höher, um eine Verbindung mit dem Citrix Cloud-Dienst und anderen Back-End-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

- **Erweiterte Sicherheitsoption zum Starten von SaaS- und Enterprise-Web-Apps innerhalb des Remote Browser Isolation-Dienstes**

  Administratoren können jetzt die erweiterte Sicherheitsoption **verwenden. Wählen Sie „Anwendung immer im Citrix Remote Browser Isolation-Dienst starten** “, um eine Anwendung immer im Remote Browser Isolation-Dienst zu starten, unabhängig von anderen erweiterten Sicherheitseinstellungen.

  [ACS-123]

08. Oktober 2020

- **Konfigurieren von Sitzungstimeouts für die Citrix Secure Workspace Access-Browsererweiterung**

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

  [NGSWS-13754]

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

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

  [NGSWS-14427]

24. September 2020

- **Aktivieren Sie den VPN-losen Zugriff auf Enterprise-Web-Apps über einen lokalen Browser**

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

  [ACS-286]

07. Juli 2020

- **Überprüfen der Kerberos-Konfiguration auf dem Citrix Gateway Connector**

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

  [NGSWS-8581]

19. Juni 2020

- **Nur-Lese-Zugriff auf Administratoren des Citrix Gateway-Dienstes und des Citrix Secure Private Access-Dienstes**

  Sicherheitsadministratorteams, die den Citrix Gateway-Dienst verwenden, können jetzt detaillierte Steuerelemente bereitstellen, z. B. schreibgeschützten Zugriff für Administratoren des Citrix Gateway-Dienstes und des Citrix Secure Private Access-Dienstes.

- Administratoren mit schreibgeschütztem Zugriff auf den Citrix Gateway-Dienst können nur die App-Details anzeigen.
- Administratoren mit schreibgeschütztem Zugriff auf den Citrix Secure Workspace Access-Dienst können die Inhaltszugriffseinstellungen nur anzeigen.

[ACS-205]

08 May 2020

- **Neue Tools zur Fehlerbehebung in Citrix Gateway Connector 13.0**
  - **Netzwerkablaufverfolgung:** Sie können jetzt die Funktion **Ablaufverfolgung** verwenden, um Registrierungsprobleme beim Citrix Gateway Connector zu beheben. Sie können die Ablaufverfolgungsdatei herunterladen und zur Fehlerbehebung an die Administratoren weitergeben. Weitere Informationen finden Sie unter Beheben von Registrierungsproblemen beim Citrix 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 Citrix Gateway Connector.

    [NGSWS-8580]

Version 2019.04.02

- **Kerberos-Authentifizierungsunterstützung für Citrix Gateway Connector zum ausgehenden Proxy** [NGSWS-6410]

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

Version 2019.04.01

- **Der Datenverkehr von Web-/SaaS-Apps kann jetzt über einen im Unternehmensnetzwerk gehosteten Gateway-Connector geleitet 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 für diese App zu authentifizieren und ihn über einen lokalen Gateway Connector laufen zu lassen.

Nehmen wir beispielsweise an, ein Kunde verfügt über eine durch Okta geschützte SaaS-App (wie Workday). Der Kunde möchte möglicherweise, dass der Authentifizierungsverkehr zum Okta-Server über einen lokalen Gateway Connector über den Citrix Gateway-Dienst geleitet wird, obwohl der eigentliche Workday-Datenverkehr nicht über den Citrix Gateway-Dienst geleitet wird. Auf diese Weise kann ein Kunde eine Zwei-Faktor-Authentifizierung vom Okta-Server vermeiden, da der Benutzer sich innerhalb des Unternehmensnetzwerks mit dem Okta-Server verbindet.

[NGSWS-6445]

- **Filtern von Website-Listen und Website-Kategorisierung deaktivieren**. Das Filtern von Website-Listen und die Website-Kategorisierung können deaktiviert werden, wenn der Administrator diese Funktionen für einen bestimmten Kunden nicht anwenden möchte.

  [NGSWS-6532]

- **Automatisches Georouting für Weiterleitungen des Remote Browser Isolation-Dienstes.** Für Umleitungen des Remote Browser Isolation-Dienstes ist jetzt das automatische Georouting aktiviert.

  [NGSWS-6926]

Version 2019.03.01

- **Die Schaltfläche „Erkennen“wurde auf der Seite „Gateway-Connector hinzufügen “hinzugefügt.** Mit der Schaltfläche „ **Erkennen** “wird die Liste der Konnektoren aktualisiert, sodass der neu hinzugefügte Konnektor im Abschnitt „Konnektivität der Web-App“angezeigt wird.

  [CGOP-6358]

- **Eine neue Kategorie „Bösartig und gefährlich“wurde in den Kategorien „Zugriffskontrolle –Webfilterung“hinzugefügt.** Eine neue Kategorie mit dem Namen **Bösartig und gefährlich** in den Kategorien **Zugriffskontrolle** –**Webfilterung** wird unter der Gruppe **Malware und Spam** hinzugefügt.

  [CGOP-6205]

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

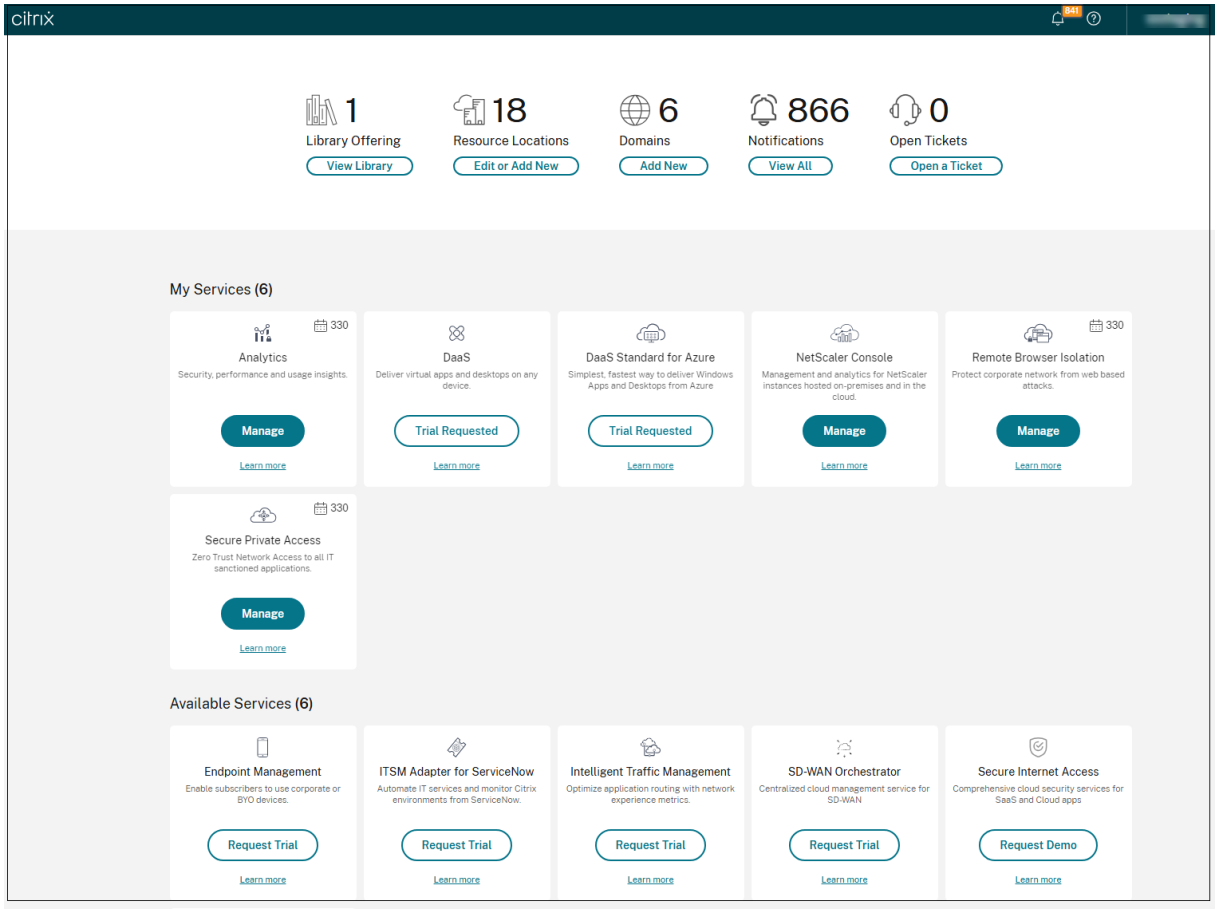
Schritt 1: **Melden Sie sich für Citrix Cloud an**

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-Servicelösung

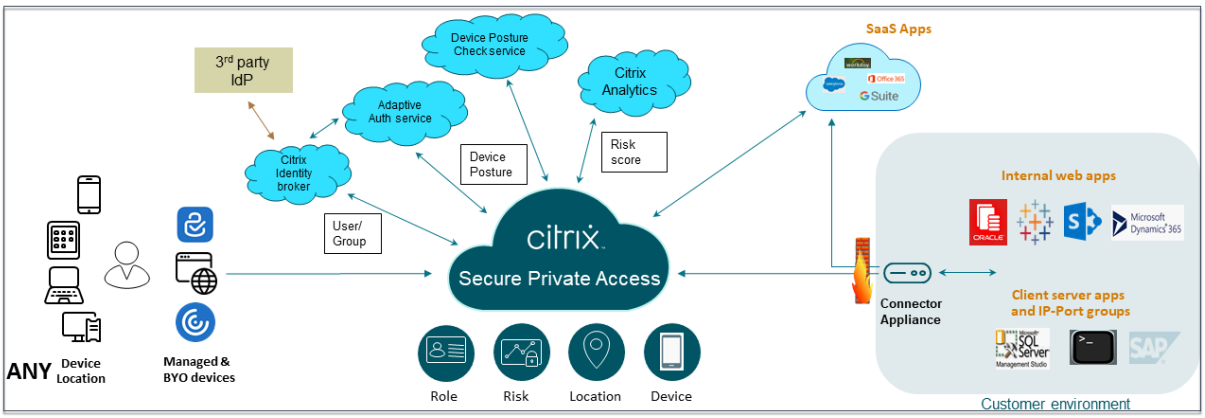
October 21, 2024

Lösungsübersicht

Herkömmliche VPN-Lösungen erfordern die Verwaltung von Endbenutzergeräten, ermöglichen den Zugriff auf Netzwerkebene und setzen statische Zugriffskontrollrichtlinien durch. Citrix Secure Private Access bietet der IT eine Reihe von Sicherheitskontrollen zum Schutz vor Bedrohungen durch

BYO-Geräte und gibt Benutzern die Möglichkeit, von jedem Gerät aus auf ihre von der IT genehmigten Anwendungen zuzugreifen, unabhängig davon, ob es verwaltet wird oder BYO.

Citrix Secure Private Access bietet adaptive Authentifizierung, Single Sign-On-Unterstützung und erweiterte Sicherheitskontrollen für die Anwendungen. Secure Private Access bietet außerdem die Möglichkeit, das Endbenutzergerät vor dem Aufbau 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 die Gerätehaltung, den geografischen Standort, das Netzwerksegment und die Organisation/Abteilungszugehörigkeit des Benutzers identifizieren. Basierend auf den erhaltenen Informationen kann ein Administrator festlegen, wie er Benutzer bei seinen von der IT genehmigten Apps authentifizieren möchte. Auf diese Weise können Organisationen für alle Ressourcen, einschließlich öffentlicher SaaS-Apps, privater Web-Apps, privater Client-Server-Apps und Desktops as a Service (DaaS), dasselbe Framework für die Authentifizierungsrichtlinie implementieren. Einzelheiten finden Sie unter Adaptive Security.

Anwendungszugriff

Secure Private Access kann eine Verbindung zu den lokalen Web-Apps herstellen, ohne auf ein VPN angewiesen zu sein. Diese VPN-lose Verbindung verwendet ein lokal bereitgestelltes Connector Appliance. Das Connectorgerät erstellt einen ausgehenden Steuerungskanal 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

Mithilfe der adaptiven Authentifizierung können Unternehmen strenge Authentifizierungsrichtlinien bereitstellen und so das Risiko kompromittierter Benutzerkonten 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.

Browser-Sicherheit

Secure Private Access ermöglicht Endbenutzern das sichere Surfen im Internet mit einem zentral verwalteten und sicheren 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 kann. Einzelheiten finden Sie unter Browsersicherheit.

Gerätehaltung

Mit dem Device Posture Service kann ein Administrator Richtlinien definieren, um die Haltung von Endpunktgeräten zu überprüfen, die versuchen, remote auf Unternehmensressourcen zuzugreifen. Basierend auf dem Konformitätsstatus eines Endpunkts kann der Gerätestatusdienst den Zugriff auf Unternehmensanwendungen und -Desktops verweigern oder eingeschränkten/vollständigen Zugriff gewähren.

Wenn ein Endbenutzer eine Verbindung mit Citrix Workspace initiiert, sammelt der Device Posture-Client Informationen zu den Endpunktparametern und gibt diese Informationen an den Device Posture-Dienst weiter, um zu bestimmen, ob die Haltung des Endpunkts die Richtlinienanforderungen erfüllt.

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

Unterstützung für TCP- und UDP-Anwendungen

Manchmal benötigen Remotebenutzer Zugriff auf private Client-Server-Apps, deren Front-End auf dem Endpunkt und deren Back-End in einem Rechenzentrum liegt. Organisationen können zu Recht strenge Sicherheitsrichtlinien für diese internen und privaten Apps durchsetzen und es Remotebenutzern so erschweren, auf diese Anwendungen zuzugreifen, ohne die Sicherheitsprotokolle zu gefährden.

Der Secure Private Access-Dienst behebt die Sicherheitslücken von TCP und UDP, indem er ZTNA ermöglicht, sicheren Zugriff auf diese Apps zu gewähren. Benutzer können jetzt über einen nativen

Browser oder eine native Clientanwendung über den auf ihren Computern ausgeführten Citrix Secure Access-Client auf alle privaten Apps zugreifen, einschließlich TCP-, UDP- und HTTPS-Apps.

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

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

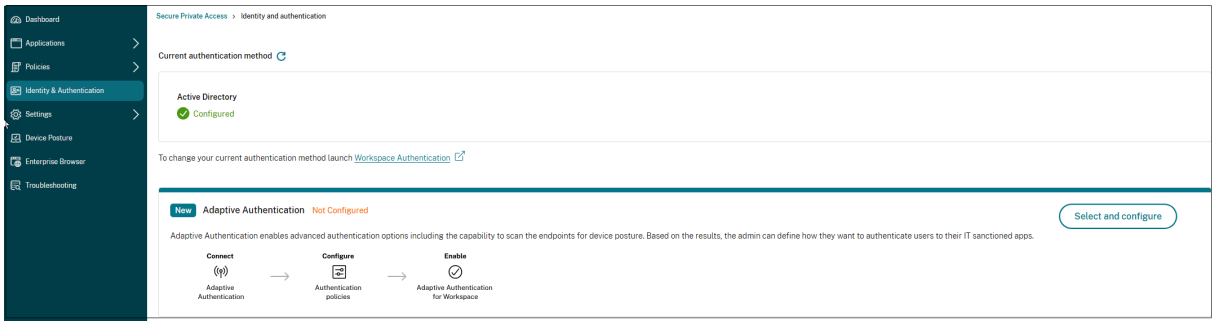
Einzelheiten finden Sie unter Unterstützung für Client-Server-Apps.

Einrichten von Citrix Secure Workspace Access

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

Einrichten von Identität und Authentifizierung

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.

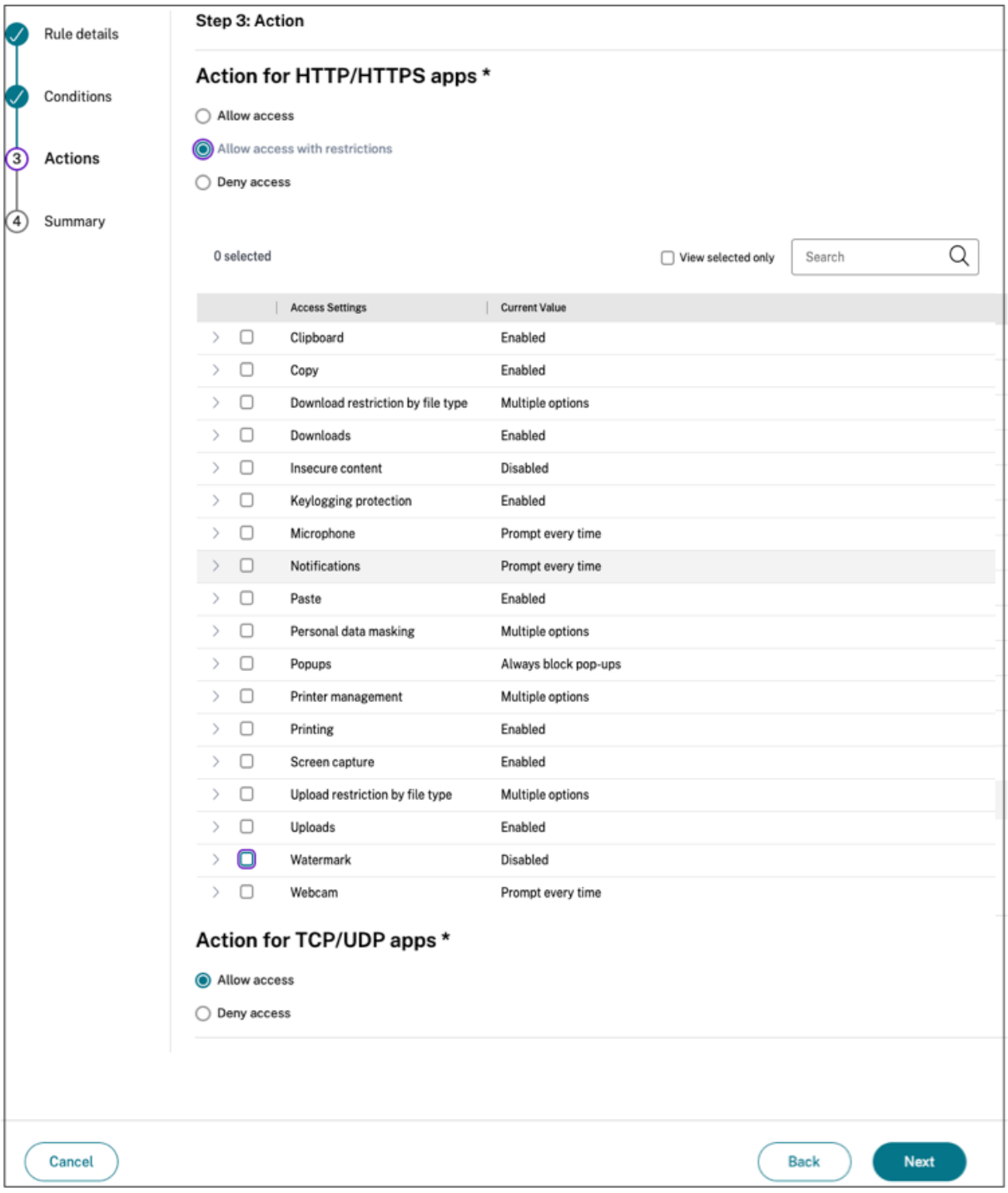
Aufzählen und Veröffentlichen von Apps

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

Erweiterte Sicherheitskontrollen aktivieren

Zum Schutz von Inhalten integrieren Unternehmen erweiterte Sicherheitsrichtlinien in die SaaS-Anwendungen. Jede Richtlinie erzwingt eine Einschränkung des Citrix Enterprise Browsers bei Verwendung der Workspace-App für den Desktop oder des Secure Browsers bei Verwendung der Workspace-App im Web oder auf Mobilgeräten.

- **Zugriff auf die Zwischenablage einschränken**: Deaktiviert Ausschneiden/Kopieren/Einfügen-Vorgänge zwischen der App und der Systemzwischenablage.
- **Drucken einschränken**: Deaktiviert die Möglichkeit zum Drucken aus dem Citrix Enterprise Browser heraus.
- **Downloads einschränken**: Deaktiviert die Möglichkeit des Benutzers, aus der App heraus Downloads durchzuführen.
- **Uploads einschränken**: Deaktiviert die Möglichkeit des Benutzers, innerhalb der App hochzuladen.
- **Wasserzeichen anzeigen**: Zeigt auf dem Benutzerbildschirm ein Wasserzeichen mit dem Benutzernamen und der IP-Adresse des Computers des Benutzers an.
- **Keylogger einschränken**: Schützt vor Keyloggern. Wenn ein Benutzer versucht, sich mit Benutzernamen und Kennwort bei der App anzumelden, werden alle Schlüssel auf den Keyloggern verschlüsselt. Darüber hinaus sind sämtliche Aktivitäten, die der Benutzer in der App ausführt, gegen Keylogging geschützt. Wenn beispielsweise App-Schutzrichtlinien für Office 365 aktiviert sind und der Benutzer ein Office 365-Word-Dokument bearbeitet, werden alle Tastenanschläge in Keyloggern verschlüsselt.
- **Bildschirmaufnahme einschränken**: Deaktiviert die Möglichkeit, Bildschirme mit Bildschirmaufnahmeprogrammen oder -apps aufzunehmen. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm erfasst.



Einzelheiten finden Sie unter Konfigurieren einer Zugriffsrichtlinie.

Aktivieren Sie den Citrix Enterprise Browser für Anwendungsstarts

Secure Private Access ermöglicht Endbenutzern, ihre Apps mit dem Citrix Enterprise Browser (CEB) zu starten. CEB ist ein Chromium-basierter 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-Domänen in einer sicheren und kontrollierten Umgebung zu öffnen.

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

Konfiguration mit API:

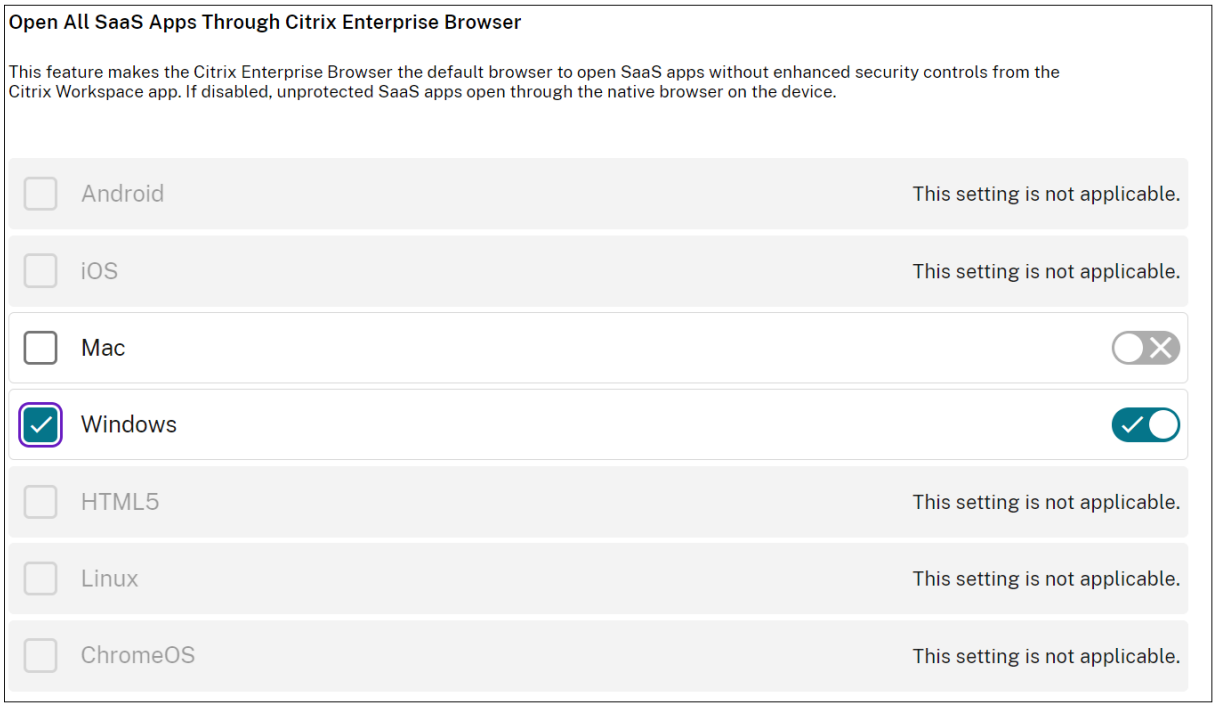
Zur Konfiguration finden Sie hier eine Beispiel-JSON-Datei, um Citrix Enterprise Browser standardmäßig für alle Apps zu aktivieren:

```
"settings": [
                    {

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

                    ]
```

Der Standardwert ist true.

Konfiguration über GUI:

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



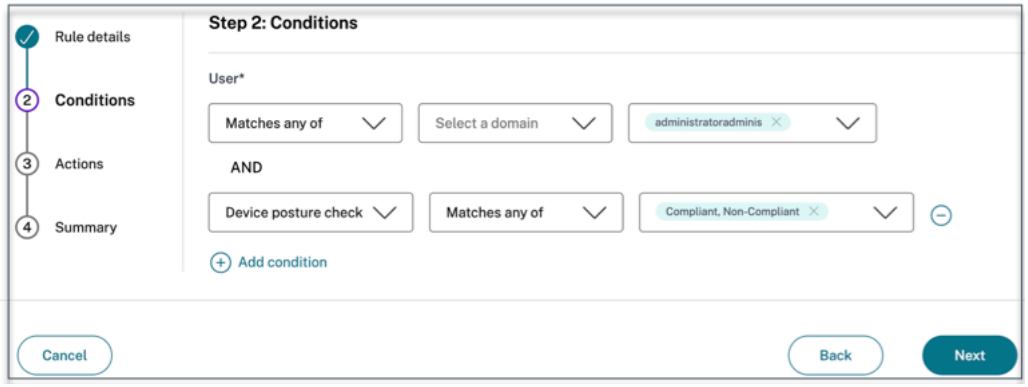
Einzelheiten finden Sie unter Verwalten des Citrix Enterprise Browsers über GACS.

Konfigurieren von Tags für den kontextbezogenen Zugriff mithilfe von Device Posture

Nach der Überprüfung der Gerätehaltung darf sich das Gerät anmelden und wird als konform oder nicht konform klassifiziert. Diese Klassifizierung wird dem Secure Private Access-Dienst als Tags zur Verfügung gestellt und wird verwendet, um kontextbezogenen Zugriff basierend auf der Gerätehaltung zu ermöglichen.

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Kachel „Secure Private Access“auf **Verwalten**.
3. Klicken Sie in der linken Navigation auf **Zugriffsrichtlinien** und dann auf **Richtlinie erstellen**.
4. Geben Sie den Richtliniennamen und eine Beschreibung der Richtlinie ein.
5. Wählen Sie unter **Anwendungen**die App oder die Gruppe von Apps aus, für die diese Richtlinie erzwungen werden soll.
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 obligatorische Bedingung, die erfüllt werden muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren.

9. Klicken Sie auf **+** , um die Gerätehaltungsbedingung hinzuzufügen.
10. Wählen Sie **Gerätehaltungsprüfung** und den logischen Ausdruck aus dem Dropdown-Menü.
11. Geben Sie in benutzerdefinierten Tags einen der folgenden Werte ein:



- **Konform** - Für kompatible Geräte
- **Nicht konform** - Für nicht konforme Geräte

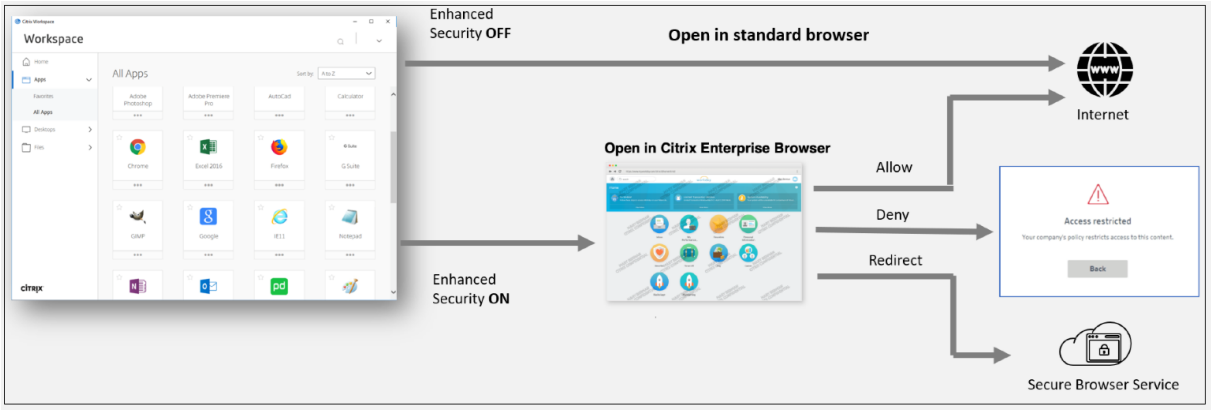
12. Klicken Sie auf **Weiter**.
13. Wählen Sie die Aktionen aus, die basierend auf der Bedingungsauswertung angewendet werden müssen, und klicken Sie dann auf **Weiter**.

    Auf der Seite „Zusammenfassung“werden die Richtliniendetails angezeigt.
14. Überprüfen Sie die Angaben und klicken Sie auf **Fertig stellen**.

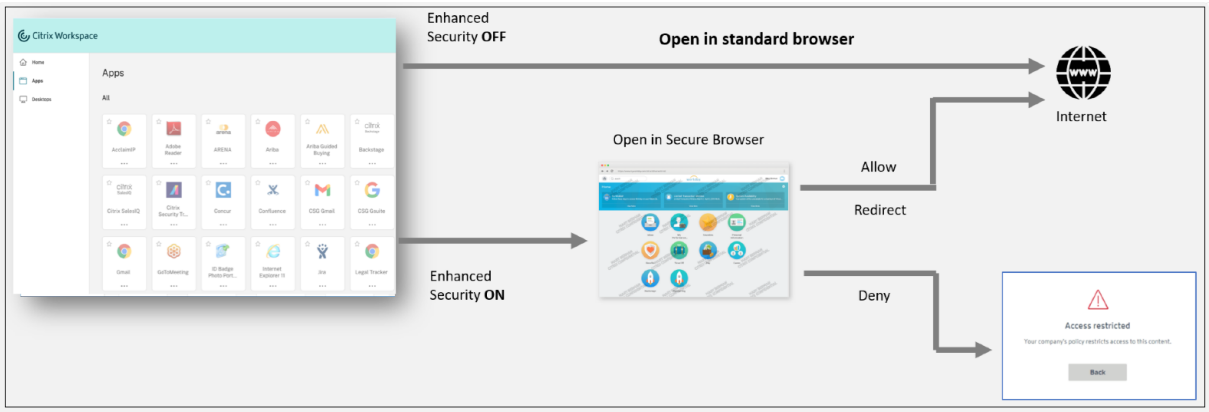
> **Hinweis:**
>
> Jede Secure Private Access-Anwendung, die in der Zugriffsrichtlinie nicht als konform oder nicht konform gekennzeichnet ist, wird als Standardanwendung behandelt und ist auf allen Endpunkten unabhängig vom Gerätestatus zugänglich.

Erfahrung für Endbenutzer

Der Citrix-Administrator hat die Möglichkeit, 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-Web-Benutzeroberfläche 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 bei deaktivierter erweiterter Sicherheit auf die SaaS-Anwendung klickt, wird die Anwendung in einem lokal installierten Standardbrowser geöffnet. Wenn der Administrator die erweiterte Sicherheit aktiviert hat, werden die SaaS-Apps auf dem CEB innerhalb der Workspace-App geöffnet. Der Zugriff auf Hyperlinks in SaaS-Apps und Web-Apps wird basierend auf den Richtlinien für nicht genehmigte Websites kontrolliert. Einzelheiten zu nicht genehmigten Websites finden Sie unter Nicht genehmigte Websites.



Ähnlich verhält es sich mit dem Workspace-Webportal: Wenn die erweiterte Sicherheit deaktiviert ist, werden SaaS-Anwendungen in einem nativ installierten Standardbrowser geöffnet. Wenn die erweiterte Sicherheit aktiviert ist, werden SaaS-Apps im sicheren Remote-Browser geöffnet. Benutzer können auf die Websites innerhalb von SaaS-Apps basierend auf den Richtlinien für nicht genehmigte Websites zugreifen. Einzelheiten zu nicht genehmigten Websites finden Sie unter Nicht genehmigte Websites.

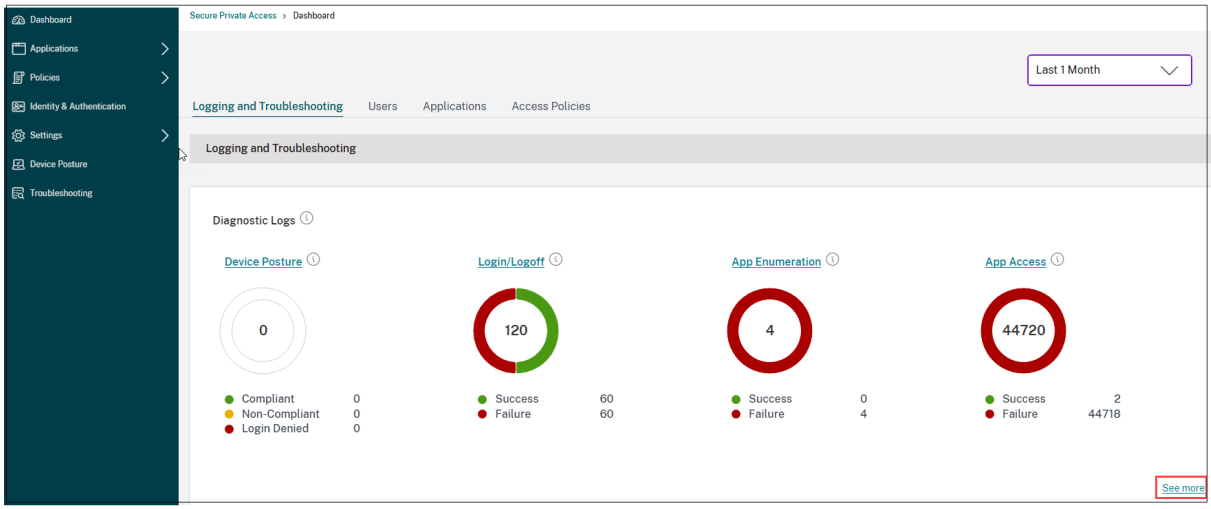
Analyse-Dashboard

Das Dashboard des Secure Private Access-Dienstes zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Über das Dashboard haben Administratoren an einem einzigen Ort vollständige Einblicke in den Integritätsstatus ihrer Apps, Benutzer und Konnektoren sowie in die Band-

breitennutzung. Diese Daten werden von Citrix Analytics abgerufen. Die Metriken werden grob in die folgenden Kategorien eingeteilt.

- Protokollierung und Fehlerbehebung
- Benutzer
- Anwendungen
- Zugriffsrichtlinien

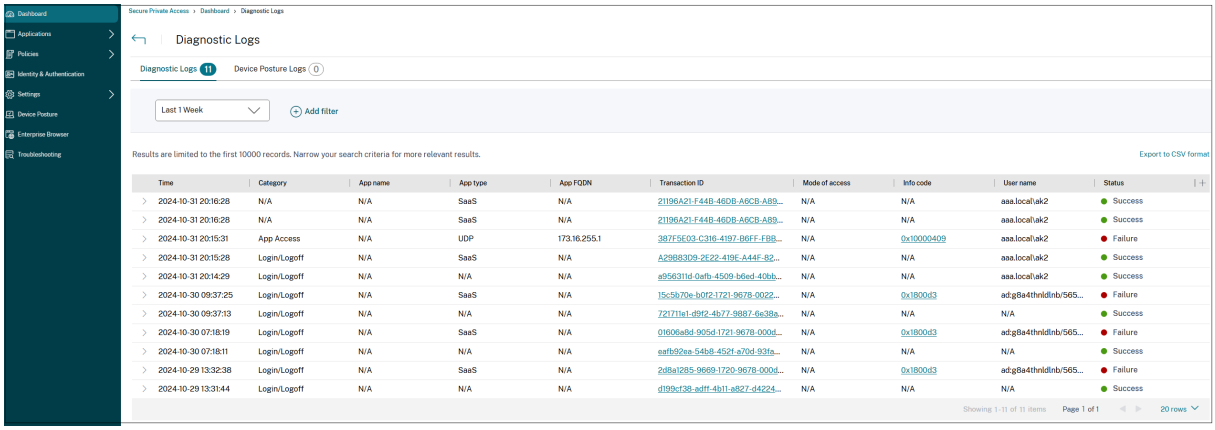
Einzelheiten finden Sie unter Dashboard.



Beheben von App-Problemen

Das Diagramm „Diagnoseprotokolle“im Secure Private Access-Dashboard bietet Einblick in die Protokolle im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Aufzählung und Gerätestatusprotokollen.

- **Infocode**: Einige Protokollereignisse wie z. B. Fehler haben einen zugehörigen Infocode. Durch Klicken auf den Infocode werden die Benutzer zu den Lösungsschritten oder weiteren Informationen zu diesem Ereignis weitergeleitet.
- **Transaktions-ID**: Die Diagnoseprotokolle zeigen auch eine Transaktions-ID an, die alle Secure Private Access-Protokolle für eine Zugriffsanforderung korreliert. Für eine App-Zugriffsanforderung können mehrere Protokolle generiert werden, beginnend mit der Authentifizierung, dann der App-Aufzählung innerhalb der Arbeitsbereichs-App und schließlich dem App-Zugriff selbst. Alle diese Ereignisse generieren eigene Protokolle. Die Transaktions-ID wird zum Korrelieren aller dieser Protokolle verwendet. Sie können die Diagnoseprotokolle mithilfe der Transaktions-ID filtern, um alle Protokolle zu finden, die sich auf eine bestimmte App-Zugriffsanforderung beziehen. Weitere Einzelheiten finden Sie unter Beheben von Secure Private Access-Problemen.



Beispiele für Anwendungsfälle

- Greifen Sie mithilfe eines Zero-Trust-Ansatzes auf interne Anwendungen (Web/TCP/UDP) zu, ohne den eingehenden Datenverkehr auf der Firewall zu öffnen.
- Wechseln Sie zu einem Zero-Trust-Ansatz, indem Sie die von Benutzern aufgerufenen Anwendungen ermitteln
- Beschränken Sie den Zugriff auf SaaS-Anwendungen auf den Citrix Enterprise Browser
- Beschränken Sie den Zugriff auf SaaS-Anwendungen auf öffentliche IP-Adressen des Unternehmens.
- 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
- Administratorgeführter Workflow für einfaches Onboarding und Einrichten

Referenzvideos

- Zero Trust Network Access (ZTNA) auf Apps
- Privater Web-App-Zugriff mit Citrix Secure Workspace Access
- Öffentlicher SaaS-App-Zugriff mit Citrix Secure Private Access
- Privater Client-Server-App-Zugriff mit Citrix Secure Private Access

- Keylogger-Schutz mit Citrix Secure Workspace Access
- Bildschirmfreigabeschutz mit Citrix Secure Workspace Access
- Endbenutzererfahrung mit Citrix Secure Workspace Access
- ZTNA versus VPN-Anmeldeerfahrung mit Citrix Secure Private Access
- ZTNA versus VPN-Portscans mit Citrix Secure Private Access

Neuigkeiten zu 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

Administratorgeführter Workflow für einfaches Onboarding und Einrichten

October 21, 2024

Im Secure Private Access-Dienst ist eine neue optimierte Administratorerfahrung mit einem schrittweisen Prozess zum Konfigurieren des Zero Trust Network Access für SaaS-Apps, interne Web-Apps und TCP-Apps verfügbar. Es umfasst die Konfiguration der adaptiven Authentifizierung, von Anwendungen wie Benutzerabonnements, adaptiven Zugriffsrichtlinien und mehr innerhalb einer einzigen Administratorkonsole.

Dieser Assistent unterstützt Administratoren dabei, entweder beim Onboarding oder bei wiederholter Verwendung eine fehlerfreie Konfiguration zu erreichen. Außerdem ist ein neues Dashboard mit vollständiger Transparenz der allgemeinen Nutzungsmetriken und anderer wichtiger Informationen verfügbar.

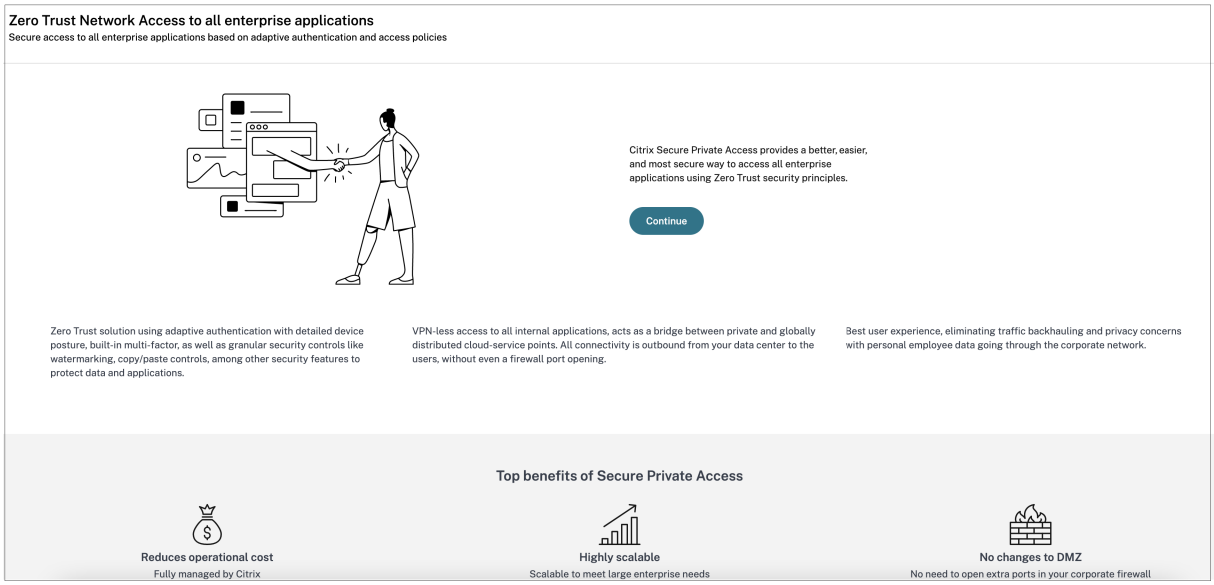
Die wichtigsten Schritte umfassen Folgendes:

1. Wählen Sie die Authentifizierungsmethode für die Abonnenten zur Anmeldung bei Citrix Workspace.
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 App-Konfiguration.

Greifen Sie auf den Administrator-Workflow-Assistenten von Secure Workspace Access zu

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

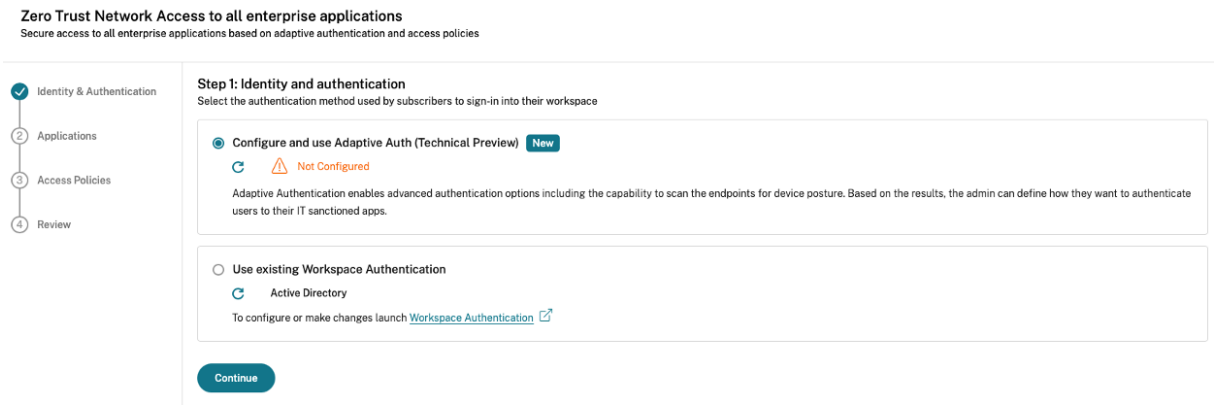
1. Klicken Sie auf der Service-Kachel **Secure Private Access** auf **Verwalten**.
2. Klicken Sie auf der Übersichtsseite auf **Weiter**.



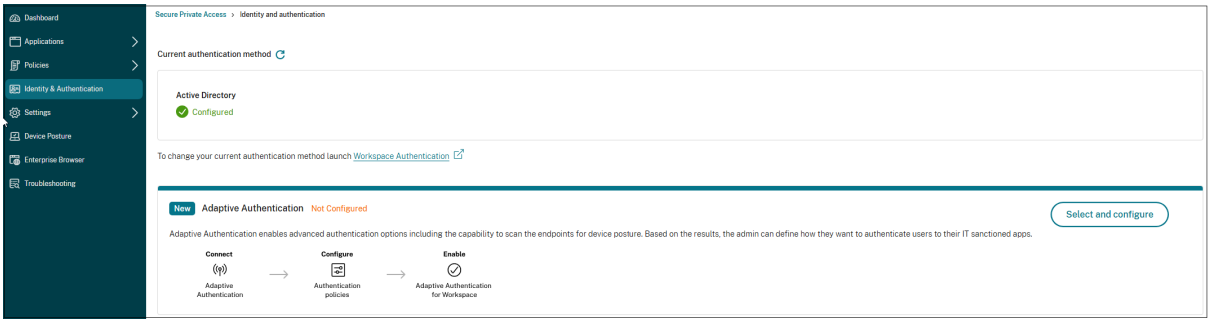
Schritt 1: Identität und Authentifizierung einrichten

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, verwalteter und in der Cloud gehosteter Citrix ADC, der alle erweiterten Authentifizierungsfunktionen wie die folgenden bereitstellt.

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



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



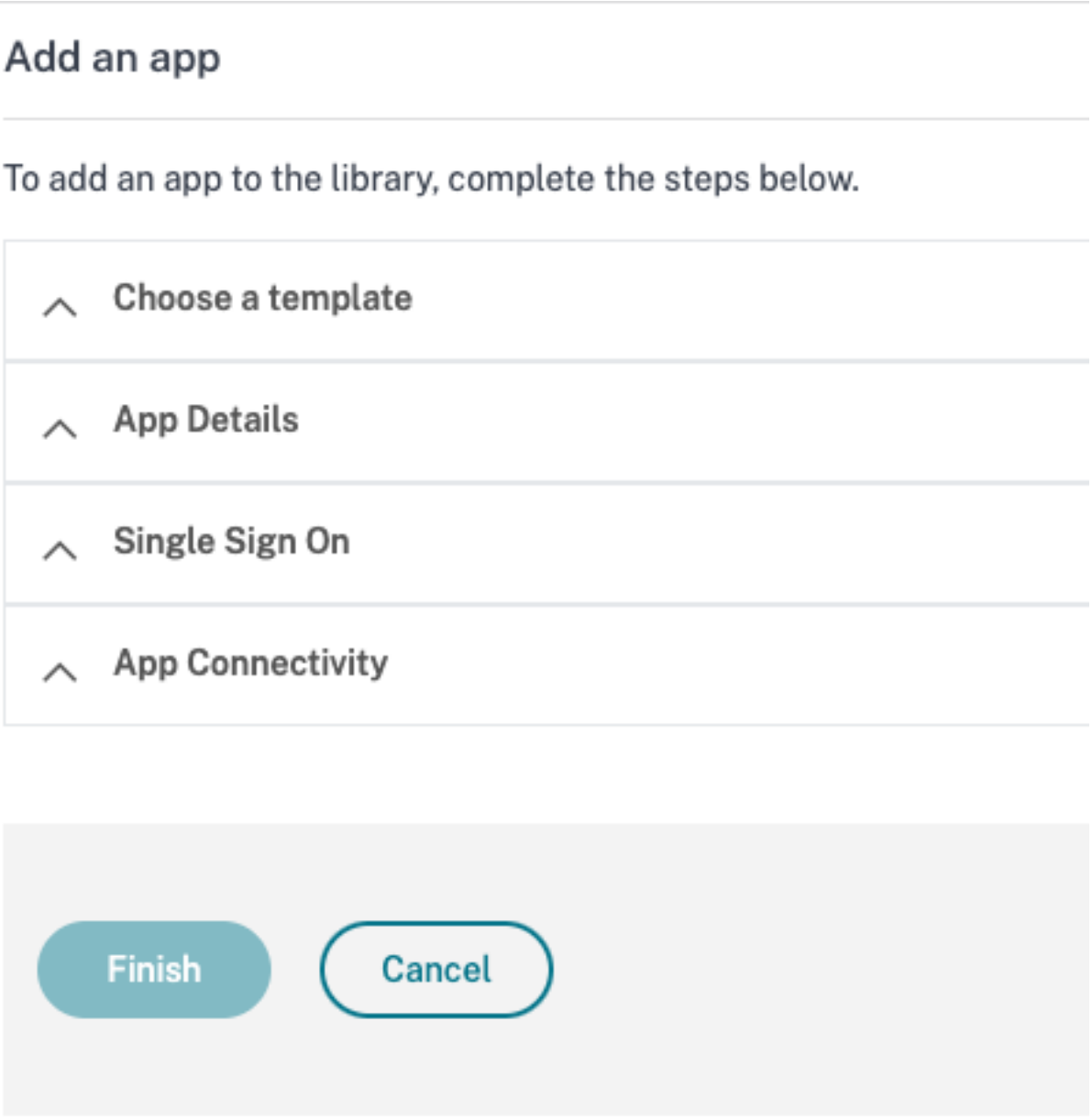
Um die vorhandene Authentifizierungsmethode zu ändern oder die vorhandene Authentifizierungsmethode zu ändern, klicken Sie auf **Arbeitsbereichsauthentifizierung**.

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. Sie können von dieser Seite SaaS-Apps, Web-Apps und TCP/UDP-Apps hinzufügen. Um eine App hinzuzufügen, klicken Sie auf **App hinzufügen**.

Sobald Sie eine App hinzufügen, wird sie hier aufgelistet angezeigt.

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



- **Hinzufügen einer Enterprise-Web-App**
  - Unterstützung für Enterprise-Web-Apps
  - Konfigurieren des direkten Zugriffs auf Web-Apps
- **Hinzufügen einer SaaS-App**
  - Unterstützung für Software-as-a-Service-App
  - SaaS-App-Server-spezifische Konfiguration
- **Konfigurieren von Client-Server-Apps**
  - Unterstützung für Client-Server-Apps

- **Starten einer App**
  - Starten einer konfigurierten App –Endbenutzer-Workflow
- **Aktivieren Sie schreibgeschützten Zugriff für Administratoren**
  - Schreibgeschützter Zugriff für Administratoren auf SaaS und Web-Apps

Schritt 3: Konfigurieren einer Zugriffsrichtlinie mit mehreren Regeln

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

Mithilfe der Zugriffsrichtlinien in Secure Private Access können Sie den Zugriff auf die Apps basierend auf dem Kontext des Benutzers oder des Geräts des Benutzers aktivieren oder deaktivieren. Darüber hinaus können Sie den eingeschränkten Zugriff auf die Apps aktivieren, indem Sie die folgenden Sicherheitsbeschränkungen hinzufügen:

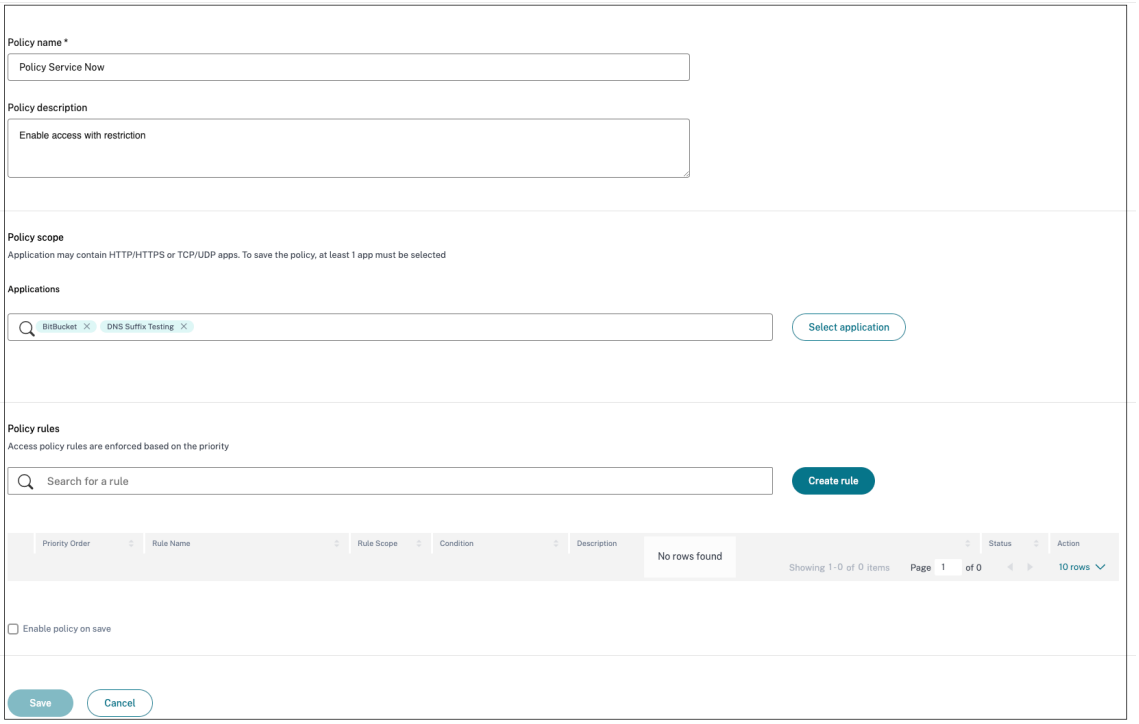
- Zugriff auf Zwischenablage einschränken
- Drucken einschränken
- Downloads einschränken
- Uploads einschränken
- Wasserzeichen anzeigen
- Beschränken Sie die Tastenprotokollierung
- Bildschirmaufnahme einschränken

Weitere Informationen zu diesen Einschränkungen finden Sie unter Verfügbare Zugriffsbeschränkungen.

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, wird sie hier aufgelistet angezeigt.

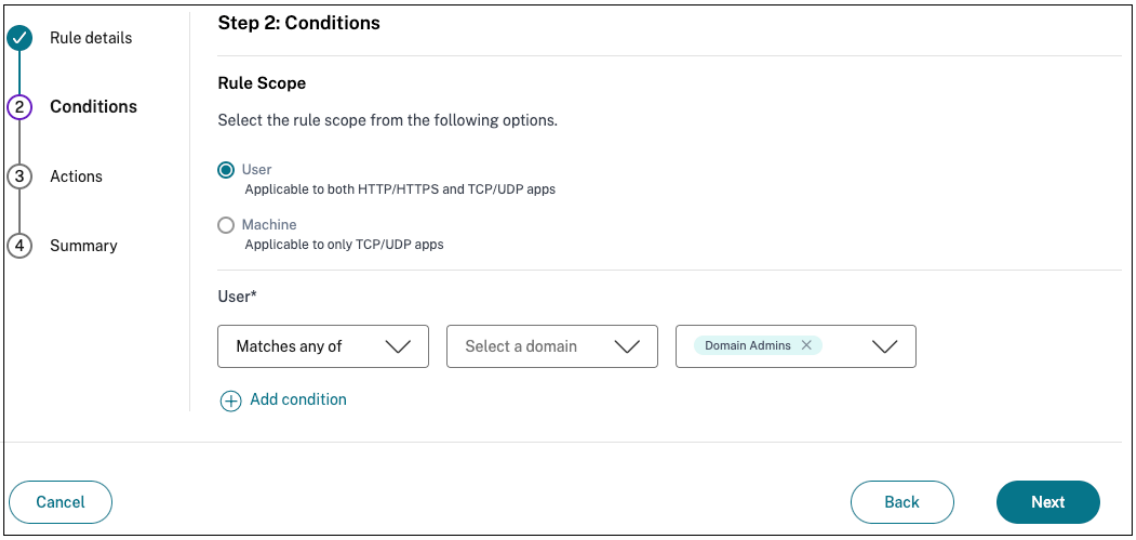
2. Geben Sie den Richtliniennamen und eine Beschreibung der Richtlinie ein.
3. Wählen Sie unter **Anwendungen**die App oder die Gruppe von Apps aus, für die diese Richtlinie erzwungen werden soll.
4. Klicken Sie auf **Regel erstellen** , um Regeln für die Richtlinie zu erstellen.



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 Bedingung **Benutzer** ist eine obligatorische Bedingung, die erfüllt werden muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren. Wählen Sie eine Option aus:

- **Entspricht einem der Werte** –Nur den Benutzern oder Gruppen, die mit einem der im Feld aufgeführten Namen übereinstimmen und zur ausgewählten Domäne gehören, wird der Zugriff gestattet.
- **Stimmt mit keiner überein** - Allen Benutzern oder Gruppen außer den im Feld aufgeführten und zur ausgewählten Domäne gehörenden Benutzern oder Gruppen wird der Zugriff gestattet.



7. (Optional) Klicken Sie auf +, um kontextabhängig mehrere Bedingungen hinzuzufügen.

   Wenn Sie kontextbasierte Bedingungen hinzufügen, wird eine UND-Operation auf die Bedingungen angewendet. Dabei wird die Richtlinie nur ausgewertet, wenn die **Benutzer** und die optionalen kontextbasierten Bedingungen erfüllt sind. Sie können die folgenden Bedingungen kontextabhängig anwenden.

   - **Desktop** oder **Mobilgerät** –Wählen Sie das Gerät aus, für das Sie den Zugriff auf die Apps aktivieren möchten.
   - **Geo-Standort** –Wählen Sie die Bedingung und den geografischen Standort aus, von dem aus die Benutzer auf die Apps zugreifen.
     - **Stimmt mit einem der folgenden überein:** Nur Benutzern oder Benutzergruppen, die von einem der aufgeführten geografischen Standorte aus auf die Apps zugreifen, wird der Zugriff auf die Apps ermöglicht.
     - **Stimmt mit keinem überein:** Allen Benutzern oder Benutzergruppen außer denen aus den aufgelisteten geografischen Standorten wird der Zugriff ermöglicht.
   - **Netzwerkstandort** –Wählen Sie die Bedingung und das Netzwerk aus, über das die Benutzer auf die Apps zugreifen.
     - **Stimmt mit einem der folgenden überein:** Nur Benutzern oder Benutzergruppen, die von einem der aufgeführten Netzwerkstandorte aus auf die Apps zugreifen, wird der Zugriff auf die Apps ermöglicht.

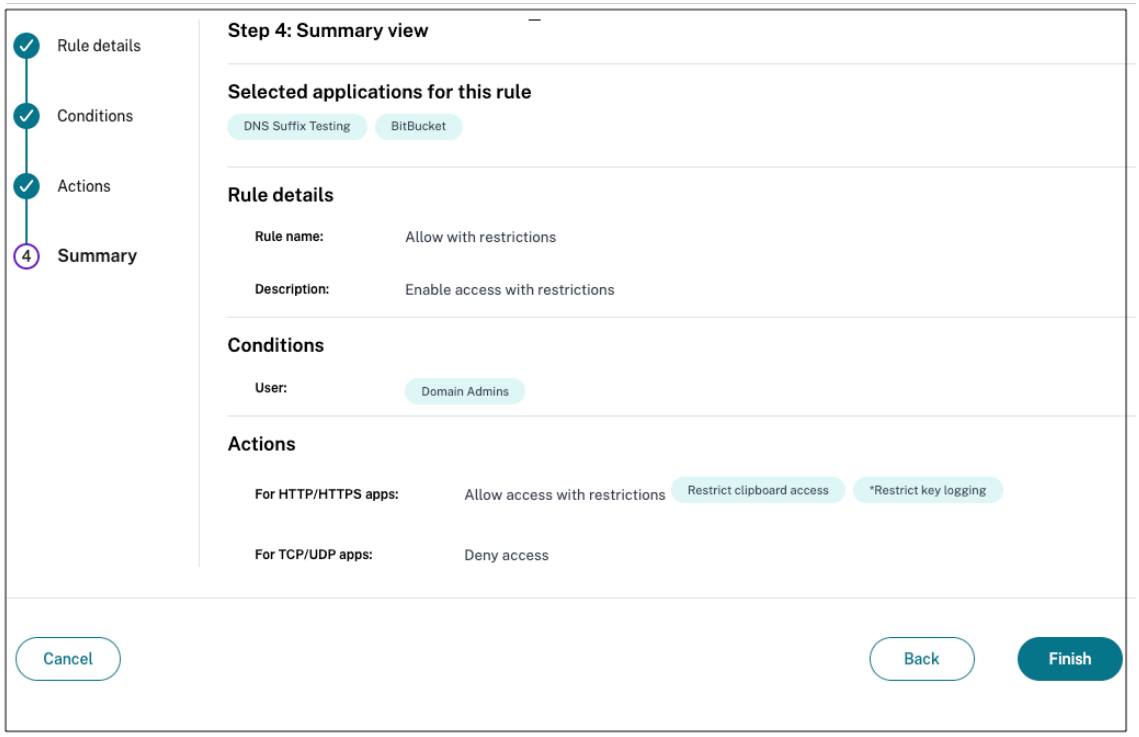
  - **Stimmt mit keinem überein:** Allen Benutzern oder Benutzergruppen außer denen aus den aufgelisteten Netzwerkstandorten wird der Zugriff ermöglicht.
- **Gerätestatusprüfung** –Wählen Sie die Bedingungen aus, die das Benutzergerät erfüllen muss, um auf die Anwendung zugreifen zu können.
- **Benutzerrisikobewertung** –Wählen Sie die Risikobewertungskategorien aus, auf deren Grundlage den Benutzern Zugriff auf die Anwendung gewährt werden muss.
- **Arbeitsbereich-URL** –Administratoren können Filter basierend auf dem vollqualifizierten Domänennamen angeben, der dem Arbeitsbereich entspricht.
  - **Stimmt mit einem der Werte von** überein –Erlaubt den Zugriff nur, wenn die eingehende Benutzerverbindung auf eine der konfigurierten Workspace-URLs trifft.
  - **Stimmt mit allem von** überein –Ermöglicht den Zugriff nur, wenn die eingehende Benutzerverbindung alle konfigurierten Workspace-URLs erfüllt.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie die Aktionen aus, die basierend auf der Bedingungsbewertung 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 Zugriffsbeschränkungen. Sie können auch angeben, ob die App in einem Remotebrowser oder im Citrix Secure Browser geöffnet werden soll.

```
-  Für den TCP/UDP-Zugriff können Sie Folgendes auswählen:
    -  **Zugriff erlauben**
    -  **Zugriff verweigern**

![Regelaktion erstellen](/en-us/citrix-secure-private-access/media/
   secure-private-access-policy-rule-actions.png)
```

1. Klicken Sie auf **Weiter**. Auf der Seite „Zusammenfassung“werden die Richtliniendetails angezeigt.
2. Sie können die Angaben überprüfen und auf **Fertig stellen**klicken.



Zu beachtende Punkte nach der Erstellung einer Richtlinie

- 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 wird standardmäßig eine Prioritätsreihenfolge zugewiesen. Die Priorität mit dem niedrigeren Wert hat die höchste Präferenz. Die Regel mit der niedrigsten Prioritätsnummer wird zuerst ausgewertet. Wenn die Regel (n) die definierten Bedingungen nicht erfüllt, wird die nächste Regel (n+1) ausgewertet und so weiter.

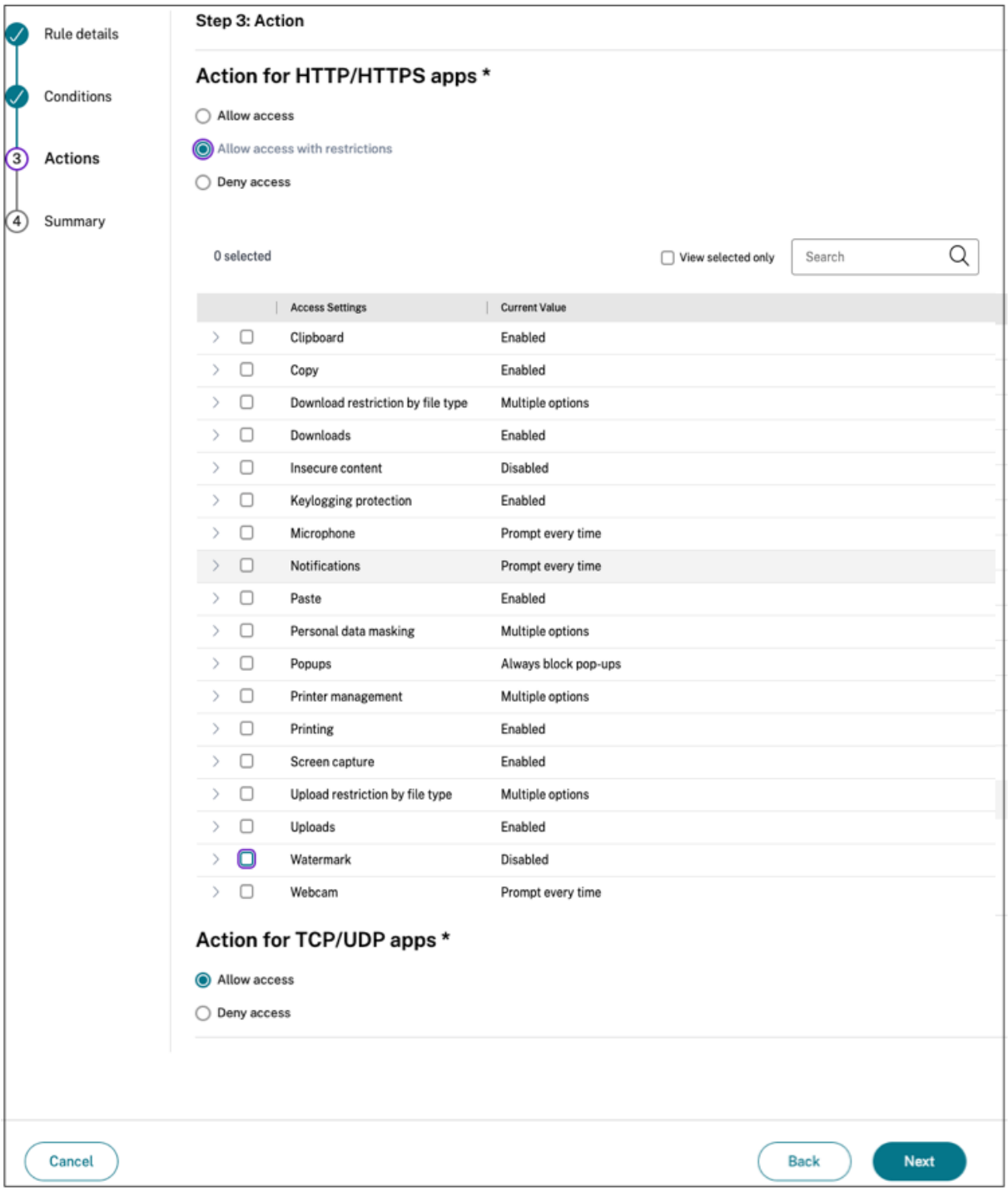
Beispiel für die Auswertung von Regeln mit Prioritätsreihenfolge:

Nehmen Sie an, Sie haben zwei Regeln erstellt: Regel 1 und Regel 2. Regel 1 wird dem Benutzer A und Regel 2 dem Benutzer B zugewiesen, anschließend 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 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 den Benutzern nicht aufgelistet.

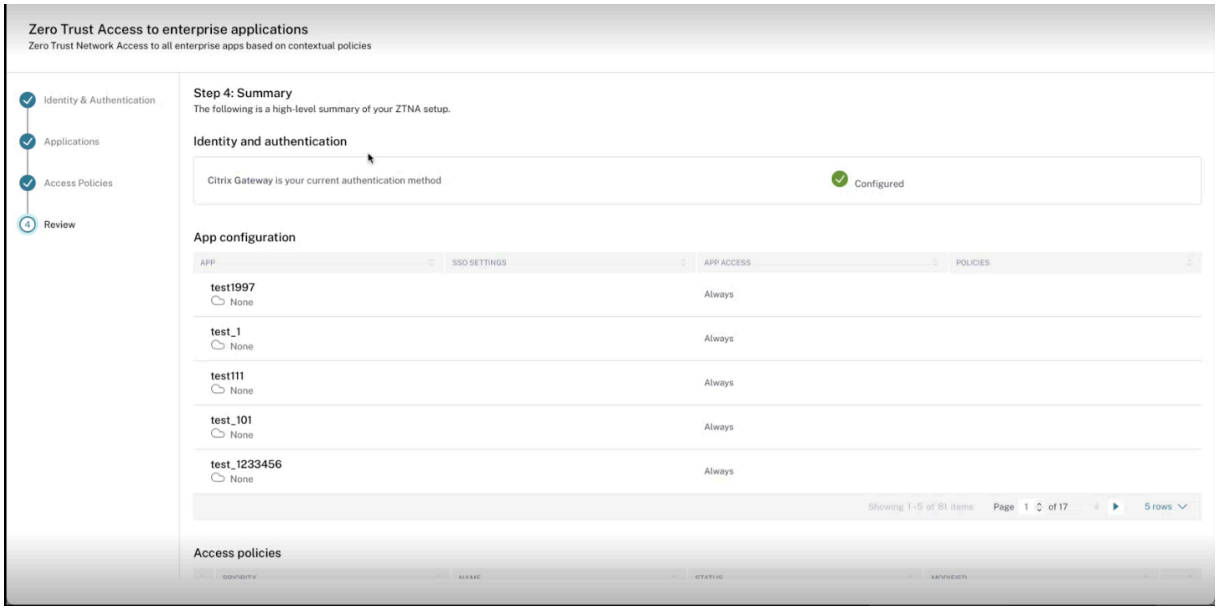
Verfügbare Optionen für Zugriffsbeschränkungen

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

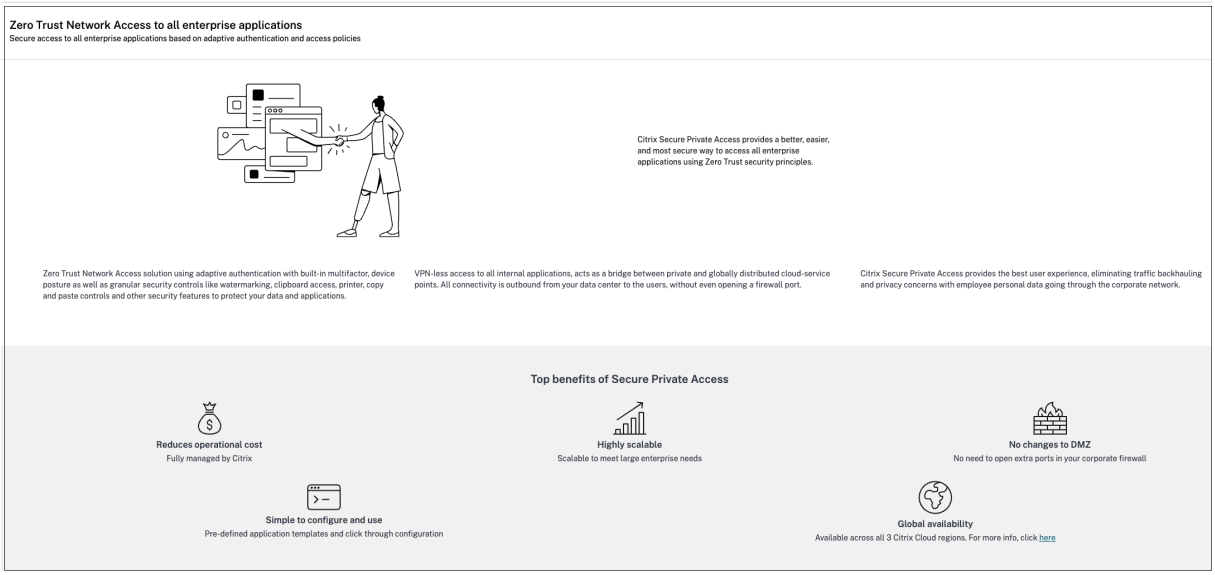


Schritt 4: Zusammenfassung der einzelnen Konfigurationen prüfen

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

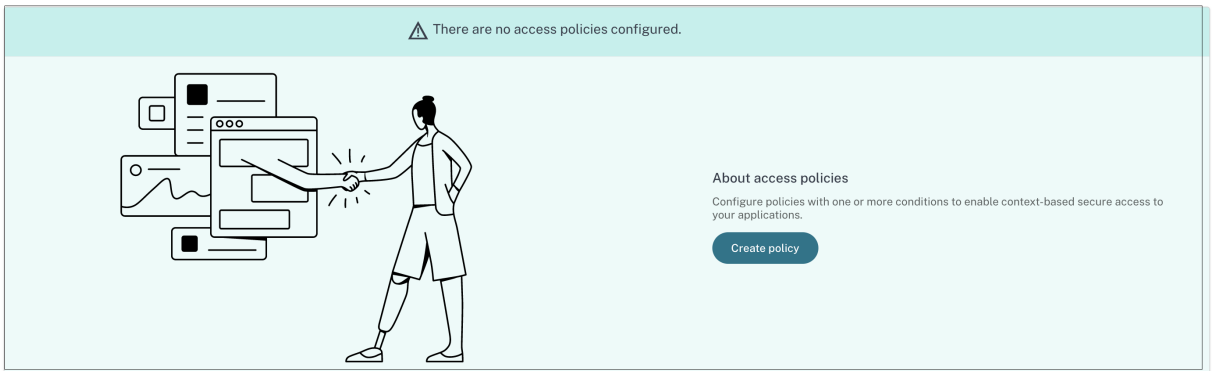


Die folgende Abbildung zeigt die Seite, nachdem Sie die 4-stufige Konfiguration abgeschlossen haben.



Wichtig:

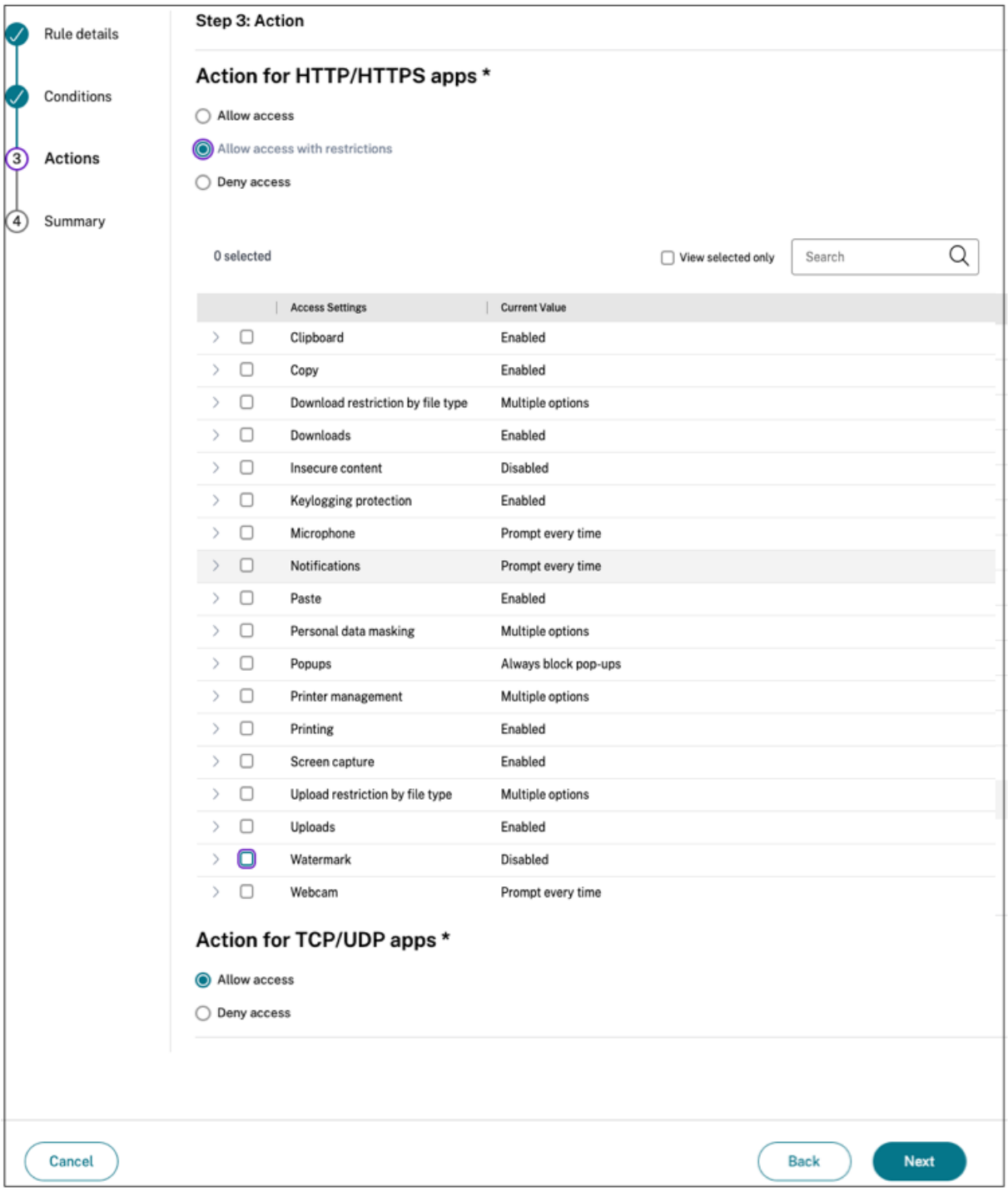
- Nachdem Sie die Konfiguration mit dem Assistenten abgeschlossen haben, können Sie die Konfiguration eines Abschnitts ändern, indem Sie direkt zu diesem Abschnitt gehen. Sie müssen die Reihenfolge nicht einhalten.
- Wenn Sie alle konfigurierten Apps oder Richtlinien löschen, müssen Sie diese erneut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



Optionen zur Zugriffsbeschränkung

October 21, 2024

Wenn Sie beim Erstellen einer Zugriffsrichtlinie die Aktion **Zugriff mit Einschränkungen zulassen** auswählen, können Sie die Zugriffsbeschränkungen auswählen. Diese Einschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen. Einzelheiten zum Erstellen einer Zugriffsrichtlinie und Aktivieren von Zugriffsbeschränkungen finden Sie unter Konfigurieren einer Zugriffsrichtlinie.



Zwischenablage

Aktivieren/deaktivieren Sie Ausschneide-/Kopieren-/Einfügevorgänge für eine SaaS- oder interne Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

Kopieren

Aktivieren/deaktivieren Sie das Kopieren von Daten aus einer SaaS- oder internen Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> - Wenn in einer Richtlinie sowohl die Einschränkung **Zwischenablage** als auch **Kopieren** aktiviert sind, hat die Einschränkung **Zwischenablage** Vorrang vor der Einschränkung **Kopieren** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 2405 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.
> - Zur detaillierten Kontrolle des Kopiervorgangs innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Zwischenablageeinschränkung für Sicherheitsgruppen.

Downloadbeschränkung nach Dateityp

Aktivieren/Deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, bestimmte MIME-Typen (Dateien) aus der SaaS- oder internen Web-App herunterzuladen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> - Die Download-Beschränkung **nach Dateityp** ist zusätzlich zur Download-Beschränkung ** verfügbar.
> - Wenn in einer Richtlinie sowohl die Einschränkung **Downloads** als auch die Einschränkung **Downloadbeschränkung nach Dateityp** aktiviert sind, hat die Einschränkung **Downloads** Vorrang vor der Einschränkung **Downloadbeschränkung nach Dateityp** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 2405 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um das Herunterladen von MIME-Typen zu aktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Downloadbeschränkung nach Dateityp** und dann auf **Bearbeiten**.

4. Wählen Sie auf der Seite „Downloadbeschränkung nach Dateitypeinstellungen “ eine der folgenden Optionen aus:

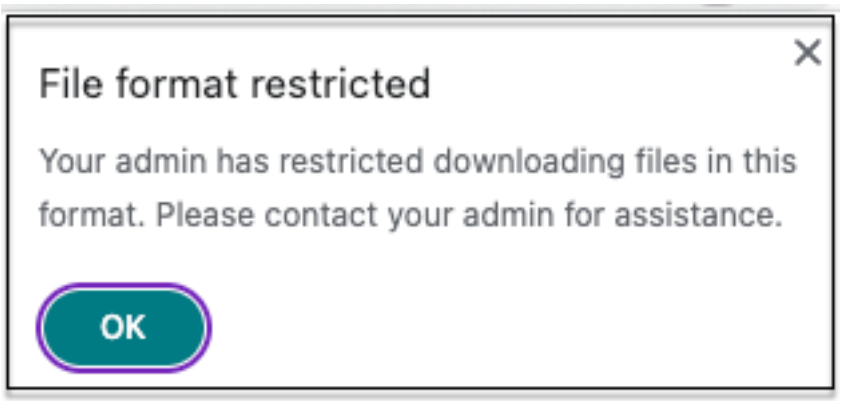
   - **Alle Downloads mit Ausnahmen zulassen** –Wählen Sie die Typen aus, die blockiert werden müssen, und lassen Sie alle anderen Typen zu.
   - **Alle Downloads mit Ausnahmen blockieren.** –Nur die Typen auswählen, die hochgeladen werden können, und alle anderen Typen blockieren.

5. Wenn der Dateityp nicht in der Liste vorhanden ist, gehen Sie wie folgt vor:

   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie in **MIME-Typen hinzufügen**den MIME-Typ im Format `Kategorie/Unterkategorie<extension>`ein. Zum Beispiel `image/png`.
   c) Klicken Sie auf **Fertig**.
   d) Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

   Der MIME-Typ wird jetzt in der Liste der Ausnahmen angezeigt.

Wenn ein Endbenutzer versucht, einen eingeschränkten Dateityp herunterzuladen, zeigt Citrix Enterprise Browser die folgende Meldung an:



Downloads

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, Downloads aus der SaaS- oder internen Web-App heraus durchzuführen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> Wenn in einer Richtlinie sowohl die Beschränkungen **Downloads** als auch **Downloadbeschränkung nach Dateityp** aktiviert sind, hat die Beschränkung **Downloads** Vorrang vor der Beschränkung **Downloadbeschränkung nach Dateityp**.

Unsicherer Inhalt

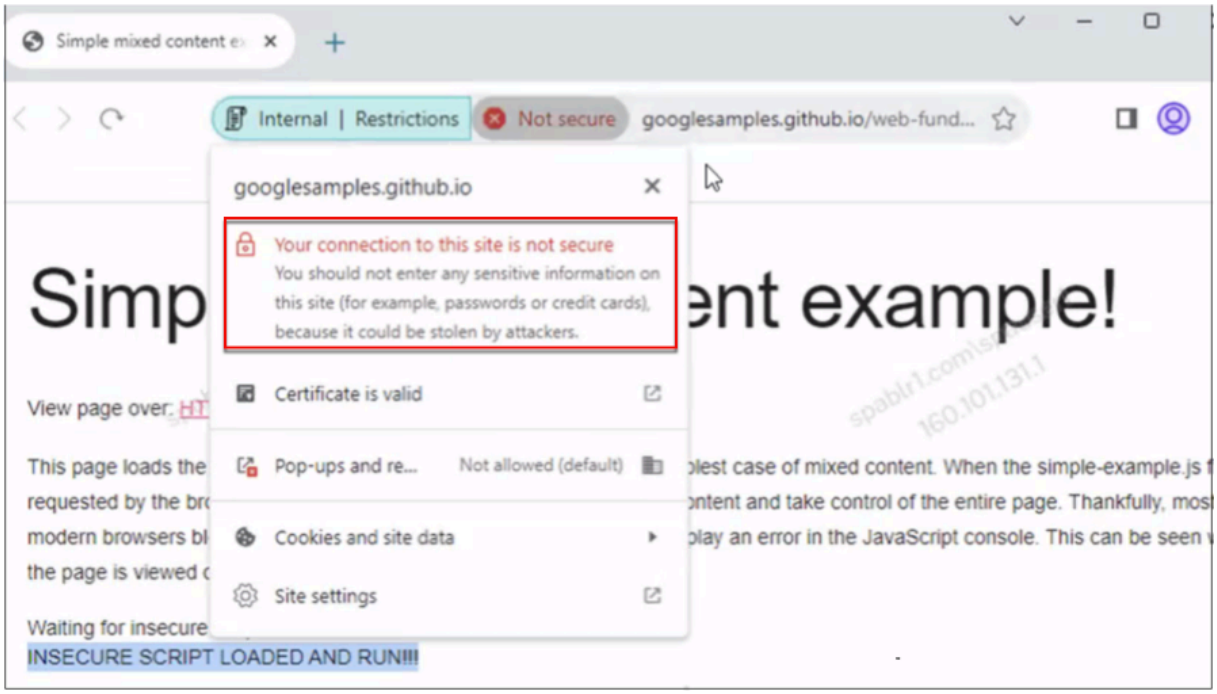
Aktivieren/deaktivieren Sie den Zugriff von Endbenutzern auf unsichere Inhalte innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Als unsicherer Inhalt gelten alle Dateien, auf die von einer Webseite aus über einen HTTP-Link und nicht über einen HTTPS-Link verwiesen wird. Standardwert: Deaktiviert.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um den Zugriff auf unsichere Inhalte zu deaktivieren.

Um den Zugriff auf unsichere Inhalte zu ermöglichen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Wählen Sie **Unsicherer Inhalt**.
4. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Die folgende Abbildung zeigt eine Beispielbenachrichtigung, wenn Sie auf unsichere Inhalte zugreifen.



Keylogging-Schutz

Aktivieren/deaktivieren Sie mit dieser Zugriffsrichtlinie die Erfassung von Tastatureingaben durch Keylogger aus der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

Mikrofon

Fordern Sie Benutzer bei jedem Zugriff auf das Mikrofon innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App auf/fordern Sie sie nicht auf, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die die Einschränkung **Mikrofon** aktiviert ist.

Um das Mikrofon jederzeit ohne Nachfrage zuzulassen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Mikrofon** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite **Mikrofoneinstellungen** auf **Zugriff immer erlauben**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

> **Hinweis:**
>
> - Wenn die Einschränkung **Mikrofon** in der Secure Workspace-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen**an.
> - Wenn die Option **Jedes Mal nachfragen** in der Secure Workspace-Richtlinie ist, variiert die auf Citrix Enterprise Browser angewendete Einstellung je nachdem, ob der Global App Configuration Service (GACS) zum Verwalten von Citrix Enterprise Browser verwendet wird.
> - Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser angewendet.
> - Wenn GACS nicht verwendet wird, zeigt der Citrix Enterprise Browser die Einstellung **Ask**an.

Weitere Informationen zu GACS finden Sie unter Verwalten des Citrix Enterprise Browsers über den Global App Configuration-Dienst.

Benachrichtigungen

Erlauben/fordern Sie Benutzer jedes Mal auf, die Benachrichtigungen innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App anzuzeigen, wenn auf sie über den Citrix Enterprise Browser zugegriffen wird. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist.

Um Benachrichtigungen ohne Aufforderung zu blockieren, führen Sie die folgenden Schritte aus.

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Benachrichtigungen** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Benachrichtigungseinstellungen** “auf **Benachrichtigungen immer blockieren**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Einfügen

Aktivieren/deaktivieren Sie das Einfügen kopierter Daten in die SaaS- oder interne Web-App mit dieser Zugriffsrichtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> - Wenn in einer Richtlinie sowohl die Einschränkung **Zwischenablage** als auch **Einfügen** aktiviert sind, hat die Einschränkung **Zwischenablage** Vorrang vor der Einschränkung **Einfügen** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.
> - Zur detaillierten Steuerung von Einfügevorgängen innerhalb der Apps können Administratoren die Einschränkung **Sicherheitsgruppen** verwenden. Einzelheiten finden Sie unter Zwischenablageeinschränkung für Sicherheitsgruppen.

Maskierung personenbezogener Daten

Aktivieren/deaktivieren Sie mit dieser Richtlinie das Redigieren oder Maskieren personenbezogener Daten (PII) in der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Zu den personenbezogenen Daten können Kreditkartennummern, Sozialversicherungsnummern, Daten usw. gehören. Sie können auch benutzerdefinierte Regeln zum Erkennen bestimmter Arten vertraulicher Informationen und zum entsprechenden Maskieren dieser Informationen definieren. Die Einschränkungen zur Maskierung personenbezogener Daten bieten auch die Möglichkeit, die Informationen vollständig oder teilweise zu maskieren.

> **Hinweis:**
>
> Endbenutzer müssen Citrix Enterprise Browser Version 2405 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwen-

> dungszugriff eingeschränkt.

Führen Sie die folgenden Schritte aus, um personenbezogene Daten zu redigieren oder zu maskieren:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Maskierung personenbezogener Daten** und anschließend auf **Bearbeiten**.
4. Wählen Sie den Informationstyp aus, den Sie verschleiern oder maskieren möchten, und klicken Sie dann auf **Hinzufügen**.

   Wenn der Informationstyp nicht in der vordefinierten Liste angezeigt wird, können Sie einen benutzerdefinierten Informationstyp hinzufügen. Einzelheiten finden Sie unter Benutzerdefinierten Informationstyp hinzufügen.
5. Wählen Sie den Maskierungstyp aus.

   - **Vollständige Maskierung** –Verdecken Sie die vertraulichen Informationen vollständig, um sie unlesbar zu machen.
   - **Teilweise Maskierung** –Verdecken Sie die vertraulichen Informationen teilweise. Es werden nur die relevanten Abschnitte behandelt, der Rest bleibt unverändert.

     Wenn Sie **Teilmarkierung**auswählen, müssen Sie Zeichen auswählen, die am Anfang oder am Ende des Dokuments beginnen. Sie müssen die Zahlen in die Felder **Erste maskierte Zeichen** und **Letzte maskierte Zeichen** eingeben.

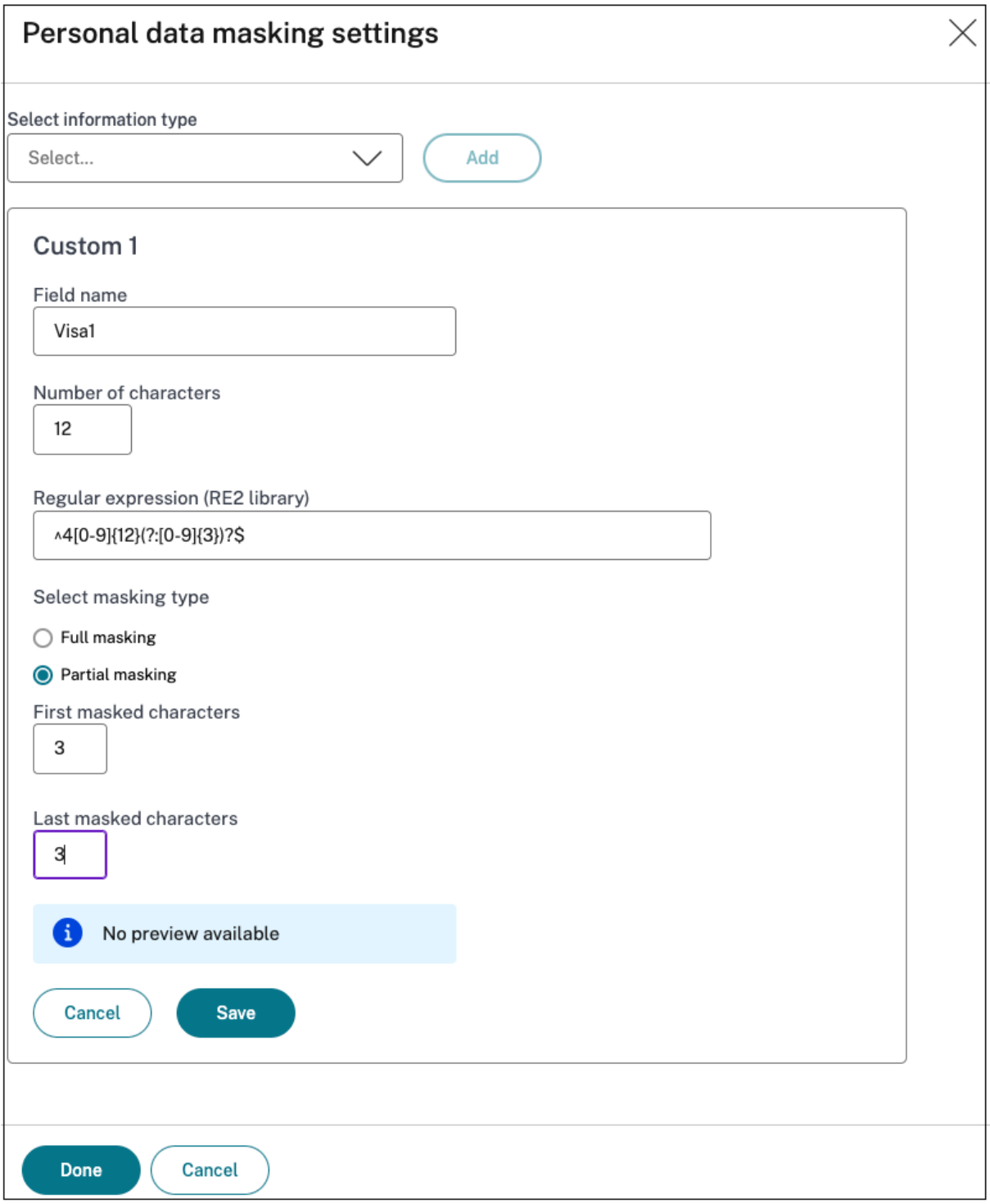
     Das Feld **Vorschau** zeigt das Maskierungsformat an. Diese Vorschau ist für benutzerdefinierte Richtlinien nicht verfügbar.
6. Klicken Sie auf **Speichern** und dann auf **Fertig**.
7. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Benutzerdefinierten Informationstyp hinzufügen

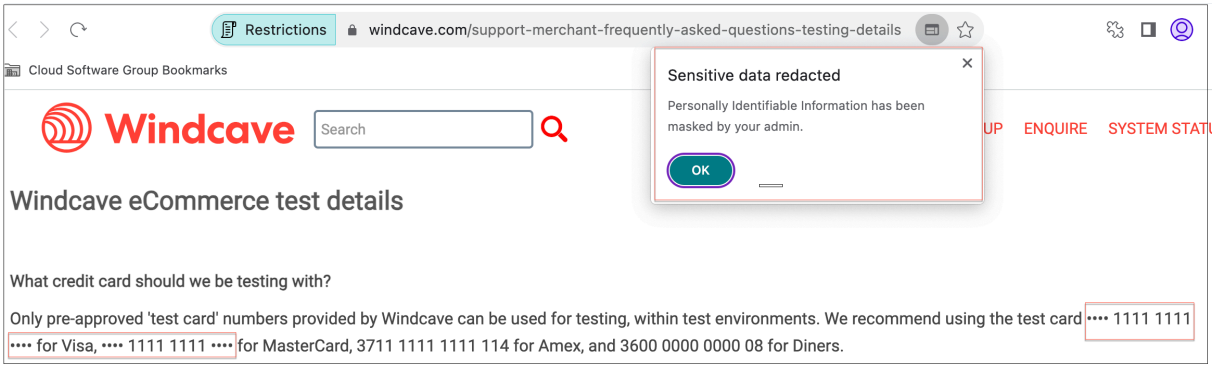
Sie können einen benutzerdefinierten Informationstyp hinzufügen, indem Sie den regulären Ausdruck des Informationstyps hinzufügen.

1. Wählen Sie in **Informationstyp**aus, wählen Sie **Benutzerdefiniert**aus und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie in **Feldname**den Namen für den Informationstyp ein, den Sie maskieren möchten.
3. Geben Sie in **Anzahl der Zeichen**die Anzahl der Zeichen des Informationstyps ein.

4. Geben Sie in **Regulärer Ausdruck (RE2-Bibliothek)**den Ausdruck für den benutzerdefinierten Informationstyp ein. Beispiel: `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Wählen Sie den Maskierungstyp aus, wenn Sie die gesamten Informationen oder die ersten bzw. letzten Zeichen maskieren möchten.
6. Klicken Sie auf **Speichern**und dann auf **Fertig**.
7. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.



Die folgende Abbildung zeigt eine Beispiel-App, in der die PII maskiert sind. In der Abbildung wird auch die Benachrichtigung zur Maskierung der PII angezeigt.



Popups

Aktivieren/deaktivieren Sie die Anzeige von Popups innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App beim Zugriff über den Citrix Enterprise Browser. Standardmäßig sind Popups auf Webseiten deaktiviert. Standardwert: Popups immer blockieren.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist.

Um die Anzeige von Popups zu aktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Popups** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Popup-Einstellungen** “auf **Popups immer zulassen**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Drucken

Aktivieren/deaktivieren Sie mit dieser Richtlinie das Drucken von Daten aus den konfigurierten SaaS- oder internen Web-Apps beim Zugriff über den Citrix Enterprise Browser. Standardwert: Aktiviert.

Die folgende Meldung wird angezeigt, wenn ein Endbenutzer versucht, Inhalte aus der Anwendung zu drucken, für die die Druckbeschränkung aktiviert ist.

> **Hinweis:**
>
> Wenn in einer Richtlinie sowohl die Einschränkungen **Drucken** als auch **Druckerverwaltung** aktiviert sind, hat die Einschränkung **Drucken** Vorrang vor der Einschränkung **Druckerverwaltung** .

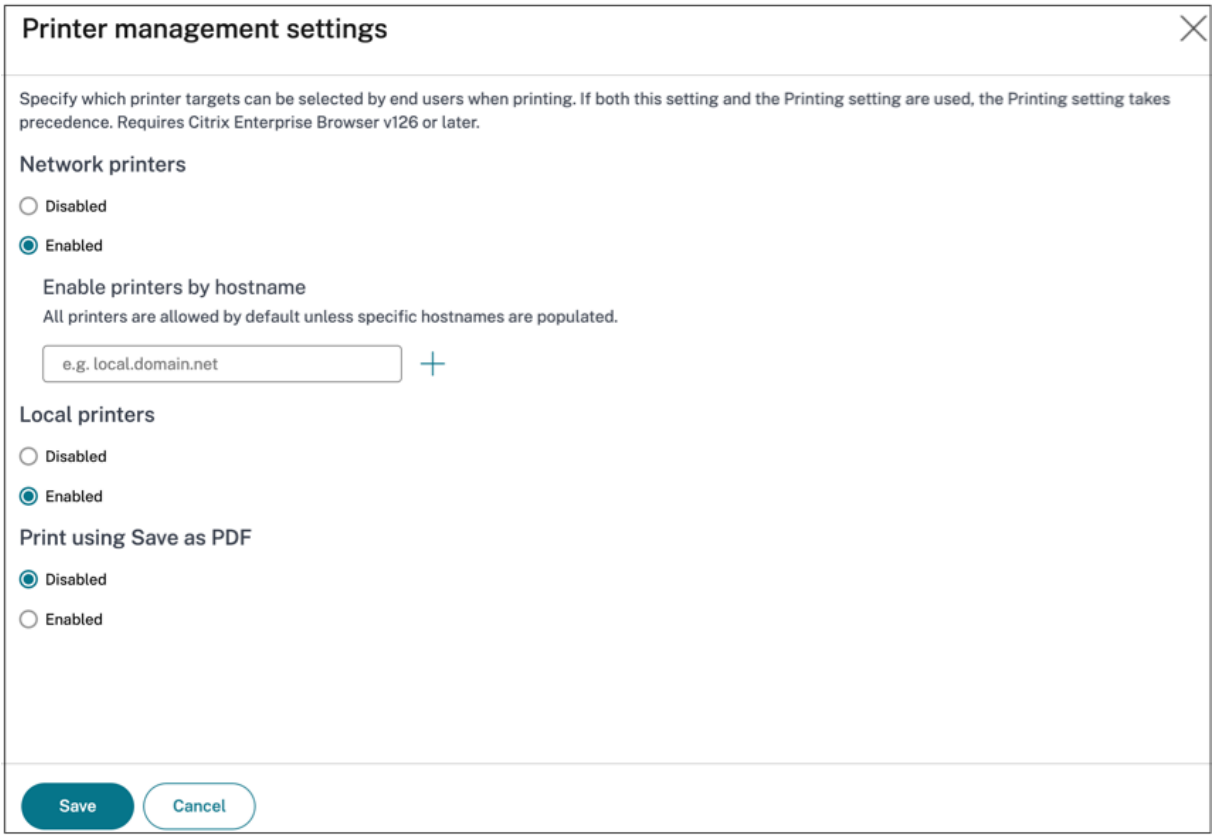
Druckerverwaltung

Aktivieren/deaktivieren Sie das Drucken von Daten mithilfe der vom Administrator konfigurierten Drucker aus den konfigurierten SaaS- oder internen Web-Apps mit dieser Richtlinie, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> - Die Einschränkung **Druckerverwaltung** ist zusätzlich zur Einschränkung **Drucken** verfügbar, bei der das Drucken entweder aktiviert oder deaktiviert wird. Wenn in einer Zugriffsrichtlinie sowohl die Einschränkungen **Drucken** als auch **Druckerverwaltung** aktiviert sind, hat die Einschränkung **Drucken** Vorrang vor der Einschränkung **Druckerverwaltung** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 2405 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um Druckbeschränkungen zu aktivieren/deaktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Druckerverwaltung** und anschließend auf **Bearbeiten**.



1. Wählen Sie die Ausnahmen entsprechend Ihrem Bedarf aus.

   - **Netzwerkdrucker** - Ein Netzwerkdrucker ist ein Drucker, der an ein Netzwerk angeschlossen und von mehreren Benutzern verwendet werden kann.
     - **Deaktiviert:** Das Drucken von allen Netzwerkdruckern im Netzwerk ist deaktiviert.
     - **Aktiviert:** Das Drucken von allen Netzwerkdruckern ist aktiviert. Wenn Drucker-Hostnamen angegeben werden, werden alle anderen Netzwerkdrucker außer den angegebenen blockiert.

     Hinweis: Netzwerkdrucker werden anhand ihres Hostnamens identifiziert.

   - **Lokale Drucker** –Ein lokaler Drucker ist ein Gerät, das über eine Kabelverbindung direkt mit einem einzelnen Computer verbunden ist. Diese Verbindung wird normalerweise über USB, parallele Anschlüsse oder andere direkte Schnittstellen hergestellt.
     - **Deaktiviert:** Das Drucken von allen lokalen Druckern ist deaktiviert.
     - **Aktiviert:** Das Drucken von allen lokalen Druckern ist aktiviert.

   - **Drucken mit Als PDF speichern**
     - **Deaktiviert**: Das Speichern des Inhalts der Anwendung im PDF-Format ist deaktiviert.
     - **Aktiviert:** Das Speichern des Inhalts der Anwendung im PDF-Format ist aktiviert.

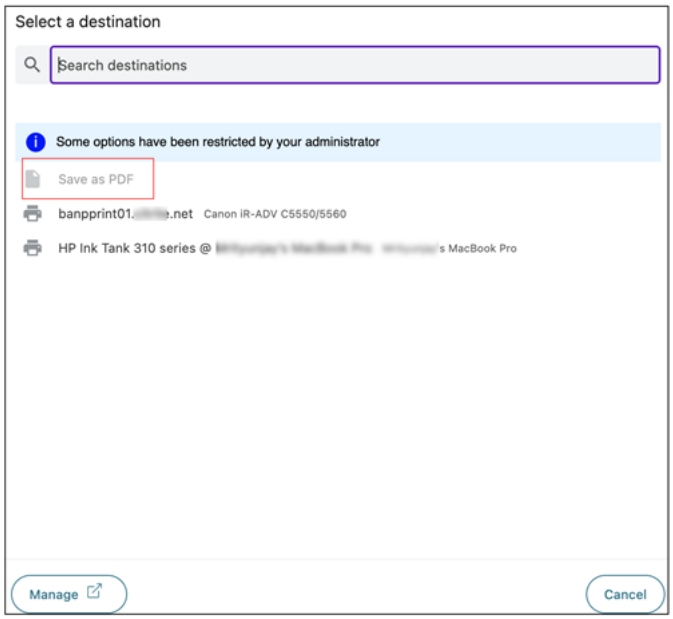
2. Klicken Sie auf **Speichern**.

3. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Wenn ein Netzwerkdrucker deaktiviert ist, wird der jeweilige Druckername ausgegraut angezeigt, wenn Endbenutzer versuchen, den Drucker im Feld **Ziel** auszuwählen.

Wenn außerdem **Drucken mit „Als PDF speichern“** deaktiviert ist, wird die Option **Als PDF speichern** ausgegraut angezeigt, wenn Sie im Feld **Ziel** auf den Link **Mehr anzeigen** klicken.

Wenn die Endbenutzer die Netzwerkdrucker umbenennen, können sie den Netzwerkdrucker nicht verwenden.



Bildschirmaufnahme

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit zum Erfassen der Bildschirme der SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser mithilfe eines der Bildschirmerfassungsprogramme oder -apps erfolgt. Wenn ein Benutzer versucht, den Bildschirm zu erfassen, wird ein leerer Bildschirm erfasst. Standardwert: Aktiviert.

Uploadbeschränkung nach Dateityp

Aktivieren/deaktivieren Sie mit dieser Richtlinie die Möglichkeit des Benutzers, bestimmte MIME-Typen (Dateien) aus der SaaS- oder internen Web-App herunterzuladen, wenn der Zugriff über den Citrix Enterprise Browser erfolgt.

> **Hinweis:**
>
> - Die Upload-Beschränkung **nach Dateityp** ist zusätzlich zur Upload-Beschränkung ** verfüg-

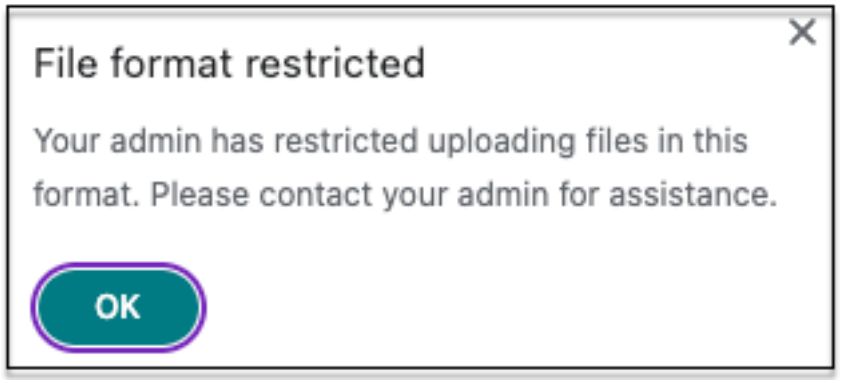
> bar.
> - Wenn in einer Richtlinie sowohl die Beschränkungen **Upload** als auch **Uploadbeschränkung nach Dateityp** aktiviert sind, hat die Einschränkung **Uploads** Vorrang vor der Einschränkung **Uploadbeschränkung nach Dateityp** .
> - Endbenutzer müssen Citrix Enterprise Browser Version 2405 oder höher verwenden, um auf Anwendungen zuzugreifen, für die diese Einschränkung aktiviert ist. Andernfalls ist der Anwendungszugriff eingeschränkt.

Um das Hochladen von MIME-Typen zu aktivieren/deaktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Klicken Sie auf **Upload-Beschränkung nach Dateityp** und dann auf **Bearbeiten**.
4. Wählen Sie auf der Seite „Uploadbeschränkung nach Dateitypeinstellungen “ eine der folgenden Optionen aus:
   - **Alle Uploads mit Ausnahmen zulassen.** –Alle Dateien außer den ausgewählten Typen hochladen.
   - **Alle Uploads mit Ausnahmen blockieren.** –Blockiert das Hochladen aller Dateitypen außer den ausgewählten Typen.
5. Wenn der Dateityp nicht in der Liste vorhanden ist, gehen Sie wie folgt vor:
   a) Klicken Sie auf **Benutzerdefinierte MIME-Typen hinzufügen**.
   b) Geben Sie in **MIME-Typen hinzufügen**den MIME-Typ im Format `Kategorie/Unterkategorie<extension>`ein. Zum Beispiel `image/png`.
   c) Klicken Sie auf **Fertig**.
   d) Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

   Der MIME-Typ wird jetzt in der Liste der Ausnahmen angezeigt.

Wenn ein Endbenutzer versucht, einen eingeschränkten Dateityp hochzuladen, zeigt Citrix Enterprise Browser eine Warnmeldung an.



Uploads

Aktivieren/deaktivieren Sie die Möglichkeit des Benutzers zum Hochladen innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Aktiviert.

> **Hinweis:**
>
> Wenn in einer Richtlinie sowohl die Beschränkungen **Uploads** als auch **Uploadbeschränkung nach Dateityp** aktiviert sind, hat die Beschränkung **Uploads** Vorrang vor der Beschränkung **Uploadbeschränkung nach Dateityp**.

Wasserzeichen

Aktivieren/deaktivieren Sie das Wasserzeichen auf dem Benutzerbildschirm, das den Benutzernamen und die IP-Adresse des Computers des Benutzers anzeigt. Standardwert: Deaktiviert.

Webcam

Fordern Sie Benutzer bei jedem Zugriff auf die Webcam innerhalb der mit dieser Richtlinie konfigurierten SaaS- oder internen Web-App auf/fordern Sie sie nicht auf, wenn der Zugriff über den Citrix Enterprise Browser erfolgt. Standardwert: Jedes Mal nachfragen.

Endbenutzer müssen Citrix Enterprise Browser Version 126 oder höher verwenden, um auf Anwendungen zuzugreifen, für die die Einschränkung **Webcam** aktiviert ist.

Um die Webcam jedes Mal ohne Nachfrage zuzulassen, führen Sie die folgenden Schritte aus:

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Einzelheiten finden Sie unter Erstellen von Zugriffsrichtlinien.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.

3. Klicken Sie auf **Webcam** und dann auf **Bearbeiten**.
4. Klicken Sie auf der Seite „ **Webcam-Einstellungen** “auf **Zugriff immer erlauben**.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

> **Hinweis:**
>
> - Wenn die Einschränkung **Webcam** in der Secure Workspace-Richtlinie aktiviert ist, zeigt Citrix Enterprise Browser die Einstellungen **Zulassen**an.
> - Wenn die Option **Bei jedem** nachfragen in der Secure Workspace-Richtlinie aktiviert ist, variiert die auf Citrix Enterprise Browser angewendete Einstellung je nachdem, ob der Global App Configuration Service (GACS) zum Verwalten von Citrix Enterprise Browser verwendet wird.
> - Wenn GACS verwendet wird, wird die GACS-Einstellung auf den Citrix Enterprise Browser angewendet.
> - Wenn GACS nicht verwendet wird, zeigt der Citrix Enterprise Browser die Einstellung **Ask**an.

Weitere Informationen zu GACS finden Sie unter Verwalten des Citrix Enterprise Browsers über den Global App Configuration-Dienst.

Zwischenablagebeschränkung für Sicherheitsgruppen

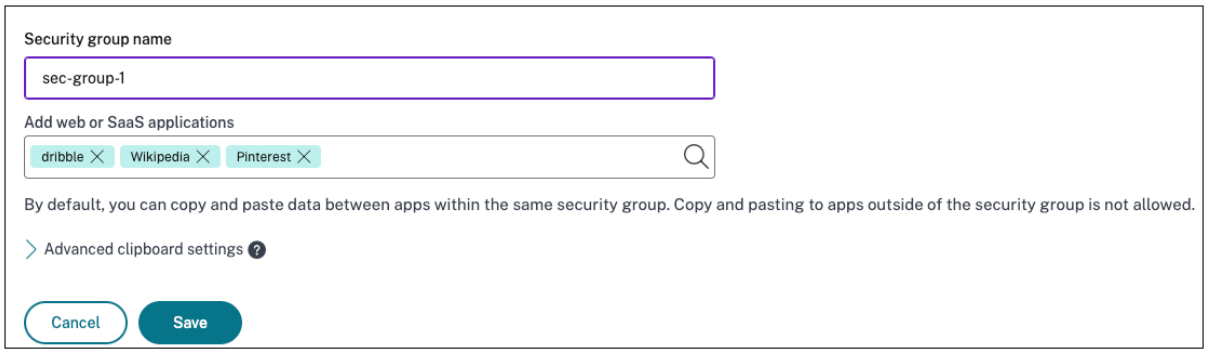
Sie können den Zugriff auf die Zwischenablage auf jede beliebige App-Gruppe beschränken. Diese bestimmten App-Gruppen werden als Sicherheitsgruppen erstellt, sodass die Endbenutzer Inhalte nur innerhalb dieser Sicherheitsgruppen kopieren und einfügen dürfen. Um den Zugriff auf die Zwischenablage innerhalb der Apps in einer Sicherheitsgruppe zu aktivieren, müssen Sie lediglich eine Zugriffsrichtlinie mit der Aktion **Zulassen** oder **Zulassen mit Einschränkungen** konfigurieren, ohne eine Zugriffseinstellung auszuwählen.

- Wenn die Einschränkung **Sicherheitsgruppen** aktiviert ist, können Sie keine Daten zwischen Anwendungen in verschiedenen Sicherheitsgruppen kopieren/einfügen. Wenn beispielsweise die App „ProdDocs“zur Sicherheitsgruppe „SG1“und die App „Edocs“zur Sicherheitsgruppe „SG2 “gehört, können Sie Inhalte nicht von „Edocs“nach „ProdDocs“kopieren/einfügen, selbst wenn die Einschränkung **Kopieren** / **Einfügen** für beide Gruppen aktiviert ist.
- Für Apps, die nicht Teil einer Sicherheitsgruppe sind, können Sie eine Zugriffsrichtlinie mit der Aktion **Zulassen mit Einschränkungen** erstellen und die Einschränkungen auswählen (**Kopieren**, **Einfügen**oder **Zwischenablage**). In diesem Fall ist die App nicht Teil einer Sicherheitsgruppe und die Einschränkung „ **Kopieren/Einfügen** “kann auf diese App angewendet werden.

> **Hinweis:**
>
> Sie können den Zwischenablagezugriff für Apps, auf die über Citrix Enterprise Browser zugegriffen wird, auch über den Global App Configuration Service (GACS) einschränken. Wenn Sie GACS zum Verwalten des Citrix Enterprise Browsers verwenden, verwalten Sie den Zugriff auf die Zwischenablage mit der Option **Enabled Sandboxed Clipboard** . Wenn Sie den Zwischenablagezugriff über GACS einschränken, gilt dies für alle Apps, auf die über den Citrix Enterprise Browser zugegriffen wird.

Führen Sie die folgenden Schritte aus, um eine Sicherheitsgruppe zu erstellen:

1. Klicken Sie in der Secure Private Access-Konsole auf **Anwendungen** und dann auf **Sicherheitsgruppen**.
2. Klicken Sie auf **. Fügen Sie eine neue Sicherheitsgruppe hinzu**.

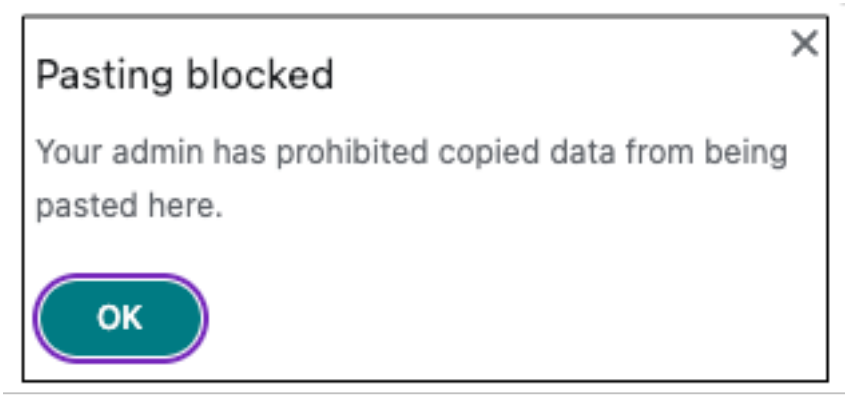


1. Geben Sie einen Namen für die Sicherheitsgruppe ein.
2. Wählen Sie unter **Web- oder SaaS-Anwendungen hinzufügen**die Anwendungen aus, die Sie gruppieren möchten, um die Kopier- und Einfügesteuerung zu aktivieren. Zum Beispiel Wikipedia, Pinterest und Dribble.
3. Klicken Sie auf **Speichern**.

Einzelheiten zu den **Erweiterten Zwischenablageeinstellungen** finden Sie unter Kopier-/Einfügesteuerelemente für native Anwendungen und unveröffentlichte Apps aktivieren.

Wenn Endbenutzer diese Anwendungen (Wikipedia, Pinterest und Dribble) von Citrix Workspace aus starten, müssen sie Daten (Kopieren/Einfügen) von einer Anwendung mit den anderen Anwendungen innerhalb der Sicherheitsgruppe teilen können. Das Kopieren/Einfügen erfolgt unabhängig von anderen Sicherheitsbeschränkungen, die für die Anwendungen bereits aktiviert sind.

Endbenutzer können jedoch keine Inhalte aus den lokalen Anwendungen auf ihren Computern oder aus unveröffentlichten Anwendungen in diese bestimmten Anwendungen kopieren und einfügen und umgekehrt. Beim Kopieren des Inhalts aus der angegebenen Anwendung in eine andere Anwendung wird folgende Meldung angezeigt:



> **Hinweis:**
>
> Sie können den Inhalt zwischen den Apps in einer Sicherheitsgruppe und anderen lokalen Apps auf den Computern oder unveröffentlichten Web-Apps kopieren und einfügen, indem Sie die Optionen in **Erweiterte Zwischenablageeinstellungen**verwenden. Einzelheiten hierzu finden Sie unter Aktivieren von Kopier-/Einfügesteuerelementen für native Anwendungen und unveröffentlichte Apps.

Aktivieren Sie den detaillierten Zugriff auf die Zwischenablage

Sie können den Zugriff auf die Zwischenablage in detaillierten Stufen innerhalb der Anwendungen einer bestimmten Gruppe aktivieren. Sie können dies tun, indem Sie Zugriffsrichtlinien für die Anwendungen erstellen und die Einschränkung **Kopieren/Einfügen** entsprechend Ihrem Bedarf aktivieren.

> **Hinweis:**
>
> Stellen Sie sicher, dass die spezifische Zugriffsrichtlinie, die Sie für den granularen Zwischenablagezugriff erstellt haben, eine höhere Priorität hat als die Richtlinie, die Sie für die Sicherheitsgruppen erstellt haben.

Beispiel:

Nehmen wir an, Sie haben eine Sicherheitsgruppe mit drei Anwendungen erstellt, nämlich Wikipedia, Pinterest und Dribble.

Jetzt möchten Sie das Einfügen von Inhalten aus Wikipedia oder Dribble in Pinterest einschränken. Führen Sie dazu die folgenden Schritte aus:

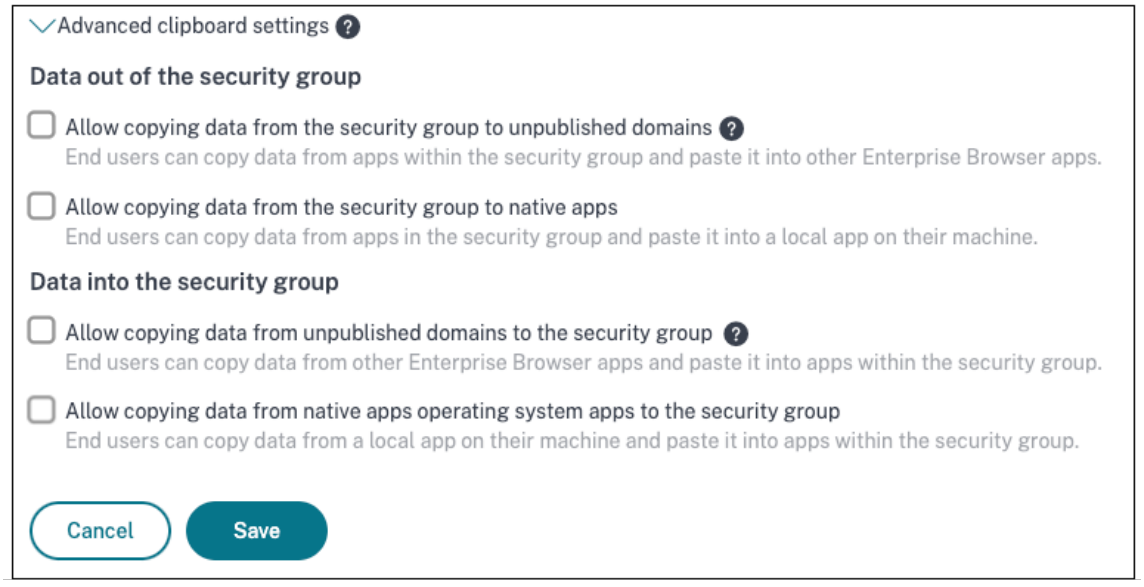
1. Erstellen oder bearbeiten Sie eine der Anwendung `Pinterest`zugewiesene Zugriffsrichtlinie. Einzelheiten zum Erstellen einer Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien erstellen.
2. Wählen Sie auf der Seite **Schritt 3: Aktion** die Option **Zulassen mit Einschränkungen**aus.
3. Wählen Sie **und fügen Sie**ein.

Obwohl Pinterest Teil einer Sicherheitsgruppe ist, die auch Wikipedia und Dribble enthält, können Benutzer aufgrund der mit Pinterest verknüpften Zugriffsrichtlinie, in der die Einschränkung **Einfügen** deaktiviert ist, keine Inhalte von Wikipedia oder Dribble nach Pinterest kopieren.

Aktivieren Sie Kopier-/Einfügekontrollen für native Anwendungen und unveröffentlichte Apps

Sie können den Inhalt zwischen den Apps in einer Sicherheitsgruppe und anderen lokalen Apps auf den Maschinen oder unveröffentlichten Web-Apps kopieren und einfügen, indem Sie die Optionen in **Erweiterte Zwischenablageeinstellungen**verwenden.

1. Erstellen Sie eine Sicherheitsgruppe. Einzelheiten finden Sie unter Sicherheitsgruppen erstellen.
2. Erweitern Sie **Erweiterte Zwischenablageeinstellungen**.



3. Wählen Sie je nach Bedarf eine der folgenden Optionen aus:

   - **Kopieren von Daten aus der Sicherheitsgruppe in nicht veröffentlichte Domänen zulassen.** –Kopieren von Daten aus Anwendungen in den Sicherheitsgruppen in die Apps aktivieren, die nicht in Secure Private Access veröffentlicht sind.
   - **Kopieren von Daten aus der Sicherheitsgruppe in native Apps zulassen.** –Aktivieren Sie das Kopieren von Daten aus den Anwendungen in den Sicherheitsgruppen in die lokalen Anwendungen auf Ihren Computern.

- **Kopieren von Daten aus nicht veröffentlichten Domänen in die Sicherheitsgruppe zulassen.** –Kopieren von Daten aus nicht über Secure Private Access veröffentlichten Apps in die Anwendungen in den Sicherheitsgruppen aktivieren.
- **Erlaubt das Kopieren von Daten aus nativen Apps des Betriebssystems. Die Sicherheitsgruppe** - Aktiviert das Kopieren von Daten aus lokalen Anwendungen auf den Maschinen in die Anwendungen.

Bekannte Probleme

- Die Routing-Tabelle in (**Einstellungen > Anwendungsdomäne**) behält die Domänen einer gelöschten Anwendung bei. Daher werden diese Anwendungen auch im Secure Private Access als veröffentlichte Anwendungen betrachtet. Wenn auf diese Domänen direkt über den Citrix Enterprise Browser zugegriffen wird, ist Kopieren/Einfügen aus diesen Anwendungen deaktiviert, unabhängig von den Optionen, die Sie in **Erweiterte Zwischenablageeinstellungen**ausgewählt haben.

  Nehmen wir beispielsweise das folgende Szenario an:

  - Sie haben eine Anwendung namens Jira2 (`https://test.citrite.net`) gelöscht, die Teil einer Sicherheitsgruppe war.
  - Sie haben die Option **Kopieren von Daten aus der Sicherheitsgruppe in nicht veröffentlichte Domänen zulassen**aktiviert.

  Wenn der Benutzer in diesem Szenario versucht, Daten aus dieser Anwendung in eine andere Anwendung in derselben Sicherheitsgruppe zu kopieren, wird die Einfügesteuerung deaktiviert. Dem Benutzer wird eine entsprechende Benachrichtigung angezeigt.

- Bei einer SaaS-App kann der App-Zugriff verweigert werden, wenn die Anwendung mit einer Zugriffsrichtlinie mit der Aktion **Zugriff verweigern konfiguriert ist.** Die Endbenutzer können weiterhin auf die App zugreifen, da der App-Verkehr nicht über Secure Private Access getunnelt wird. Auch wenn die Anwendung Teil der Sicherheitsgruppe ist, werden die Einstellungen der Sicherheitsgruppe nicht berücksichtigt und Sie können daher keine Inhalte aus der Anwendung kopieren/einfügen.

Tool zur Richtlinienmodellierung

October 21, 2024

Bei mehreren Anwendungen und verschiedenen Zugriffsrichtlinien ist es für Administratoren möglicherweise schwierig, das genaue Ergebnis des App-Zugriffs des Endbenutzers zu verstehen, d.

h. ob dem Endbenutzer basierend auf allen Konfigurationen der Zugriff auf eine Anwendung erlaubt oder verweigert wird.

Das Tool zur Richtlinienmodellierung (A**Zugriffsrichtlinien > Richtlinienmodellierung**) löst dieses Problem, indem es den Administratoren basierend auf ihren vorhandenen Konfigurationen vollständige Transparenz über die erwarteten App-Zugriffsergebnisse (zugelassen/mit Einschränkung zugelassen/verweigert) bietet. Administratoren können die Zugriffsergebnisse für jeden Benutzer anhand von Benutzerbedingungen wie Gerätetyp, Gerätestatus, geografischem Standort, Netzwerkstandort, Benutzerrisikobewertung und Arbeitsbereichs-URL überprüfen.

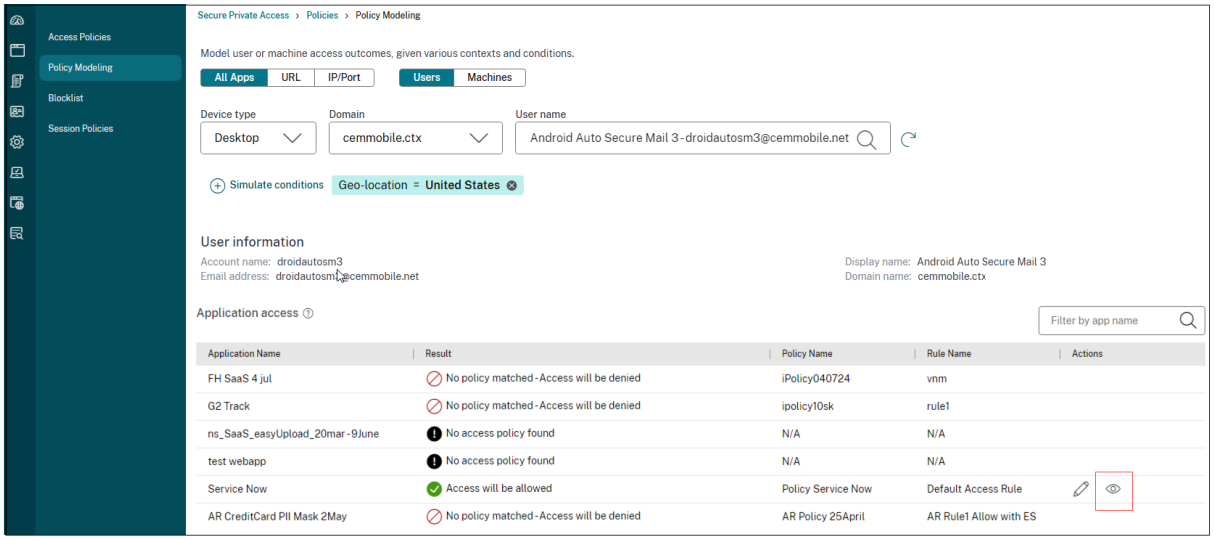
Führen Sie die folgenden Schritte aus, um die Zugriffsrichtlinienkonfiguration zu analysieren.

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.)
    - **Domäne**: Wählen Sie die mit dem Benutzer verknüpfte Domäne aus.
    - **Benutzer**: Wählen Sie den Benutzernamen aus, für den Sie die Anwendungen und zugehörigen Richtlinien analysieren möchten.

3. Sie können auch eine Reihe von Bedingungen/Einschränkungen für den Endbenutzer und seine Geräte simulieren. >**Hinweis:** > >Fügen Sie die genauen Benutzerbedingungen hinzu, um genaue Ergebnisse zu erhalten.
4. Klicken Sie auf **Bedingungen simulieren**.
5. Wählen Sie die Bedingung (Gerätestatus, Geostandort, Netzwerkstandort, Benutzerrisikobewertung und Arbeitsbereichs-URL) und wählen Sie dann den zugehörigen Wert aus.
6. Klicken Sie auf das Zeichen **+** , um weitere Bedingungen hinzuzufügen.
7. Klicken Sie auf **Anwenden**.

Die Anwendungen, zugehörigen Richtlinien und Regeln für den ausgewählten Benutzer werden in einem tabellarischen Format angezeigt.



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 Enterprise-Web-Apps

October 21, 2024

Die Bereitstellung von Web-Apps mithilfe des Secure Private Access-Dienstes ermöglicht die Remote-Bereitstellung unternehmensspezifischer Anwendungen als webbasierter Dienst. Zu den häufig verwendeten Webanwendungen gehören SharePoint, Confluence, OneBug usw.

Auf Web-Apps kann über Citrix Workspace mithilfe des Secure Private Access-Dienstes zugegriffen werden. Der Secure Private Access-Dienst bietet in Verbindung mit Citrix Workspace 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:

- Sicherer privater Zugriffsstandard
- Secure Private Access Advanced

Systemanforderungen

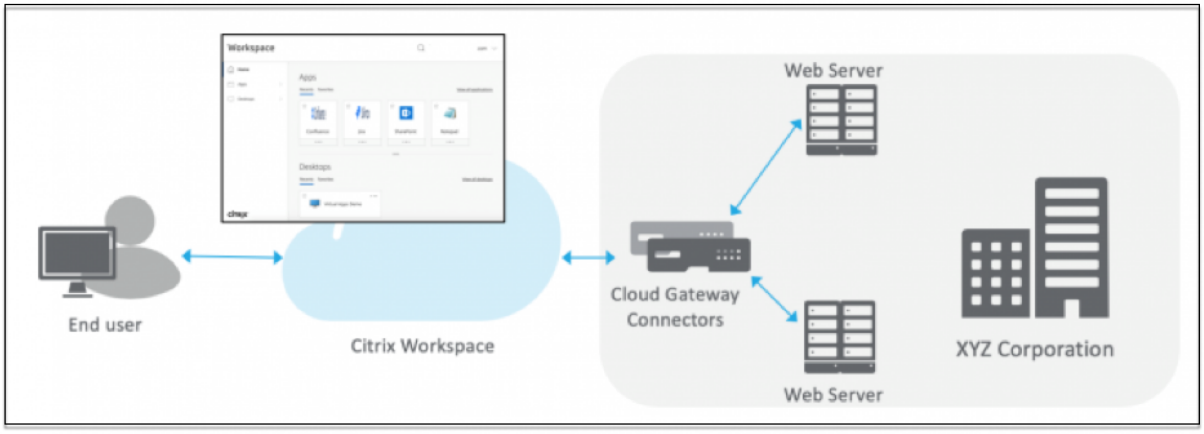
Connector Appliance –Verwenden Sie die Connector Appliance mit dem Citrix Secure Private Access-Dienst, um VPN-losen Zugriff auf die Enterprise-Web-Apps im Rechenzentrum der Kunden zu unterstützen. Einzelheiten finden Sie unter Sicherer Zugriff auf den Arbeitsbereich mit Connector Appliance.

Funktionsweise

Der Citrix Secure Private Access-Dienst stellt über den lokal bereitgestellten Connector eine sichere Verbindung zum lokalen Rechenzentrum her. Dieser Connector fungiert als Brücke zwischen lokal bereitgestellten Enterprise-Web-Apps und dem Citrix Secure Private Access-Dienst. Diese Konnektoren können in einem HA-Paar eingesetzt werden und erfordern nur eine ausgehende Verbindung.

Eine TLS-Verbindung zwischen dem Connectorgerät und dem Citrix Secure Private Access-Dienst in der Cloud sichert die lokalen Anwendungen, die im Cloud-Dienst aufgelistet sind. Der Zugriff auf Webanwendungen und die Bereitstellung dieser erfolgen über Workspace über eine VPN-freie Verbindung.

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



Konfigurieren einer Web-App

Das Konfigurieren einer Web-App umfasst die folgenden allgemeinen Schritte.

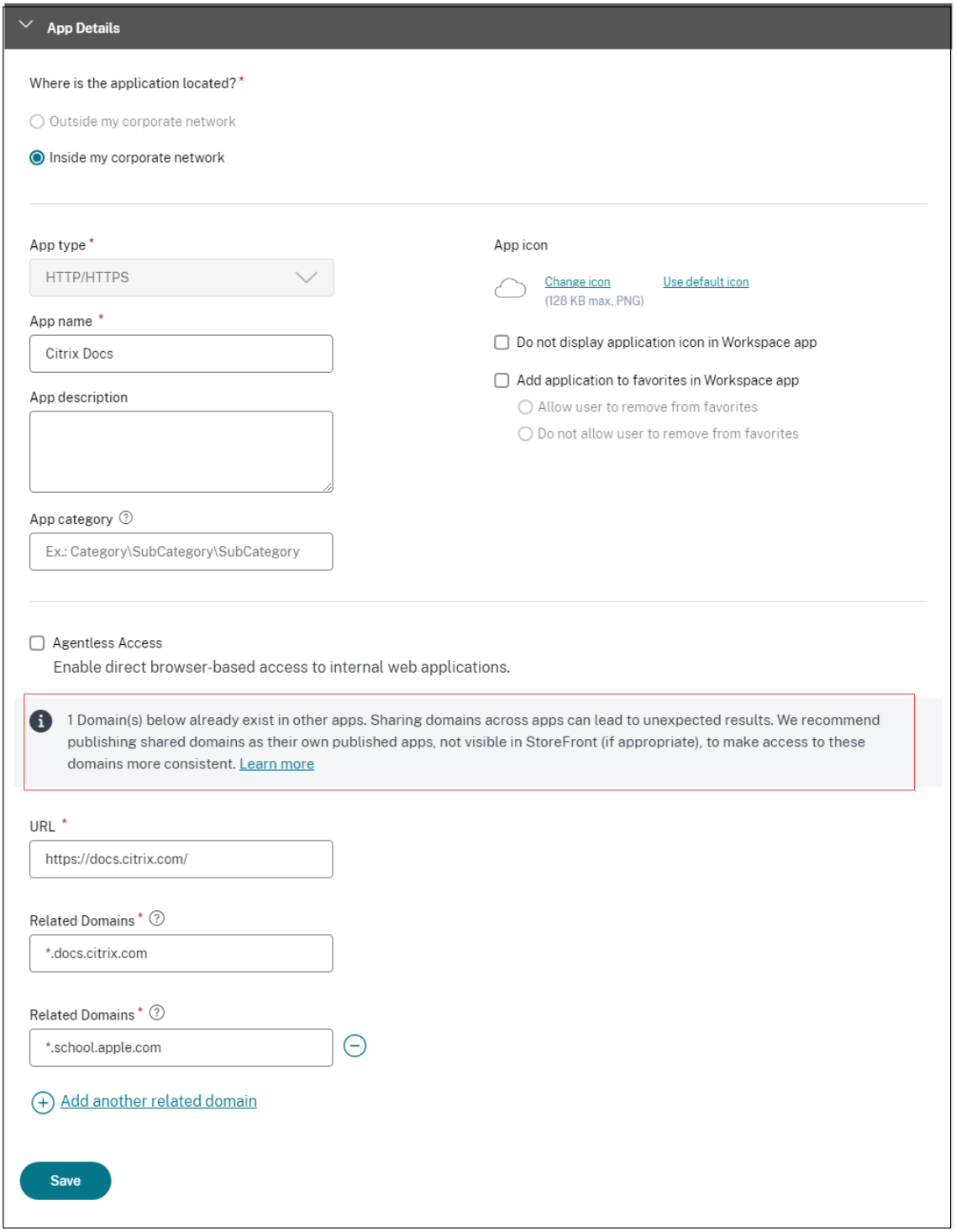
1. Konfigurieren der Anwendungsdetails
2. Festlegen der bevorzugten Anmeldemethode
3. Definieren des Anwendungsroutings

Konfigurieren der Anwendungsdetails

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

> **Hinweis:**
>
> Die Schaltfläche **Weiter** wird nur beim ersten Verwenden des Assistenten angezeigt. Bei der nachfolgenden Verwendung können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen klicken.**

1. Wählen Sie die App aus, die Sie hinzufügen möchten, und klicken Sie auf **Überspringen.**
2. Wählen Sie unter **Wo befindet sich der Anwendungsspeicherort?**den Speicherort aus.
3. Geben Sie die folgenden Details im Abschnitt **App-Details** ein und klicken Sie auf **Weiter.**

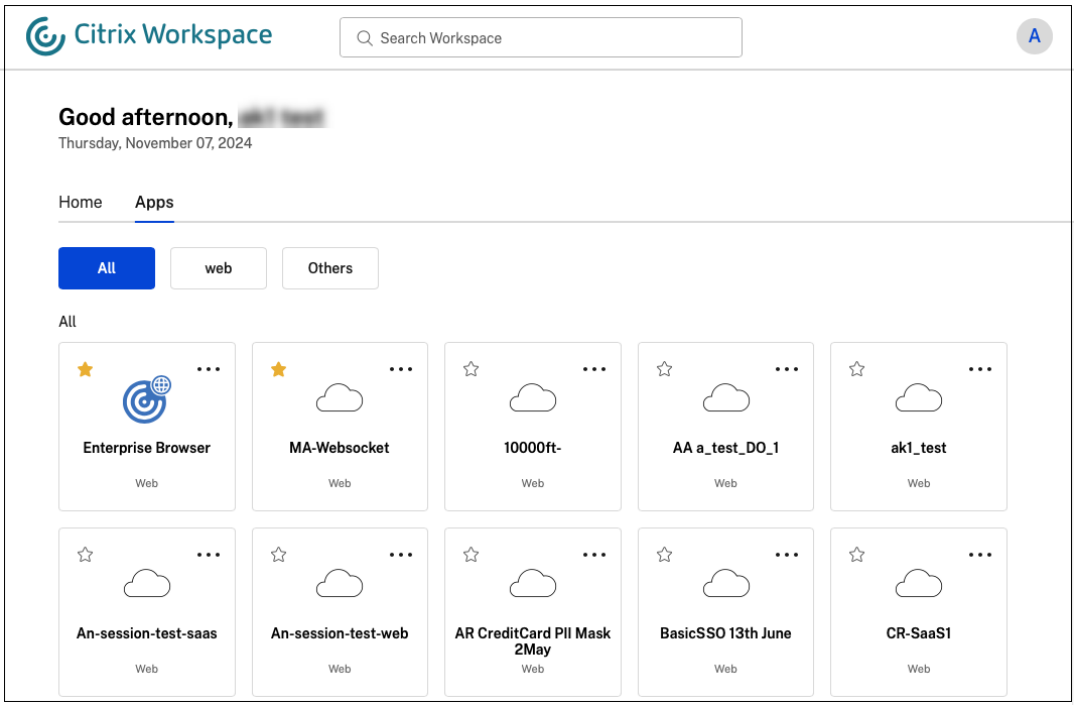


- **App-Typ** –Wählen Sie den App-Typ aus. Sie können zwischen **HTTP/HTTPS** oder **UDP/TCP** Apps wählen.
- **App-Name** –Name der Anwendung.
- **App-Beschreibung** –Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier

eingeben, wird Ihren Benutzern im Arbeitsbereich angezeigt.

- **App-Kategorie** –Fügen Sie die Kategorie und den Unterkategorienamen (falls zutreffend) hinzu, unter dem die von Ihnen veröffentlichte App in der Citrix Workspace-Benutzeroberfläche angezeigt werden muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien aus der Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angeben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.
  - Die Kategorien/Unterkategorien können vom Administrator konfiguriert werden und Administratoren 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 Kategorie-/Unterkategoriennamen müssen durch einen Backslash getrennt werden. Beispiel: **Business And Productivity\Engineering**. Außerdem muss in diesem Feld die Groß- und Kleinschreibung beachtet werden. 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** fälschlicherweise als **Geschäft und Produktivität** in das Feld **App-Kategorie** eingeben, wird in der Citrix Workspace-Benutzeroberfläche zusätzlich zur Kategorie **Geschäft und Produktivität** eine neue Kategorie mit dem Namen **Geschäft und Produktivität** aufgeführt.



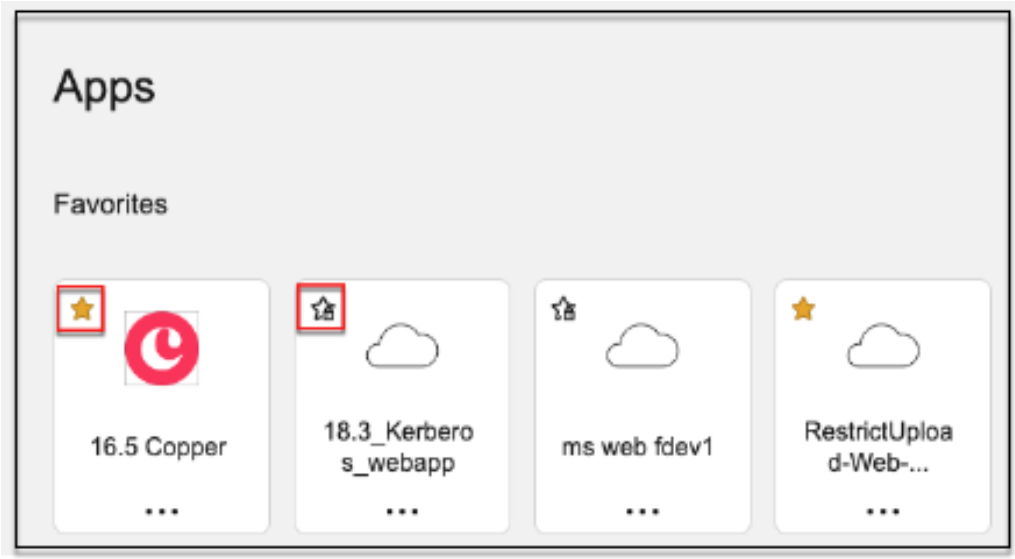
- **App-Symbol** –Klicken Sie auf **Symbol ändern** , um das App-Symbol zu ändern. Die Symboldateigröße muss 128 x 128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

```
If you do not want to display the app icon, select **Do not
   display application icon to users.**
```

- Wählen Sie **Direktzugriff** , um Benutzern den direkten Zugriff auf die App über einen Client-Browser zu ermöglichen. Einzelheiten finden Sie unter Direkter Zugriff auf Enterprise-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 Registrieren für Citrix Cloud. Falls SSO fehlschlägt oder Sie SSO nicht verwenden möchten, wird der Benutzer zu dieser URL umgeleitet.

```
**Customer domain name** and **Customer domain ID** -
   Customer domain name and ID are used to create the app URL
    and other subsequent URLs in the SAML SSO page.

For example, if you're adding a Salesforce app, your domain
   name is `salesforceformyorg` and ID is 123754, then the
   app URL is `https://salesforceformyorg.my.salesforce.com/?
   so=123754.`

Customer domain name and Customer ID fields are specific to
   certain apps.
```

- **Zugehörige Domänen** –Die zugehörige Domäne wird automatisch anhand der von Ihnen angegebenen URL eingetragen. Die zugehörige Domäne hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine zugehörige Domäne hinzufügen.
- Klicken Sie auf **Anwendung automatisch zu Favoriten hinzufügen** , um diese App als Favoriten-App in der Citrix Workspace-App hinzuzufügen.
  - Klicken Sie auf **Benutzer das Entfernen aus Favoriten erlauben** , um App-Abonnenten das Entfernen der App aus der Liste der Favoriten-Apps in der Citrix Workspace-App zu erlauben. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein gelbes Sternsymbol angezeigt.
  - Klicken Sie auf **Benutzer darf die App nicht aus Favoriten entfernen** , um zu verhindern, dass Abonnenten die App aus der Liste der Favoriten-Apps in der Citrix Workspace-App entfernen. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein Sternsymbol mit einem Vorhängeschloss angezeigt.



Wenn Sie die als Favoriten markierten Apps aus der Secure Workspace Access-Dienstkonsole 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-Dienstkonsole entfernt werden.

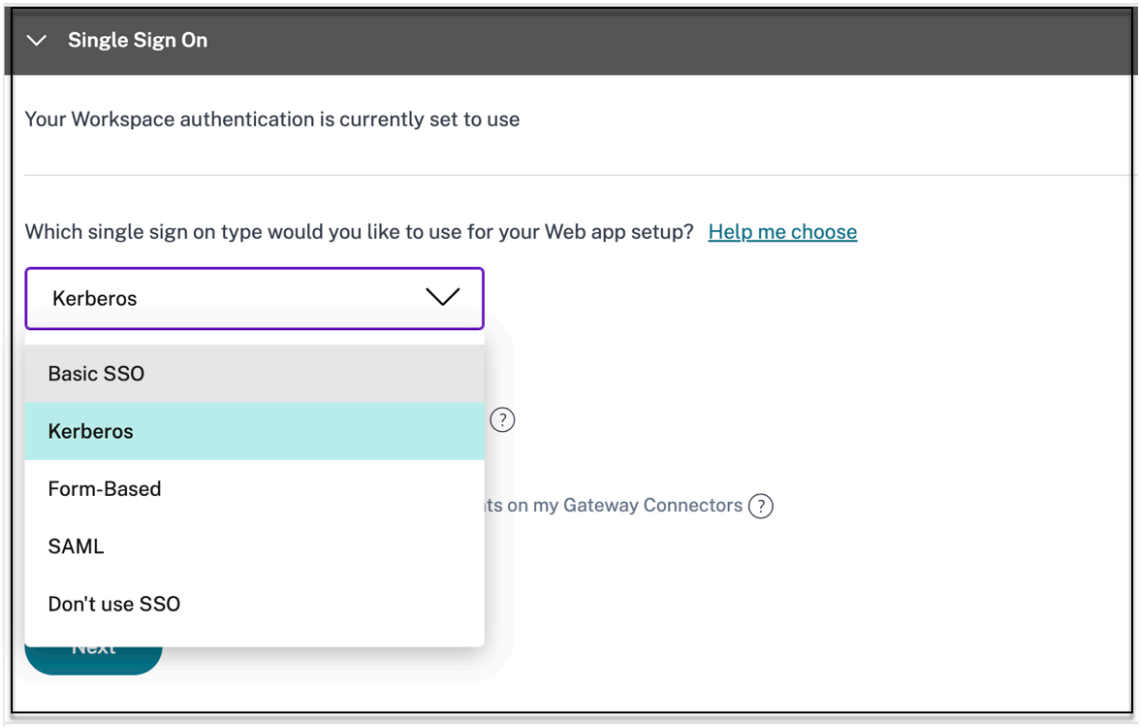
4. Klicken Sie auf **Weiter.**

Wichtig:

- Um einen Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps wird nur aktiviert, wenn der Anwendung eine Zugriffsrichtlinie zugeordnet ist. Einzelheiten hierzu finden Sie unter . Zugriff auf die Apps verweigert, standardmäßig.
- Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, kann dies zu Konfigurationskonflikten führen. Weitere Einzelheiten finden Sie unter Konfliktreiche Konfiguration, die zu App-Zugriffsproblemen führen kann.

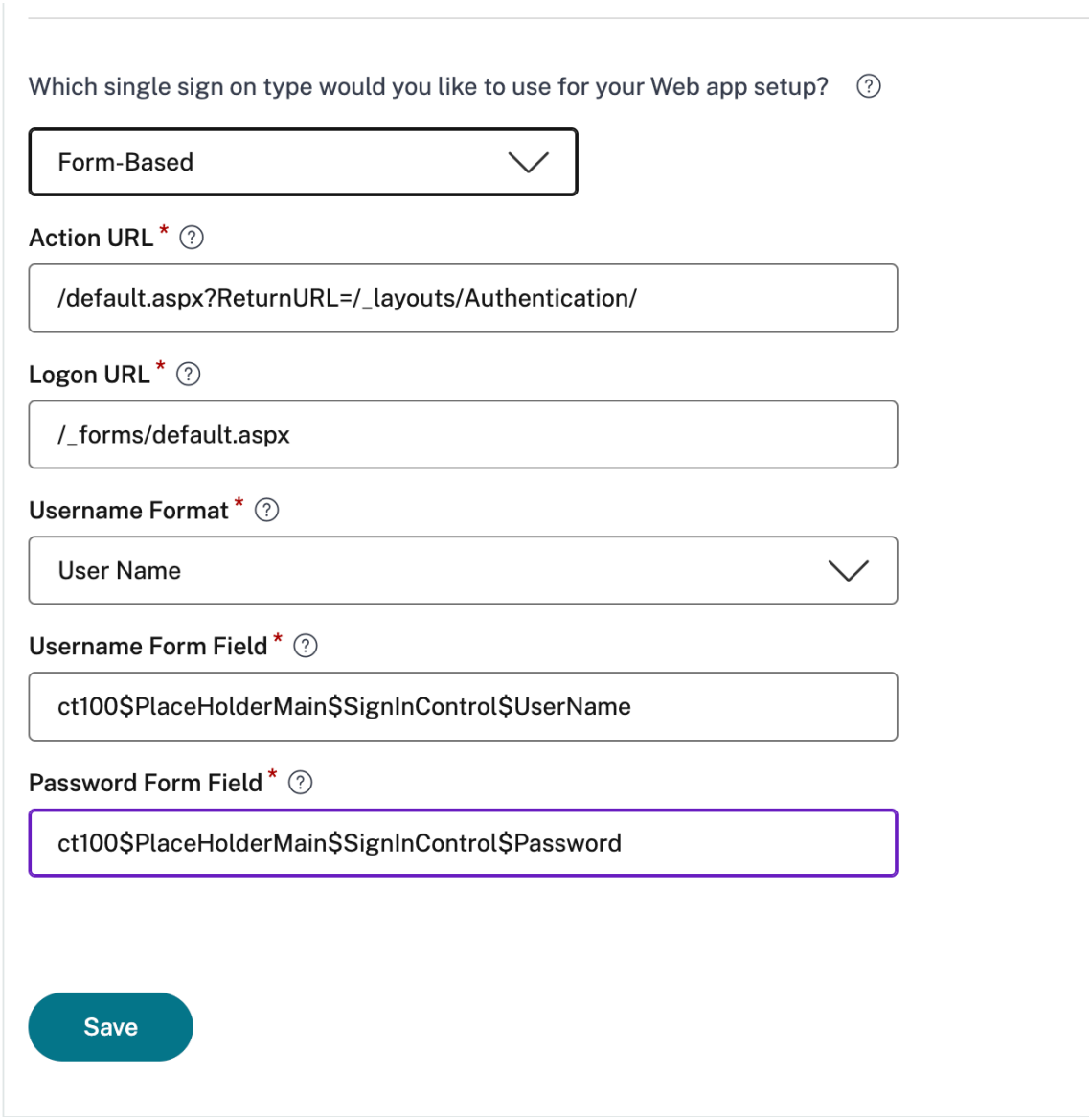
Festlegen der bevorzugten Anmeldemethode

1. Wählen Sie im Abschnitt **Single Sign On** den gewünschten Single Sign-On-Typ für Ihre Anwendung aus und klicken Sie auf **Speichern.** Die folgenden Single-Sign-On-Typen sind verfügbar.



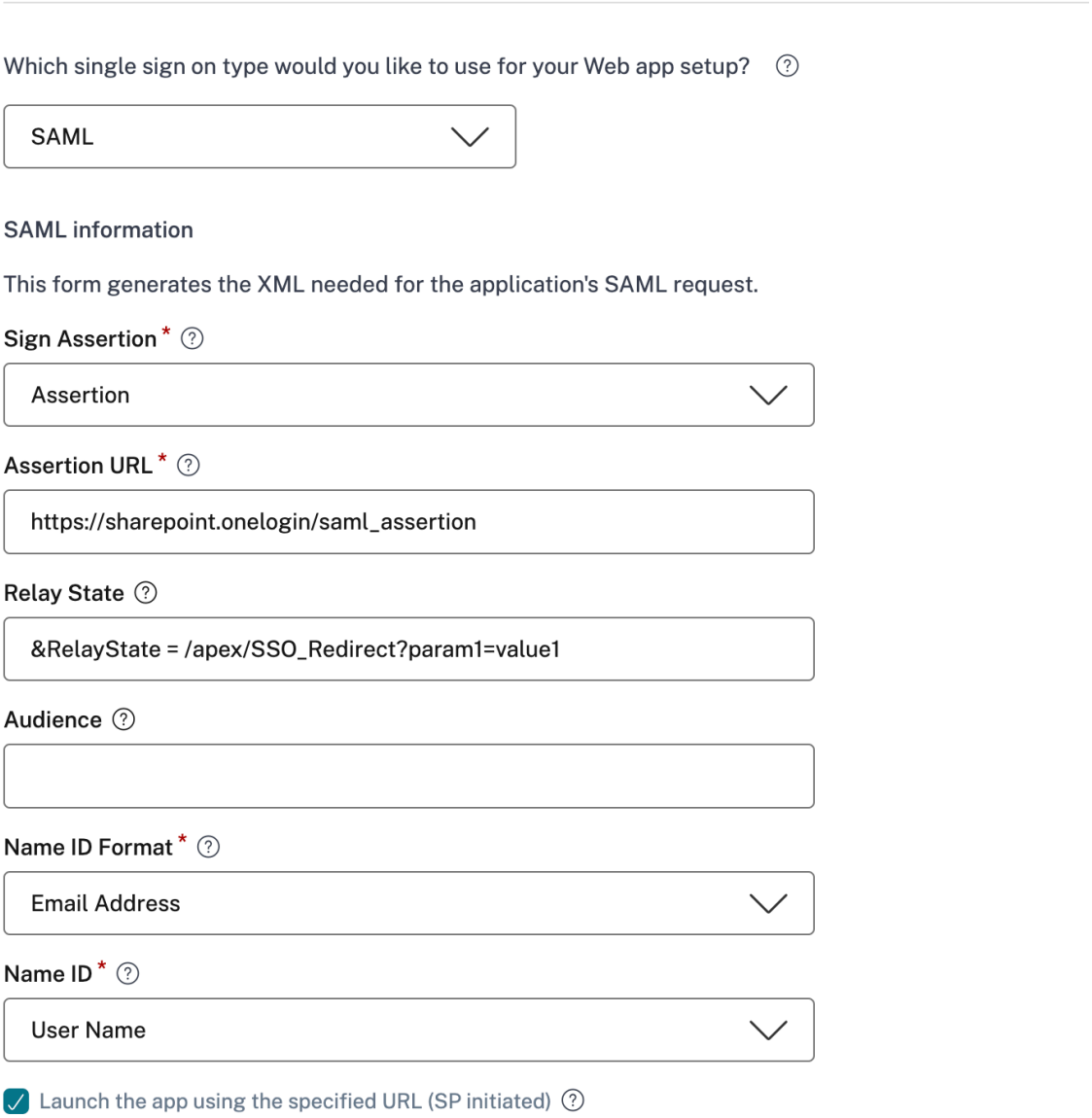
- **Basic** –Wenn Ihr Back-End-Server Ihnen eine Basic-401-Herausforderung präsentiert, wählen Sie **Basic SSO**. Für den SSO-Typ **Basic** müssen Sie keine Konfigurationsdetails angeben.
- **Kerberos** –Wenn Ihr Back-End-Server Ihnen die Negotiate-401-Aufforderung präsentiert, wählen Sie **Kerberos**. Sie müssen keine Konfigurationsdetails für den SSO-Typ **Kerberos** angeben.
- **Formularbasiert** –Wenn Ihr Back-End-Server Ihnen ein HTML-Formular zur Authentifizierung vorlegt, wählen Sie **Formularbasiert**. Geben Sie die Konfigurationsdetails für die **Formularbasiert** SSO-Typ.
- **SAML** –Wählen Sie **SAML** für SAML-basiertes SSO in Webanwendungen. Geben Sie die Konfigurationsdetails für den SSO-Typ **SAML** ein.
- **SSO nicht verwenden** –Verwenden Sie die Option **SSO nicht verwenden** , wenn Sie einen Benutzer auf dem Back-End-Server nicht authentifizieren müssen. Wenn die Option **SSO nicht verwenden** ausgewählt ist, wird der Benutzer zu der im Abschnitt **App-Details** konfigurierten URL umgeleitet.

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



- **Aktions-URL** –Geben Sie die URL ein, an die das ausgefüllte Formular gesendet wird.
- **URL des Anmeldeformulars** –Geben Sie die URL ein, unter der das Anmeldeformular angezeigt wird.
- **Benutzernamenformat** –Wählen Sie ein Format für den Benutzernamen.
- **Benutzernamen-Formularfeld** –Geben Sie ein Benutzernamenattribut ein.
- **Kennwortformularfeld** –Geben Sie ein Kennwortattribut ein.

SAML: Geben Sie im Abschnitt „Anmelden“die folgenden Details ein und klicken Sie auf „Speichern“.



- **Signierbehauptung** - Durch das Signieren einer Behauptung oder Antwort wird die Nachrichtenintegrität sichergestellt, wenn die Antwort oder Behauptung an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Response, Both,** oder **None**auswählen.
- **Assertion-URL** –Die Assertion-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.
- **Relay-Status** –Der Relay-Status-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die die Benutzer zugreifen, nachdem sie sich angemeldet und zum Verbundserver der vertrauenden Seite weitergeleitet wurden. Relay State 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 wird.
- **Namens-ID-Format** –Wählen Sie das unterstützte Namenskennungsformat aus.
- **Namens-ID** –Wählen Sie die unterstützte Namens-ID aus.

2. Fügen Sie in **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 beim Konfigurieren von SSO auf dem SaaS-App-Server verwenden.
> - Sie können das Zertifikat auch aus der Liste „ **Zertifikat** “herunterladen und es beim Konfigurieren von SSO auf dem SaaS-App-Server verwenden.

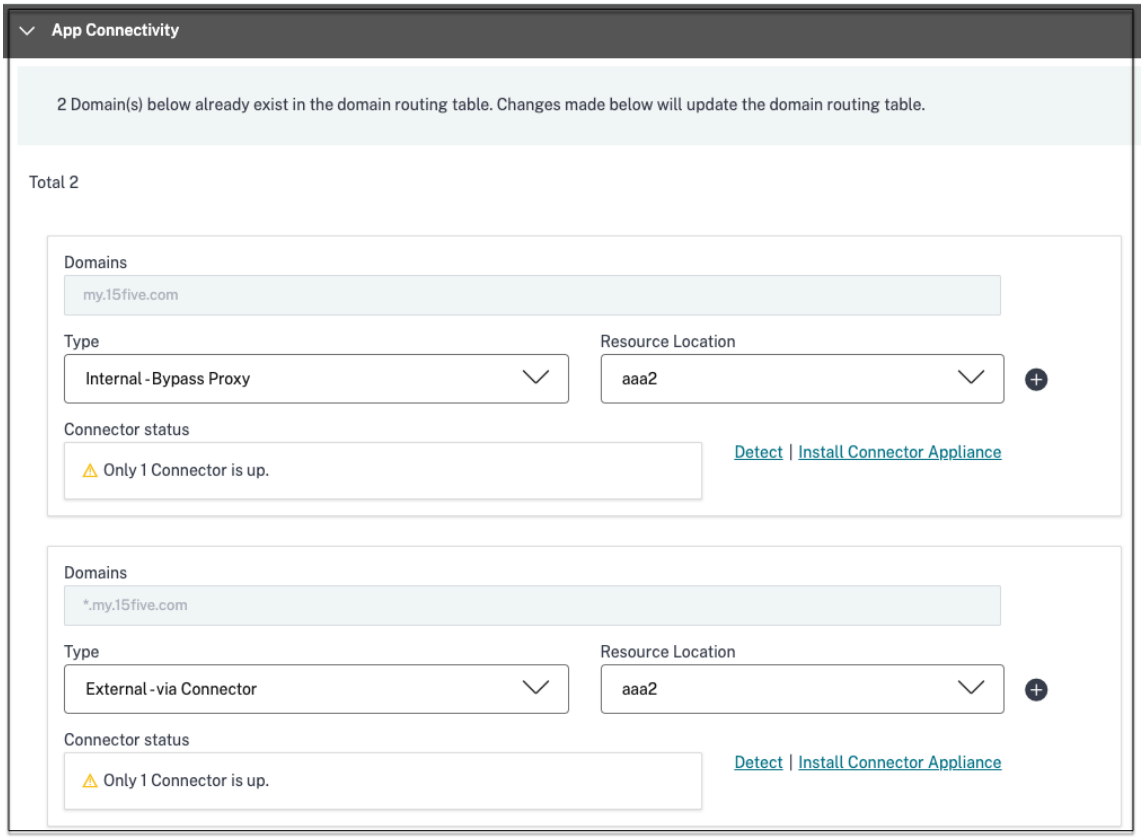
1. Klicken Sie auf **Weiter.**

Definieren des Anwendungsroutings

1. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die entsprechenden Anwendungsdomänen, ob die Domänen extern oder intern über das Citrix Connector Appliance geroutet werden müssen.

   - **Intern –Proxy umgehen** –Der Domänenverkehr wird über Citrix Cloud Connector geleitet und der auf dem Connector Appliance konfigurierte Webproxy des Kunden wird umgangen.
   - **Intern über Connector** –Die Apps können extern sein, aber der Datenverkehr muss über das Connector-Gerät zum externen Netzwerk fließen.
   - **Extern** –Der Datenverkehr fließt direkt ins Internet.

   Weitere Einzelheiten finden Sie unter Routentabellen zum Lösen von Konflikten, wenn die zugehörigen Domänen in SaaS- und Web-Apps identisch sind.

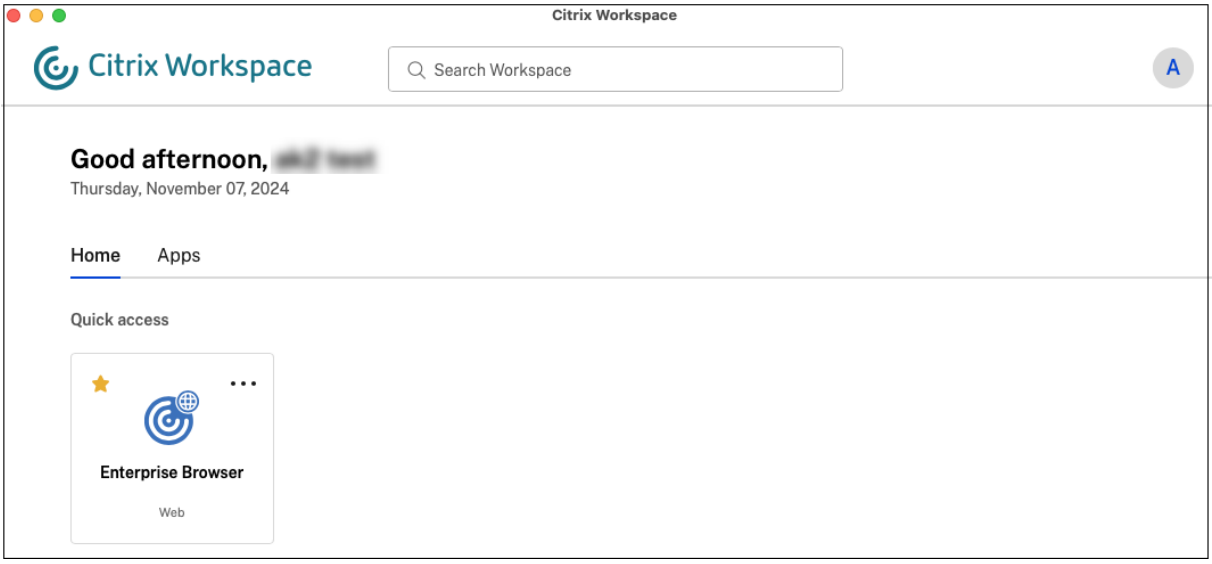


2. Klicken Sie auf **„Fertig“.**

   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 auf die Auslassungspunkte-Schaltfläche einer App und wählen Sie die entsprechenden Aktionen aus.

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

Wenn Sie eine Web- oder SaaS-App vom Secure Workspace Access-Dienst 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 Arbeitsbereichsbrowser ohne URL starten und über den Arbeitsbereichsbrowser 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.

Direkter Zugriff auf Enterprise-Web-Apps

October 21, 2024

Auf Unternehmens-Webanwendungen wie SharePoint, JIRA, Confluence und andere, die beim Kunden entweder vor Ort oder in öffentlichen Clouds gehostet werden, kann jetzt direkt über einen Client-Browser zugegriffen werden. Endbenutzer müssen den Zugriff auf ihre Unternehmens-Web-Apps nicht mehr über Citrix Workspace initiieren. Mithilfe dieser Funktion können Endbenutzer außerdem auf die Web-Apps zugreifen, indem sie in ihren E-Mails, Collaboration-Tools oder Browser-Lesezeichen auf Links klicken. Auf diese Weise wird den Kunden eine echte Zero-Footprint-Lösung bereitgestellt.

Funktionsweise

- Fügen Sie einen neuen DNS-Eintrag hinzu oder ändern Sie einen vorhandenen DNS-Eintrag für die konfigurierten Enterprise-Web-Apps.

- Der IT-Administrator würde einen neuen öffentlichen DNS-Eintrag hinzufügen oder einen vorhandenen öffentlichen DNS-Eintrag für den konfigurierten FQDN der Unternehmens-Web-App ändern, um den Benutzer zum Citrix Secure Private Access-Dienst umzuleiten.
- Wenn der Endbenutzer den Zugriff auf die konfigurierte Unternehmens-Web-App initiiert, wird der App-Datenverkehr an den Citrix Secure Private Access-Dienst umgeleitet, der dann den Zugriff auf die App über einen Proxy verwaltet.
- Sobald die Anforderung beim Citrix Secure Workspace Access-Dienst eingeht, überprüft dieser die Benutzerauthentifizierung und Anwendungsautorisierung, einschließlich kontextbezogener Überprüfungen der Zugriffsrichtlinien.
- Nach erfolgreicher Validierung kommuniziert der Citrix Secure Private Access-Dienst mit Citrix Cloud Connector Appliances, die in der Umgebung des Kunden (entweder vor Ort oder in der Cloud) bereitgestellt werden, um den Zugriff auf die konfigurierte Unternehmens-Web-App zu ermöglichen.

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

Voraussetzungen

Bevor Sie beginnen, müssen Sie Folgendes für die Anwendung konfigurieren.

- Anwendungs-FQDN
- SSL-Zertifikat –Öffentliches Zertifikat für die zu konfigurierende App
- Ressourcenstandort –Installieren Sie Citrix Cloud Connector Appliances
- Zugriff auf den öffentlichen DNS-Eintrag, um ihn mit dem kanonischen Namen (CNAME) zu aktualisieren, der von Citrix während der App-Konfiguration bereitgestellt wird.

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

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

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

> **Hinweis:**
>
> Die Schaltfläche **Weiter** wird nur beim ersten Verwenden des Assistenten angezeigt. Bei der nachfolgenden Verwendung können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen**klicken.

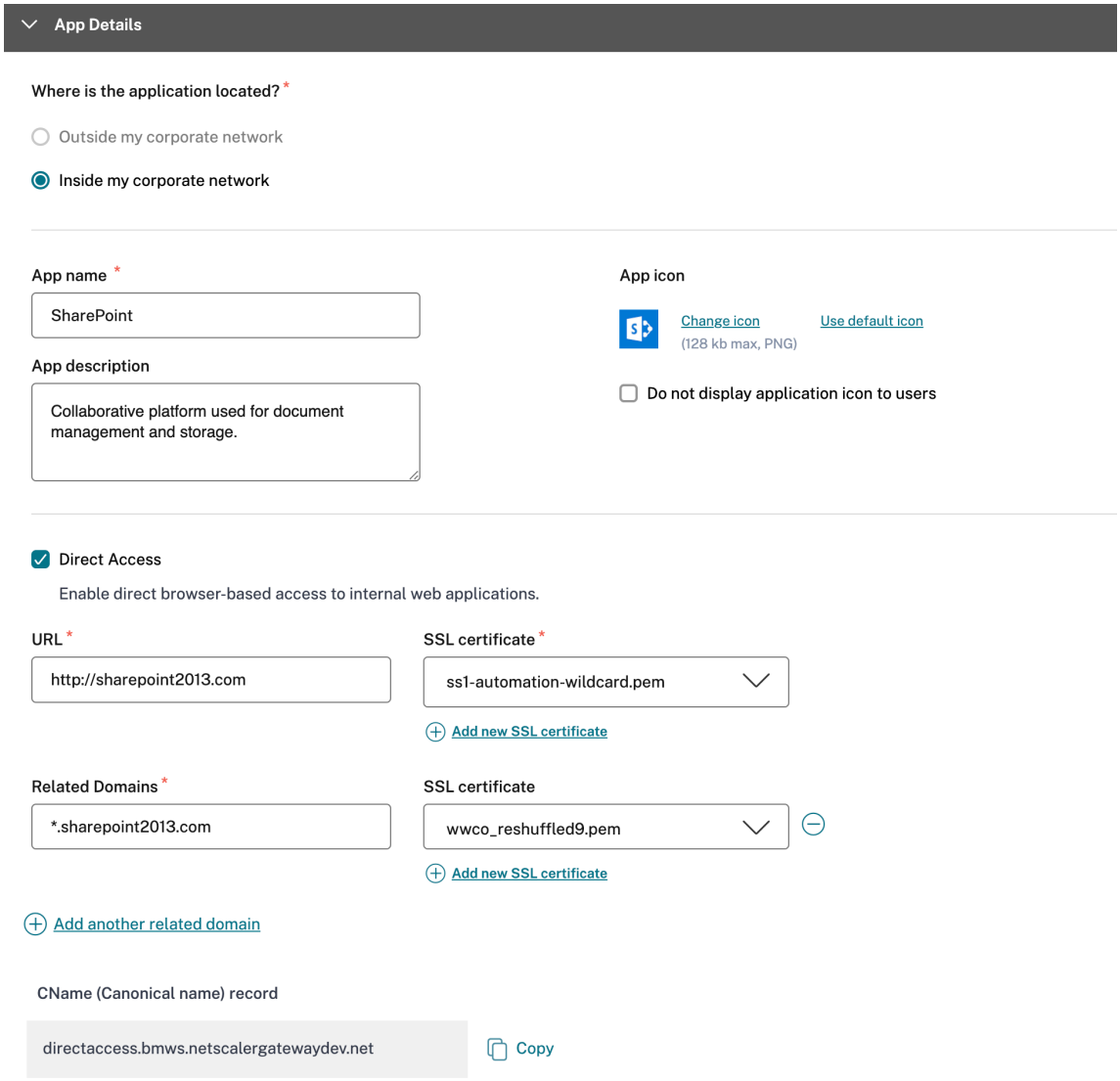
1. Richten Sie Identität und Authentifizierung ein. Weitere Einzelheiten finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichten.
2. Fahren Sie mit dem Hinzufügen einer App fort. Einzelheiten finden Sie unter Anwendungen hinzufügen und verwalten.
3. Wählen Sie die App aus, die Sie hinzufügen möchten, und klicken Sie auf **Überspringen.**
4. Wählen Sie unter **Wo befindet sich der Anwendungsspeicherort?**den Speicherort aus.
5. Geben Sie die folgenden Details im Abschnitt **App-Details** ein und klicken Sie auf **Weiter**.
   - **App-Typ** –Wählen Sie den App-Typ (HTTP oder HTTPS).
   - **App-Name** –Name der Anwendung.
   - **App-Beschreibung** –Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Arbeitsbereich angezeigt.
   - **App-Symbol** –Klicken Sie auf **Symbol ändern** , um das App-Symbol zu ändern. Die Symboldateigröße muss 128 x 128 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**.
6. Wählen Sie **Direktzugriff** , um Benutzern den direkten Zugriff auf die App über einen Client-Browser zu ermöglichen. 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 ein vorhandenes SSL-Zertifikat aus dem Dropdown-Menü aus oder fügen Sie ein neues SSL-Zertifikat hinzu, indem Sie auf **Neues SSL-Zertifikat hinzufügen**klicken.

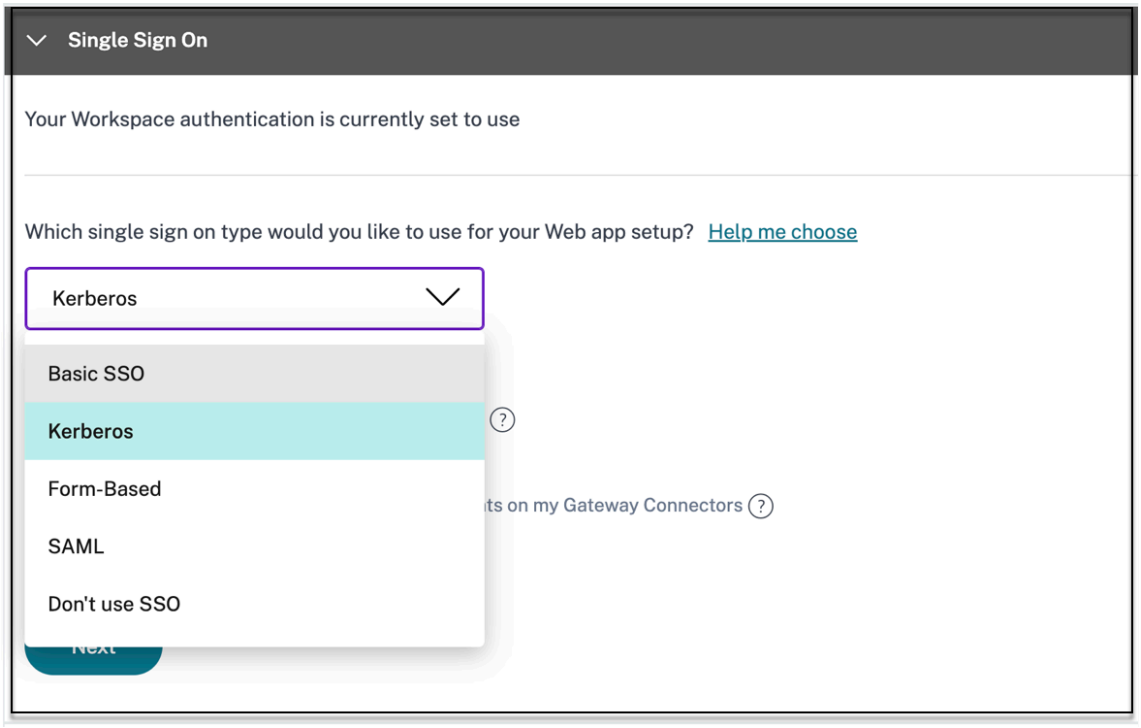
     Wichtige Hinweise:

     - Es wird nur ein öffentliches oder vertrauenswürdiges CA-Zertifikat unterstützt. Selbstsignierte Zertifikate werden nicht unterstützt.
     - Es muss eine vollständige Zertifikatskette hochgeladen werden.
   - **Zugehörige Domänen** –Die zugehörige Domäne wird automatisch anhand der von Ihnen angegebenen URL eingetragen. Die zugehörige Domäne hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine zugehörige Domäne hinzufügen. Sie können an jede zugehörige Domäne ein SSL-Zertifikat binden, dies ist optional.

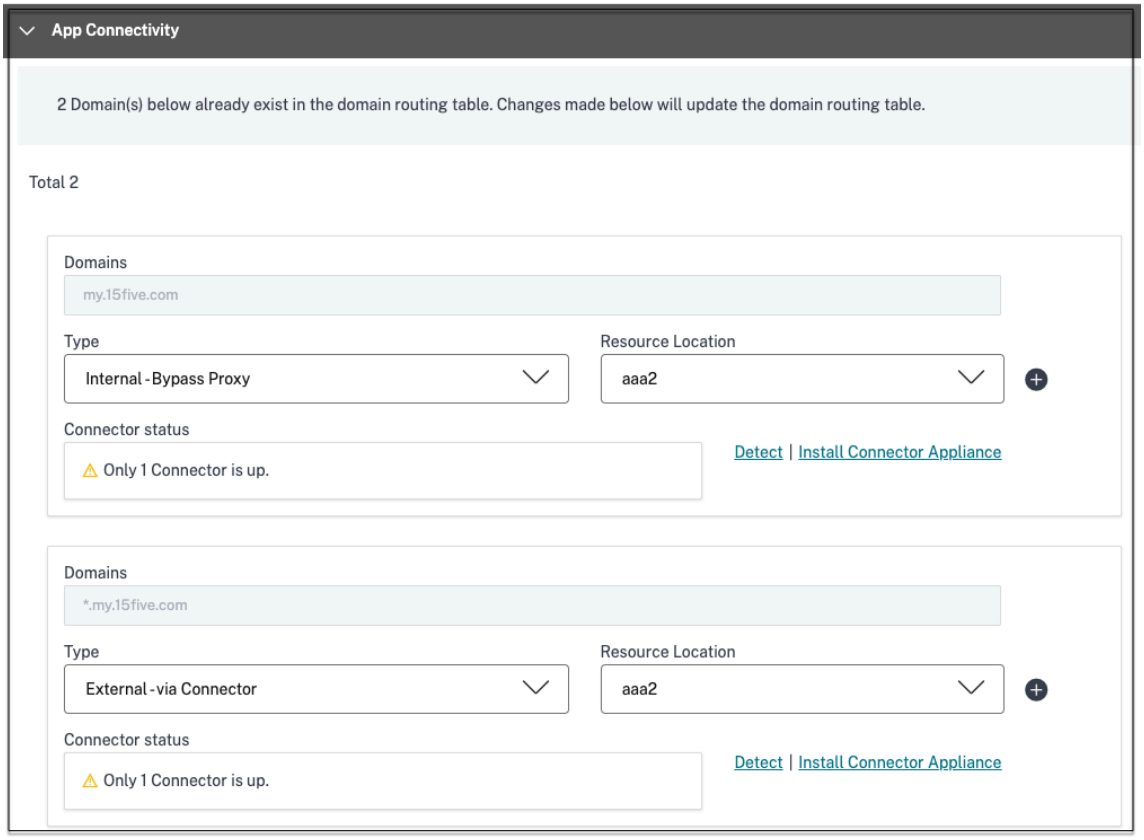
- **CName-Eintrag** –Automatisch generiert von Secure Private Access. Dies ist der Wert, der im DNS eingetragen werden muss, um den direkten Zugriff auf die Anwendung zu ermöglichen.



7. Klicken Sie auf **Weiter.**
8. Wählen Sie im Abschnitt **Single Sign-On** den gewünschten Single Sign-On-Typ für Ihre Anwendung aus und klicken Sie auf**Weiter**.



9. Im Abschnitt **App-Konnektivität** können Sie entweder einen vorhandenen Ressourcenstandort auswählen oder einen erstellen und ein neues Connector-Gerät bereitstellen. Um einen vorhandenen Ressourcenstandort auszuwählen, klicken Sie in der Liste der Ressourcenstandorte auf einen davon, beispielsweise „Mein Ressourcenstandort“, und klicken Sie auf**Weiter**. Weitere Einzelheiten finden Sie unter Routentabellen zum Lösen von Konflikten, wenn die zugehörigen Domänen in SaaS- und Web-Apps identisch sind.



10. Klicken Sie auf **Fertigstellen**. Die App wird zur Seite „Anwendungen“hinzugefügt. Sie können eine Anwendung auf der Seite „Anwendungen“bearbeiten oder löschen, nachdem Sie sie konfiguriert haben. Klicken Sie dazu auf die Auslassungspunkte-Schaltfläche einer App und wählen Sie die entsprechenden Aktionen aus.

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

> **Wichtig:**
>
> - Um einen Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps wird 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 Konfigurationskonflikten führen. Informationen zum Vermeiden von Konfigurationskonflikten finden Sie unter Best Practices für Web- und SaaS-Anwendungskonfigurationen.

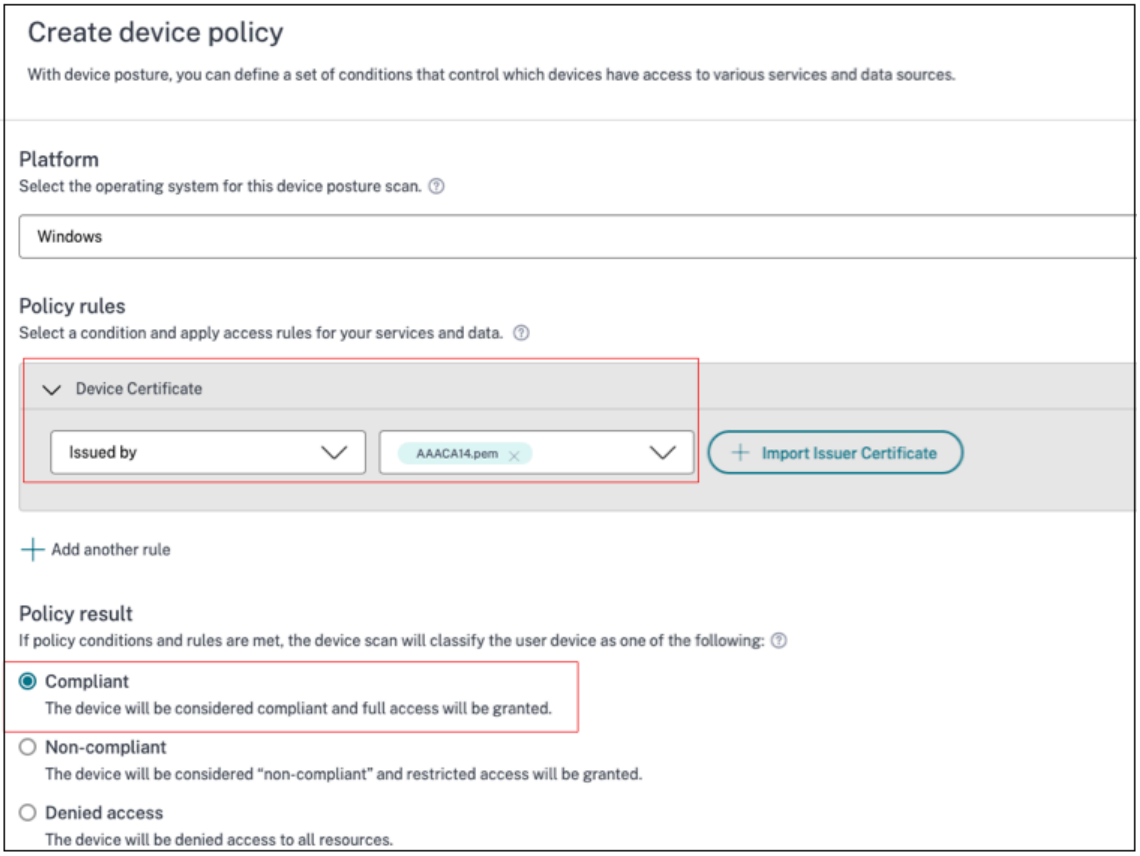
Device Posture-Dienst mit Direktzugriffs-Apps

Citrix Secure Private Access mit Direktzugriffs-Apps kann in Kombination mit dem Device Posture-Dienst sicherstellen, dass nur konforme Geräte per Direktzugriff auf vertrauliche Anwendungen zugreifen. Administratoren können den Zugriff auf nicht konforme oder nicht verwaltete Geräte basierend auf den Scan-Ergebnissen des Device Posture-Dienstes blockieren.

Schritte zum Aktivieren des direkten Zugriffs nur für kompatible Geräte

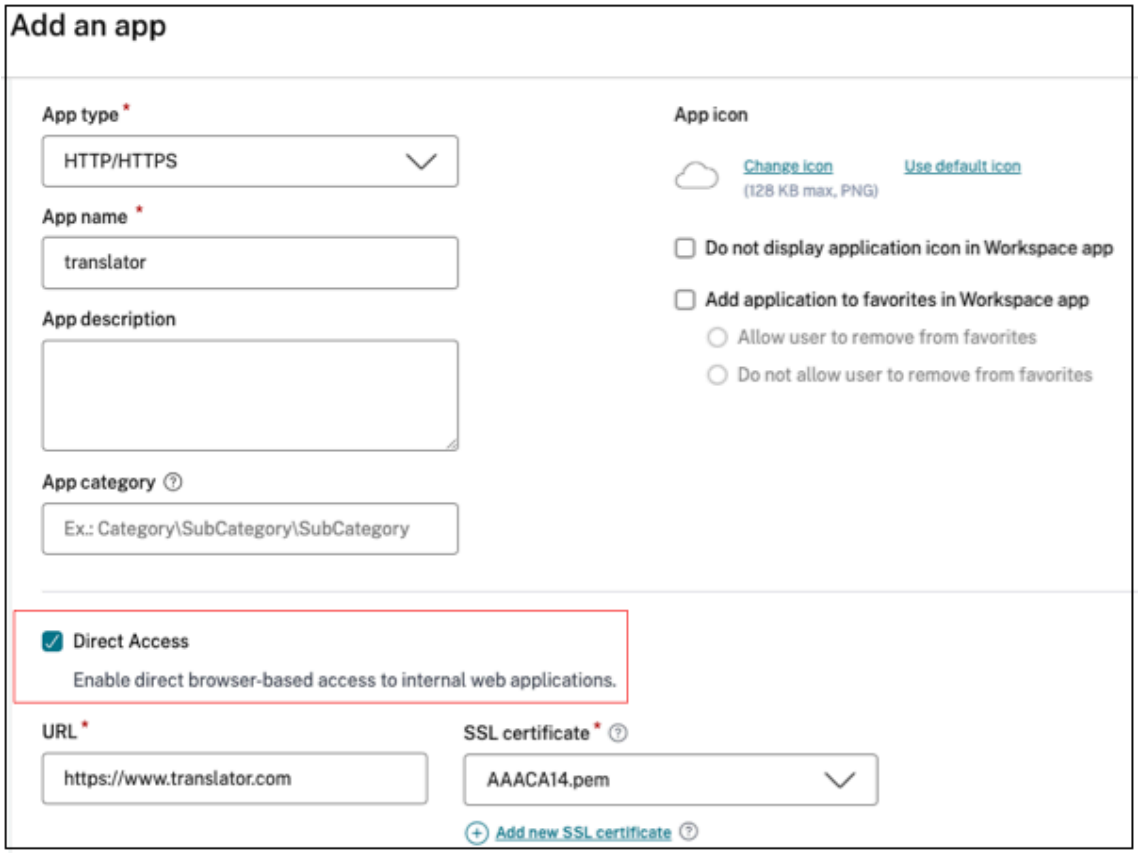
Um den direkten Zugriff nur auf kompatible Geräte zu ermöglichen, muss der Administrator die folgenden Schritte ausführen:

1. Erstellen Sie in der Verwaltungskonsole des Device Posture-Dienstes eine Geräte-Posture-Richtlinie, um die Bedingungen des Geräte-Posture-Scans zu überprüfen, z. B. Gerätezertifikat, Antivirus, Browser, und wählen Sie dann „ **Konform** “als Richtlinienergebnisaktion aus. Einzelheiten finden Sie unter Gerätehaltung konfigurieren.



2. Führen Sie in der Secure Workspace Access-Administratorkonsole Folgendes aus:

   - Erstellen Sie eine Anwendung, für die Sie den direkten Zugriff aktivieren möchten. Einzelheiten finden Sie unter Direkter Zugriff auf Enterprise-Web-Apps.



- Konfigurieren Sie Secure Private Access mit Device Posture. Wählen Sie in **Regelbereich Gerätehaltungsprüfung > Entspricht einem von** aus und geben Sie das Tag **Konform**ein. Dieses Tag wird vom Device Posture-Dienst gesendet.

> **Hinweis:**
>
> Das Tag muss genauso eingegeben werden, wie es zuvor erfasst wurde, mit Großbuchstaben am Anfang (konform). Andernfalls funktionieren die Gerätehaltungsrichtlinien nicht wie vorgesehen. Einzelheiten finden Sie unter Citrix Secure Private Access-Konfiguration mit Device Posture.

```
1 ![Gerätehaltung für Direktzugriff3](/en-us/citrix-secure-private-access
    /media/spa-direct-access-device-posture-3.png)
```

Sobald diese Konfiguration durchgeführt wurde, wird das Gerät basierend auf den Ergebnissen des Gerätestatus-Scans als konform, nicht konform oder Anmeldung verweigert gekennzeichnet und der App-Zugriff entsprechend aktiviert.

Beispiel:

Nehmen wir an, Sie haben eine Gerätestatusrichtlinie erstellt, um das Vorhandensein eines Gerätezertifikats auf einem Endpunktgerät zu überprüfen und dessen Anmeldestatus zu bestimmen. Sobald die Gerätehaltungsrichtlinien festgelegt und die Gerätehaltung aktiviert ist, werden die folgenden Ak-

tionen ausgeführt, wenn sich ein Endbenutzer bei Citrix Workspace anmeldet.

1. Der Gerätestatus-Scan überprüft das Endpunktgerät auf das Vorhandensein eines Gerätezertifikats.
    - Wenn das Gerätezertifikat auf dem Gerät vorhanden ist, wird das Gerät als **-konform**gekennzeichnet.
    - Wenn das Gerätezertifikat auf dem Gerät nicht vorhanden ist, wird das Gerät als **nicht konform**gekennzeichnet.
2. Diese Informationen werden dann als Tags an den Citrix Secure Workspace Access-Dienst weitergegeben.
3. Die Zugriffsrichtlinie wird basierend auf der Geräteklassifizierung ausgewertet.
    - Wenn das Gerät kompatibel ist, ist der direkte Zugriff auf die Apps erlaubt.
    - Wenn das Gerät nicht kompatibel ist, wird der direkte Zugriff auf die Apps deaktiviert.

Endbenutzererfahrung

Das Endbenutzererlebnis basiert auf der Einstufung des Geräts als konform oder nicht konform.

- **Kompatibles Gerät:**

  Der Benutzer kann die Direktzugriffs-App von Citrix Workspace oder über die App-URL vom Browser aus starten.

- **Nicht konformes Gerät:**
    - Die App ist in Citrix Workspace nicht aufgeführt.
    - Der Benutzer kann die App nicht über die App-URL vom Browser aus starten.
    - Dem Benutzer wird eine Seite mit gesperrtem Zugriff angezeigt.

Unterstützung für Software-as-a-Service-Apps

October 21, 2024

Software as a Service (SaaS) ist ein Softwareverteilungsmodell zur Remote-Bereitstellung von Software als webbasierter Dienst. Zu den häufig verwendeten SaaS-Apps gehören Salesforce, Workday, Concur, GoToMeeting usw.

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

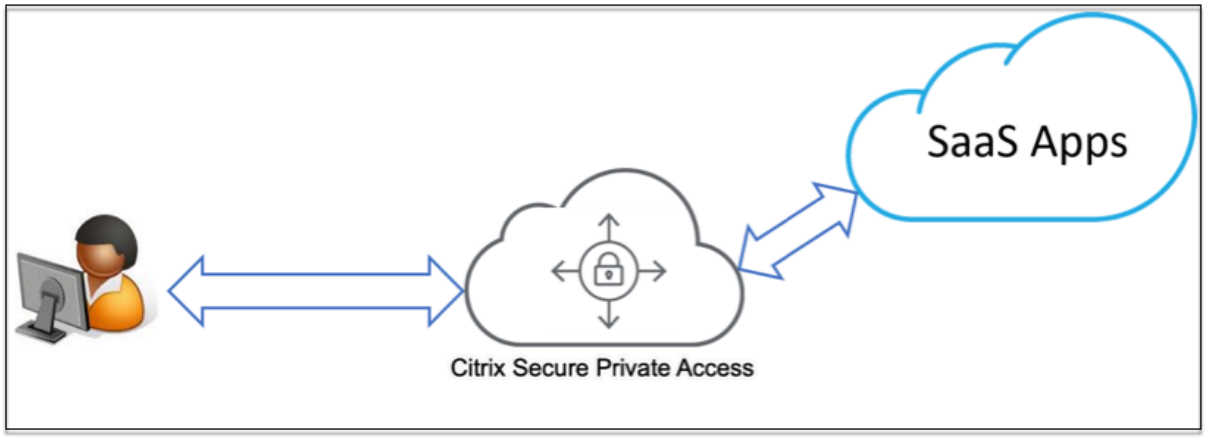
Die Bereitstellung von SaaS-Apps mithilfe des Secure Private Access-Dienstes bietet Ihnen eine einfache, sichere, robuste und skalierbare Lösung zur Verwaltung der Apps. Über die Cloud bereitgestellte SaaS-Apps bieten die folgenden Vorteile:

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

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

1. Der Kundenadministrator konfiguriert SaaS-Apps mithilfe der Benutzeroberfläche des Secure Private Access-Dienstes.
2. Der Administrator stellt den Benutzern die Service-URL für den Zugriff auf Citrix Workspace zur Verfügung.
3. Um die App zu starten, klickt ein Benutzer auf das aufgelistete SaaS-App-Symbol.
4. Die SaaS-App vertraut der vom Secure Private Access-Dienst bereitgestellten SAML-Assertion 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 aggregiert, um ein einheitliches Benutzererlebnis zu ermöglichen.



Konfigurieren einer SaaS-App

Das Konfigurieren einer SaaS-App umfasst die folgenden allgemeinen Schritte.

1. Konfigurieren der Anwendungsdetails
2. Festlegen der bevorzugten Anmeldemethode
3. Definieren des Anwendungsroutings

Konfigurieren der Anwendungsdetails

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

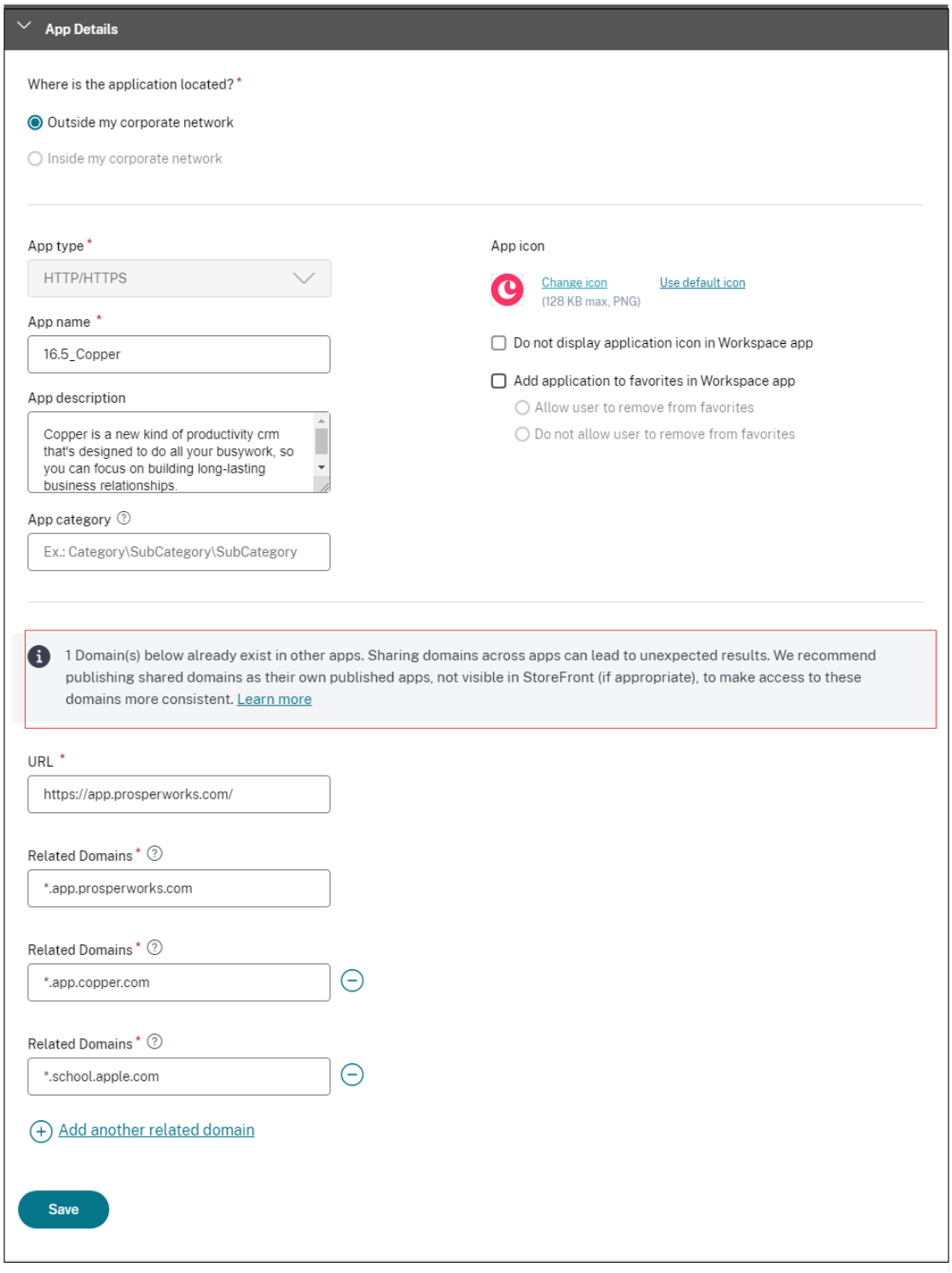
> **Hinweis:**
>
> - Die Schaltfläche **Weiter** wird nur beim ersten Verwenden des Assistenten angezeigt. Bei der nachfolgenden Verwendung können Sie direkt zur Seite **Anwendungen** navigieren und dann auf **App hinzufügen klicken.**
> - Sie können eine SaaS-App manuell hinzufügen, indem Sie die App-Details eingeben oder eine App-Vorlage auswählen, die für eine Liste beliebter SaaS-Apps verfügbar ist. Viele der für die Anwendungskonfiguration erforderlichen Informationen sind in der Vorlage bereits eingetragen. Die Angabe kundenspezifischer Informationen ist allerdings weiterhin erforderlich. Einzelheiten zur Konfigurationsvorlage für SaaS-Apps finden Sie unter SaaS-App-Server-spezifische Konfiguration.

1. Konfigurieren Sie 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 für eine SaaS-App standardmäßig aktiviert.

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

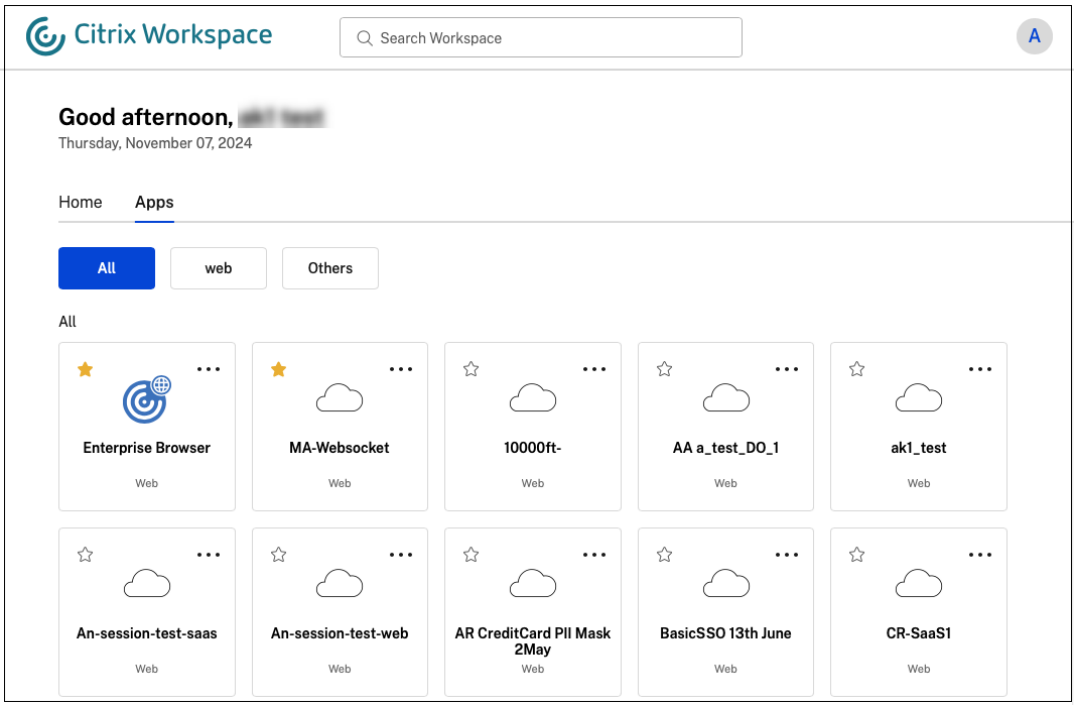


- **App-Name** –Name der Anwendung.
- **App-Beschreibung** –Eine kurze Beschreibung der App. Diese Beschreibung, die Sie hier eingeben, wird Ihren Benutzern im Arbeitsbereich angezeigt.
- **App-Kategorie** –Fügen Sie die Kategorie und den Unterkategorienamen (falls zutr-

effend) hinzu, unter dem die von Ihnen veröffentlichte App in der Citrix Workspace-Benutzeroberfläche angezeigt werden muss. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien aus der Citrix Workspace-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angeben, wird die App in der Workspace-Benutzeroberfläche unter der jeweiligen Kategorie angezeigt.

- Die Kategorien/Unterkategorien können vom Administrator konfiguriert werden und Administratoren 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 Kategorie-/Unterkategoriennamen müssen durch einen Backslash getrennt werden. Beispiel: **Business And Productivity\Engineering**. Außerdem muss in diesem Feld die Groß- und Kleinschreibung beachtet werden. 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** fälschlicherweise als **Geschäft und Produktivität** in das Feld **App-Kategorie** eingeben, wird in der Citrix 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 Symboldateigröße muss 128 x 128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das

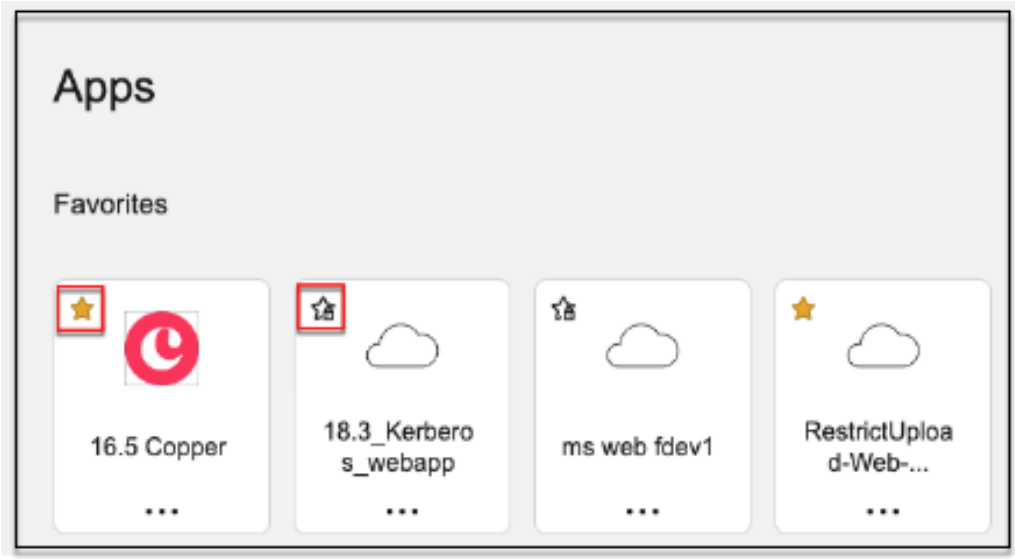
Standardsymbol angezeigt.

```
If you do not want to display the app icon, select **Do not
   display application icon to users**.
```

- **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 Registrieren für Citrix Cloud. Falls SSO fehlschlägt oder Sie SSO nicht verwenden möchten, wird der Benutzer zu dieser URL umgeleitet.
- **Kundendomänenname** und **Kundendomänen-ID** –Kundendomänenname und -ID werden verwendet, um die App-URL und andere nachfolgende URLs auf der SAML-SSO-Seite zu erstellen.

```
For example, if you're adding a Salesforce app, your domain
   name is `salesforceformyorg` and ID is 123754, then the
   app URL is `https://salesforceformyorg.my.salesforce.com/?
   so=123754.`

Customer domain name and Customer ID fields are specific to
   certain apps.
```

- **Zugehörige Domänen** –Die zugehörige Domäne wird automatisch anhand der von Ihnen angegebenen URL eingetragen. Die zugehörige Domäne hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine zugehörige Domäne hinzufügen.
- Klicken Sie auf **Anwendung automatisch zu Favoriten hinzufügen** , um diese App als Favoriten-App in der Citrix Workspace-App hinzuzufügen.
  - Klicken Sie auf **Benutzer das Entfernen aus Favoriten erlauben** , um App-Abonnenten das Entfernen der App aus der Liste der Favoriten-Apps in der Citrix Workspace-App zu erlauben. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein gelbes Sternsymbol angezeigt.
  - Klicken Sie auf **Benutzer darf die App nicht aus Favoriten entfernen** , um zu verhindern, dass Abonnenten die App aus der Liste der Favoriten-Apps in der Citrix Workspace-App entfernen. Wenn Sie diese Option auswählen, wird in der oberen linken Ecke der App in der Citrix Workspace-App ein Sternsymbol mit einem Vorhängeschloss angezeigt.



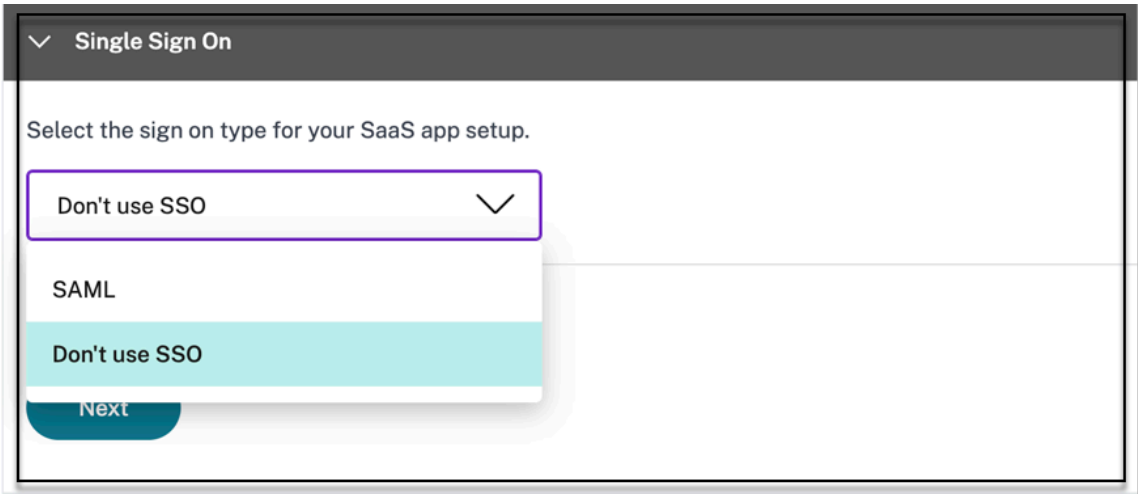
Wenn Sie die als Favoriten markierten Apps aus der Secure Workspace Access-Dienstkonsole entfernen, müssen diese Apps manuell aus der Favoritenliste in Citrix Workspace entfernt werden. Die Apps werden nicht automatisch aus der Workspace-App gelöscht, wenn sie aus der Secure Private Access-Dienstkonsole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

3. Klicken Sie auf **Weiter.**

> **Wichtig:**
>
> - Um einen Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird Apps standardmäßig der Zugriff verweigert. Der Zugriff auf die Apps wird nur aktiviert, wenn der Anwendung eine Zugriffsrichtlinie zugeordnet ist. Einzelheiten hierzu finden Sie unter . Zugriff auf die Apps verweigert, standardmäßig.
> - Wenn mehrere Apps mit demselben FQDN oder einer Variante des Platzhalter-FQDN konfiguriert sind, kann dies zu Konfigurationskonflikten führen. Weitere Einzelheiten finden Sie unter Konfliktreiche Konfiguration, die zu App-Zugriffsproblemen führen kann.

Festlegen einer bevorzugten Anmeldemethode

1. Wählen Sie im Abschnitt **Single Sign On** den gewünschten Single Sign-On-Typ für Ihre Anwendung aus und klicken Sie auf **Speichern.** Die folgenden Single-Sign-On-Typen sind verfügbar.

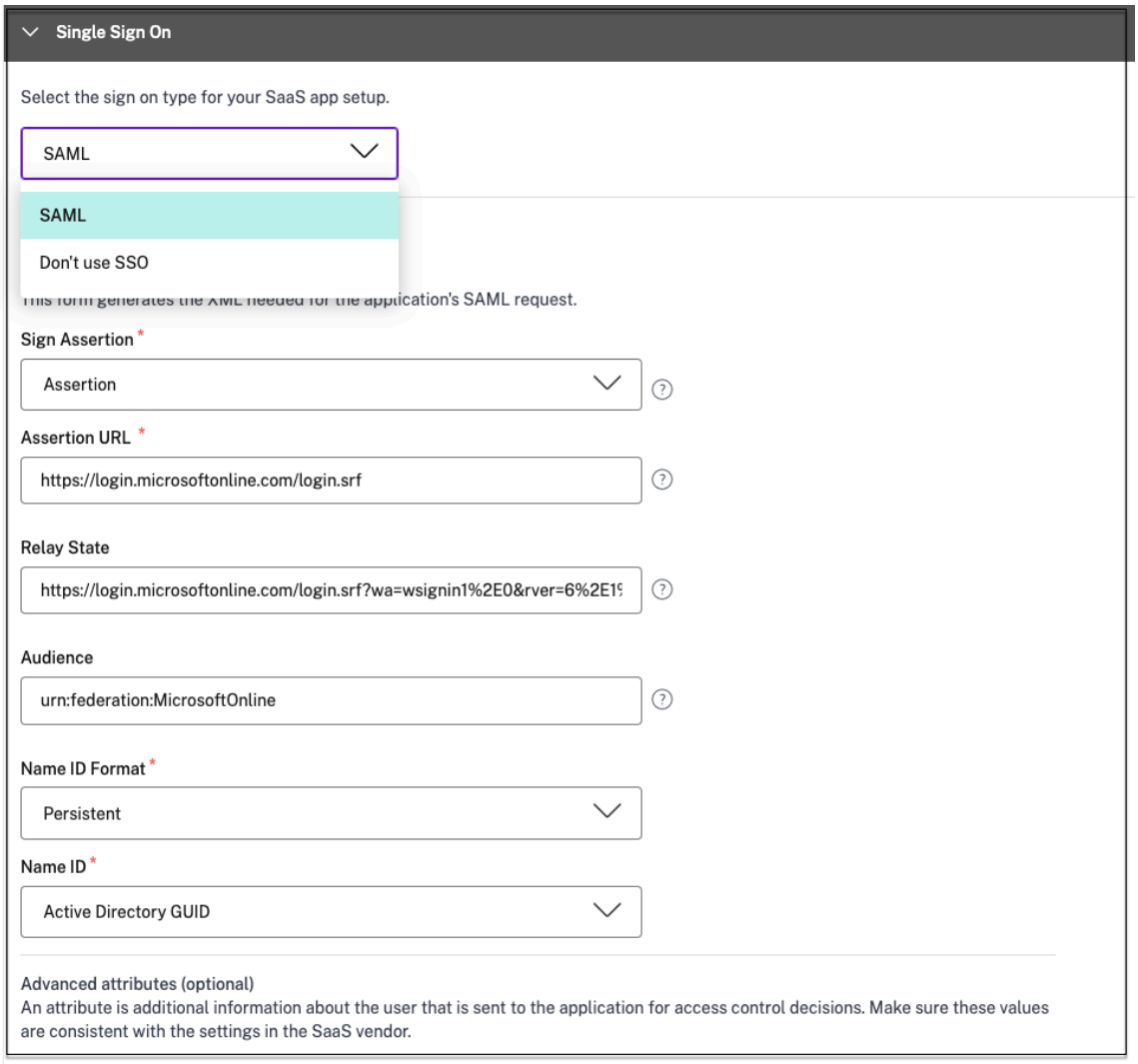


- **SSO nicht verwenden** –Verwenden Sie die Option **SSO nicht verwenden** , wenn Sie einen Benutzer auf dem Back-End-Server nicht authentifizieren müssen. Wenn die Option **SSO nicht verwenden** ausgewählt ist, wird der Benutzer zu der im Abschnitt **App-Details** konfigurierten URL umgeleitet.
- **SAML**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

  Geben Sie im Abschnitt „Anmelden“die folgenden Details ein und klicken Sie auf **Speichern**.

  - **Signierbehauptung** - Durch das Signieren einer Behauptung oder Antwort wird die Nachrichtenintegrität sichergestellt, wenn die Antwort oder Behauptung an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Response, Both,** oder **None**auswählen.
  - **Assertion-URL** –Die Assertion-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.
  - **Relay-Status** –Der Relay-Status-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die die Benutzer zugreifen, nachdem sie sich angemeldet und zum Verbundserver der vertrauenden Seite weitergeleitet wurden. Relay State 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 wird.
  - **Namens-ID-Format** –Wählen Sie das unterstützte Namenskennungsformat aus.
  - **Namens-ID** –Wählen Sie die unterstützte Namens-ID aus.
  - Wählen Sie **. Starten Sie die App mit der spezifischen URL (vom SP initiiert)** , um den vom Identitätsanbieter initiierten Ablauf zu überschreiben und nur den vom Dienstanbieter initiierten Ablauf zu verwenden.

2. Fügen Sie in **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 beim Konfigurieren von SSO auf dem SaaS-App-Server verwenden.
> - Sie können das Zertifikat auch aus der Liste „ **Zertifikat** “herunterladen und es beim Konfigurieren von SSO auf dem SaaS-App-Server verwenden.

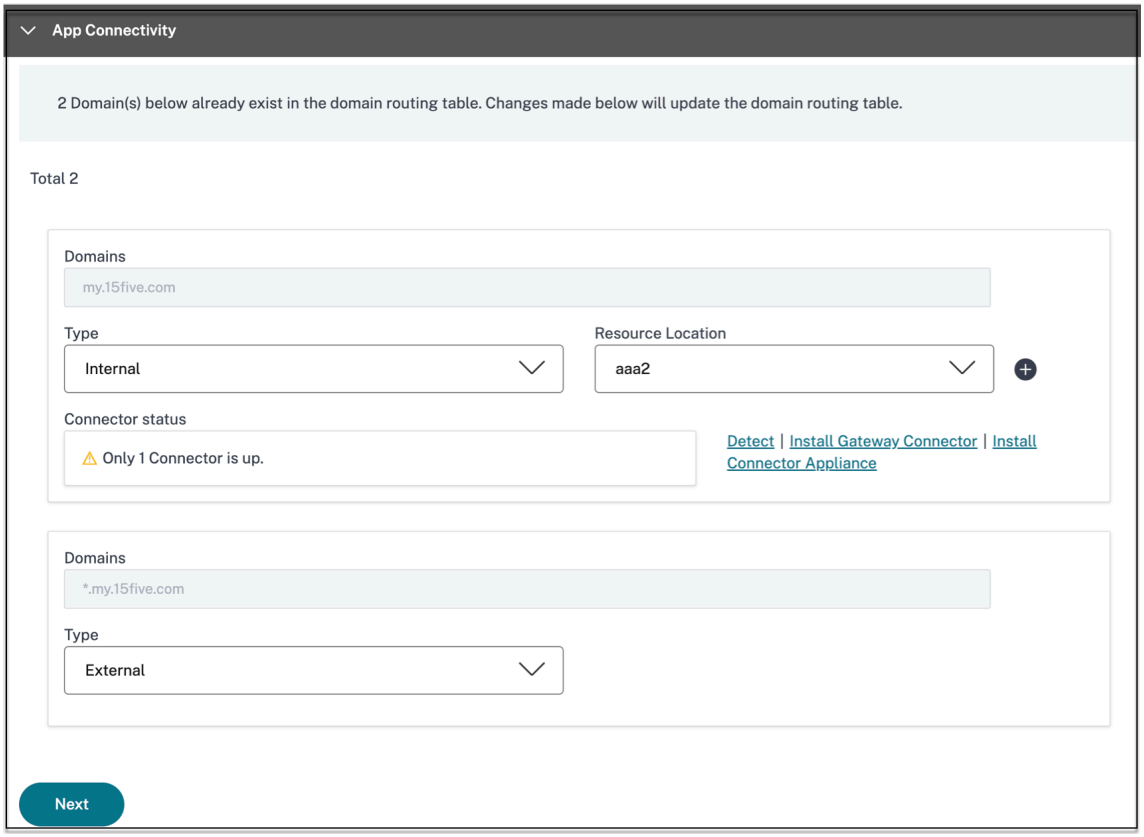
1. Klicken Sie auf **Weiter.**

Definieren des Anwendungsroutings

1. Definieren Sie im Abschnitt **App-Konnektivität** das Routing für die entsprechenden Anwendungsdomänen, wenn die Domänen extern oder intern über Citrix Connector Appliances geroutet werden müssen.

   - **Intern –Proxy umgehen** –Der Domänenverkehr wird über Citrix Cloud Connector geleitet und umgeht dabei den auf dem Connector Appliance konfigurierten Webproxy des Kunden.
   - **Intern über Connector** –Die Apps können extern sein, aber der Datenverkehr muss über das Connector-Gerät zum externen Netzwerk fließen.

   Weitere Einzelheiten finden Sie unter Routentabellen zum Lösen von Konflikten, wenn die zugehörigen Domänen in SaaS- und Web-Apps identisch sind.



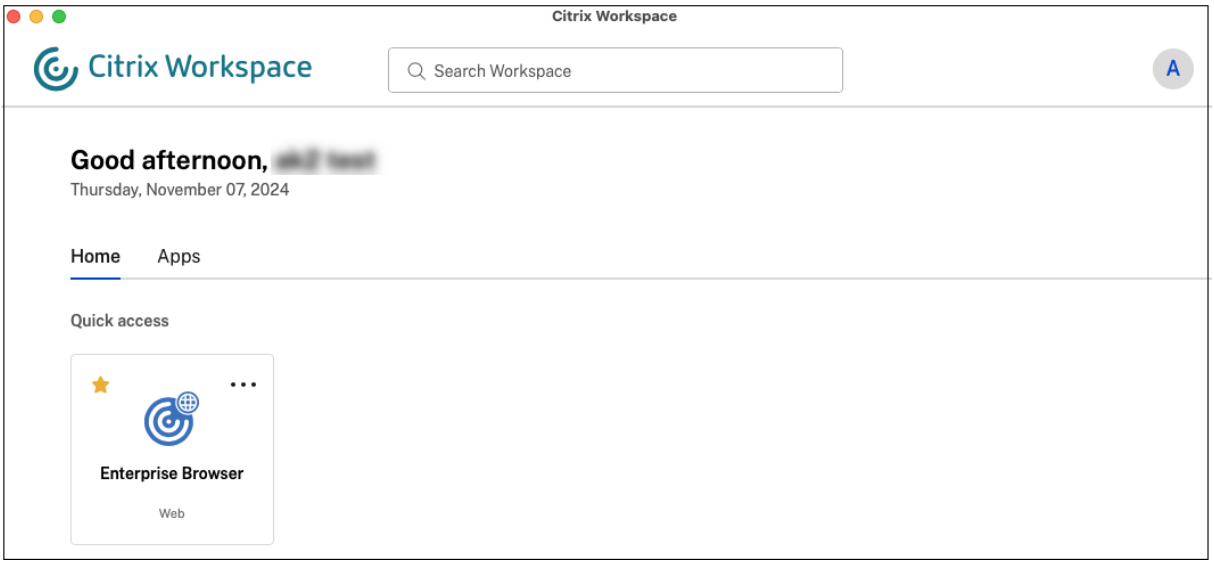
2. Klicken Sie auf **„Fertig“.**

   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 auf die Auslassungspunkte-Schaltfläche einer App und wählen Sie die entsprechenden Aktionen aus.

   - **Anwendung bearbeiten**

- **Löschen**

Wenn Sie eine Web- oder SaaS-App vom Secure Workspace Access-Dienst 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 Arbeitsbereichsbrowser ohne URL starten und über den Arbeitsbereichsbrowser auf interne Websites zugreifen.



Referenzen

Eine vollständige End-to-End-Konfiguration einer App finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichten.

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.

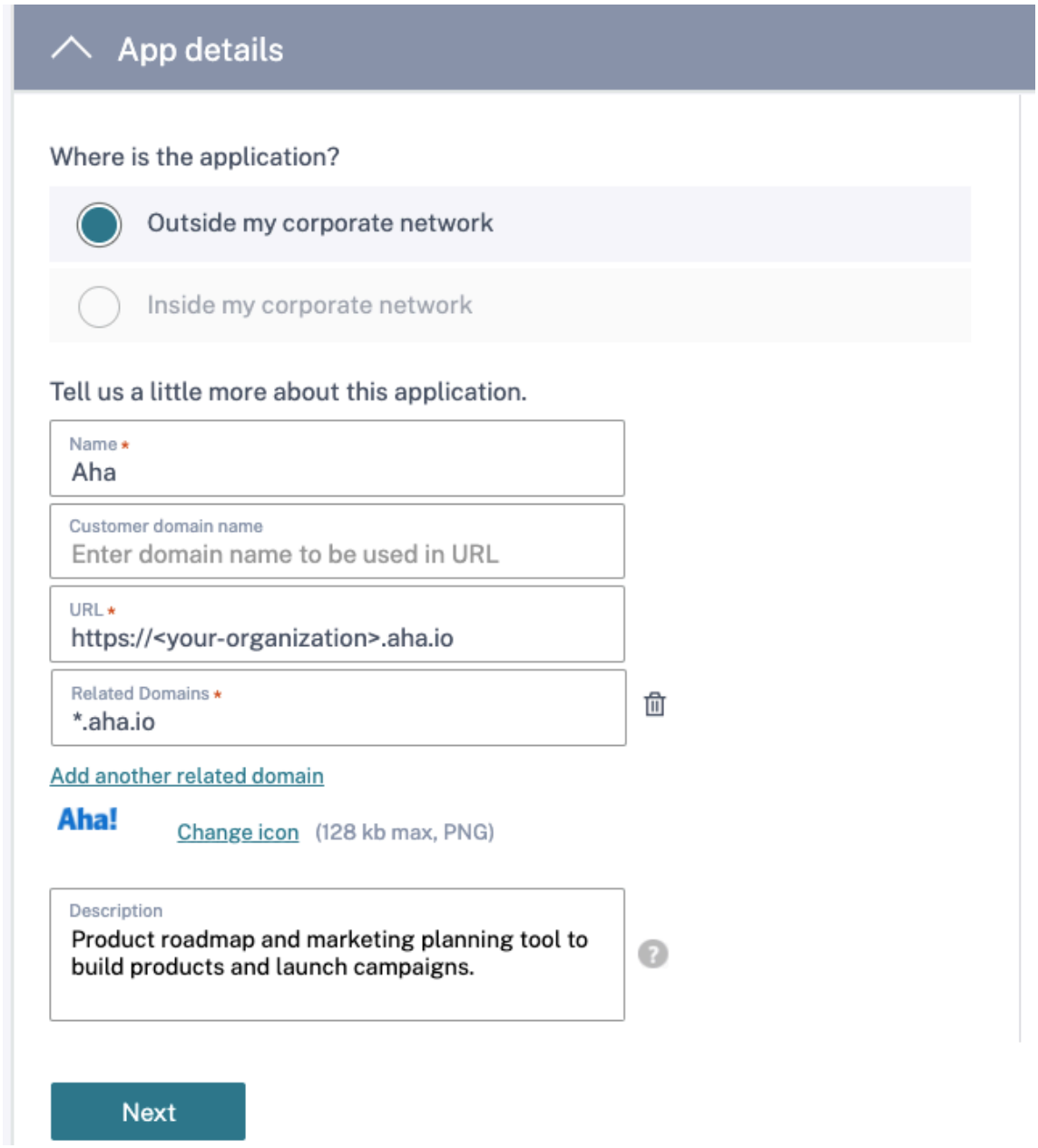
   Kundendomänenname und **Kundendomänen-ID** - Der Domänenname und die ID des Kunden werden verwendet, um eine App-URL und andere nachfolgende URLs auf der SAML-SSO-Seite zu erstellen.

   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**.

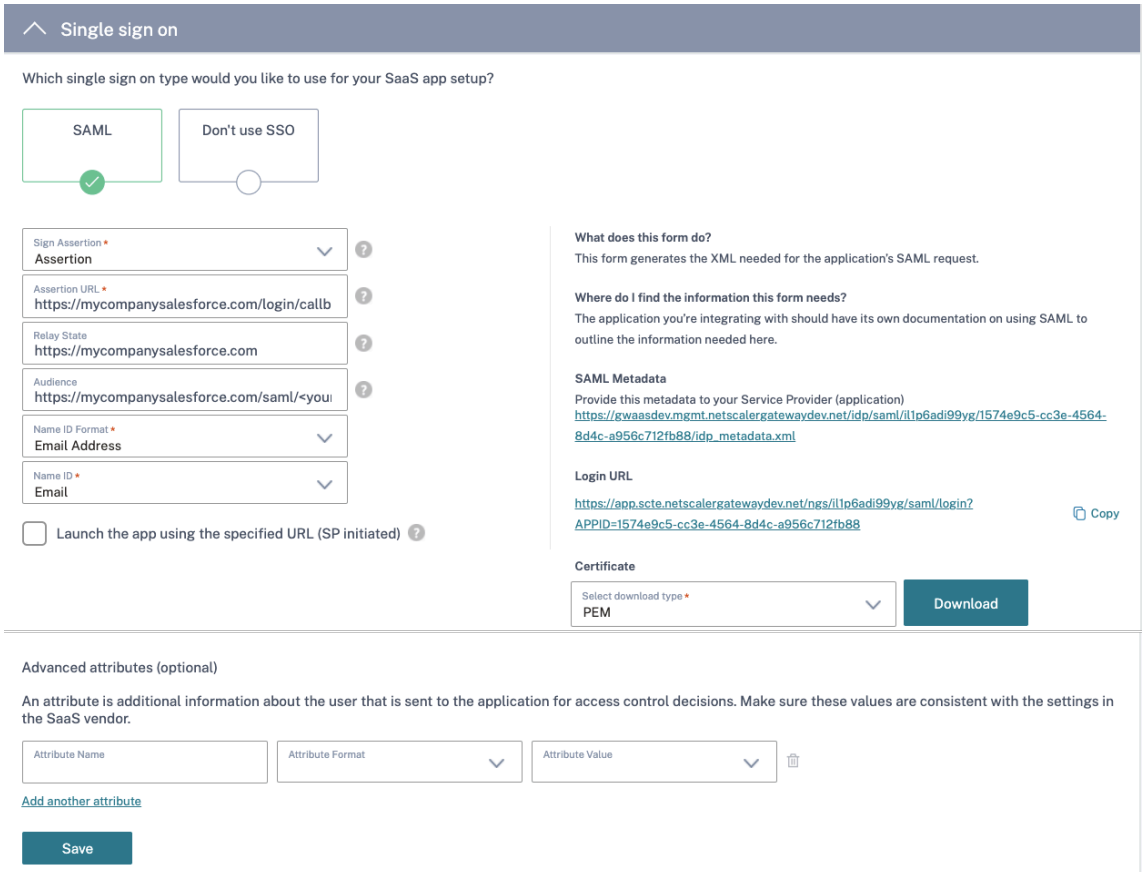
Assertion-URL —SaaS-App-SAML-Assertion-URL, die vom Anwendungsanbieter bereitgestellt wird. Die SAML-Assertion wird an diese URL gesendet.

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:

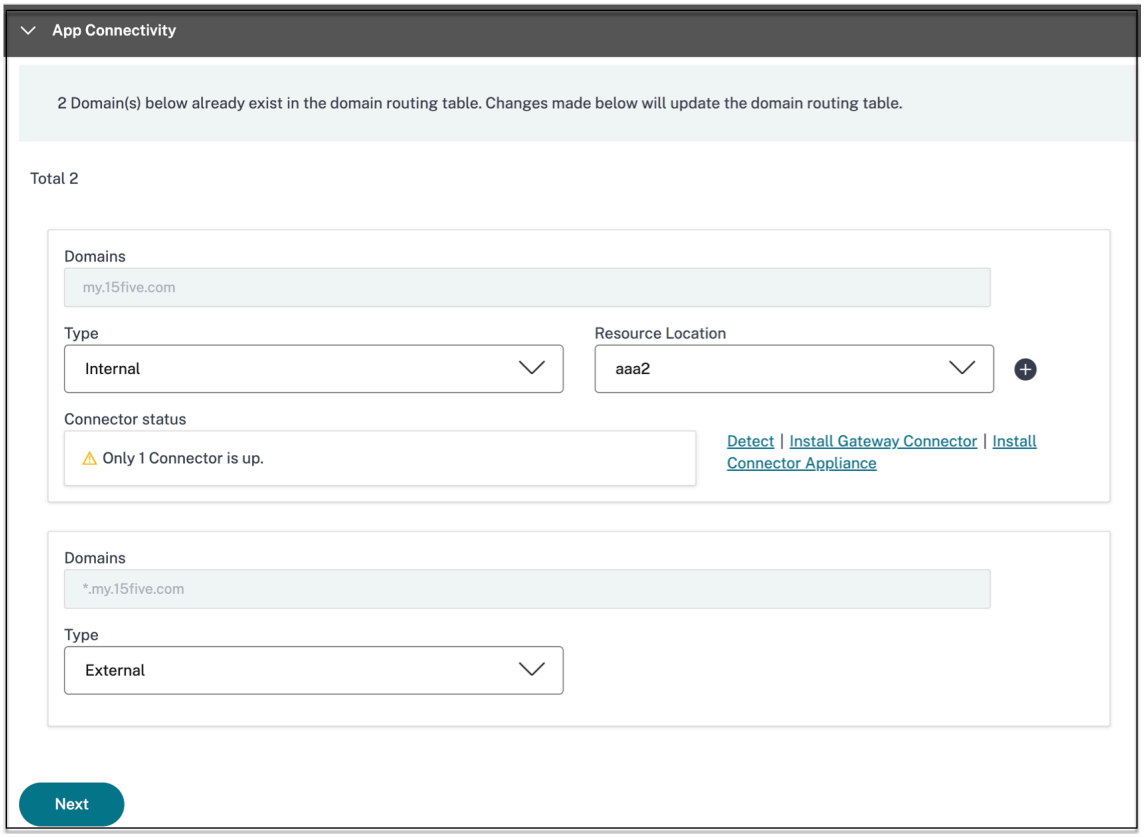
Wenn die Option **SSO nicht verwenden** ausgewählt ist, wird der Benutzer zu der im Abschnitt **App-Details** konfigurierten URL umgeleitet.

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 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.



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.

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.

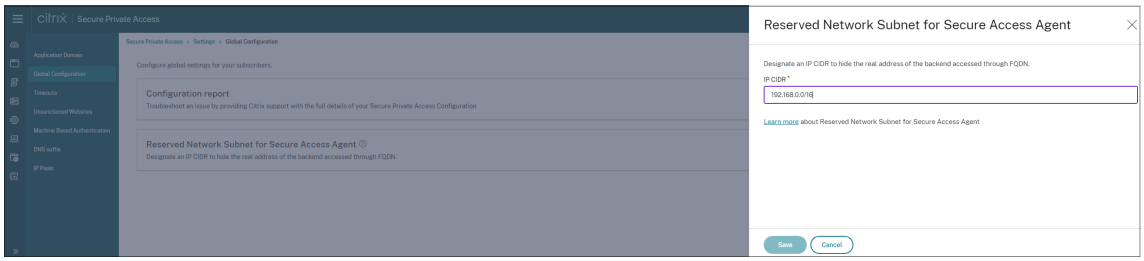
Im Folgenden sind die zulässigen reservierten CIDR-IP-Adressbereiche aufgeführt:

- 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.

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**.

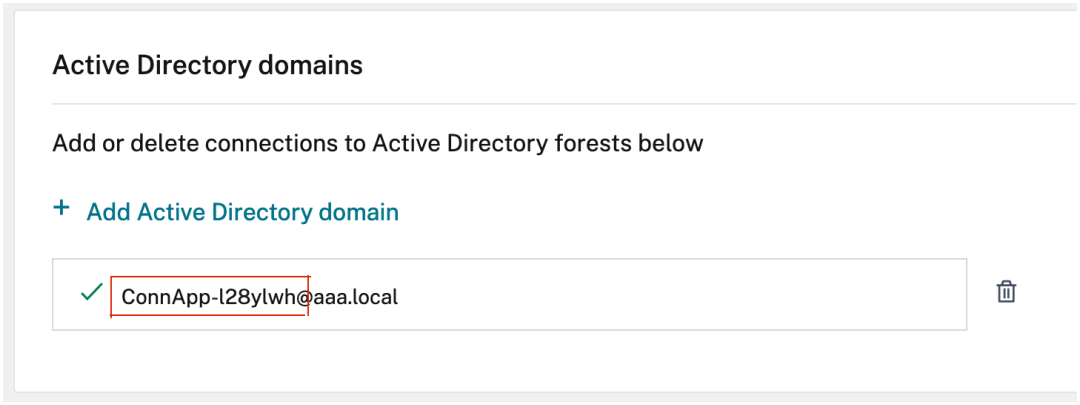
        Wenn Ihre Verwaltungsseite keinen Abschnitt **Active Directory-Domänen** enthält, wenden Sie sich an Citrix, um die Registrierung für die Preview anzufordern.
      - Geben Sie den Domänennamen in das Feld **Domänenname** ein. Klicken Sie auf **Hinzufügen**.
      - Die Connector Appliance überprüft 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.

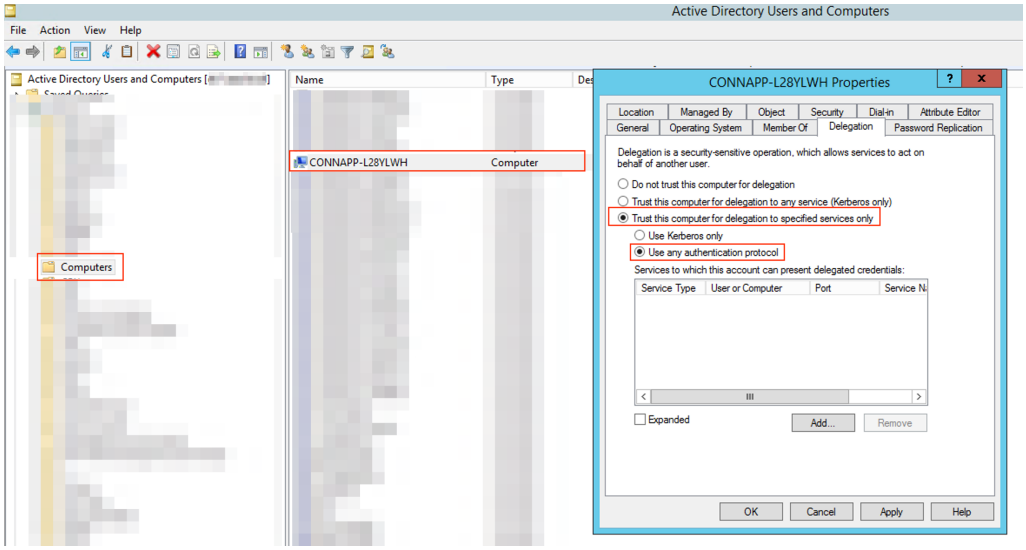
Dieser Maschinenname wird in der Active Directory-Domäne erstellt, wenn die Connector Appliance beitritt.

- Klicken Sie auf **Beitreten**.

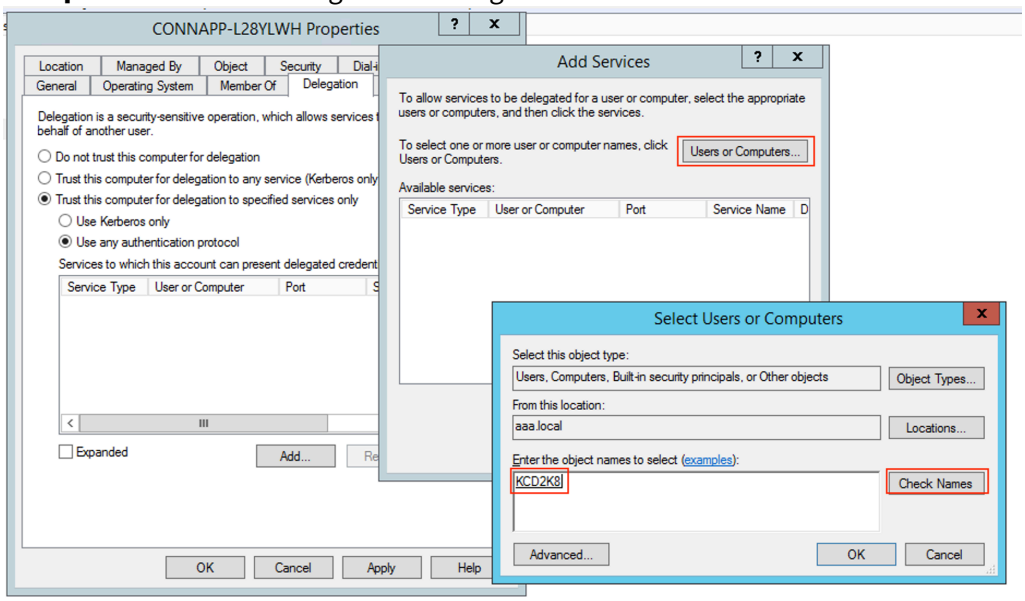
b) Konfigurieren Sie die Kerberos-Einschränkungsdelegierung für Webserver ohne Load Balancer.



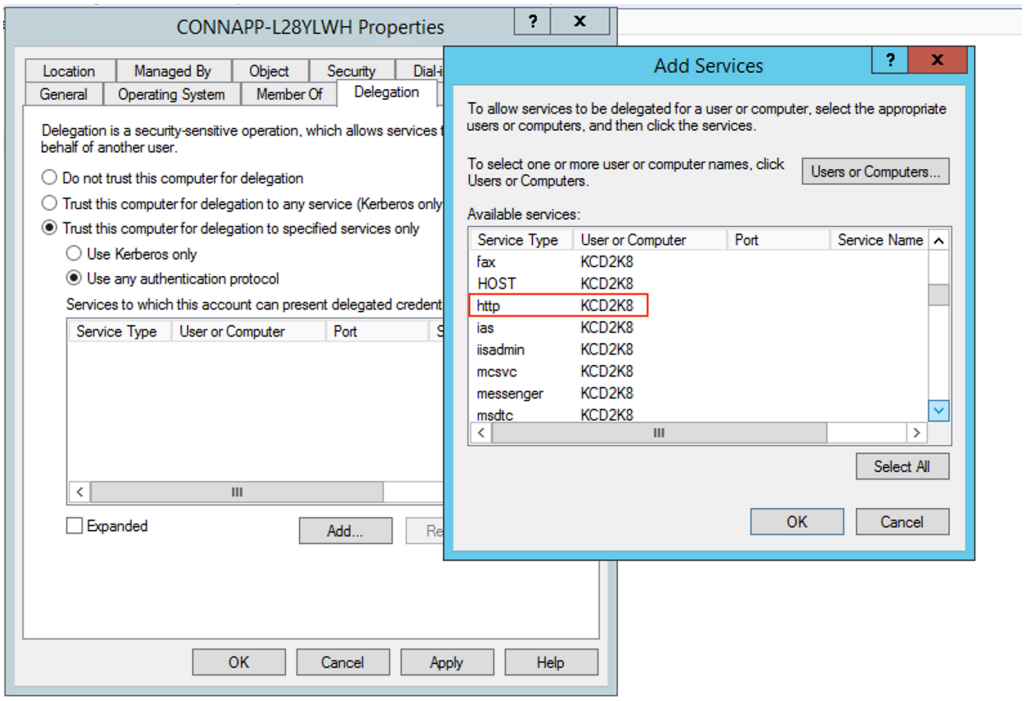
- Identifizieren Sie den Computernamen des Connector-Geräts Sie können diesen Namen entweder von dem Ort erhalten, an dem Sie gehostet haben, oder einfach von der Connector-Benutzeroberfläche.
- Suchen Sie auf Ihrem Active Directory-Controller nach dem Connector-Appliance-Computer.
- Wechseln Sie zu 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.



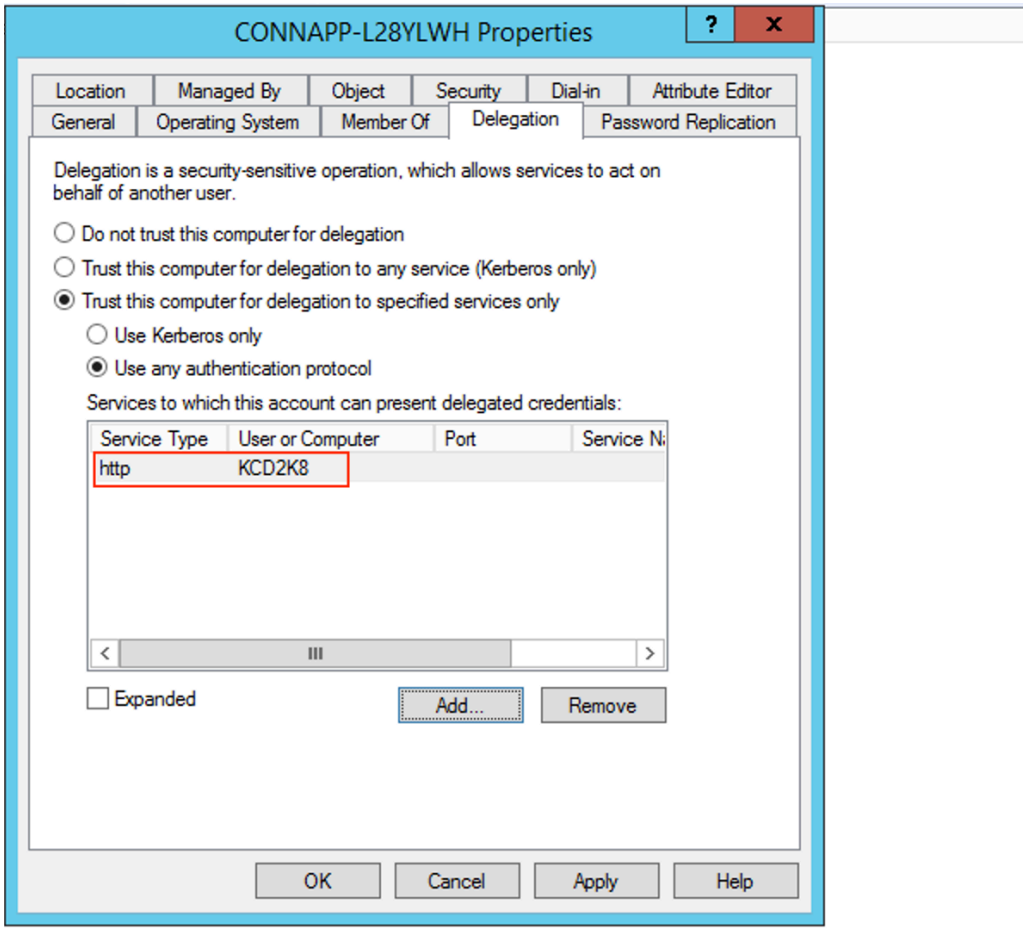
- Klicken Sie auf **Hinzufügen.**
- Klicken Sie auf **Benutzer oder Computer**.
- Geben Sie den Namen des Ziel-Webservers ein, und klicken Sie dann auf **Namen überprüfen**. In der vorherigen Abbildung ist **KCD2K8** der Webserver.



- 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.

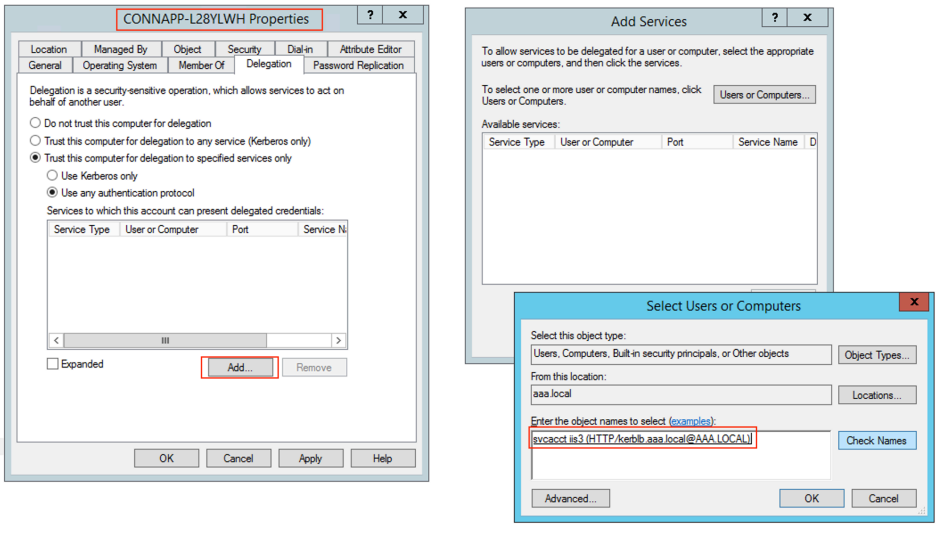
c) Konfigurieren Sie die eingeschränkte Kerberos-Delegierung (KCD) für einen Webserver hinter einem Load Balancer.

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

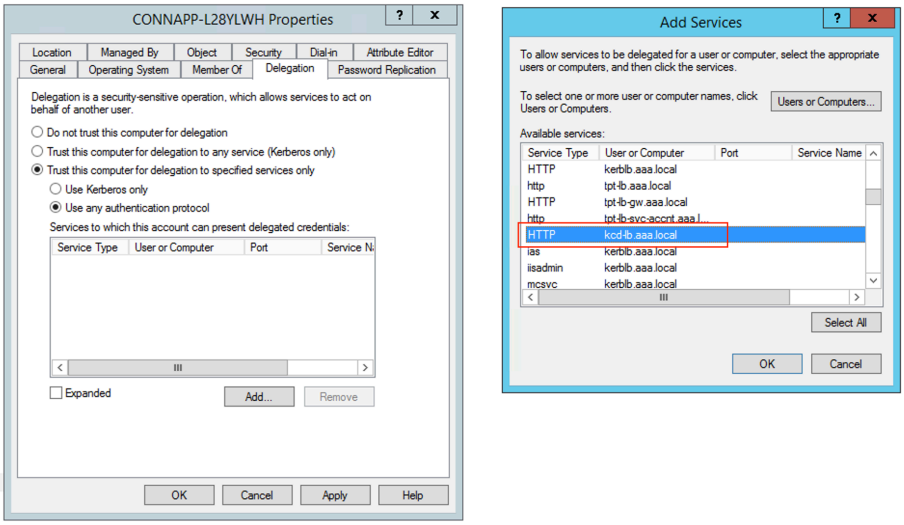
```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local

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>`

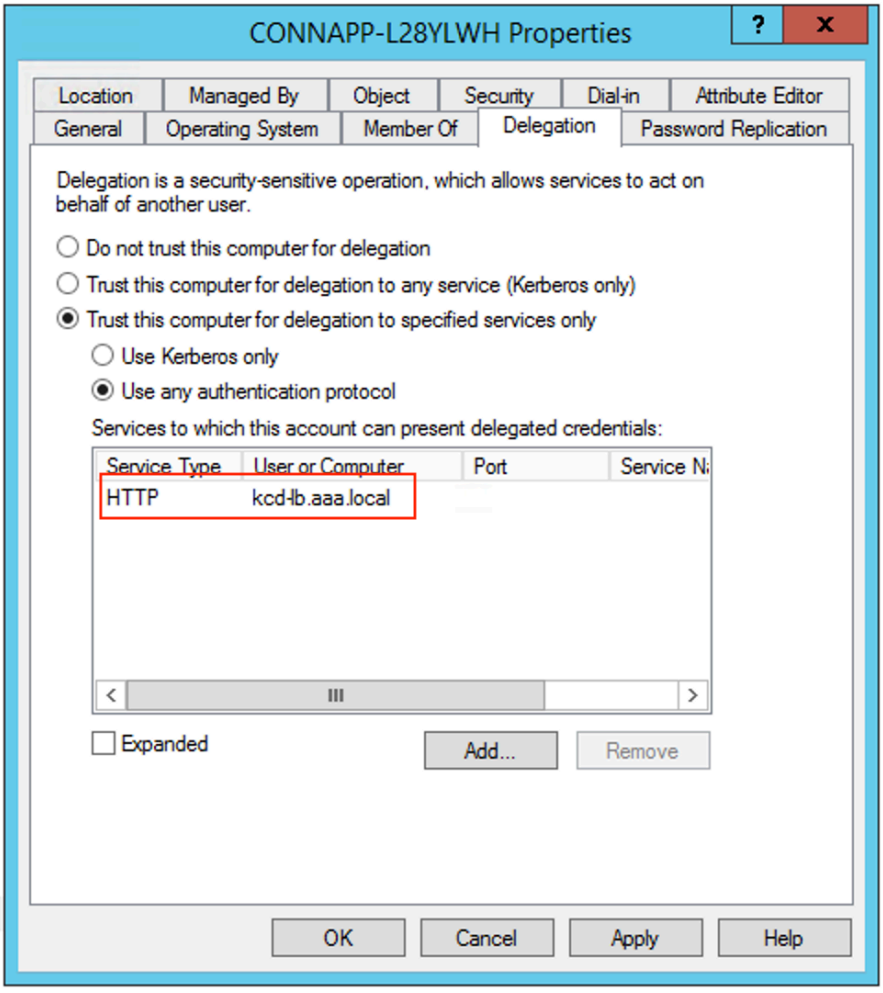
- Erstellen Sie eine Delegierung für das Computerkonto der Connector-Appliance.
  - Führen Sie die Schritte zum *Konfigurieren der Kerberos-Beschränkungsdelegierung für den Webserver* ohne Load Balancer aus, um den CA-Computer zu identifizieren und zur Delegierungs-Benutzeroberfläche zu navigieren.
  - 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**.

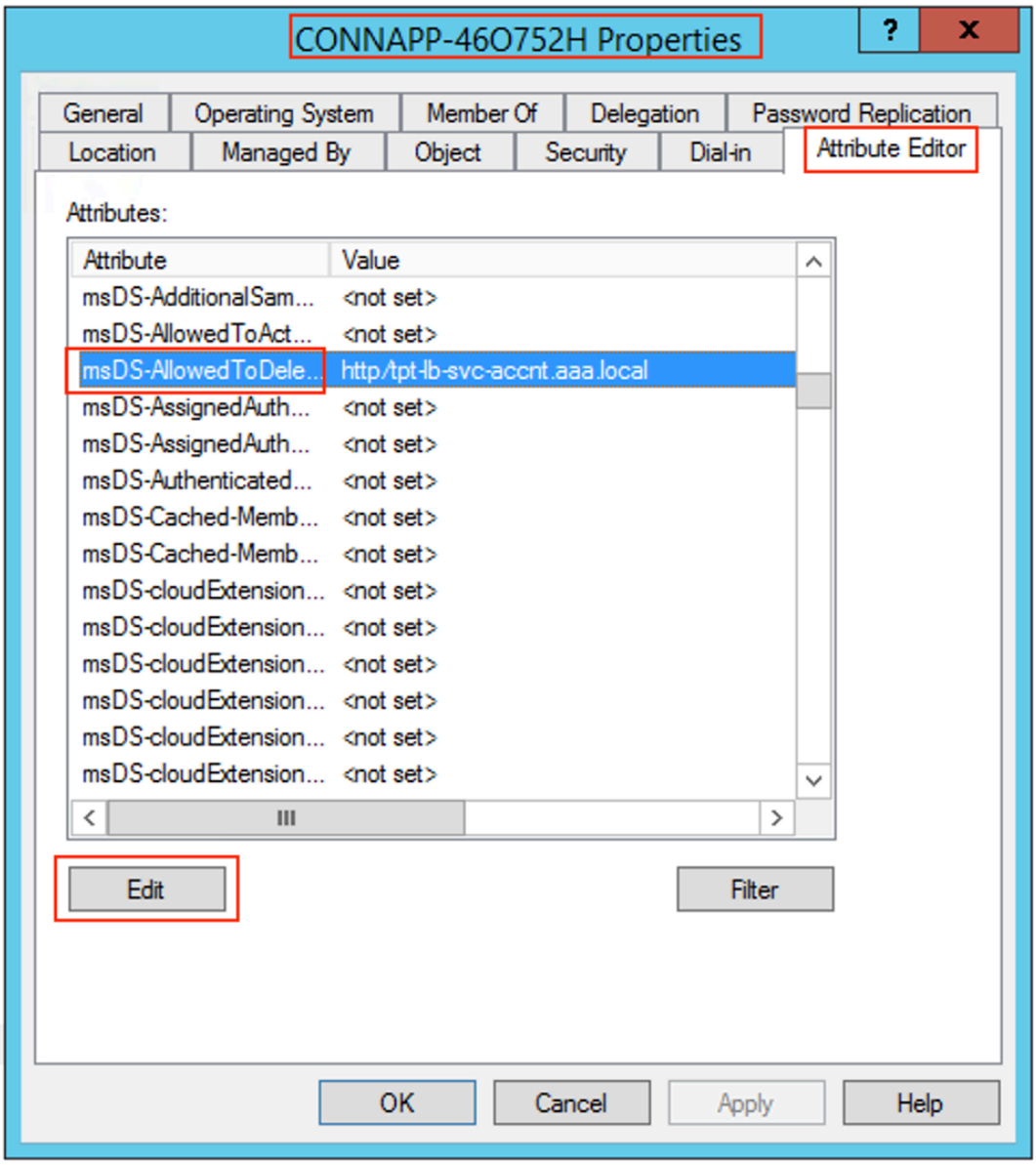


d) Konfigurieren Sie die eingeschränkte Kerberos-Delegierung (KCD) für ein gruppenverwaltetes Dienstkonto.

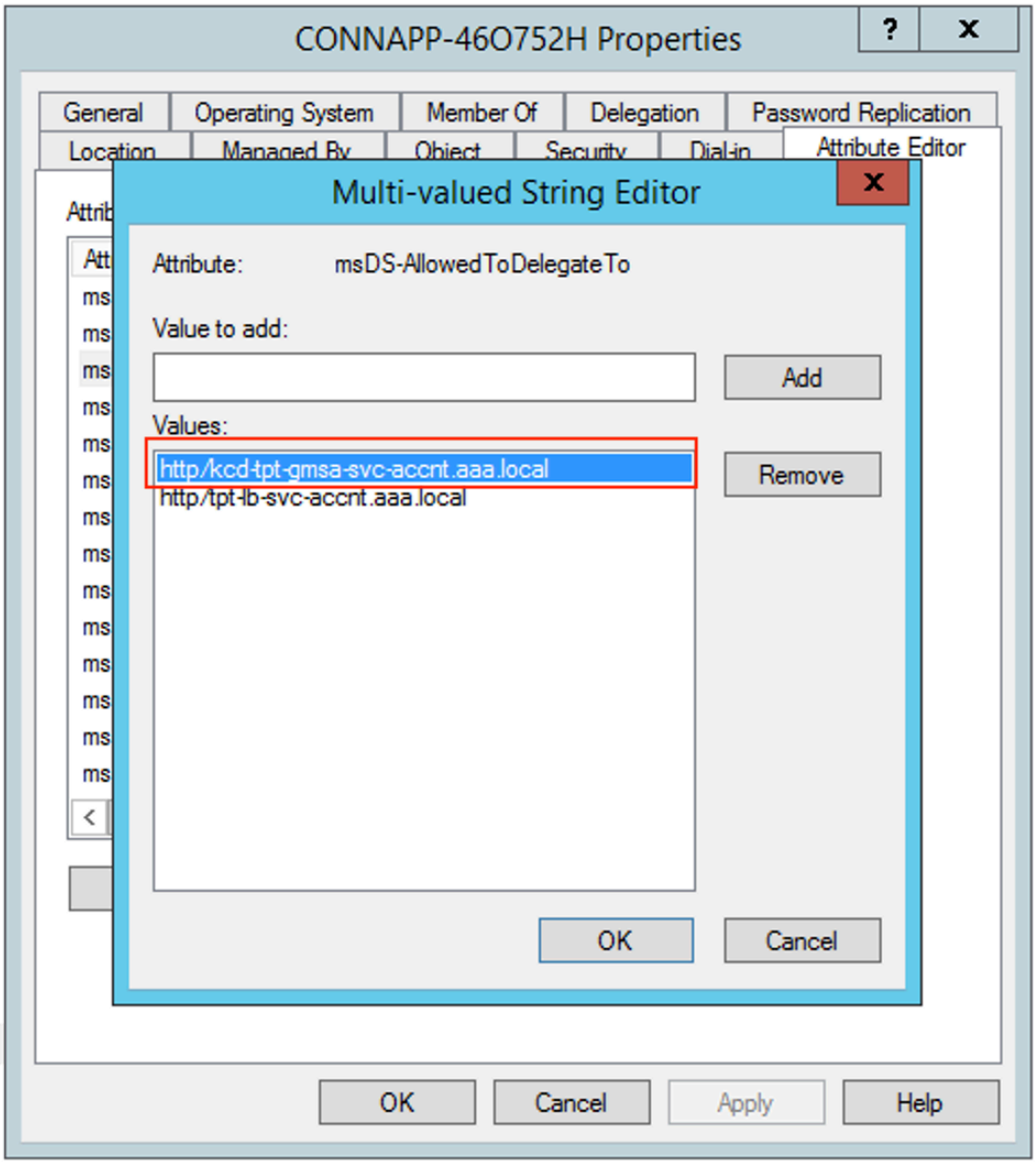
- Fügen Sie SPN dem gruppenverwalteten Dienstkonto hinzu, falls dies noch nicht geschehen ist.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Bestätigen Sie den SPN mit dem folgenden Befehl.
  `setspn -l <group_manged_service_account>`

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.

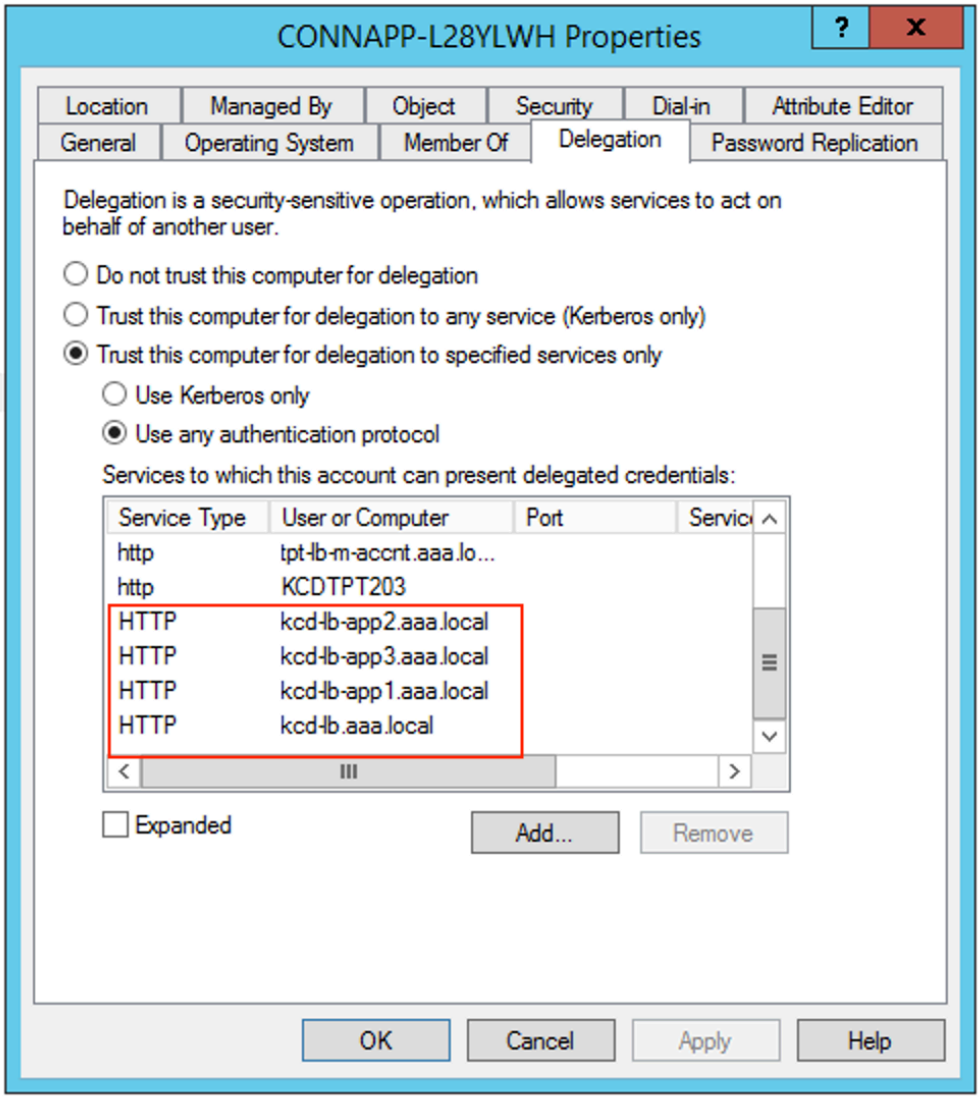
```
setspn -l <service_account>
```



```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

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

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>`

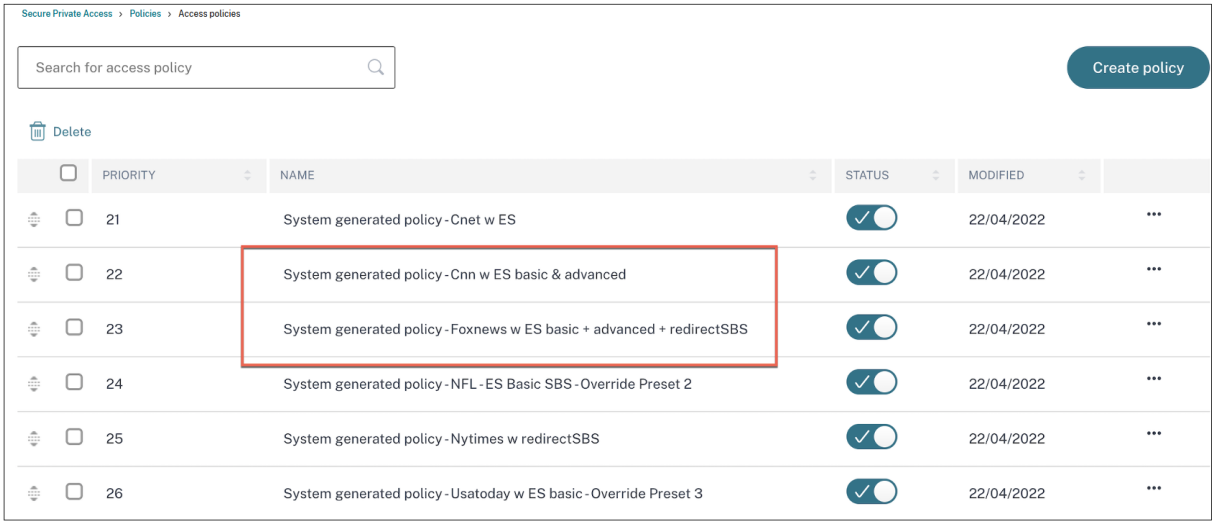
> **Hinweis:**
>
> Wenn den Apps keine Benutzer oder Gruppen hinzugefügt wurden, werden keine neuen Richtlinien erstellt.

In der folgenden Tabelle sind die Änderungen zusammengefasst.

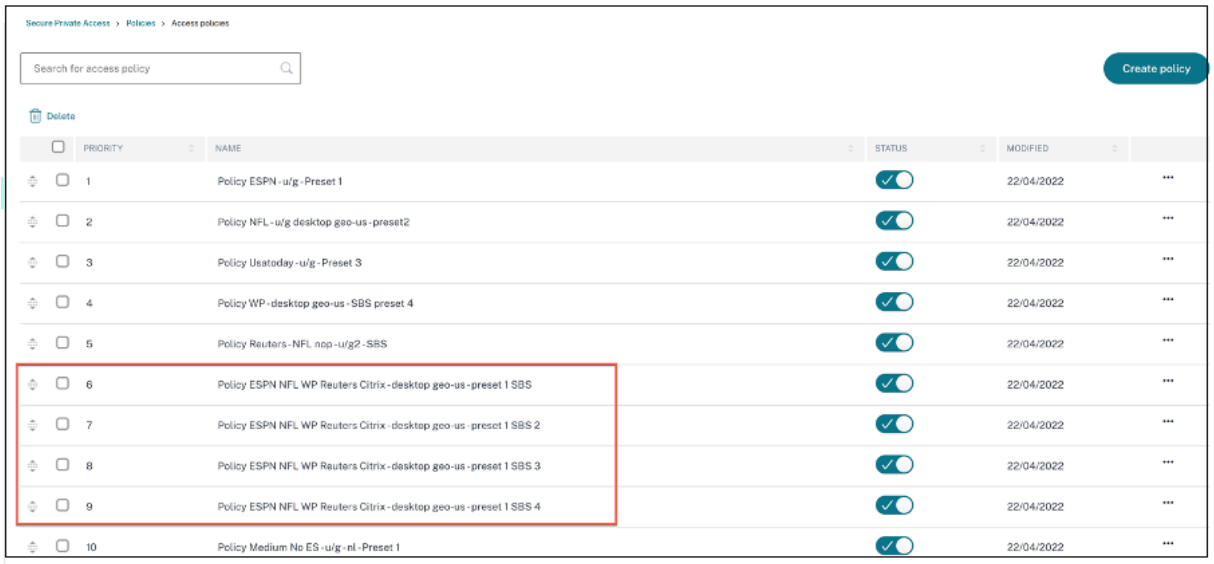
Wenn Sie eine konfiguriert hätten…	Dann…
App ohne erweiterte Sicherheitsbedingungen	Es wird eine neue Richtlinie mit Benutzern und Gruppen als obligatorische Bedingung erstellt. Die Benutzer oder Gruppen werden aus den Zugriffsrichtlinien abgeleitet. Die Aktion ist auf **Zugriff zulassen**festgelegt.

Wenn Sie eine konfiguriert hätten…	Dann…
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>.
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.



Starten einer konfigurierten App - Endbenutzerworkflow

December 27, 2023

Führen Sie als Endbenutzer folgende Schritte aus:

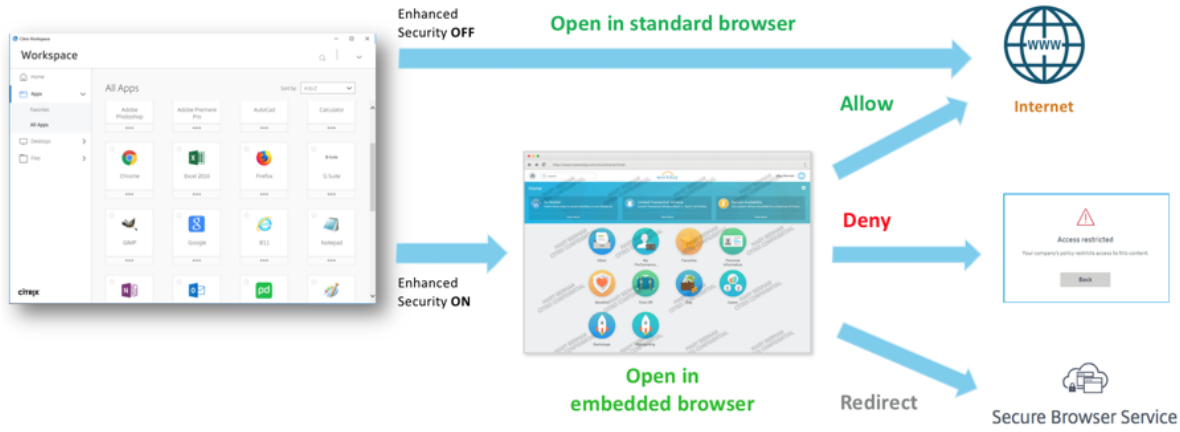
1. Laden Sie die Citrix Workspace-App von https://www.citrix.com/downloads herunter. Wählen Sie unter **Find Downloads** die **Citrix Workspace-App**.

2. Melden Sie sich an und suchen Sie nach Ihren SaaS-Anwendungen. Klicken Sie auf die App, um sie zu starten.

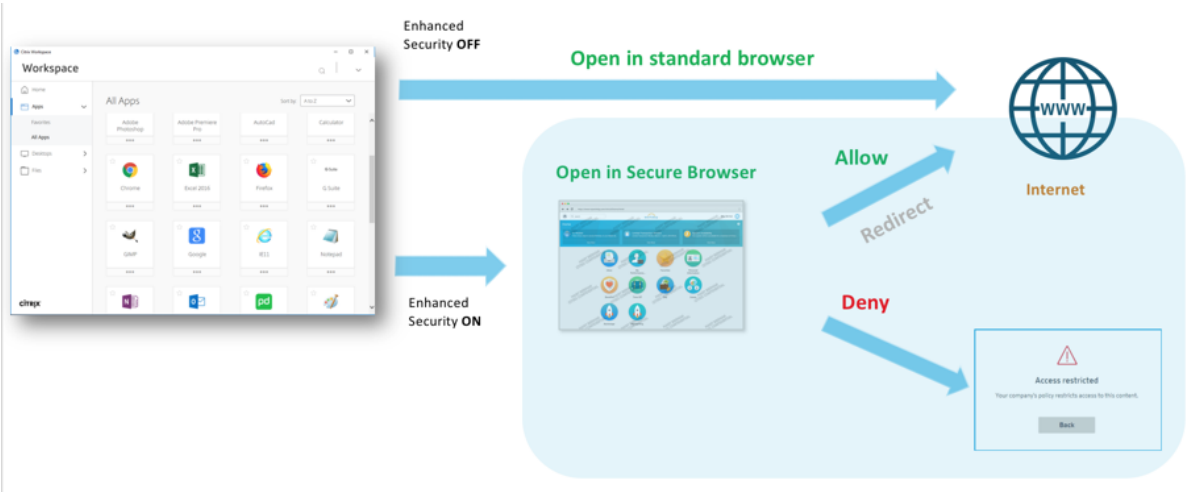
Sie können nun die SaaS-Anwendung in der Citrix Workspace-App oder im Citrix Workspace-Webportal verwenden.

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.



Ermitteln Sie Domänen oder IP-Adressen, auf die Endbenutzer zugreifen

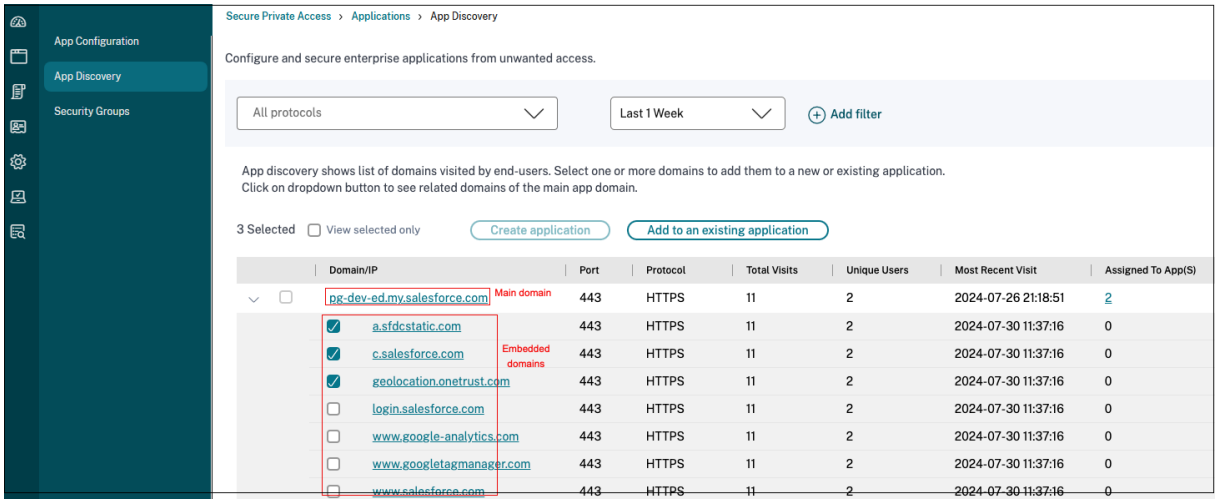
October 21, 2024

Mithilfe der Funktion „Anwendungserkennung“erhält ein Administrator Einblick in die externen und internen Anwendungen (HTTP/HTTPS- und TCP/UDP-Apps), auf die in einer Organisation zugegriffen wird. Diese Funktion erkennt und listet alle veröffentlichten oder unveröffentlichten Domänen/IP-Adressen auf. Auf diese Weise können Administratoren sehen, auf welche Domänen/IP-Adressen von wem zugegriffen wird, und entscheiden, ob sie diese als Anwendungen veröffentlichen und den entsprechenden Benutzern Zugriff gewähren möchten.

Die Funktion „Application Discovery“bietet Administratoren die folgenden Möglichkeiten:

- Bietet Einblick in die internen und externen Domänen/IP-Adressen, auf die die Endbenutzer zugreifen.
- Bietet umfassende Transparenz über alle Arten von Anwendungen, auf die zugegriffen wird (HTTP, HTTPS, TCP und UDP). Alle Zugriffsmethoden werden unterstützt, d. h. der Zugriff über Citrix Enterprise Browser, Secure Access Agent, Direct Access oder Workspace for Web.
- Zeigt sowohl veröffentlichte als auch unveröffentlichte Domänen/IP-Adressen an, auf die die Endbenutzer zugreifen.
- Zeigt sowohl die Hauptdomäne als auch die zugrunde liegenden eingebetteten Domänen an, die beim Veröffentlichen der Anwendungen für den Zugriff über Citrix Enterprise Browser als verwandte Domänen konfiguriert werden müssen.
- Zeigt die eingebetteten Domänen in einer Baumstruktur an. Administratoren können auf das Erweiterungszeichen (**>**) in der Zeile der Hauptdomäne klicken, um die eingebetteten Domänen anzuzeigen.
- Ermöglicht Administratoren, neue Anwendungen zu erstellen oder diese Domänen zu einer vorhandenen Anwendung hinzuzufügen, wenn einer Anwendung keine Hauptdomäne oder eingebettete Domäne (HTTP/HTTPS) oder die Ziel-IP-Adresse (TCP/UDP) zugeordnet ist.

Die folgende Abbildung zeigt ein Beispiel für eine **App-Erkennungsseite** . Auf der Seite „ **App-Erkennung** “können Sie Domänen basierend auf dem Protokoll (HTTP/HTTPS, TCP/UDP) sowie Domänen-/IP-Adresse und Portnummern filtern. Außerdem werden die nicht veröffentlichten (keiner App zugewiesenen) Domänen angezeigt, auf die die Endbenutzer zugreifen. Sie sehen eine Hauptdomäne mit einer Dropdown-Liste eingebetteter Domänen darunter. Diese Domänen müssen beim Veröffentlichen der Anwendung als verwandte Domänen konfiguriert werden.



Hinweis:

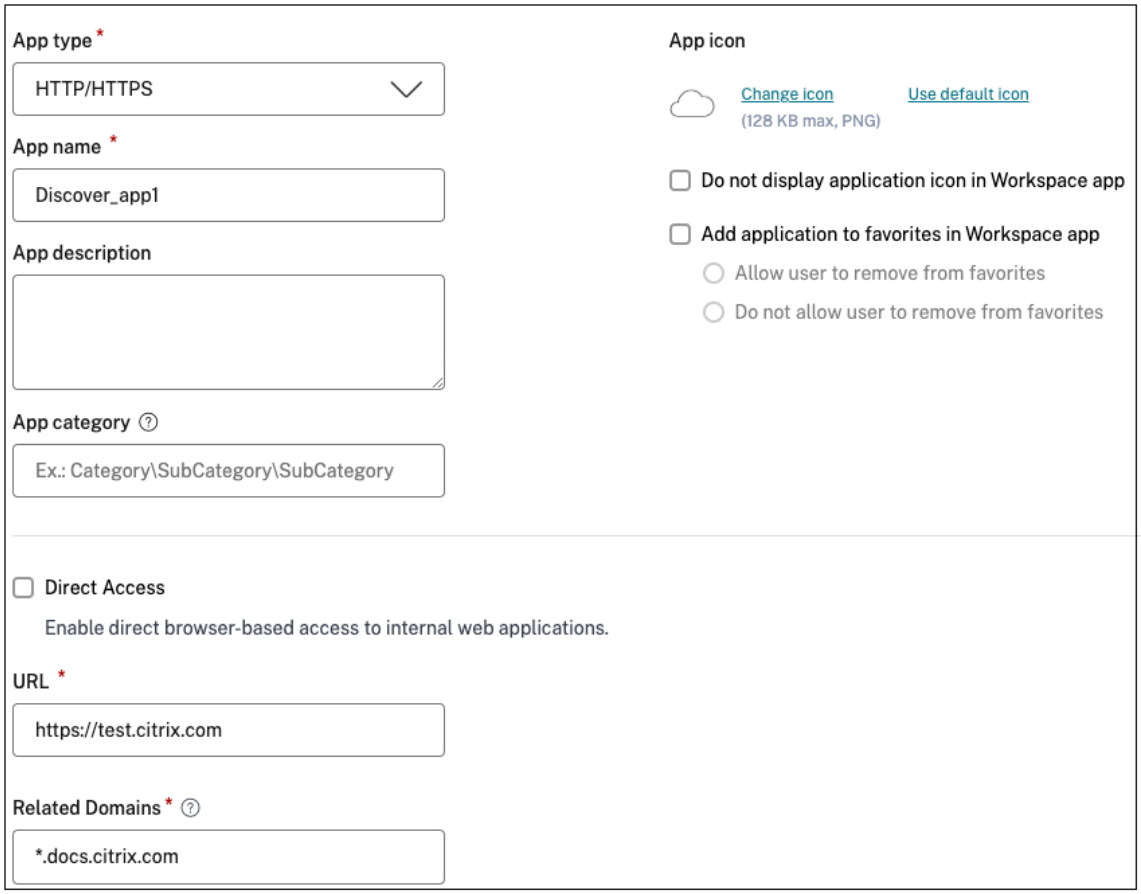
- Eingebettete Domänen werden nur für HTTP/HTTPS-Apps, auf die über den Citrix Enterprise Browser zugegriffen wird, unter der Hauptdomäne gruppiert. TCP/UDP-Domänen sind nicht unter einer Hauptdomäne gruppiert.
- Die Gruppierung eingebetteter Domänen ist nur für Apps verfügbar, auf die über den Citrix Enterprise Browser (v119 und höher) zugegriffen wird.

Anwendungserkennung für interne Domänen in einer neuen Umgebung

Die Funktion „Anwendungserkennung“kann verwendet werden, wenn Sie eine neue Secure Private Access-Umgebung einrichten und Einblick in die zu konfigurierenden Anwendungen wünschen. Diese Funktion erkennt und listet alle Domänen/IP-Adressen auf, auf die Ihre Endbenutzer zugreifen, sodass Sie sie als Anwendungen konfigurieren können. Führen Sie die folgenden Schritte aus, um die Funktion „Anwendungserkennung“beim Einrichten Ihrer Secure Workspace Access-Umgebung zu aktivieren:

- Um interne Webanwendungen zu erkennen, konfigurieren Sie eine Anwendung in Secure Private Access und geben Sie die Platzhalterdomäne an, die zur Domäne/Subdomäne der Anwendungen gehört, die Sie erkennen möchten.

  Wenn Sie beispielsweise alle Anwendungen mit der Domäne citrix.com ermitteln möchten, erstellen Sie eine Anwendung mit einer zugehörigen Platzhalterdomäne als `*.citrix.com`. Um die Anwendungskonfiguration abzuschließen, fügen Sie eine beliebige Test-URL als Haupt-URL-Abschnitt der Web-App hinzu.

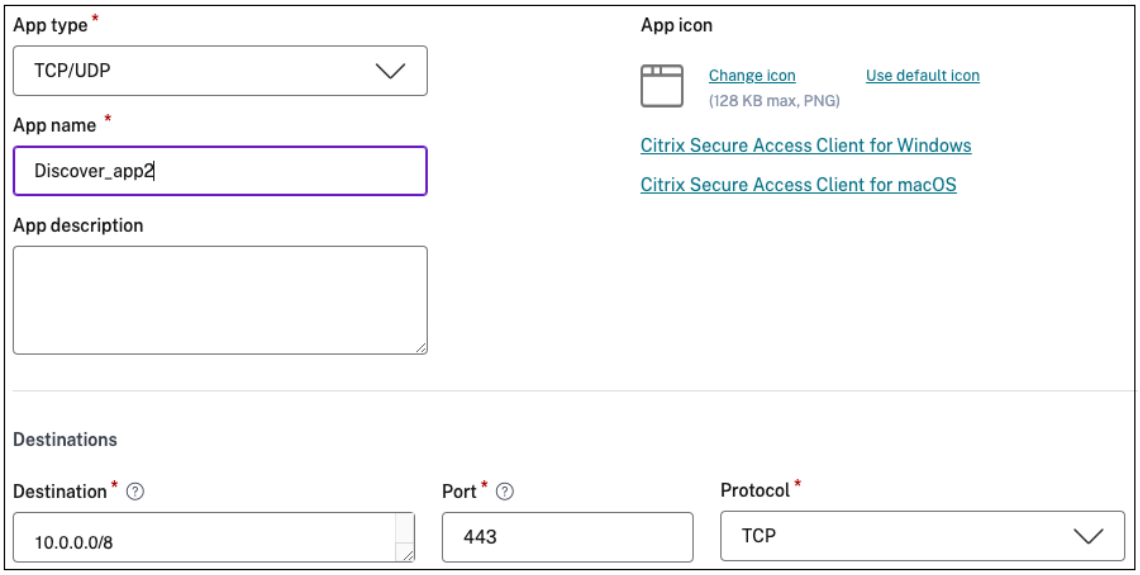


URL der Web-App: `https://test.citrix.com/` Zugehörige Domäne: `*.citrix.com`

- Konfigurieren Sie für interne TCP/UDP-Apps eine Anwendung innerhalb von Secure Private Access und geben Sie das Subnetz zusammen mit dem TCP/UDP-Protokoll und dem Portbereich an (geben Sie * ein, um den gesamten Bereich einzuschließen). Dadurch können alle TCP- und UDP-Apps vom Citrix Secure Access-Agent erkannt werden. Wenn Sie beispielsweise alle Anwendungen im Subnetz 10.0.0.0/8 ermitteln möchten, konfigurieren Sie die App mit den folgenden Details: Beispiel: 10.0.0.0/8:

  Port: (*)

  Protokoll: TCP



- Nachdem Sie die Anwendungen erstellt haben, müssen Sie auch Benutzer definieren, die auf Apps mit den konfigurierten Domänen und IP-Subnetzen zugreifen dürfen. Erstellen Sie eine Zugriffsrichtlinie und weisen Sie Benutzer zu, denen Sie Zugriff auf die in den erstellten Anwendungen konfigurierten FQDNs/IP-Adressen gewähren möchten. Dabei kann es sich um eine anfängliche Gruppe von Testbenutzern oder um eine begrenzte Anzahl von Benutzern handeln, denen Sie zunächst Zugriff gewähren möchten.
- Nach dem Erstellen der Anwendungen und der entsprechenden Zugriffsrichtlinien können Benutzer weiterhin auf Anwendungen aus der Citrix Workspace-App zugreifen und auf verschiedene Domänen zugreifen. Alle von den Endbenutzern aufgerufenen FQDN/IP-Adressen werden auf der Seite „Anwendungserkennung“angezeigt.

> **Hinweis:**
>
> - Wenn Sie innerhalb weniger Tage/Wochen die meisten Anwendungen entdeckt und identifiziert haben, empfehlen wir, die anfangs erstellten Anwendungen zu löschen, damit der breitere Zugriff über die Wildcard-Domänen und IP-Subnetze unterbunden werden kann und nur noch bestimmten entdeckten Anwendungs-URLs und IP-Adressen der Zugriff über neue Anwendungen gestattet werden muss.
> - Fügen Sie dem App-Namen das Präfix `Discover` hinzu, um anzuzeigen, dass dies eine spezielle App-Konfiguration zum Aktivieren der Erkennungsüberwachung und -berichterstattung ist. Diese Benennung hilft Ihnen bei der Erkennung und Entfernung der Platzhalterdomänen oder IP-Subnetze oder beidem, sodass Sie die allgemeine App-Zugriffszone später in einigen Wochen oder einem Monat auf die spezifischen FQDNs und IP/Port-Kombinationen reduzieren können.
> - Um auf TCP/UDP-Apps zuzugreifen, müssen Benutzer den Citrix Secure Access-Agent

verwenden. Der App-Zugriff über verschiedene Zugriffsmethoden wird basierend auf der Domänen- und Subnetzkonfiguration der Apps überwacht und auf der Seite **App Discovery** gemeldet.
- Auch nachdem Sie die erkannten Anwendungen entfernt haben, erkennt diese Funktion weiterhin die Domänen/IP-Adressen, auf die Ihre Benutzer zugreifen. Sie können also jederzeit zur Seite **App Discovery** zurückkehren, um zu sehen, worauf zugegriffen wird und ob neue Domänen/IP-Adressen entdeckt wurden, die als Anwendungen konfiguriert werden müssen.

Einzelheiten zum Hinzufügen der Domänen, FQDNs oder IP-Adressen finden Sie in den folgenden Themen.

- Unterstützung für Enterprise-Web-Apps
- Unterstützung für Software-as-a-Service-App
- Unterstützung für Client-Server-Apps

Erstellen einer Anwendung über die App-Erkennungsseite

Um auf der Seite „ **App-Erkennung** “eine Anwendung für eingebettete Domänen oder unveröffentlichte Domänen zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > App-Erkennung**.
2. Wählen Sie eine Domäne aus der Liste aus. Wenn die Domäne eingebettete Domänen hat, klicken Sie auf das Erweiterungszeichen (**>**) neben der Hauptdomäne und wählen Sie die eingebetteten Domänen aus.

Hinweis:

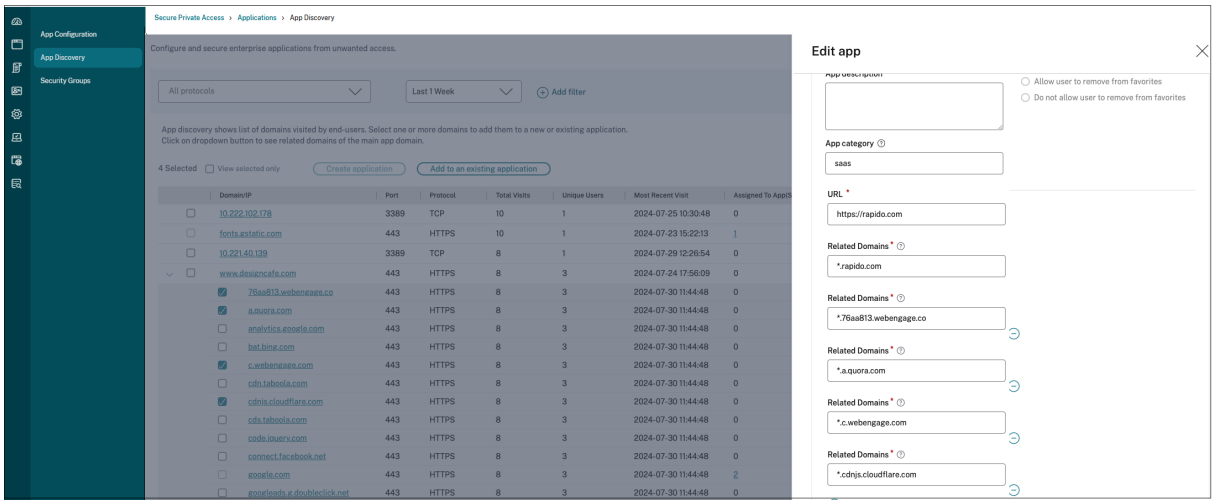
- Sie können zum Erstellen einer Anwendung keine Domänen auswählen, die zu verschiedenen Protokollen gehören. Wenn Sie Domänen auswählen, die zu unterschiedlichen Protokollen gehören, wird eine Fehlermeldung angezeigt.
- Wenn eine Domäne bereits mit einer Anwendung verknüpft ist, können Sie diese Domäne nicht erneut auswählen, um eine Anwendung zu erstellen. Das dieser Domäne entsprechende Kontrollkästchen ist ausgegraut. Wenn Sie mit der Maus über das Kontrollkästchen fahren, wird ein Tooltip angezeigt.
- Sie können eingebettete Domänen, die unter verschiedenen Hauptdomänen gruppiert sind, nicht auswählen und einer Anwendung hinzufügen. Mit der Funktion „Anwendungserkennung“können einer App nur eingebettete Domänen hinzugefügt werden, die unter einer einzigen Hauptdomäne gruppiert sind. Werden eingebettete Domänen aus unterschiedlichen Hauptdomänen ausgewählt und zur gleichen App hinzugefügt, erscheint eine Fehlermeldung.

1. Klicken Sie auf **Anwendung erstellen**. Einzelheiten zum Erstellen einer Anwendung finden Sie unter Support für Enterprise-Web-Apps, Support für Software-as-a-Service-Appsund Support für Client-Server-Apps](/en-us/citrix-secure-private-access/service/spa-support-for-client-server-apps).

Aktualisieren einer vorhandenen Anwendung

Um einer vorhandenen Anwendung eine Domäne hinzuzufügen, wählen Sie die Domäne aus der Liste aus. Wenn die Domäne eingebettete Domänen hat, klicken Sie auf das Erweiterungszeichen (**>**) neben der Hauptdomäne und wählen Sie die eingebetteten Domänen aus.

1. Wählen Sie die eingebettete Domäne aus, die einer Anwendung hinzugefügt werden muss.
2. Klicken Sie auf **Zu einer vorhandenen Anwendung hinzufügen**.
3. Wählen Sie unter **Anwendungen**die Anwendung aus, zu der Sie diese Domänen hinzufügen möchten.
4. Klicken Sie auf **App-Details abrufen**.
5. Das Feld **Verwandte Domänen** zeigt alle eingebetteten Domänen, die Sie zuvor ausgewählt haben, in separaten Zeilen an.
6. Klicken Sie auf **Fertigstellen**.



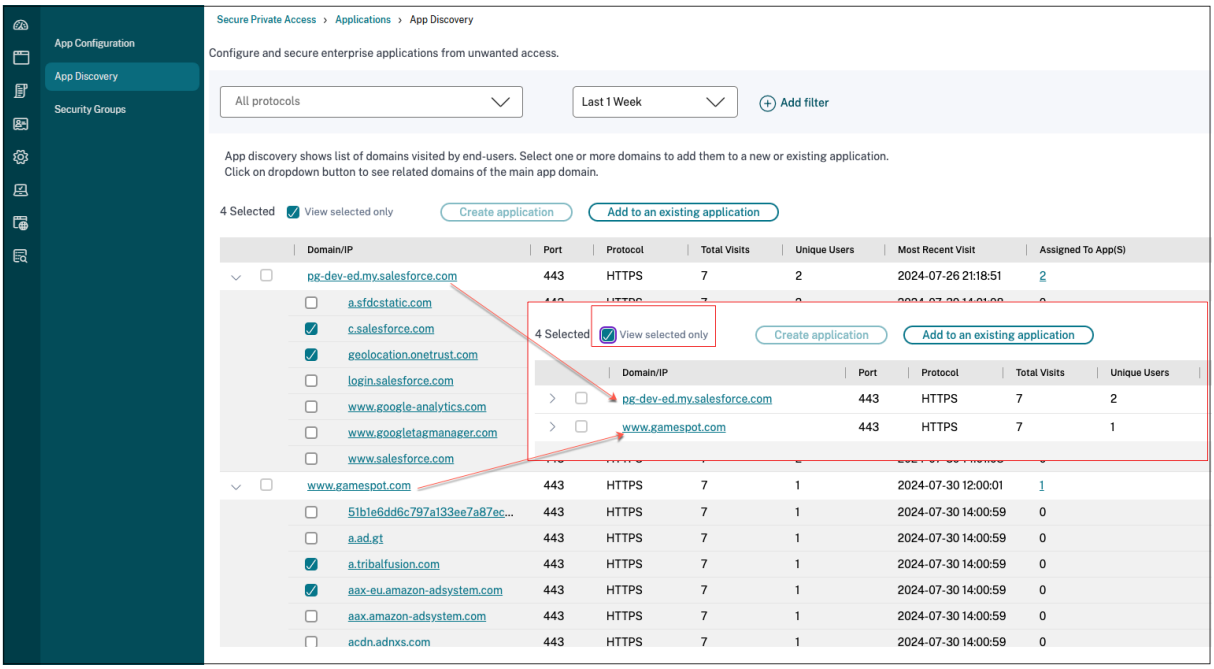
Hinweis:

- Sie können einer vorhandenen TCP/UDP-Anwendung nur eine TCP/UDP-Ziel-IP-Adresse hinzufügen. Das Feld „Anwendungen“listet nur die im System konfigurierten TCP/UDP-Apps auf.
- Sie können eine vorhandene HTTP/HTTPS- oder TCP/UDP-App auswählen, um Domänen (Haupt-, Einzeleintrag- oder eingebettete Domänen) hinzuzufügen, deren Protokoll HTTP/HTTPS ist.

- Sie können keine Domäne auswählen, die bereits einer Anwendung zugeordnet ist.

Alle ausgewählten eingebetteten Domänen anzeigen

Nachdem Sie die Domänen ausgewählt haben, können Sie das Kontrollkästchen **Nur ausgewählte anzeigen** aktivieren und mit dem Erstellen oder Aktualisieren der Anwendung fortfahren. Wenn sich die Liste der FQDN/IP-Adressen auf der App-Erkennungsseite über mehrere Seiten erstreckt, können Sie außerdem das Kontrollkästchen **Nur ausgewählte anzeigen** verwenden, um alle Haupt- und eingebetteten Domänen anzuzeigen, die Sie zum Erstellen oder Aktualisieren der Anwendung ausgewählt haben. Wenn dieses Kontrollkästchen aktiviert ist, werden alle Hauptdomänen der ausgewählten eingebetteten Domänen angezeigt.



Bekannte Einschränkungen

- Obwohl die Optionen **Anwendung erstellen** und **Zu vorhandener Anwendung hinzufügen** im Secure Private Access-Dashboard (Diagramm**Am häufigsten entdeckte Anwendungen nach Gesamtzahl der Besuche**) verfügbar sind, wird empfohlen, eine Anwendung über die Registerkarte **App-Erkennung** (**Anwendungen > App-Erkennung**) zu erstellen oder zu aktualisieren. Dies liegt daran, dass beim Hinzufügen oder Aktualisieren einer Anwendung über das Dashboard die Seite neu geladen und infolgedessen alle Einstellungen zurückgesetzt werden, wenn Sie den Vorgang abbrechen.
- Manchmal bemerken Sie möglicherweise das Erweiterungszeichen (>) neben einer Hauptdomäne, aber die eingebetteten Domänen werden für diesen bestimmten FQDN nicht

abgerufen. Dieses Problem kann in den folgenden Fällen auftreten:

- Fehler beim Laden der Hauptwebseite aufgrund einiger Zugriffsbeschränkungen für die Benutzer.
- Ein Fehler verhindert das Laden der Webseite.
- Zwischenspeichern der eingebetteten Domänenressourcen durch Citrix Enterprise Browser, was dazu führt, dass die eingebetteten Domänen nicht von der Quelle abgerufen werden.

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`

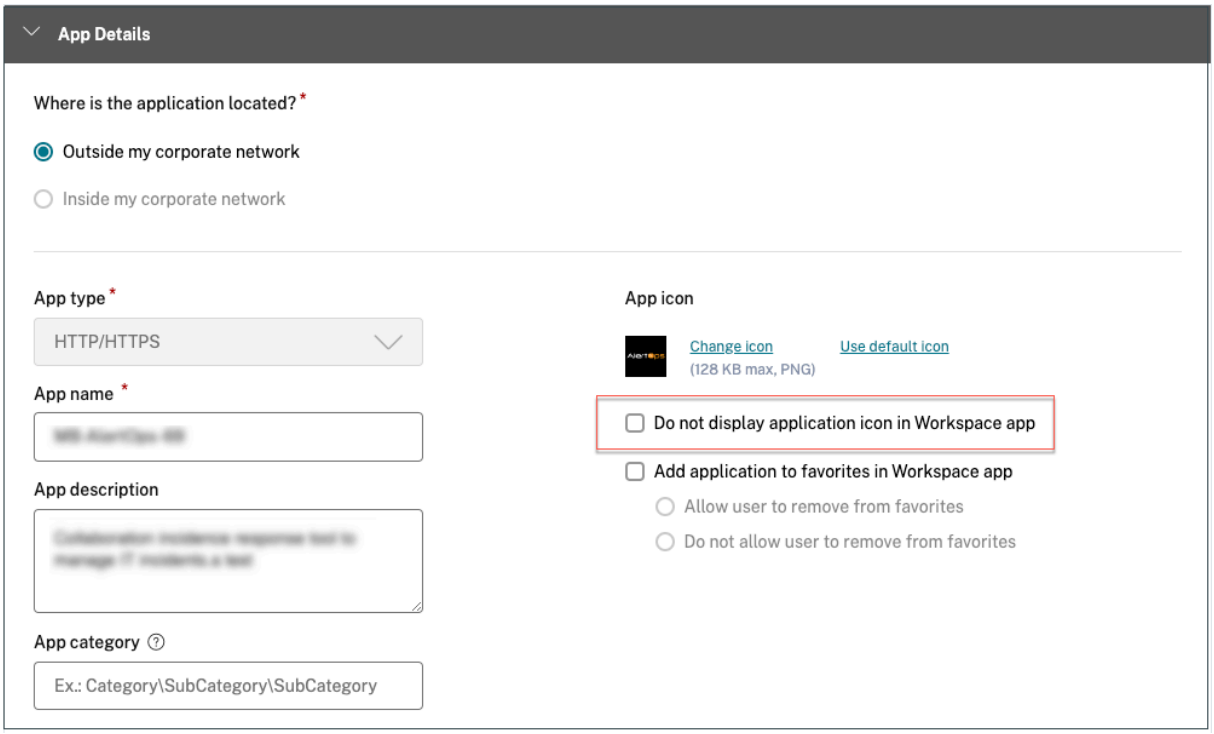
Hätte App1 jedoch stattdessen eine `*.intranet.local` verwandte Domain, dann `Eng-User5` wäre der Zugriff für verweigert worden, da genau gepasst `app.intranet.local` hätte `PolicyB`, für die der Benutzer, `Eng-User5`, keinen Zugriff hat.

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
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`.

Beenden Sie aktive Benutzersitzungen und fügen Sie Benutzer zur Benutzersperrliste hinzu

October 21, 2024

Administratoren können alle aktiven Endbenutzersitzungen sofort beenden und die Benutzer zur Benutzersperrliste hinzufügen. Durch das Hinzufügen eines Benutzers zu dieser Benutzersperrliste werden alle aktiven Secure Workspace Access-Anwendungssitzungen beendet und zukünftige Anwendungszugriffe blockiert.

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

> **Hinweis:**
>
> - Durch das Hinzufügen eines Benutzers zur Benutzersperrliste wird die konfigurierte Secure Private Access-Zugriffsrichtlinie weder geändert noch bearbeitet. Die Beendigung und Sperrung des Zugriffs erfolgt unabhängig von der konfigurierten Zugriffsrichtlinie. Sobald

> der Benutzer aus der Liste entfernt wird, werden die vorhandenen Secure Workspace Access-Zugriffsrichtlinien für den Benutzer wiederhergestellt.
> - Lediglich der Zugriff auf veröffentlichte Secure Private Access-Anwendungen ist blockiert. Der Internetzugriff über den Citrix Enterprise Browser wird zugelassen oder verweigert, auch nachdem ein Benutzer basierend auf Ihrer Webfilterkonfigurationzur Sperrliste hinzugefügt wurde.

Anwendungsfälle

Sie können diese Funktion in den folgenden Szenarien verwenden.

- Ein Mitarbeiter verlässt das Unternehmen oder wird entlassen. In diesem Fall widerruft der Administrator sämtlichen Secure Private Access-App-Zugriff, indem er aktive Secure Private Access-Sitzungen beendet und jeden zukünftigen App-Zugriff blockiert.
- Ein Gerät geht verloren oder wird gestohlen. In diesem Fall wird der Zugriff gesperrt und alle aktuellen Sitzungen werden beendet. Der Benutzer kann aus der Benutzersperrliste entfernt werden, nachdem die Situation unter Kontrolle ist.
- Ein Benutzer missbraucht den App-Zugang. In diesem Fall kann die Zugangsberechtigung des Nutzers umgehend widerrufen werden. Der Zugriff ist gesperrt, bis der Benutzer zur Liste hinzugefügt wird.

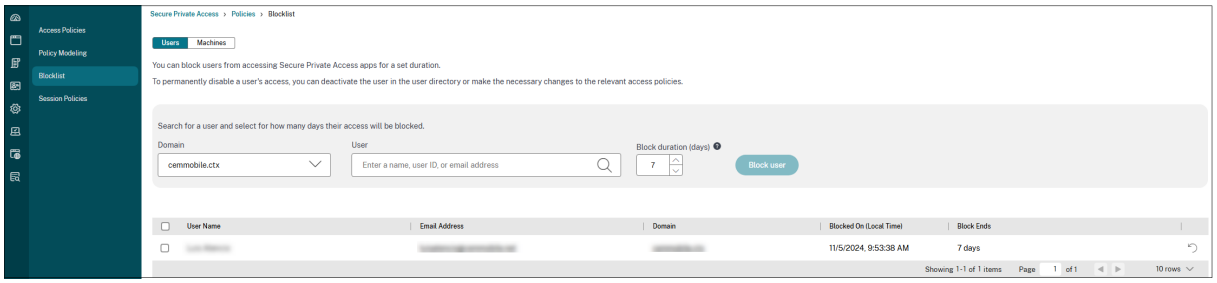
Benutzer zur Benutzersperrliste hinzufügen

1. Navigieren Sie zu **Sicherer privater Zugriff > Zugriffsrichtlinien** und klicken Sie dann auf die Registerkarte **Benutzersperrliste** .
2. Wählen Sie unter **Domäne**die Domäne aus, für die der Zugriff deaktiviert werden muss.
3. Suchen Sie in **Benutzer**nach dem Benutzernamen, der zur Benutzersperrliste hinzugefügt werden muss. Es werden alle Benutzernamen angezeigt, die den Suchkriterien entsprechen. Wenn der Benutzer aus dem Verzeichnisdienst entfernt wird, wird dieser Benutzername nicht in der Liste **Benutzer** angezeigt.
4. Geben Sie unter **Sperrdauer (Tage)**die Anzahl der Tage ein, für die dieser Benutzer gesperrt werden soll. Sobald Sie den Benutzer zur Sperrliste hinzufügen, ist er standardmäßig 7 Tage lang gesperrt. Sie können die Dauer jedoch auf einen Wert zwischen 1 und 99 Tagen ändern. Nach Ablauf der Dauer wird der Benutzerzugriff basierend auf dem Benutzerverzeichnis und der Richtlinienkonfiguration wiederhergestellt. Darüber hinaus bleibt dieser Wert für den Benutzer bei zukünftigen Ergänzungen erhalten. Wenn ein Administrator beispielsweise die Sperrdauer für einen Benutzer auf 30 Tage festlegt, bleibt diese Einstellung für den Benutzer auch bei zukünftigen Erweiterungen bestehen.

5. Klicken Sie auf **Benutzer**blockieren.

   Der Benutzer wird zur Benutzersperrliste hinzugefügt. Sobald der Benutzer zur Benutzersperrliste hinzugefügt wurde, werden die folgenden Aktionen ausgeführt:

   - Alle aktiven Secure Private Access-Sitzungen werden sofort beendet.
   - Der zukünftige Zugriff auf alle veröffentlichten Secure Private Access-Anwendungen ist blockiert.
   - Der Internetzugriff über den Citrix Enterprise Browser ist auch dann erlaubt, wenn ein Benutzer zur Benutzersperrliste hinzugefügt wurde. Nur der Zugriff auf veröffentlichte Secure Private Access-Anwendungen ist blockiert.



Sie können den Zugriff auch vor Ablauf der Sperrdauer wiederherstellen, indem Sie einen der folgenden Schritte ausführen.

- Wählen Sie den Zugang aus, für den Sie den Zugang wiederherstellen müssen und klicken Sie dann auf **Zugang wiederherstellen**.
- Klicken Sie auf das Wiederherstellen-Symbol neben dem Benutzer, für den Sie den Zugriff wiederherstellen möchten.

In beiden Fällen erscheint ein Bestätigungsdialog.

> **Empfehlungen:**
>
> - Um den Zugriff eines Benutzers auf unbestimmte Zeit zu widerrufen, entfernen Sie den Benutzer aus Ihrem entsprechenden Verzeichnisdienst, beispielsweise Active Directory, und fügen Sie ihn anschließend zur Benutzersperrliste hinzu. Dadurch wird die aktive Secure Workspace Access-Sitzung des Benutzers beendet, zukünftige App-Zugriffe werden blockiert und nachdem der Benutzer aus Workspace abgemeldet wurde, kann er sich aufgrund inaktiver Verzeichnisanmeldeinformationen nicht erneut anmelden.

Timeouts für Benutzersitzungen

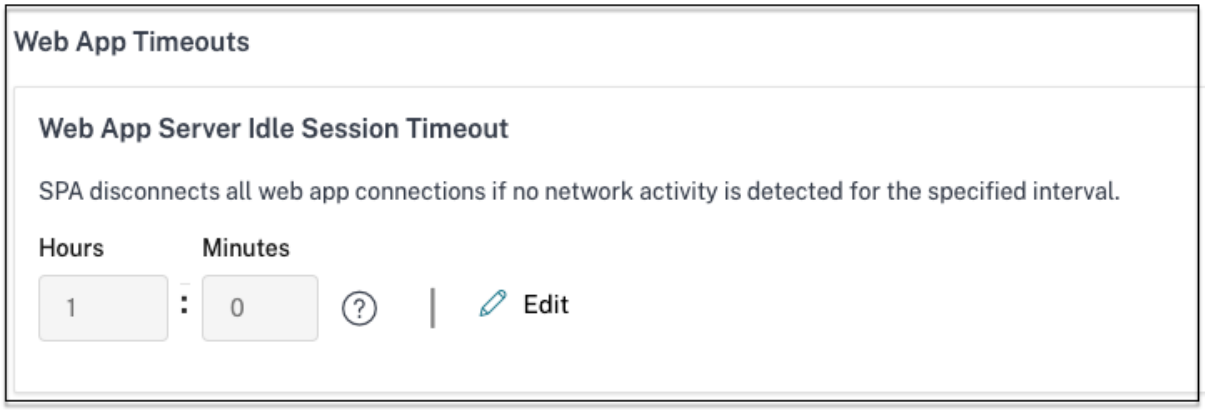
December 27, 2023

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.

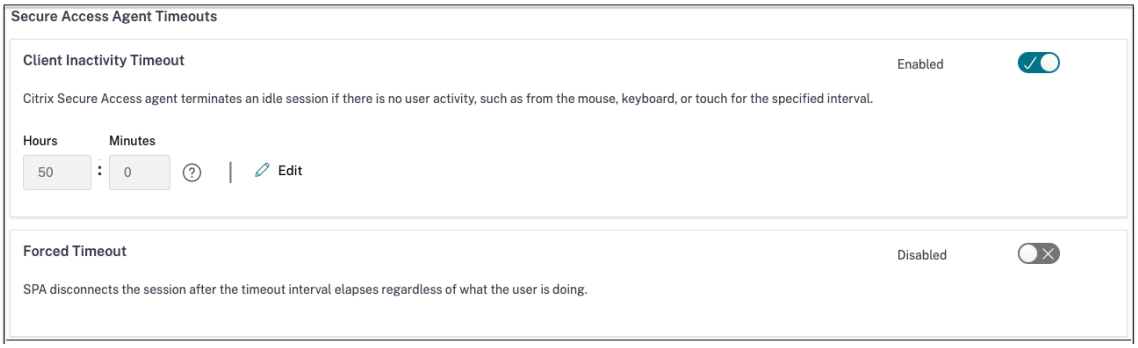


Timeouts für den Citrix Secure Access Client

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.

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.

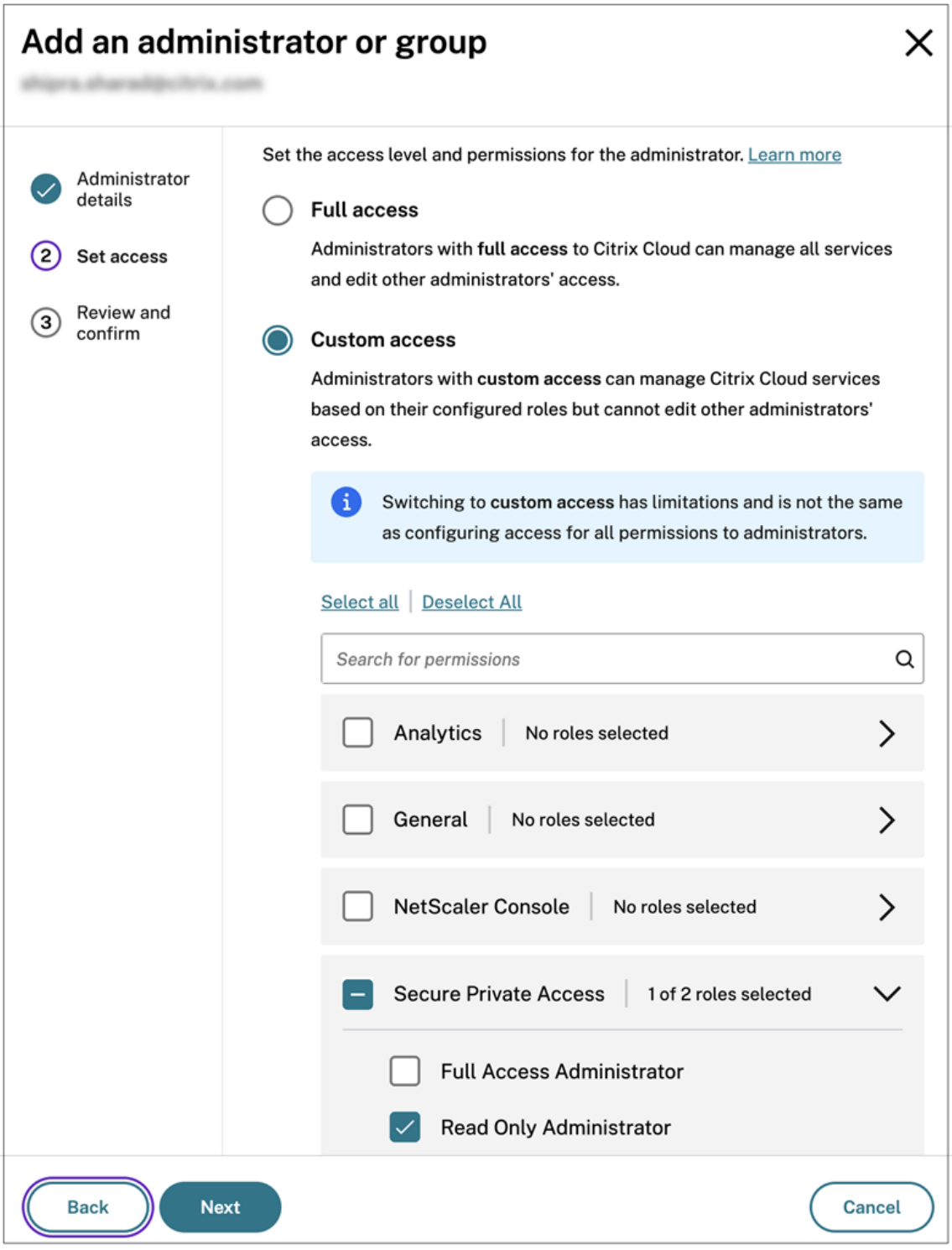
- Fügen Sie Enterprise Web- oder SaaS-Apps hinzu.
- Fügen Sie neue Connector-Appliances an bestehenden oder neuen Ressourcenstandorten hinzu.

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**.

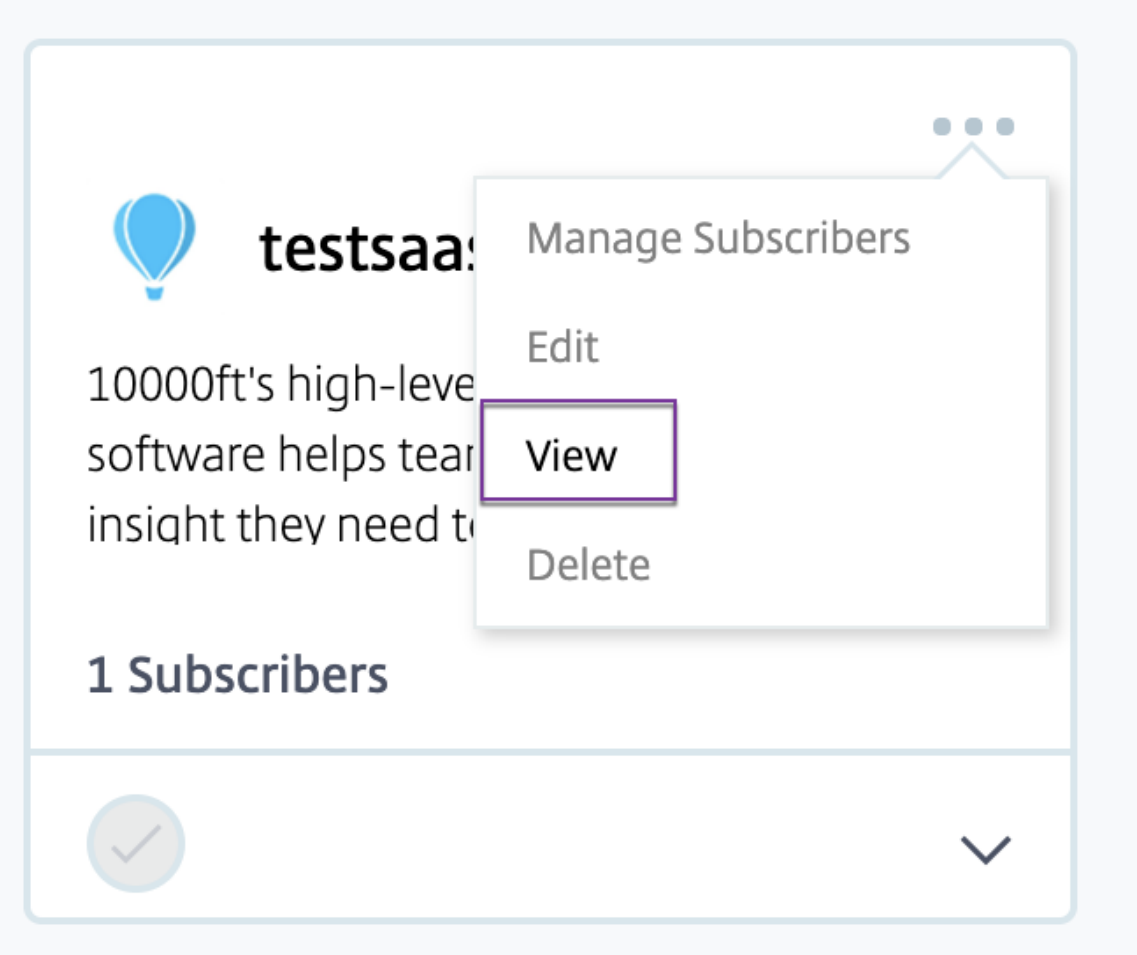
> **Wichtig:**
>
> - Wenn Sie Citrix Gateway **Service-Administratoren nur Lese-Administratorzugriff**

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.

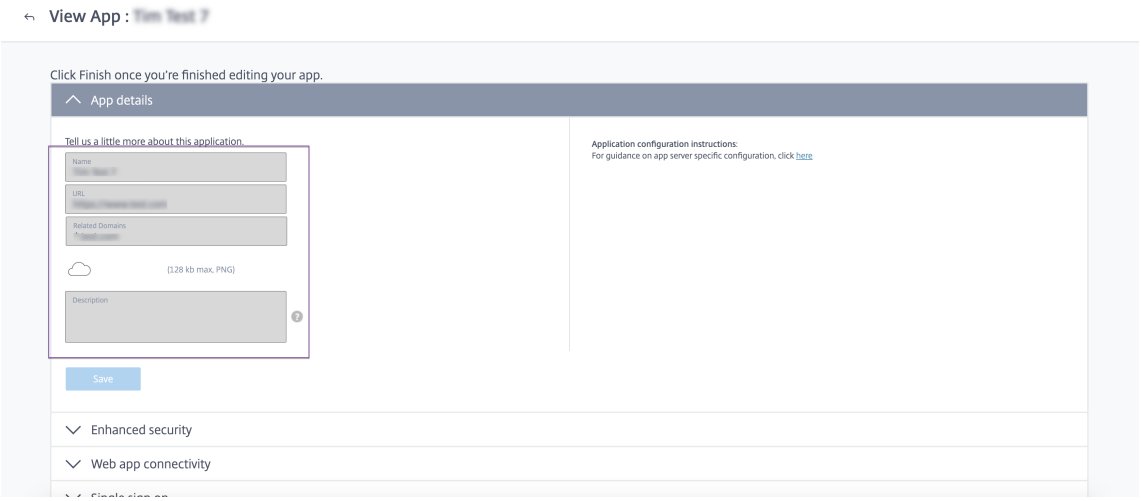
- Die Schaltfläche **Web-/SaaS-App hinzufügen** ist für Benutzer mit **Nur-Lese-Administratorzugriff** deaktiviert.

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**.



Dashboard-Übersicht

October 21, 2024

Das Dashboard des Secure Private Access-Dienstes zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Über das Dashboard haben Administratoren an einem einzigen Ort vollständige Einblicke in den Integritätsstatus ihrer Apps, Benutzer und Konnektoren sowie in die Bandbreitennutzung. Diese Daten werden von Citrix Analytics abgerufen. Die Daten für die verschiedenen Entitäten können für die voreingestellte Zeit oder für eine benutzerdefinierte Zeitachse angezeigt werden. Bei einigen Entitäten können Sie einen Drilldown durchführen, um weitere Details anzuzeigen.

Die Metriken werden grob in die folgenden Kategorien eingeteilt.

- **Protokollierung und Fehlerbehebung**
  - Diagnoseprotokolle: Protokolle im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Aufzählung und Gerätestatusprüfungen.
- **Benutzer**
  - Aktive Benutzer: Gesamtzahl der eindeutigen Benutzer, die im ausgewählten Zeitraum auf die Anwendungen (SaaS, Web und TCP) zugreifen.
  - Uploads: Gesamtvolumen der über den Secure Private Access-Dienst hochgeladenen Daten für das ausgewählte Zeitintervall.
  - Downloads: Gesamtvolumen der über den Secure Private Access-Dienst für das ausgewählte Zeitintervall heruntergeladenen Daten.
- **Anwendungen:**

  - Anwendungen: Gesamtzahl der aktuell konfigurierten Anwendungen (unabhängig vom Zeitintervall).
  - Anzahl der Anwendungsstarts: Gesamtzahl der von jedem Benutzer im ausgewählten Zeitintervall gestarteten Anwendungen (App-Sitzungen).
  - Konfigurierte Domänen: Gesamtzahl der für das ausgewählte Zeitintervall konfigurierten Domänen.
  - Erkannte Anwendungen: Gesamtzahl eindeutiger, einzelner Domänen, auf die zugegriffen wurde, die jedoch keiner Anwendung zugeordnet sind.

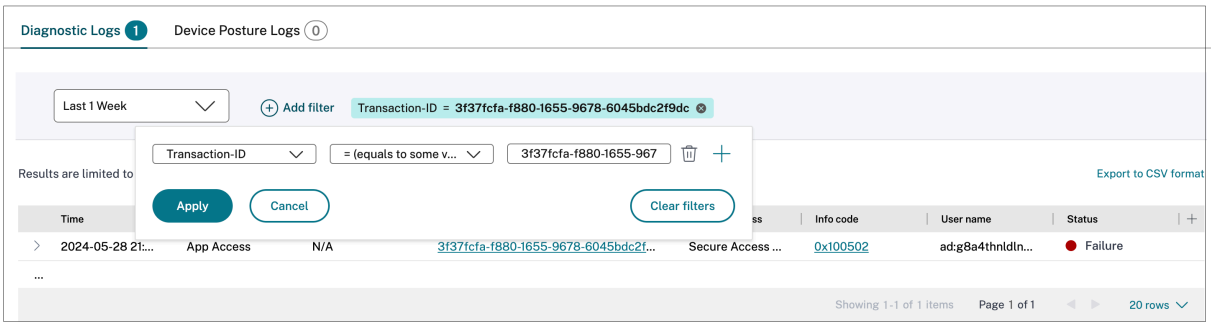
- **Zugriffsrichtlinien**

  - Zugriffsrichtlinien: Gesamtzahl der aktuell konfigurierten Zugriffsrichtlinien (unabhängig vom Zeitintervall).

Diagnoseprotokolle

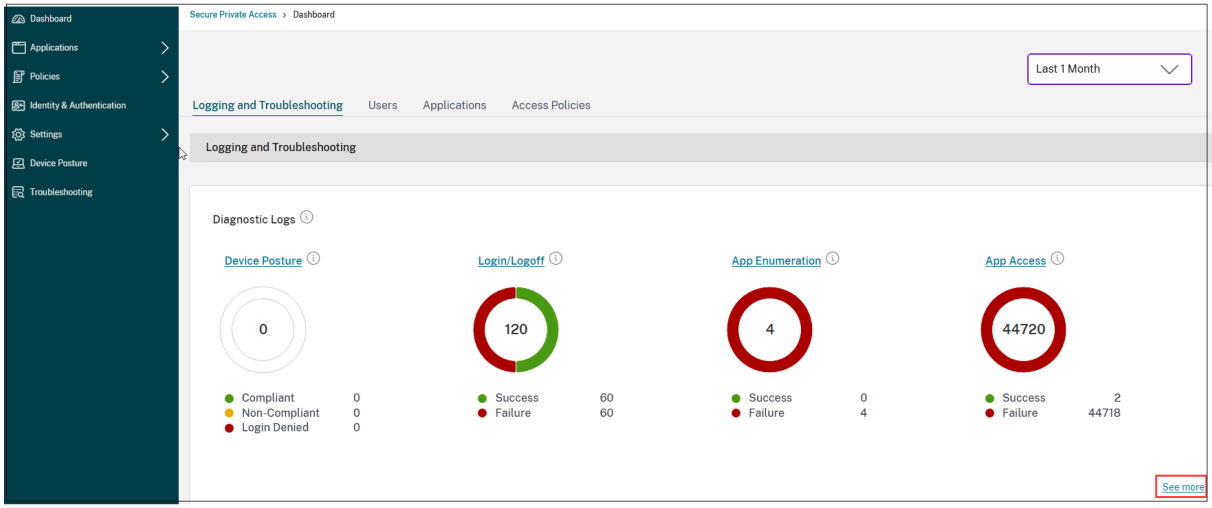
Verwenden Sie das Diagramm **Diagnoseprotokolle** , um die Protokolle im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Aufzählung sowie Protokolle im Zusammenhang mit der Gerätehaltung anzuzeigen. Sie können auf den Link **Mehr anzeigen** klicken, um die Details der Protokolle anzuzeigen. 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 +-Zeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerprotokolle im CSV-Format exportieren.

- Mit der Option **Filter hinzufügen** können Sie Ihre Suche anhand verschiedener Kriterien wie App-Typ, Kategorie und Beschreibung verfeinern. Sie können in den Suchfeldern beispielsweise `Transaktions-ID`, `= (entspricht einem bestimmten Wert)` auswählen und `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`in dieser Reihenfolge eingeben, um nach allen Protokollen zu suchen, die mit dieser Transaktions-ID in Zusammenhang stehen. Einzelheiten zu den Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.

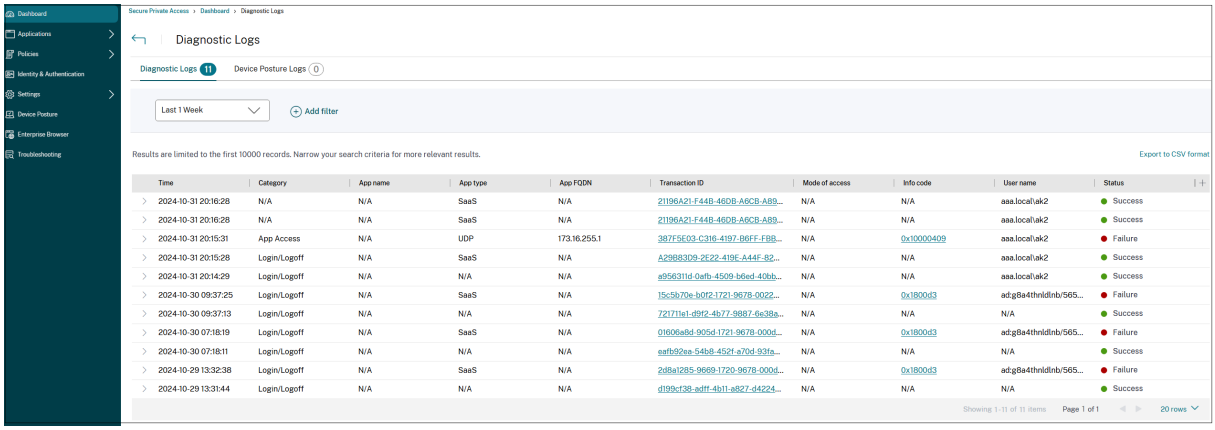


- **Gerätestatusprotokolle:** Sie können Ihre Suche basierend auf den Richtlinienergebnissen (**Konform, Nicht konform und Anmeldung verweigert**) verfeinern. Einzelheiten zur Gerätehaltung finden Sie unter Gerätehaltung.

> **Hinweis:**
>
> - Jedem Fehlerereignis im Dashboard der Diagnoseprotokolle von Secure Private Access ist ein Infocode zugeordnet. Einzelheiten finden Sie unter Infocode.
> - Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanforderung. 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 aufgerufenen Haupt-URLs angezeigt. Administratoren können die eingebetteten Domänen anzeigen, indem sie in der Haupt-URL auf das Erweiterungssymbol (>) klicken. Administratoren können die Liste der eingebetteten Domänen verwenden, um Probleme im Zusammenhang mit dem App-Zugriff oder der App-Wiedergabe zu beheben. Wenn beispielsweise in der Anwendungskonfiguration eine Domäne fehlt, kann der Endbenutzer nicht auf die entsprechende App zugreifen. In diesem Fall kann der Administrator die Liste der eingebetteten Domänen anzeigen, die fehlende Domäne identifizieren und dann die App-Konfiguration mit der fehlenden Domäne aktualisieren.

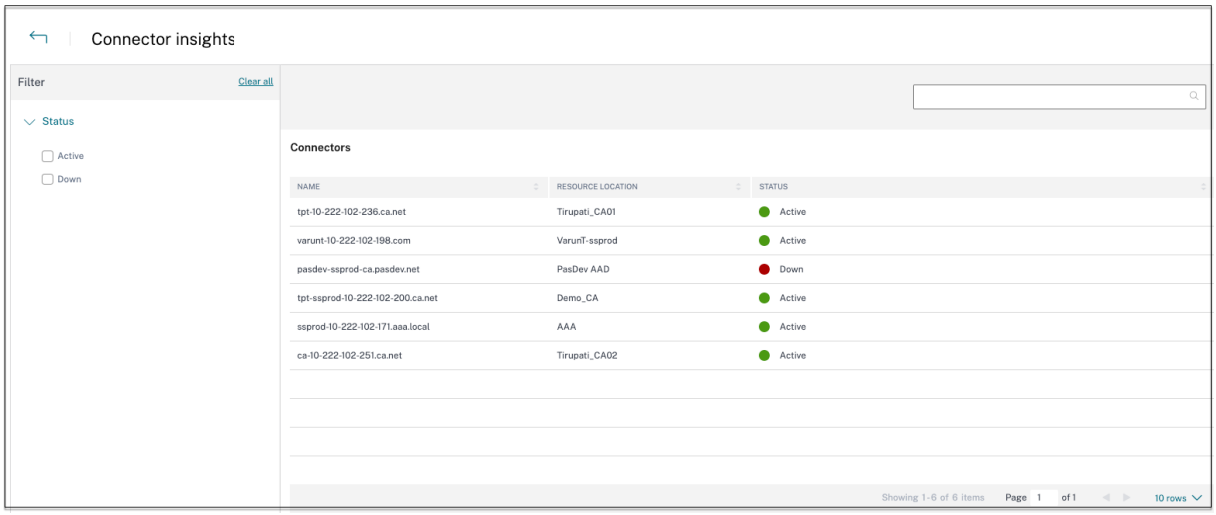


Hinweis:

- 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.

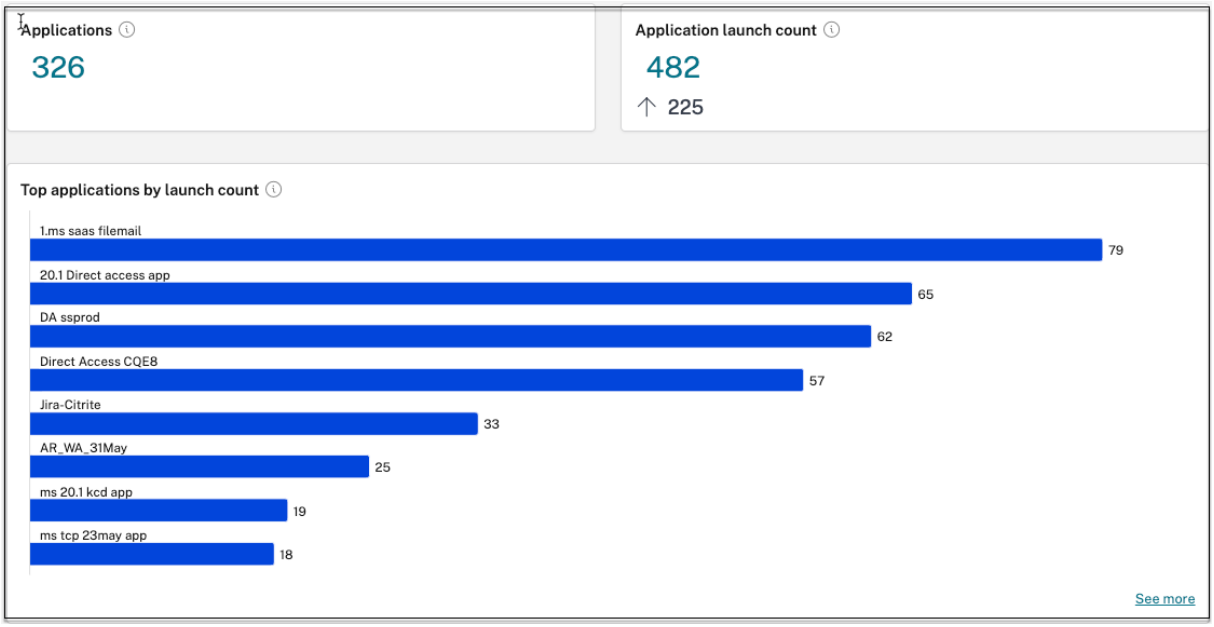
Connector-Status

Verwenden Sie das Diagramm **Connector-Status** , um den Status der Connectoren und die Ressourcenstandorte anzuzeigen, an denen die Connectoren bereitgestellt werden. Klicken Sie auf den Link **Mehr anzeigen** , um die Details anzuzeigen. Auf der Seite „ **Connector Insights** “können Sie die Filter **„Aktiv“** oder **„Inaktiv“** verwenden, um die Connectoren basierend auf ihrem Status zu filtern.



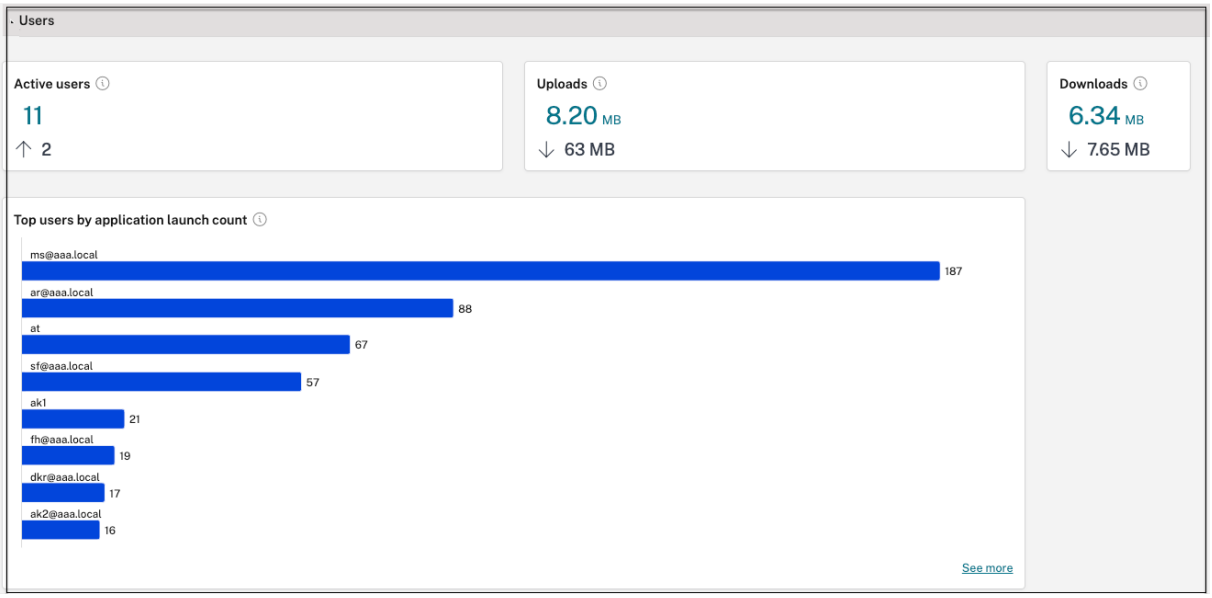
Top-Anwendungen nach Anzahl der Starts

Verwenden Sie das Diagramm „ **Top-Anwendungen nach Anzahl der Starts** “, um die Liste der Top-Anwendungen basierend auf der Anzahl der App-Starts, der Gesamtmenge der auf den App-Server hochgeladenen Daten und der Gesamtmenge der vom App-Server heruntergeladenen Daten anzuzeigen. 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 oder einer benutzerdefinierten Zeitachse filtern.



Top-Benutzer nach Anzahl der Anwendungsstarts

Verwenden Sie das Diagramm „ **Top-Benutzer nach Anzahl der Anwendungsstarts** “, um die Daten pro Benutzer anzuzeigen. Beispielsweise wie oft 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 oder einer benutzerdefinierten Zeitachse filtern.

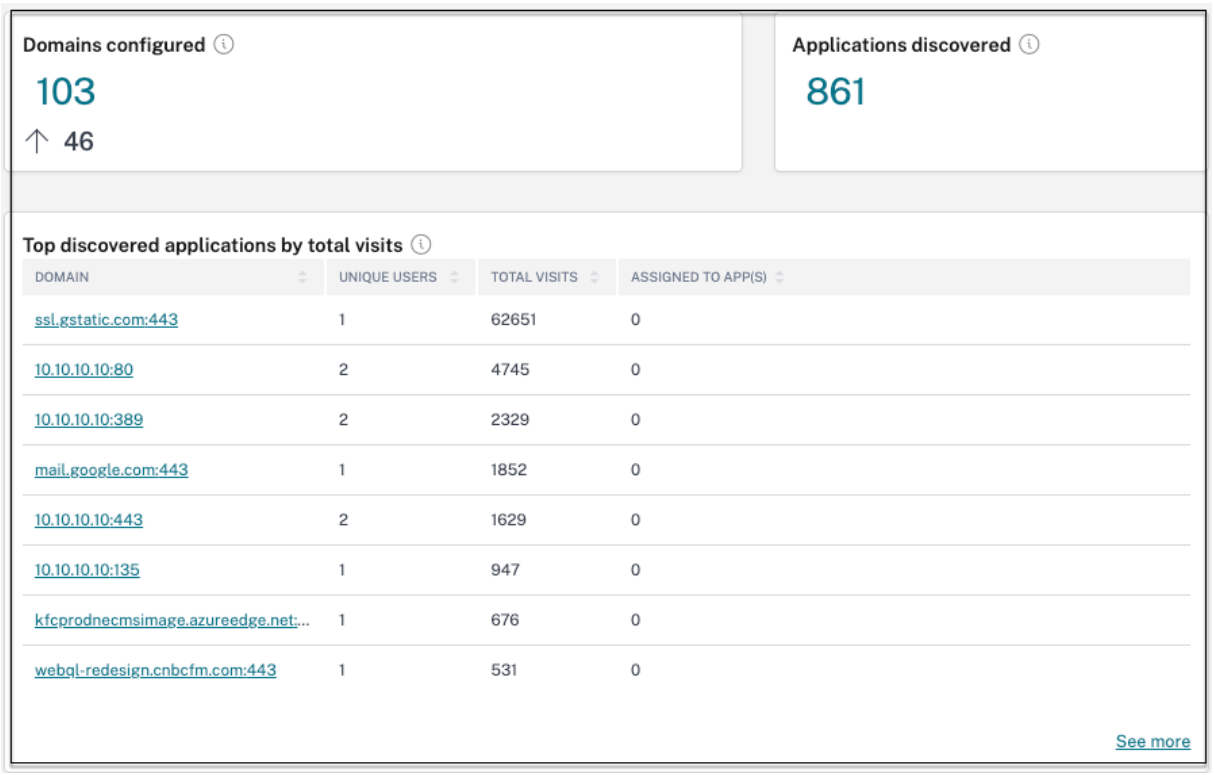


Wichtigste Zugriffsrichtlinien nach Durchsetzung

Verwenden Sie das Diagramm **Wichtigste Zugriffsrichtlinien nach Durchsetzung** , um die Liste der Zugriffsrichtlinien anzuzeigen, die für die Apps erzwungen werden. Klicken Sie auf den Link **Weitere Informationen** , um die Liste der mit den Apps verknüpften Richtlinien und die Häufigkeit der Durchsetzung der Richtlinien anzuzeigen. Sie können auch die Option **Suchen** auf der Seite „Zugriffsrichtlinien“verwenden, um die Richtlinien basierend auf dem Richtliniennamen zu filtern. Sie können auch mit den Suchoperatoren nach bestimmten Richtlinien suchen, um Ihre Suche weiter zu verfeinern. Einzelheiten finden Sie unter Suchoperatoren.

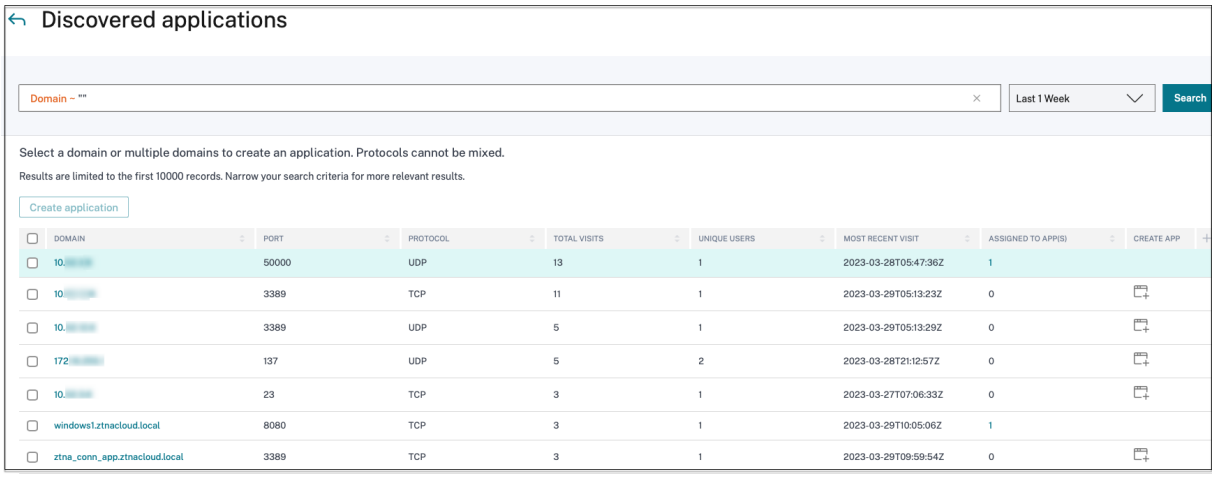
Am häufigsten entdeckte Anwendungen

Verwenden Sie das Diagramm **„Am häufigsten entdeckte Anwendungen nach Gesamtzahl der Besuche“** , um die Liste eindeutiger, einzelner Domänen anzuzeigen, auf die irgendwann zugegriffen wurde, die aber mit keinen Apps verknüpft sind. Diese Domänen werden basierend auf der Anzahl der Gesamtbesuche dieser Domänen aufgelistet. Mithilfe dieses Diagramms können Administratoren feststellen, ob auf eine Domäne von besonderem Interesse viele Benutzer zugreifen. In solchen Fällen können Administratoren für einen einfacheren Zugriff eine App mit dieser Domäne erstellen.



Im Diagramm zeigt die Spalte **ZUGEWIESEN AN APPs** die Gesamtzahl der Anwendungen an, für die diese Domäne als Teil ihrer zugehörigen URL- oder Ziel-URL-Werte konfiguriert ist. Durch Klicken auf die Nummer werden die Apps angezeigt, die dieser Domäne zugeordnet sind.

Sie können auf den Link **Mehr anzeigen** klicken, um weitere Details zu allen Domänen anzuzeigen.



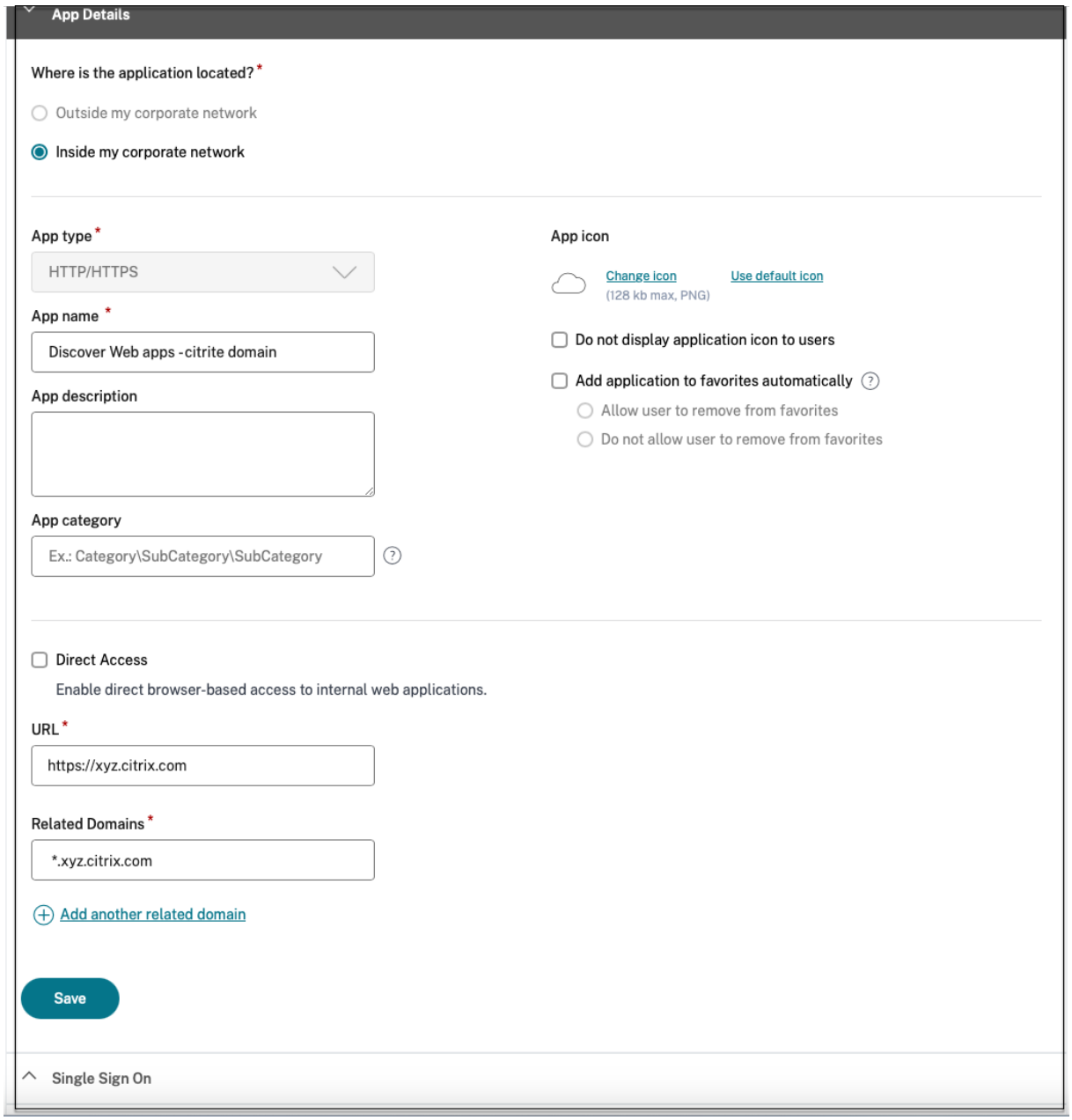
Auf der Seite „ **Entdeckte Anwendungen** “werden die Details der Domänen angezeigt, wie etwa Domänenname, Port, Protokoll, Gesamtzahl der Besuche, eindeutige Benutzer und das letzte Besuchsdatum. Alle Spalten im Diagramm sind sortierbar. Sie können die Suchleiste für die domänenbasierte Suche verwenden.

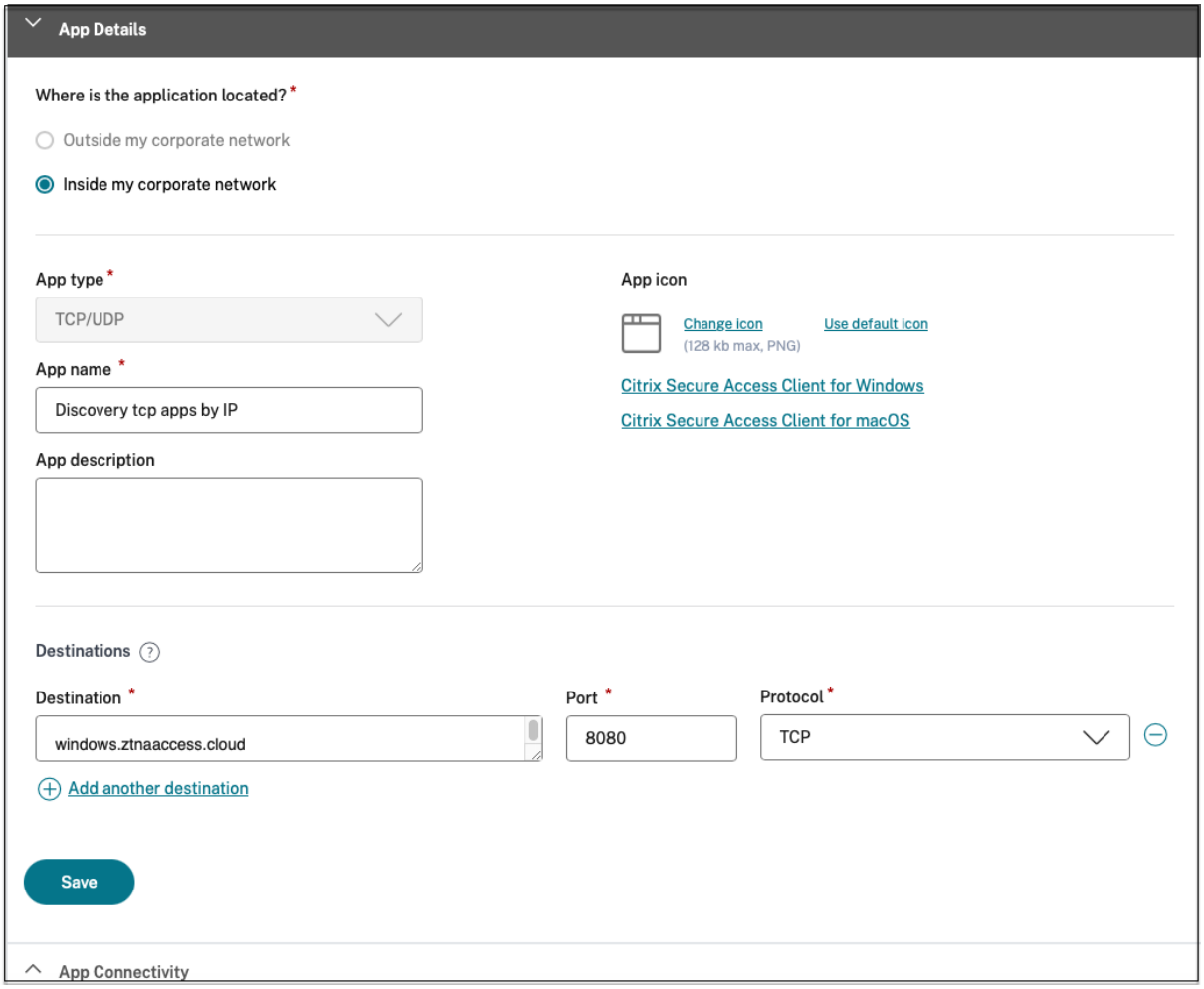
> **Hinweis:**
>
> - Die Protokolle werden auf Basis der von den Kunden verwendeten Standardports abgeleitet.
> - Die Liste der gefundenen Domänen ist auf 10.000 Datensätze begrenzt.

Erstellen einer App aus dem Diagramm

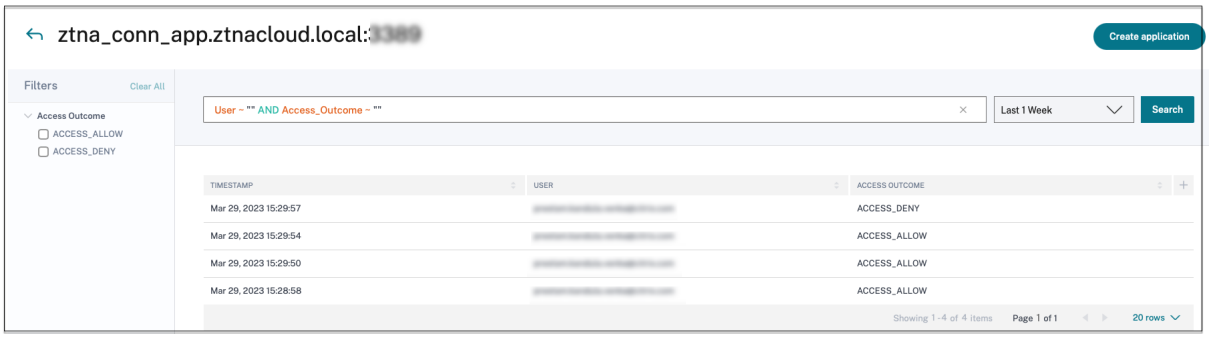
Klicken Sie auf das Symbol **+** in der jeweiligen Domäne, um eine App zu erstellen. Der App-Konfigurationsassistent wird angezeigt. Das Symbol „App erstellen“wird nicht für die Zeilen angezeigt, in denen bereits eine App mit derselben Kombination aus Domäne, Port und Protokoll erstellt wurde und sich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

- Der App-Typ wird automatisch basierend auf dem von Ihnen ausgewählten App-Protokoll ausgefüllt. Sie können den Typ jedoch bei Bedarf ändern.
- Die Werte in den Feldern **URL, Zugehörige Domänen, Ziel, Port, Protokoll** werden alle automatisch ausgefüllt. Führen Sie die Schritte zum Hinzufügen einer App aus. Weitere Einzelheiten finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichten.





Sie können auch auf den eindeutigen Domänenlink klicken, um weitere Details anzuzeigen und eine Anwendung für diese Domäne zu erstellen. Wenn Sie auf einen Domänenlink klicken, werden die Benutzerauthentifizierungsprotokolle für die Domäne angezeigt. Klicken Sie auf die Schaltfläche **Anwendung erstellen** . Führen Sie die Schritte zum Hinzufügen einer App aus.



Suchoperatoren

Mit den folgenden Suchoperatoren können Sie Ihre Suche verfeinern:

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

Protokollierung und Fehlerbehebung

October 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. Nachfolgend finden Sie einige häufig gestellte Fragen (FAQs), die Ihnen dabei helfen sollen, dieses Thema besser zu nutzen.

Häufig gestellte Fragen?

Was sind Secure Private Access-Diagnoseprotokolle?

Wo finde ich Secure Private Access-Protokolle?

Welches Widget zeigt die Diagnoseprotokolle von Secure Private Access an?

Welche Details finde ich in den Diagnoseprotokollen von Secure Private Access?

Welche Ereignisse werden in den Diagnoseprotokollen von Secure Private Access erfasst?

Wie filtere ich die Diagnoseprotokolle?

Wie verwende ich das Thema zur Fehlerbehebung bei Secure Private Access, um einen aufgetretenen Fehler zu beheben?

Was ist ein Infocode? Wo finde ich sie?

Was ist eine Transaktions-ID? Wie verwende ich es?

Was sind alle Secure Private Access PoP-Standorte?

Was kann ich tun, wenn ich meinen Fehler mithilfe des Infocodes und der Fehlernachschlagetabelle nicht beheben kann?

Infocode-Nachschlagetabelle

Die folgende Fehlernachschlagetabelle bietet einen umfassenden Überblick über die verschiedenen Fehler, die bei der Verwendung des Secure Private Access-Dienstes auftreten können.

Infocode	Beschreibung	Auflösung
0x180006, 0x1800B7	Der App-Start ist fehlgeschlagen, da die Länge des App-FQDN überschritten wurde	Der App-Start ist fehlgeschlagen, da die Länge des FQDN der App überschritten wurde
OS-Nummer	Der App-Start ist fehlgeschlagen, da der Authentifizierungsdienst ausgefallen ist.	Der App-Start ist fehlgeschlagen, da der Authentifizierungsdienst ausgefallen ist
0x180001, 0x18001A, 0x18001B, 0x18008A 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0 0x1800B1, 0x1800B2, 0x1800B3, 0x180048	Single Sign-On-Fehler, Verbindungsaufbaufehler zwischen Citrix Cloud und lokalen Connectors, SAML SSO-Fehler, ungültiger App-FQDN	Der App-Zugriff wird verweigert
OS-Version	Problem beim Verbinden mit dem Connectorgerät	Problem beim Verbinden mit dem Connectorgerät
Version	DNS-Suche/Verbindung fehlgeschlagen	Secure Browser Service –DNS-Lookup-/Verbindungsfehler
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5 0x1800A6, 0x1800A7	Der Start der Web-App ist fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte.	Der Start der Web-App ist fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte.
0x1800BC, 0x1800BF	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App zuzugreifen	Der Benutzer ist nicht berechtigt, auf die Web-/SaaS-App zuzugreifen
OS-Version	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

Infocode		Beschreibung	Auflösung
	OS-Version	Der Start der Citrix Secure Access-Agent-Sitzung ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen	Der Start der Citrix Secure Access-Agent-Sitzung ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA		Der Start der Citrix Secure Access-Agent-Sitzung ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen. Der Start der Citrix Secure Access-Agent-App ist während der Richtlinienauswertung fehlgeschlagen. Der Start der Citrix Secure Access-Agent-App ist fehlgeschlagen.	Fehlerhafte Clientanforderungen
	OS-Version	Der Start der Citrix Secure Access-Agent-App ist während der Richtlinienauswertung fehlgeschlagen	Der Start der Citrix Secure Access-Agent-App ist während der Richtlinienauswertung fehlgeschlagen
0x180055, 0x1800DF, 0x1800E3		Durch kontextbezogene Richtlinien eingeschränkte Apps, Zugriff aufgrund der Richtlinienkonfiguration verweigert	Eine oder mehrere Apps werden nicht im Benutzer-Dashboard aufgeführt
	OS-Version	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

Infocode	Beschreibung	Auflösung
0x10000001, 0x10000002, 0x10000003, 0x10000004	Citrix Secure Access-Client-Anmeldung fehlgeschlagen aufgrund eines Netzwerkproblems	Problem mit der Netzwerkkonnektivität beim Citrix Secure Access-Client
Nummer der OS-Nummer	Citrix Secure Access-Client-Anmeldefehler aufgrund eines Proxys in der Mitte	Proxyserver stört Client-Konnektivität mit Dienst
Nummer	Fehler bei der Anmeldung beim Citrix Secure Access-Client aufgrund einer nicht vertrauenswürdigen Zertifizierungsstelle	Es wurde ein Problem mit einem nicht vertrauenswürdigen Serverzertifikat beobachtet.
Nummer der Kontrollnummer	Citrix Secure Access-Client-Anmeldung fehlgeschlagen aufgrund eines ungültigen Zertifikats	Es wurde ein Problem mit einem ungültigen Serverzertifikat festgestellt.
Nummer	Citrix Secure Access-Client-Anmeldung fehlgeschlagen aufgrund eines Konfigurationsproblems	Die Anmeldung ist fehlgeschlagen, da die Konfiguration für den Benutzer leer ist
Nummer	Citrix Secure Access-Client-Anmeldung fehlgeschlagen aufgrund eines Verbindungsfehlers	Verbindung vom Netzwerk oder Endbenutzer beendet
0x10000010	Citrix Secure Access-Client-Anmeldung fehlgeschlagen aufgrund abgelaufener Sitzung	Der Download der Konfiguration ist fehlgeschlagen, da die Sitzung abgelaufen ist.
Nummer	Fehler bei der Anmeldung beim Citrix Secure Access-Client aufgrund einer großen Konfigurationsliste	Citrix Secure Access-Client konnte sich nicht anmelden
Nr.	Fehler bei der Anmeldung beim Citrix Secure Access-Client aufgrund eines Fehlers bei der Erstellung des Kontrollkanals	Der Aufbau des Kontrollkanals ist fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode		Beschreibung	Auflösung
	Nr.	Anmeldung beim Citrix Secure Access-Client fehlgeschlagen aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Die Einrichtung des Kontrollkanals ist fehlgeschlagen
	Nr.	Anmeldung beim Citrix Secure Access-Client fehlgeschlagen aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Die Einrichtung des Kontrollkanals ist fehlgeschlagen
	Nr.	Anmeldung beim Citrix Secure Access-Client fehlgeschlagen aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Die Einrichtung des Kontrollkanals ist aufgrund eines Netzwerkproblems fehlgeschlagen
	Nummer	Abmeldung vom Citrix Secure Access-Client fehlgeschlagen, da die Sitzung bereits abgelaufen ist	Abmeldung nicht möglich, da Sitzung beendet wurde
0x12000002		Abmeldung vom Citrix Secure Access-Client fehlgeschlagen, da die Sitzung bereits abgelaufen ist	Die Sitzung wird zwangsweise beendet.
0x13000001		Der App-Zugriff ist fehlgeschlagen, da die Sitzung abgelaufen ist	Der Anwendungsstart ist fehlgeschlagen, da die Sitzung abgelaufen ist
0x13000002		Der App-Zugriff ist aufgrund einer unzureichenden Lizenz fehlgeschlagen	Der Anwendungsstart ist aufgrund eines Lizenzproblems fehlgeschlagen
0x13000003, 0x13000008, 0x001800DF		Der App-Zugriff ist fehlgeschlagen, da der Zugriff verboten ist. Der TCP/UDP-App-Start wird gemäß Richtlinie verweigert.	Der Start der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde.
0x13000004, 0x13000005		Der App-Zugriff ist fehlgeschlagen, da der Server nicht verfügbar ist	Der Anwendungsstart ist fehlgeschlagen, da der Client den Dienst nicht erreichen kann

Infocode	Beschreibung	Auflösung
0x13000007	Der App-Zugriff ist fehlgeschlagen, da die Zugriffsrichtlinie deaktiviert ist oder der Benutzer nicht angemeldet 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
Version	Der Client hat die Verbindung geschlossen	Der Client hat die Verbindung mit dem Secure Private Access-Dienst geschlossen.
0x1300000C	Die FQDN-Auflösung über ZTNA ist fehlgeschlagen	FQDN kann vom DNS-Server nicht aufgelöst werden
OS-Nummer	Fehler beim Herunterladen der Anwendungskonfiguration während der Anmeldung	Die Liste der konfigurierten Anwendungsziele konnte nicht abgerufen werden.
0x001800D9, 0x001800DA	Der Start der TCP/UDP-App ist während der Analyse der Antwort zur Richtlinienauswertung fehlgeschlagen. Der Start der TCP/UDP-App ist während der Richtlinienauswertung mit einem ungültigen Ergebnis fehlgeschlagen.	Problem mit der Anwendungskonfiguration
0x001800DB	Der Start der TCP/UDP-App ist aufgrund einer ungültigen Ressourcenstandortkonfiguration fehlgeschlagen	Problem mit dem Ressourcenstandort

Infocode		Beschreibung	Auflösung
0x13000006, 0x001800DC, 0x001800DD		Der Start der TCP-App ist fehlgeschlagen, da für die App eine nicht unterstützte Richtlinie für erweiterte Sicherheit konfiguriert wurde. Der Start der TCP-App ist fehlgeschlagen, da für die TCP-App eine nicht unterstützte Umleitung des Secure Browser Service konfiguriert wurde.	Die erweiterte Sicherheitsrichtlinie ist an die HTTP-Anwendung gebunden
	OS-Nummer	Der Start der TCP/UDP-App ist fehlgeschlagen, da für das Ziel keine Anwendungskonfiguration gefunden wurde	Die Anwendung konnte nicht gefunden werden
	Version	Der Start der TCP-App ist fehlgeschlagen, da der Ziel-FQDN zu lang ist	Die Länge des Hostnamens überschreitet 256 Zeichen
	Version	Der Start der TCP-App ist aufgrund einer ungültigen Ziel-IP fehlgeschlagen.	Ungültige IP-Adresse
	Version	Der Start der TCP-App ist während des Verbindungsaufbaus zum privaten TCP-Server fehlgeschlagen	Es kann keine Ende-zu-Ende-Verbindung hergestellt werden
	OS-Version	Der Start der UDP-App ist aufgrund der IPV6-Adresse fehlgeschlagen	In der App-Anforderung empfangenes IPv6
	OS-Version	UDP-Datenverkehr konnte nicht übermittelt werden, da die Client-Verbindung verloren ging	UDP-Verkehr konnte nicht übermittelt werden
0x001800FF		Die Übermittlung des UDP-Datenverkehrs ist fehlgeschlagen	Die Übermittlung des UDP-Datenverkehrs ist fehlgeschlagen

Infocode		Beschreibung	Auflösung
0x10000401		Anwahl des Citrix Rendezvous-Servers ist fehlgeschlagen	Der Anwendungsstart ist aufgrund von Netzwerkverbindungsproblemen fehlgeschlagen
0x10000402, 0x1000040C		Das Connectorgerät kann nicht registriert werden. Initialisierungsfehler der UDP-Netzwerkverbindung	Die Registrierung des Connector-Geräts beim Secure Private Access-Dienst ist fehlgeschlagen
0x10000403, 0x10000404, 0x10000407, 0x1000040A 0x1000040B, 0x1000040F, 0x10000410		Verbindungsfehler, Fehler bei der Übertragung des Kontrollpakets, Fehler beim Lesen des Gateway-Dienstes,	Konnektivitätsproblem mit dem Connectorgerät
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412		Back-End nicht erreichbar, Fehler bei der Analyse des Kontrollpakets, Fehler beim Schreiben des Gateway-Dienstes,	Konnektivitätsprobleme mit Connector Appliance und privaten TCP/UDP-Back-End-Servern
0x10000406		UDP-Paketübertragungsfehler, UDP-Paketempfangsfehler, Fehler beim Schreiben ins DNS-Auflösung fehlgeschlagen	Connector-Gerät kann DNS für FQDNs nicht auflösen
0x10000411		Back-End, Back-End hat die Verbindung geschlossen Der Gateway-Dienst hat die Verbindung geschlossen	Private Serververbindung beendet
0x10000413		Fehler bei der Ermittlung des Grundes für den Verbindungsabbau	Verbindung zum privaten Dienst-IP oder FQDN konnte nicht hergestellt werden oder Daten konnten nicht gesendet werden
	OS-Nummer	Der Benutzerkontext entspricht nicht den Bedingungen der Zugriffsregel	Keine übereinstimmende Richtlinienbedingung
	OS-Nummer	Der Anwendung ist keine Zugriffsrichtlinie zugeordnet.	Der Anwendung ist keine Zugriffsrichtlinie zugeordnet
	Version	Ergebnisse der Richtlinienauswertung mehrerer Anwendungen, auf die der Benutzer möglicherweise Zugriff hat	App-Enumerationsinformationen

Infocode	Beschreibung	Auflösung
0x00180101	Der Start der TCP/UDP-App ist fehlgeschlagen, da in der Anwendungsdomänentabelle ein Routing-Eintrag fehlt.	Der Start der TCP/UDP-App ist fehlgeschlagen, da in der Anwendungsdomänentabelle ein Routing-Eintrag 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 fehlgeschlagen, da Connector nicht erreichbar ist	UDP/DNS-Anfrage fehlgeschlagen, da Connector nicht erreichbar ist
0x20580001	Seite konnte nicht geladen werden, da NGS-Cookie abgelaufen ist	Seite konnte nicht geladen werden, da NGS-Cookie abgelaufen ist
0x20580002	Das Abrufen der Zugriffsrichtlinie ist aufgrund eines Netzwerkfehlers fehlgeschlagen.	Das Abrufen der Zugriffsrichtlinie ist aufgrund eines Netzwerkfehlers fehlgeschlagen.
0x20580003	Beim Parsen des JSON-Web-Tokens ist der Abruf der Zugriffsrichtlinie fehlgeschlagen	Beim Parsen des JSON-Web-Tokens ist der Abruf der Zugriffsrichtlinie fehlgeschlagen
0x20580004	Netzwerkfehler beim Abrufen der Zugriffsrichtliniendetails	Netzwerkfehler beim Abrufen der Zugriffsrichtliniendetails
0x20580005	Beim Abrufen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen.	Beim Abrufen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen.
0x20580007	Beim Überprüfen der JWT-Signatur ist der Richtlinienabruf fehlgeschlagen	Beim Überprüfen der JWT-Signatur ist der Richtlinienabruf fehlgeschlagen

Infocode		Beschreibung	Auflösung
0x20580008		Beim Überprüfen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen	Beim Überprüfen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen
	OS-Nummer	Die Bestimmung der Shop-Umgebung zum Erstellen einer Richtlinien-URL ist fehlgeschlagen	Die Bestimmung der Shop-Umgebung zum Erstellen einer Richtlinien-URL ist fehlgeschlagen
	OS-Nummer	Antwort auf Anforderung zum Abrufen der Zugriffsrichtlinie konnte nicht erhalten werden	Antwort auf Anforderung zum Abrufen der Zugriffsrichtlinie konnte nicht erhalten werden
	OS-Nummer	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		Das Connector-Gerät ist nicht registriert	Das Connector-Gerät ist nicht registriert
	OS-Nummer	Verbindung zum Connector-Gerät kann nicht hergestellt werden	Verbindung zum Connector-Gerät kann nicht hergestellt werden
0x10000301		Verbindung zum Citrix SPA-Dienst ist fehlgeschlagen	Verbindung zum Citrix Secure Workspace Access-Dienst ist fehlgeschlagen
0x10000303, 0x10000304		Der Proxyserver ist nicht erreichbar	Proxyserver ist nicht erreichbar
0x10000305		Die Proxyserver-Authentifizierung ist fehlgeschlagen.	Die Proxyserver-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

Infocode	Beschreibung	Auflösung
Nummer	Anforderung kann nicht an die Ziel-URL gesendet werden	Anforderung kann nicht an die Ziel-URL gesendet werden
Nummer der OS-Nummer	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 fehlgeschlagen, falsche Konfiguration der Formular-App	FormFill SSO fehlgeschlagen, falsche Konfiguration der Formular-App
Version	FormFill SSO fehlgeschlagen, falsche Konfiguration der Formular-App	FormFill SSO fehlgeschlagen, falsche Konfiguration der Formular-App
0x10000202	Kerberos-SSO ist fehlgeschlagen	Kerberos-SSO ist fehlgeschlagen
0x10000203	SSO für Authentifizierungstyp konnte nicht verarbeitet werden	SSO für Authentifizierungstyp konnte nicht verarbeitet werden
0x10000204	Kerberos SSO ist fehlgeschlagen, aber auf NTLM zurückgegriffen	Kerberos SSO ist fehlgeschlagen, aber auf NTLM zurückgegriffen
0x14000001	Mehrere ZTNA-berechtigte Konten, die in der Citrix Workspace-Anwendung konfiguriert sind	Mehrere ZTNA-berechtigte Konten, die in der Citrix Workspace-Anwendung konfiguriert sind

Lösungsschritte

Die folgenden Abschnitte enthalten Lösungsschritte für die meisten Infocodes. Wenden Sie sich bei Codes, für die die Lösungsschritte nicht erfasst sind, an den Citrix Support.

Eine oder mehrere Apps werden nicht im Benutzer-Dashboard aufgeführt

Infocode: 0x180055, 0x1800DF, 0x1800E3

Aufgrund kontextbezogener Richtlinieneinstellungen werden Apps für manche Benutzer oder Geräte möglicherweise nicht angezeigt. Parameter wie Vertrauensfaktoren (Gerätehaltung oder Risikobewertung) können die Zugänglichkeit der Anwendungen beeinflussen.

1. Kopieren Sie die Transaktions-ID aus der Spalte „ Gründe “für den Fehlercode `0x18005C` in der CSV-Datei „Diagnoseprotokolle“.
2. Ändern Sie den Spaltenfilter `prod` in der CSV-Datei, um Ereignisse der Komponente mit dem Namen `SWA.PSE` oder `SWA.PSE.EVENTS`anzuzeigen. Dieser Filter zeigt nur Protokolle an, die sich auf die Richtlinienauswertung beziehen.
3. Suchen Sie in der Spalte „ Grund “nach der ausgewerteten Richtliniennutzlast. Diese Nutzlast zeigt die ausgewertete Richtlinie für den Kontext des Benutzers für alle Apps, die der Benutzer abonniert hat.
4. Wenn die Richtlinienauswertung ergibt, dass die App für den Benutzer verweigert wurde, kann das folgende Gründe haben:

    - Falsche Übereinstimmungsbedingungen in der Richtlinie –überprüfen Sie die App-Richtlinienkonfiguration in Citrix Cloud
    - Falsche Übereinstimmungsregeln in der Richtlinie –überprüfen Sie die App-Richtlinienkonfiguration 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 er kein Abonnement besitzt.

Stellen Sie sicher, dass der Benutzer ein Abonnement für die Anwendungen hat.

1. Zur Bewerbung gelangen Sie im Verwaltungsportal.
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 der Back-End-App

Infocode:0x18000F

Es gibt Fälle, in denen das Kundennetzwerk aufgrund ausgefallener Konnektoren an einem Ressourcenstandort instabil ist oder der Back-End-Server selbst möglicherweise nicht antwortet.

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 Back-End-Servers das Connector-Gerät nicht blockiert.
3. Überprüfen Sie, ob der Client eine Verbindung zum nächstgelegenen Cloud-POP herstellt.

   Beispielsweise `nslookup nssvc.dnsdiag.net` auf dem Client, der kanonische Name in der Antwort gibt den geospezifischen Server an, beispielsweise `aws-us-wgnssvc.net`.

Der App-Start ist fehlgeschlagen, da die Länge des App-FQDN überschritten wurde

Infocode: 0x180006, 0x1800B7

App-FQDNs dürfen nicht länger als 512 Zeichen sein. Überprüfen Sie den FQDN der Anwendung auf der App-Konfigurationsseite. Stellen Sie sicher, dass die Länge 512 Bytes nicht überschreitet.

1. Gehen Sie in der Verwaltungskonsole zur Registerkarte **Anwendungen** .
2. Suchen Sie nach der Anwendung, deren FQDN mehr als 512 Zeichen umfasst.
3. Bearbeiten Sie die Anwendung und korrigieren Sie die FQDN-Länge der App.

Länge der App-Details 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 berechtigt ist.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

Der App-Zugriff wird verweigert

Infocode: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

Dies hängt mit kontextbezogenen Richtlinien zusammen, 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 berechtigt ist.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

Nicht aufgezählte Anwendungen

Anwendungen können aufgrund von Richtlinienverweigerungen oder einer nicht aktivierten Secure Workspace Access-Integration in der aufgezählten Liste fehlen.

- Wenn für einige Apps der Zugriff aktiviert werden muss, aber keine Apps angezeigt werden, versuchen Sie, die Secure Private Access-Integration zu aktivieren.
  - Melden Sie sich bei Citrix Cloud an.
  - Wählen Sie **Arbeitsbereichskonfiguration** aus dem Hamburger-Menü und klicken Sie dann auf **Serviceintegrationen**.
  - Klicken Sie in Secure Private Access auf die Auslassungspunkte-Schaltfläche und dann auf **Aktivieren**.
- Wenn die Secure Private Access-Integration bereits aktiviert ist, deaktivieren Sie sie und aktivieren Sie sie erneut, um zu sehen, ob Sie über Apps verfügen.

Problem beim Verbinden mit dem Connectorgerät

Infocode: 0x1800EF

Das App-Routing schlägt fehl, weil TCP-Verbindungen mit lokalen Konnektoren nicht verfügbar sind.

Überprüfen von Ereignissen aus der Controllerkomponente

1. Schlagen Sie die `Transaktions-ID` für Fehlercode `0x1800EF` in der CSV-Datei der Diagnoseprotokolle.
2. Filtern Sie alle Ereignisse, die mit der Transaktions-ID in der CSV-Datei übereinstimmen.
3. Filtern Sie außerdem die Spalte `prod` in der CSV-Datei, die mit `SWA.GOCTRL`übereinstimmt.

   Wenn Sie Ereignisse mit der Meldung `connectType` sehen, `multiconnect::success`? Dann;

   - Dies zeigt an, dass die Anforderung zum Tunnelaufbau erfolgreich an den Controller weitergeleitet wurde.
   - Überprüfen Sie, ob der `Ressourcenstandort` in der Protokollnachricht korrekt ist. Wenn es falsch ist, korrigieren Sie den Ressourcenstandort im Abschnitt „App-Konfiguration“im Citrix-Verwaltungsportal.
   - Überprüfen Sie, ob die VDA-IP `und der Port` in der Protokollnachricht korrekt sind. Die VDA-IP und der VDA-Port geben die IP und den Port der Back-End-Anwendung an. Wenn es falsch ist, korrigieren Sie den FQDN oder die IP-Adresse der App im Abschnitt „App-Konfiguration“im Citrix-Verwaltungsportal.

- Fahren Sie mit der Überprüfung der Connector-Ereignisse fort, wenn Sie keine der zuvor erwähnten Probleme finden.

Wenn Sie Ereignisse mit der Meldung `connectType connect::failure` oder `multiconnect::success` sehen, dann;

- Überprüfen Sie, ob die empfohlene Lösung für diese Protokollnachricht lautet: `. Überprüfen Sie, ob der Connector noch mit demselben Pop verbunden ist:.` Dies deutet darauf hin, dass der Connector 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 Sie Ereignisse mit der Meldung `connectType IntraAll::failure` sehen, wenden Sie sich an den Citrix-Kundensupport.

Überprüfen von Ereignissen aus der Connector-Komponente

1. Schlagen Sie die `Transaktions-ID` für Fehlercode `0x1800EF` in der CSV-Datei der Diagnoseprotokolle.
2. Filtern Sie alle Ereignisse, die mit der Transaktions-ID in der CSV-Datei übereinstimmen.
3. Filtern Sie auch die Spalte `prod` in der CSV-Datei, die mit `SWA.ConnectorAppliance.WebApps` übereinstimmt.
4. Wenn Sie Ereignisse mit `Status` als `Fehler` sehen, dann;
   - Überprüfen Sie für jedes dieser Fehlerereignisse die Meldung `Grund` .
   - `UnableToRegister` zeigt an, dass sich der Connector nicht erfolgreich bei Citrix Cloud registrieren konnte. Wenden Sie sich an den Citrix-Support.
   - `IsProxyRequiredCheckError` oder `ProxyDialFailed` oder `ProxyConnectionFailed` oder `ProxyAuthenticationFailure` oder `ProxiesUnReachable` zeigt an, dass der Connector die Back-End-URL nicht über die Proxy-Konfiguration auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Richtigkeit.
   - Weitere Informationen zum Debuggen finden Sie unter Connector-SSO-Ereignisse.

Single Sign-On-Fehler

Für die einmalige Anmeldung werden verschiedene SSO-Attribute aus der App-Konfiguration extrahiert und beim App-Start angewendet. Wenn der jeweilige Benutzer die Attribute nicht besitzt oder die Attribute falsch sind, kann die einmalige Anmeldung fehlschlagen. Stellen Sie sicher, dass die Konfiguration korrekt aussieht.

1. Gehen Sie zu **Zugriffsrichtlinien.**
2. Suchen Sie nach den Richtlinien, für die die App berechtigt ist.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

SSO-Methoden wie Form SSO, Kerberos und NTLM werden vom lokalen Connector ausgeführt. Überprüfen Sie die folgenden Diagnoseprotokolle vom Connector.

Überprüfen Sie SSO-Ereignisse aus der Connector-Komponente

1. Filtern Sie den `Komponentennamen` in der CSV-Datei, der mit `SWA.ConnectorAppliance.WebApps` übereinstimmt.
2. Werden Ihnen Ereignisse mit dem Status „Fehler“angezeigt?
    - Überprüfen Sie die Meldung für jedes dieser Fehlerereignisse.
    - `IsProxyRequiredCheckError` oder `ProxyDialFailed` oder `ProxyConnectionFailed` oder `ProxyAuthenticationFailure` oder `ProxiesUnReachable` zeigt an, dass der Connector die Back-End-URL nicht über die Proxy-Konfiguration auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Richtigkeit.
    - `FailedToReadRequest` oder `RequestReceivedForNonSecureBrowse` oder `UnableToRetrieveUserCredentials` oder `CCSPolicyIsNotLoaded` oder `FailedToLoadBaseClient` oder `ProcessConnectionFailure` oder `WebAppUnSupportedAuthType` zeigt einen Tunnelfehler an. Wenden Sie sich an den Citrix-Support.
    - `UnableToConnectTargetServer` zeigt an, dass der Back-End-Server vom Connector aus nicht erreichbar ist. Überprüfen Sie die Backend-Konfiguration noch einmal.
    - `IncorrectFormAppConfiguration` oder `NoLoginFormFound` oder `FailedToConstructF` oder `FailedToLoginViaFormBasedAuth` zeigt einen Fehler bei der formularbasierten Authentifizierung an. Überprüfen Sie den Abschnitt „SSO-Konfiguration“in der App-Konfiguration im Citrix-Verwaltungsportal.
    - `NTLMAuthNotFound` zeigt einen NTLM-basierten Authentifizierungsfehler an. Überprüfen Sie den Abschnitt NTLM-SSO-Konfiguration in der App-Konfiguration im Citrix-Verwaltungsportal.
    - Weitere Informationen zum Debuggen finden Sie unter Connector-Ereignisse.

Der App-Start ist fehlgeschlagen, da der Authentifizierungsdienst ausgefallen ist

Infocode: 0x180022

Mit Secure Private Access können Administratoren einen Authentifizierungsdienst eines Drittanbieters konfigurieren, beispielsweise das herkömmliche Active Directory, AAD, Okta oder SAML. Ausfälle dieser Authentifizierungsdienste können dieses Problem verursachen.

Überprüfen Sie, ob die Server von Drittanbietern aktiv und erreichbar sind.

SAML SSO-Fehler

Infocode: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Wenn die App von einem IdP initiiert wird, tritt beim Starten eine Authentifizierungsstörung auf, und wenn die App von einem SP initiiert wird, werden den Benutzern möglicherweise unzugängliche Links angezeigt. Überprüfen Sie die SAML-App-Konfiguration auf der Seite des Secure Private Access-Dienstes und auch 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.

    - Assertions-URL
    - Relaiszustand
    - Zielgruppe
    - Namens-ID-Format, Namens-ID und andere Attribute

Dienstanbieterkonfiguration:

1. Melden Sie sich beim Dienstanbieter an.
2. Gehen Sie zu **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.

Ungültiger App-FQDN

Infocode: 0x180048

Der Kundenadministrator hat möglicherweise einen ungültigen FQDN oder einen FQDN angegeben, bei dem die DNS-Auflösung auf dem Back-End-Server fehlschlägt.

In diesem Fall sieht der Endbenutzer einen Fehler auf der Webseite. Überprüfen Sie die Anwendungseinstellungen.

SaaS-App-Validierung Prüfen Sie, ob vom Netzwerk aus auf die App zugegriffen werden kann.

Validierung von Web-Apps

1. Gehen Sie zur Registerkarte **Anwendungen** .
2. Bearbeiten Sie die problematische Anwendung.
3. Gehen Sie zur Seite **App-Details** .
4. Überprüfen Sie die URL. Die URL muss entweder im Intranet oder im Internet zugänglich sein.

Secure Browser Service –DNS-Suche/Verbindung fehlgeschlagen

Infocode: 0x18009D

Beschädigtes Surferlebnis durch den Remote Browser Isolation-Dienst. Überprüfen Sie den Back-End-Server, mit dem der Endbenutzer eine Verbindung herzustellen versucht.

1. Gehen Sie zum Back-End-Server und prüfen Sie, ob er aktiv ist und die Anfragen empfangen kann.
2. Überprüfen Sie die Proxy-Einstellungen, wenn diese die Verbindung zum Back-End-Server unterbrechen.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser-Dienst bekannt.

CWA Web - DNS-Lookup-/Verbindungsfehler für Web-Apps

Infocode: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Beschädigtes Browsing-Erlebnis bei Webanwendungen, die in einem Unternehmensnetzwerk ausgeführt werden.

1. Filtern Sie die Diagnoseprotokolle nach den FQDNs, die nicht auflösbar sind.
2. Überprüfen Sie die Erreichbarkeit des Back-End-Servers innerhalb des Unternehmensnetzwerks.
3. Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector daran gehindert wird, den Back-End-Server zu erreichen.

Direkter Zugriff –Falsch konfiguriert als Web-App

Da der Datenverkehr von Web-Apps immer über den Connector geleitet wird, führt die Konfiguration des direkten Zugriffs darauf zu einem App-Zugriffsfehler.

Suchen Sie nach Konflikten zwischen der Routingdomänentabelle und der App-Konfiguration.

1. Zur Bewerbung gelangen Sie im Verwaltungsportal.

2. Bearbeiten Sie die App und prüfen Sie, ob der Direktzugriff aktiviert ist.
3. Überprüfen Sie den App-FQDN in der Routing-Domänentabelle, 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. Zur Bewerbung gelangen Sie im Verwaltungsportal.
2. Bearbeiten Sie die App und überprüfen Sie die agentenlose Zugriffskonfiguration.

Erweiterte Sicherheitsrichtlinien –Fehlkonfiguration des Secure Browser Service

Infocode: 0x1800C3

Es wird ein falsches Verhalten festgestellt, das nicht mit den Richtlinienbestimmungen übereinstimmt. 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.

Erweiterte Sicherheitsrichtlinien –falsche Richtlinienkonfiguration

Es wird ein falsches Verhalten festgestellt, das nicht mit den Richtlinienbestimmungen übereinstimmt. Überprüfen Sie die erweiterten Sicherheitseinstellungen.

1. Hier geht's zur Bewerbung.
2. Klicken Sie auf die Registerkarte **Zugriffsrichtlinien** .
3. Überprüfen Sie die Einstellungen im Abschnitt **Verfügbare Sicherheitsbeschränkungen:** .

Der Start der Citrix Secure Access-Agent-Sitzung ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen

Infocode: 0x1800D0

Die Citrix Secure Access-App kann keinen vollständigen Tunnel zur Citrix Cloud herstellen.

1. Überprüfen Sie die Routingdomänenkonfiguration für die TCP/UDP-Apps.

2. Stellen Sie sicher, dass die maximale Anzahl der Einträge deutlich innerhalb der 16.000-Grenze liegt.

TCP/UDP-Apps –Fehlerhafte Clientanforderungen

Infocode: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

Entweder kann der VPN-Tunnel nicht hergestellt werden oder bestimmte FQDNs können nicht getunnelt werden.

1. Stellen Sie sicher, dass die Anfragen nicht durch Proxys in der Mitte gefälscht oder rekonstruiert werden.
2. Verdacht auf Man-In-Middle-Angriffe.

TCP/UDP-Apps –Fehlkonfiguration der Weiterleitung des Secure Browser Service

Infocode: 0x1800DD

Umleitungen des Remote Browser Isolation-Dienstes können nur auf Web-Apps und nicht auf TCP/UDP-Apps angewendet werden. Überprüfen Sie die App-Konfiguration in der GUI des Secure Private Access-Dienstes.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser-Dienst bekannt.

Der Start der Citrix Secure Access-Agent-App ist während der Richtlinienauswertung 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 Routingdomäneneinträge. 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 Routingdomäneneinträge. Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Back-End verweisen.

Problem mit der Netzwerkkonnektivität beim Citrix Secure Access-Client

Infocode: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Überprüfen Sie, ob das Netzwerk des Clientcomputers erreichbar ist. Wenn das Netzwerk erreichbar ist, wenden Sie sich mit den Client-Debugprotokollen an den Citrix Support.
2. Überprüfen Sie, ob der Proxy oder die Firewall das Netzwerk blockiert.

Informationen zum Sammeln von Client-Debugprotokollen finden Sie unter So sammeln Sie Clientprotokolle.

Proxyserver stört Client-Konnektivität mit Dienst

Infocode: 0x10000006

1. Überprüfen Sie, ob das Netzwerk des Clientcomputers erreichbar ist.
2. Überprüfen Sie, ob der Proxy im Client richtig konfiguriert ist.
3. Wenn bei beiden keine Probleme vorliegen, wenden Sie sich mit den Client-Debugprotokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debugprotokollen finden Sie unter So sammeln Sie Clientprotokolle.

Es wurde ein Problem mit einem nicht vertrauenswürdigen Serverzertifikat beobachtet

Infocode: 0x10000007

Wenden Sie sich an den Citrix Support, um zu überprüfen, ob das Serverzertifikat korrekt von einer gültigen Zertifizierungsstelle generiert wurde.

Es wurde ein Problem mit einem ungültigen Serverzertifikat festgestellt

Infocode: 0x10000008

Wenden Sie sich an den Citrix Support, um zu überprüfen, ob das Serverzertifikat selbstsigniert ist, abgelaufen ist oder aus 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 (**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**) nicht leer ist oder dass nicht alle Einträge deaktiviert sind. Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden dieser Tabelle automatisch hinzugefügt.

Es wird empfohlen, die Ziele oder URL einer aktiven TCP/UDP/HTTP-Anwendung nicht zu löschen oder zu deaktivieren.

Verbindung vom Netzwerk und/oder Endbenutzer beendet

Infocode: 0x1000000B

Überprüfen Sie, ob das Netzwerk unterbrochen ist oder ob der Endbenutzer die Verbindung während der ZTNA-Sitzungsverbindung abgebrochen hat.

Der Download der Konfiguration ist fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode: 0x10000010

Die VPN-Sitzung ist möglicherweise während der Anforderung zum Herunterladen der ZTNA-Sitzungskonfiguration abgelaufen. Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Citrix Secure Access-Client konnte sich nicht anmelden

Infocode: 0x10000013

Die Anmeldung des Citrix Secure Access-Clients ist fehlgeschlagen, da die Konfigurationsgröße das maximale Konfigurationslimit überschreitet.

1. Überprüfen Sie die Routingdomänenkonfiguration für die TCP/UDP-Apps in **Secure Private Access > Einstellungen > Anwendungsdomäne**
2. Stellen Sie sicher, dass die Anzahl der Einträge nicht zu groß ist. Wenn die Eintragsliste sehr groß ist, deaktivieren oder entfernen Sie nicht verwendete Ziele.

Wenn die Zielliste voraussichtlich mehr als 1.000 Elemente enthält, versuchen Sie, die maximale Downloadgröße der Konfiguration zu erhöhen, indem Sie den Registrierungsschlüssel „ConfigSize“aktualisieren. Einzelheiten finden Sie unter Registrierungsschlüssel des Citrix Gateway VPN-Clients.

Der Aufbau des Kontrollkanals ist fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode: 0x11000003

Der Steuerkanal für die Einrichtung der DNS-Anforderung 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.

Die Einrichtung des Kontrollkanals ist fehlgeschlagen

Infocode: 0x11000004

Der Steuerkanal für die Einrichtung der DNS-Anforderung 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 einen Integritätscheck für die Connector-Appliances am jeweiligen Ressourcenstandort durch.
4. Wenn das Problem dadurch nicht behoben wird, versuchen Sie, die Connector-virtuelle Maschine neu zu starten.

- **Warten des HA-Connector-Geräts:**

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.

Folgendes sicher:

- Das Ressourcenstandort-LAN ist betriebsbereit.
- Es ist keine Firewall oder kein Proxy dazwischengeschaltet, die bzw. der den Zugriff des Connector Appliance auf den Dienst oder die Back-End-Server blockiert.
- Das Client-Netzwerk ist gesund.

- Die privaten Back-End-Server sind betriebsbereit.
- Die DNS-Server sind aktiv.
- FQDNs sind auflösbar.

Wenn die vorstehenden Empfehlungen auf Sie zutreffen, gehen Sie wie folgt vor.

1. Rufen Sie für diesen Fehler die Transaktions-ID aus dem Diagnoseprotokoll ab.
2. Filtern Sie alle Ereignisse, die mit der Transaktions-ID im Secure Private Access-Dashboard übereinstimmen.
3. Überprüfen Sie, ob in den Diagnoseprotokollen des Clients, des Connectorgeräts oder des Dienstes ein Fehler aufgetreten ist, der mit der Transaktions-ID übereinstimmt. Ergreifen Sie dann entsprechend die entsprechenden Maßnahmen.
4. Überprüfen Sie, ob der Ressourcenstandort für das Ziel in der Anwendungsdomänentabelle (**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**) richtig ausgewählt ist.
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 beheben können, wenden Sie sich mit dem entsprechenden Fehlercode zur Transaktions-ID und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debugprotokollen finden Sie unter So sammeln Sie Clientprotokolle.

Die Einrichtung des Kontrollkanals ist fehlgeschlagen

Infocode: 0x11000005

Die Einrichtung des Steuerkanals (für DNS-Anforderung) ist fehlgeschlagen.

1. Überprüfen Sie die Lizenzberechtigung für den Secure Private Access-Dienst.
2. Wenn Sie keinen Anspruch haben, wenden Sie sich zur Überprüfung der Lizenz an den Citrix Support.

Weitere Informationen finden Sie unter https://www.citrix.com/buy/licensing/product.html.

Die Einrichtung des Kontrollkanals ist aufgrund eines Netzwerkproblems fehlgeschlagen

Infocode: 0x11000006

Die Einrichtung des Steuerkanals (für DNS-Anfragen) ist aufgrund eines Netzwerkproblems fehlgeschlagen.

1. Überprüfen Sie, ob der Secure Private Access-Dienst erreichbar ist.
2. Wenn Sie nicht erreichbar sind, wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix-Support.

Informationen zum Sammeln von Client-Debugprotokollen finden Sie unter So sammeln Sie Client-protokolle.

Die Einrichtung des Kontrollkanals ist aufgrund unzureichender IIPs fehlgeschlagen

Infocode: 0x11000007

Die Einrichtung des Steuerkanals (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-Debugprotokollen finden Sie unter So sammeln Sie Client-protokolle.

Abmeldung nicht möglich, da Sitzung beendet wurde

Dieses Problem kann aufgetreten sein, weil der Clientcomputer (Tastatur oder Maus) länger als die konfigurierte Zeitüberschreitung im Leerlauf war.

Infocode: 0x12000001

Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Die Sitzung wird zwangsweise beendet

Die Sitzung wird zwangsweise beendet, wenn das konfigurierte Timeout erreicht ist.

Infocode: 0x12000002

Versuchen Sie, sich erneut beim Citrix Secure Access-Client anzumelden.

Der Anwendungsstart ist fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode: 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

Infocode: 0x13000002

1. Überprüfen Sie, ob eine Berechtigung für die Secure Private Access-Dienstlizenz besteht.
2. Wenn Sie keinen Anspruch haben, wenden Sie sich zur Überprüfung der Lizenz an den Citrix Support.

Weitere Informationen finden Sie unter https://www.citrix.com/buy/licensing/product.html.

Der Start der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde

Infocode: 0x13000003, 0x13000008, 0x001800DF

Der Anwendungsstart wird gemäß der Richtlinienkonfiguration für den Benutzer und die Anwendung verweigert.

Folgendes sicher.

- Dieselben Ziele werden nicht in mehreren Anwendungen verwendet (HTTP, HTTPS, TCP, UDP)
- Es gibt keine überlappenden Ziele bei mehreren Anwendungen.
- Zugriffsrichtlinien sind an die Anwendungen gebunden.

Überprüfen Sie auch die Bedingungen und Aktionen der für die abgelehnte Anwendung konfigurierten Richtlinien. Überprüfen Sie dann die Richtlinienbedingungen und -maßnahmen.

Einzelheiten finden Sie unter Zugriffsrichtlinien.

Der Anwendungsstart ist fehlgeschlagen, da der Client den Dienst nicht erreichen kann

Infocode: 0x13000004, 0x13000005

1. Überprüfen 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-Debugprotokollen finden Sie unter So sammeln Sie Client-protokolle.

Der Anwendungsstart ist fehlgeschlagen, da die Richtlinienauswertung und die Konfigurationsüberprüfung fehlgeschlagen sind

Infocode: 0x13000007

Der Anwendungsstart ist fehlgeschlagen, da die Richtlinienauswertung und Konfigurationsvalidierung durch den Secure Private Access-Dienst fehlgeschlagen ist.

Für das aufgerufene Zielkonnte keine Anwendung gefunden werden.

Der Start der Anwendung ist fehlgeschlagen, da der Zugriff vom Dienstverweigert wurde.

Der Anwendungsstart ist aufgrund von Problemen in der Anwendungsdomänentabelle fehlgeschlagen

Infocode: 0x13000009

Der Anwendungsstart ist fehlgeschlagen, da in der Anwendungsdomänentabelle kein Eintrag für das aufgerufene Ziel vorhanden ist.

Überprüfen Sie, ob der Routeneintrag für die Anwendung in **Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**richtig konfiguriert ist.

Der Client hat die Verbindung mit dem Secure Private Access-Dienst geschlossen

Infocode: 0x1300000B

1. Überprüfen 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-Debugprotokollen finden Sie unter So sammeln Sie Clientprotokolle.

FQDN kann vom DNS-Server nicht aufgelöst werden

Infocode: 0x1300000C

Dieses Problem tritt auf, wenn das Connectorgerät DNS für FQDNs nicht auflösen kann.

1. Prüfen Sie den DNS-Eintrag für den jeweiligen App-FQDN im DNS-Server.
2. Stellen Sie sicher, dass in den Connector Appliances ein geeigneter DNS-Server konfiguriert ist. Weitere Einzelheiten finden Sie unter Konfigurieren der Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite.

Die Anwendung konnte nicht gefunden werden

Infocode: 0x001800DE

Möglicherweise können Sie die Anwendung für das aufgerufene Ziel für den Benutzer nicht finden. Dies kann auftreten, wenn die Zuordnung des Ziels zum Ressourcenstandort in der Anwendungsdomänentabelle fehlt.

- Stellen Sie sicher, dass die TCP/UDP- oder HTTP-Anwendung für das aufgerufene Ziel konfiguriert ist.
- Stellen Sie sicher, dass der Benutzer über ein Abonnement der Anwendung für das aufgerufene Ziel verfügt.

1. Zur Bewerbung gelangen Sie im Verwaltungsportal.
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 **Anwendungsdomäne** das Ziel und den entsprechenden Ressourcenspeicherort hat.

Die Liste der konfigurierten Anwendungsziele konnte nicht abgerufen werden

Infocode: 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 „Anwendungsdomäne“(**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**) nicht leer ist oder dass nicht alle Einträge deaktiviert sind. Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden dieser Tabelle automatisch hinzugefügt. Es wird empfohlen, die Ziele oder URLs der aktiven TCP/UDP/HTTP-Anwendung in der Anwendungsdomänentabelle nicht zu löschen oder zu deaktivieren.

Problem mit der Anwendungskonfiguration

Die Anwendungskonfiguration enthält ein Sonderzeichen oder ein Problem mit der Richtlinienkonfiguration.

Infocode: 0x001800D9, 0x001800DA

Folgendes sicher:

- Die App-Konfiguration enthält keine nicht unterstützten Zeichen.
- Die Ziel-IP-Adresse oder der IP-Adressbereich oder die IP-CIDR sind gültig.
- Das Anwendungsziel ist in der Anwendungsdomänentabelle aktiviert (**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**).
- Die Richtlinien werden konfiguriert und an die jeweilige Anwendung gebunden.
- Die Konfiguration der Zugriffsrichtlinie ist korrekt.

Problem mit dem Ressourcenstandort

Infocode: 0x001800DB

- Stellen Sie sicher, dass ein Ressourcenstandort konfiguriert ist.
  1. Wählen Sie im Citrix Cloud-Hamburgermenü **Ressourcenstandort**aus.
  2. Stellen Sie sicher, dass der erwartete Ressourcenstandort konfiguriert ist und sich im Status „Aktiv“befindet.
- Stellen Sie sicher, dass in der Anwendungsdomänentabelle ein korrekter Ressourcenstandort für das Ziel ausgewählt ist (**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**).

Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden dieser Tabelle automatisch 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 HTTP-Anwendungen, die an eine erweiterte Sicherheitsrichtlinie gebunden sind, wird über den Citrix Secure Access-Client zugegriffen.

- Stellen Sie sicher, dass nicht dasselbe Ziel sowohl für TCP/UDP- als auch für 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-Dienst 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-Verwaltungsportal.
  - Klicken Sie auf die Registerkarte **Anwendungen** und suchen Sie nach dem Richtliniennamen für die aufgerufene HTTP/HTTPS-Zielanwendung.
  - Klicken Sie auf die Registerkarte **Zugriffsrichtlinien** und suchen Sie nach dem zuvor ermittelten Richtliniennamen.
  - Wählen Sie die Richtlinie aus und klicken Sie auf **Bearbeiten**.
  - Ändern Sie die Aktion von **Zugriff erlauben mit Einschränkung** in **Zugriff erlauben.**

Einzelheiten zur Konfiguration finden Sie unter Anwendungen hinzufügen und verwalten.

> **Hinweis:**
>
> Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser-Dienst bekannt.

Die Länge des Hostnamens überschreitet 256 Zeichen

Infocode: 0x001800EA

Der in der Anwendungsstartanforderung empfangene Hostname überschreitet 256 Zeichen.

Es wird empfohlen, dass die FDQN-Zeichenlänge 256 nicht überschreitet.

Ungültige IP-Adresse

Infocode: 0x001800ED

Die in der Anwendungsstartanforderung empfangene IP-Adresse ist ungültig.

Es wird empfohlen, von den Clients aus nur auf eine gültige private IP-Adresse zuzugreifen.

Es kann keine Ende-zu-Ende-Verbindung hergestellt werden

Infocode: 0x001800EF

Es kann keine End-to-End-Verbindung zwischen dem Client und dem im Ressourcenstandort konfigurierten Server hergestellt werden.

- Stellen Sie sicher, dass der Ressourcenstandort den Status „Aktiv“hat.
  - Wählen Sie im Citrix Cloud-Hamburgermenü **Ressourcenstandort**aus.
  - Führen Sie eine Integritätsprüfung für die Connector Appliances am jeweiligen Ressourcenstandort durch.
  - Wenn das Problem dadurch nicht behoben wird, starten Sie die Connector-virtuelle Maschine neu.
- Verwalten eines Connectorgeräts mit hoher Verfügbarkeit
  - Wählen Sie im Citrix Cloud-Hamburgermenü **Ressourcenstandort**aus.
  - Stellen Sie sicher, dass der Ressourcenstandort über mindestens zwei Connector Appliances verfügt.
- Folgendes sicher:
  - Das LAN des Ressourcenstandorts ist betriebsbereit.

- Keine Firewalls oder Proxys in der Mitte, die den Anschluss des Connector Appliance an den Dienst oder die Back-End-Server blockieren.
- Das Client-Netzwerk ist intakt.
- Private Back-End-Server sind fehlerfrei.
- Die DNS-Server sind fehlerfrei.
- FQDNs sind auflösbar.

Wenn damit keine Probleme bestehen, gehen Sie wie folgt vor:

1. Rufen Sie die Transaktions-ID für diesen Fehler aus den Diagnoseprotokollen ab.
2. Filtern Sie alle Ereignisse, die mit der Transaktions-ID im Dashboard des Secure Private Access-Dienstes übereinstimmen.
3. Überprüfen Sie die Diagnoseprotokolle entsprechend der Transaktions-ID vom Dashboard des Secure Private Access-Dienstes und ergreifen Sie dann entsprechend die entsprechenden Maßnahmen.
4. Überprüfen Sie, ob in der Anwendungsdomänentabelle ein korrekter Ressourcenstandort als Ziel ausgewählt ist (**Sicherer privater Zugriff > Einstellungen > Anwendungsdomäne**).
5. Überprüfen Sie, ob die Anwendung (**Secure Private Access > Applications**) mit der richtigen IP-Adresse, dem richtigen Port und dem richtigen FQDN konfiguriert ist.

Wenn keiner dieser Schritte das Problem behebt, wenden Sie sich mit dem der Transaktions-ID entsprechenden Fehlercode an den Citrix Support und sammeln Sie Client-Protokolle.

Informationen zum Sammeln von Client-Debugprotokollen finden Sie unter So sammeln Sie Client-protokolle.

In der App-Anforderung empfangenes IPv6

Infocode: 0x001800F5

In der App-Anforderung wird eine IPv6-Datei 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-Verwaltungsportal.
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

Infocode: 0x001800F9

UDP-Verkehr konnte nicht übermittelt werden, da die Client-Verbindung verloren ging

1. Überprüfen Sie, ob die Client-Sitzung aktiv ist.
2. Melden Sie sich ab und erneut an.

Die Übermittlung des UDP-Datenverkehrs ist fehlgeschlagen

Infocode: 0x001800FF

- Suchen Sie die Transaktions-ID für den Fehlercode und filtern Sie alle Ereignisse, die mit der Transaktions-ID übereinstimmen, im Dashboard des Secure Private Access-Dienstes.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Wenn bei anderen Komponenten ein Problem festgestellt wird, ergreifen Sie die entsprechenden Maßnahmen.
- Wenn das Problem dadurch nicht behoben wird, wenden Sie sich mit dem Fehlercode und der entsprechenden Transaktions-ID an den Citrix Support.

Der Anwendungsstart ist aufgrund von Netzwerkverbindungsproblemen fehlgeschlagen

Infocode: 0x10000401

Fehler beim Starten der Anwendung aufgrund von Netzwerkkonnektivitätsproblemen zwischen Connector Appliance und Secure Workspace Access-Dienst

1. Überprüfen Sie die öffentliche Internetverbindung des Connectorgeräts.
2. Überprüfen Sie, ob Proxy- oder Firewall-Regeln die Verbindung blockieren.
3. Wenn ein Proxy das Problem verursacht, umgehen Sie den Proxy und versuchen Sie, die App erneut zu starten.
4. Überprüfen Sie den Integritätsstatus des Connector Appliance (**Citrix Cloud > Ressourcenstandort**).

Einzelheiten zu den Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Die Registrierung des Connectorgeräts beim Secure Private Access-Dienst ist fehlgeschlagen

Infocode: 0x10000402, 0x1000040C

1. Gehen Sie zur Administratorseite der Connector Appliances und überprüfen Sie die Connector-Zusammenfassung.
2. Wenn der Connector-Status nicht gut ist, gehen Sie zum Ressourcenstandort im Verwaltungsportal.

3. Führen Sie eine Integritätsprüfung für die Connector Appliances am jeweiligen Ressourcenstandort durch.
4. Wenn die Integritätsprüfung fehlschlägt, starten Sie die Connector-VM 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.

Konnektivitätsproblem mit dem Connectorgerät

Infocode: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Suchen Sie in der Transaktions-ID nach dem Fehlercode.
- Filtern Sie alle Ereignisse, die mit der Transaktions-ID im Secure Private Access-Dashboard übereinstimmen.
- Überprüfen Sie, ob in der anderen Komponente, die mit der Transaktions-ID übereinstimmt, ein Fehler aufgetreten ist. Führen Sie ggf. die entsprechende Problemumgehung durch, die zu diesem Fehlercode passt.
- Wenn bei anderen Komponenten kein Fehler gefunden wird, gehen Sie wie folgt vor:
  - Gehen Sie zur Administratorseite von Connector Appliances.
  - Laden Sie den Diagnosebericht herunter. Einzelheiten finden Sie unter Erstellen eines Diagnoseberichts.
  - Erfassen Sie die Paketverfolgung. Weitere 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.

Konnektivitätsprobleme mit Connector Appliance und privaten TCP/UDP-Back-End-Servern

Infocode: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Connector Appliance hat ein Verbindungsproblem mit den privaten TCP/UDP-Back-End-Servern.

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv ist und die Anforderungen empfangen kann.
- Überprüfen Sie die Erreichbarkeit der Back-End-Server innerhalb des Unternehmensnetzwerks.
- Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector daran gehindert wird, den Back-End-Server zu erreichen.

- Wenn die Anfrage eine FQDN-basierte App betrifft, prüfen Sie den DNS-Eintrag für die jeweilige App im DNS-Server.

Connector Appliance kann DNS für FQDNs nicht auflösen

Infocode: 0x10000406

- Prüfen Sie den DNS-Eintrag für den jeweiligen App-FQDN im DNS-Server.
- Stellen Sie sicher, dass in den Connector Appliances ein geeigneter DNS-Server konfiguriert ist. Weitere Einzelheiten finden Sie unter Konfigurieren der Netzwerkeinstellungen auf der Connector Appliance-Verwaltungsseite.

Private Serververbindung beendet

Infocode: 0x10000411

Die Verbindung zum privaten Server wird vom Client oder dem Secure Private Access-Dienst beendet.

1. Überprüfen Sie, ob der Endbenutzer die Anwendung geschlossen hat.
2. Überprüfen Sie andere Diagnoseprotokolle, die mit der Transaktions-ID dieses Protokolls übereinstimmen, und ergreifen Sie entsprechend 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.

Verbindung zum privaten Dienst-IP oder FQDN konnte nicht hergestellt werden oder Daten konnten nicht gesendet werden

Infocode: 0x10000413

- Private Serververbindung beendet
- [Konnektivitätsprobleme mit Connector Appliance und privaten TCP/UDP-Backend-Servern](/en-us/citrix-secure-private-access/service/secure-private-access-troubleshooting. html#Konnektivitätsprobler mit Connector-Appliance und privaten TCP/UDP-Backend-Servern). Überprüfen Sie die Routingdomäneneinträge. Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Back-End verweisen.

Keine übereinstimmende Richtlinienbedingung

Infocode: 0x100508

Der Benutzerkontext entspricht nicht den Zugriffsregelbedingungen, die in den der App zugewiesenen Richtlinien definiert sind.

Aktualisieren Sie die Richtlinienkonfiguration, damit sie dem Kontext des Benutzers entspricht.

Der Anwendung ist keine Zugriffsrichtlinie zugeordnet

Infocode: 0x100509

1. Klicken Sie in der GUI 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 Erstellen von Zugriffsrichtlinien.
4. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Für den FQDN oder die IP-Adresse wurde keine Anwendungskonfiguration gefunden

Infocode: 0x10050A

Für den eingehenden FQDN oder die IP-Adressanforderung wurde keine passende Anwendung gefunden. Daher wird die App als unveröffentlichte Anwendung klassifiziert. Wenn dies nicht erwartet wird, gehen Sie wie folgt vor.

1. Gehen Sie zum Administratorportal des Secure Private Access-Dienstes.
2. Klicken Sie in der linken Navigation 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 Domäne, IP-Adresse oder eine Platzhalterdomäne hinzufügen.

   Hinweis: Das Hinzufügen eines FQDN oder einer IP-Adresse in **Secure Private Access > Einstellungen > Anwendungsdomäne** löst dieses Problem nicht. Es muss als Teil der Anwendungskonfiguration hinzugefügt werden.

App-Enumerationsinformationen

Infocode: 0x10050C

Dieser Code erfasst die Ergebnisse der Richtlinienbewertung mehrerer Anwendungen, auf die der Benutzer möglicherweise Anspruch hat. Der App-Zugriff kann aus folgenden Gründen verweigert werden:

- Der Benutzerkontext entspricht nicht den Zugriffsregelbedingungen, die in den der App zugewiesenen Richtlinien definiert sind. Weitere Einzelheiten finden Sie unter Keine übereinstimmende Richtlinienbedingung.
- Der Anwendung ist keine Zugriffsrichtlinie zugeordnet. Einzelheiten finden Sie unter Der Anwendung ist keine Zugriffsrichtlinie zugeordnet..
- Eine mit der Anwendung verknüpfte Richtlinie ist so konfiguriert, dass der Zugriff verweigert wird. In diesem Fall ist keine Aktion erforderlich, da dies beabsichtigt ist.
- Unerwarteter interner Fehler beim Durchsetzen der Zugriffsrichtlinie. Weitere Informationen erhalten Sie vom Citrix-Support.

Der Start der TCP/UDP-App ist fehlgeschlagen, da in der Anwendungsdomänentabelle ein Routing-Eintrag 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 (**Sicherer privater Zugriff > 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 aktiv ist/auf die neue Verbindung reagiert.

Führen Sie eine Integritätsprüfung für die Connector Appliances am jeweiligen Ressourcenstandort durch.

UDP/DNS-Anforderung fehlgeschlagen, da 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, die App erneut zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Der Abruf der Zugriffsrichtlinie ist aufgrund eines Netzwerkfehlers fehlgeschlagen

Infocode: 0x20580002

1. Überprüfen Sie die URL und die Netzwerkverbindung.
2. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Beim Parsen des JSON-Web-Tokens ist der Abruf der Zugriffsrichtlinie fehlgeschlagen

Infocode:0x20580003

1. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Netzwerkfehler beim Abrufen der Zugriffsrichtliniendetails

Infocode:0x20580004

1. Überprüfen Sie, ob die Zugriffsrichtlinie aktiviert ist.
2. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Beim Abrufen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen

Infocode: 0x20580005

1. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Beim Überprüfen der Signatur des JSON-Web-Tokens ist der Richtlinienabruf fehlgeschlagen

Infocode: 0x20580007

1. Überprüfen Sie, ob die Netzwerkzeit und die Zeit des Benutzergeräts synchronisiert sind.
2. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
3. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Beim Überprüfen des öffentlichen Zertifikats ist der Richtlinienabruf fehlgeschlagen

Infocode: 0x20580008

1. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Die Bestimmung der Store-Umgebung zum Erstellen einer Richtlinien-URL ist fehlgeschlagen

Infocode: 0x2058000A

1. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
2. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Es konnte keine Antwort auf die Anforderung zum Abrufen der Zugriffsrichtlinie erhalten werden

Infocode: 0x2058000B

1. Starten Sie den Browser neu und versuchen Sie, die App erneut 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, die App erneut 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 Connector Appliance-Registrierung.

Einzelheiten finden Sie unter Registrieren Sie Ihr Connector Appliance bei Citrix Cloud.

Verbindung zum Connectorgerät kann nicht hergestellt werden

Infocode: 0x10200003

Das Connectorgerät 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.

Verbindung zum Citrix Secure Workspace Access-Dienst ist fehlgeschlagen

Infocode: 0x10000301

Überprüfen Sie die Netzwerkeinstellungen des Connectorgeräts. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Proxyserver ist nicht erreichbar

Infocode: 0x10000303, 0x10000304

Überprüfen Sie die Proxyservereinstellungen und stellen Sie sicher, dass diese für das Connectorgerät erreichbar sind. Einzelheiten finden Sie unter Registrieren Sie Ihr Connector Appliance bei Citrix Cloud.

Die Proxyserver-Authentifizierung ist fehlgeschlagen

Infocode: 0x10000305

Überprüfen Sie die Anmeldeinformationen des Proxyservers und stellen Sie sicher, dass sie im Connectorgerät richtig konfiguriert sind. Weitere 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 Connectorgeräts. Ausführliche Informationen 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, wenn es sich nicht um einen erwarteten Code handelt.

Anforderung kann nicht an die Ziel-URL gesendet werden

Infocode: 0x10000005

Überprüfen Sie die Ziel-URL oder die Netzwerkeinstellungen des Connectorgeräts. 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 Connectorgeräts und stellen Sie sicher, dass der NTP-Server konfiguriert ist und keine Zeitstreifenprobleme vorliegen. Einzelheiten finden Sie unter Netzwerkeinstellungen für Ihr Connector Appliance.

Verbindung zum Citrix Secure Workspace Access-Dienst ist fehlgeschlagen

Infocode: 0x10000108, 0x1000010B

Überprüfen Sie die Netzwerkeinstellungen des Connectorgeräts. 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 fehlgeschlagen, falsche Konfiguration der Formular-App

Infocode: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Überprüfen Sie die App-Konfiguration des SSO-Formulars und stellen Sie sicher, dass die Felder Benutzername, Kennwort, Aktion und Anmelde-URL in den App-Einstellungen richtig 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 Fallback-NTLM-Authentifizierungseinstellungen.

Informationen zu den Kerberos-SSO-Einstellungen finden Sie unter Validieren Ihrer Kerberos-Konfiguration.

SSO für Authentifizierungstyp konnte nicht verarbeitet werden

Infocode: 0x10000203

Überprüfen Sie die SSO-Einstellungen im Secure Private Access-Dienst und im Backend-Server. Informationen zum Secure Private Access-Dienst finden Sie unter . Legen Sie die bevorzugte Anmeldemethode fest:.

Kerberos SSO ist fehlgeschlagen, aber auf NTLM zurückgegriffen

Infocode: 0x10000204

Das Abrufen des Kerberos-Tickets vom Domänencontroller ist fehlgeschlagen. Als sekundäre Authentifizierung hat Connector Appliance die Fallback-NTLM-Authentifizierung versucht.

Um eine erfolgreiche Kerberos-Authentifizierung zu ermöglichen, überprüfen Sie die Kerberos-SSO-Einstellungen auf dem Backend-Server und dem Domänencontroller.

Weitere Einzelheiten finden Sie unter Validieren Ihrer Kerberos-Konfiguration.

Mehrere ZTNA-berechtigte Konten, die in der Citrix Workspace-Anwendung konfiguriert sind

Infocode: 0x14000001

Konfigurieren Sie in der Citrix Workspace-Anwendung nur ein ZTNA-berechtigtes Konto.

So erfassen Sie Clientprotokolle

- **Windows-Client:**
  1. Öffnen Sie die App und stellen Sie sicher, dass die Protokollierung aktiviert ist.
  2. Stellen Sie jetzt eine Verbindung zum Secure Private Access-Dienst her und reproduzieren Sie das aufgetretene Problem.
  3. Gehen Sie in der App zu **Protokollieren** und klicken Sie auf **Protokolldateien sammeln**. Dadurch wird die Protokolldatei generiert.
  4. Speichern Sie die Protokolldatei auf dem Desktop des Clientcomputers.
- **Mac-Client:**
  1. Öffnen Sie die App und gehen Sie zu **Logs > Ausführlich**.
  2. Löschen Sie die Protokolle und fahren Sie mit der Reproduktion des Problems fort.
  3. Gehen Sie zurück zu **Protokollen > Protokolle exportieren**. Dadurch wird eine ZIP-Datei erstellt, die Protokolldateien enthält.

Antworten auf häufig gestellte Fragen

Was sind Secure Private Access-Diagnoseprotokolle?

Die Diagnoseprotokolle von Secure Private Access erfassen alle Ereignisse, die auftreten, wenn ein Benutzer auf eine beliebige Anwendung (Web/SaaS/TCP/UDP) zugreift. Diese Protokolle erfassen Gerätestatus, App-Authentifizierung, App-Aufzählung und App-Zugriffsprotokolle. 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 +-Zeichen klicken, je nachdem, welche Informationen Sie im Dashboard sehen möchten. Sie können die Benutzerprotokolle im CSV-Format exportieren.

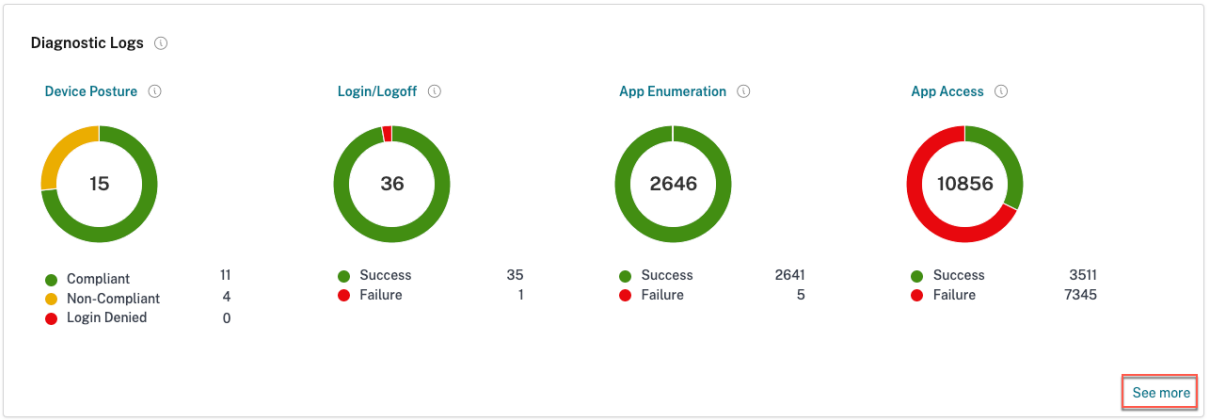
Wo finde ich Secure Private Access-Protokolle?

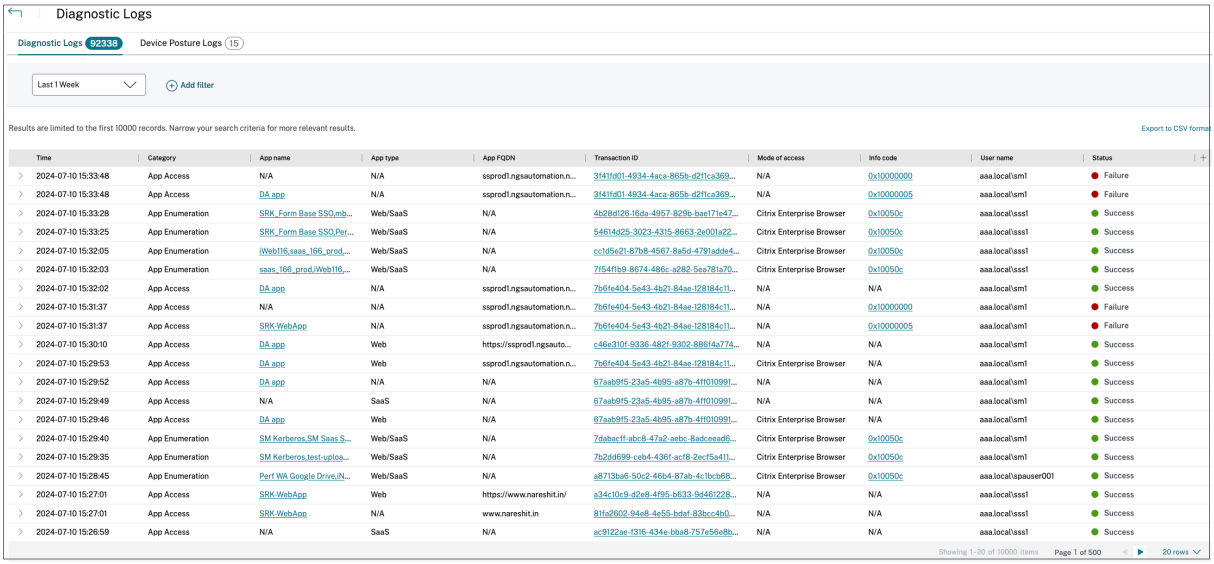
1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Dienstkachel „Secure Private Access“auf **Verwalten**.
3. Klicken Sie in der Administrator-Benutzeroberfläche in der linken Navigation auf **Dashboard** .
4. Klicken Sie im Diagramm „ **Diagnoseprotokolle** “auf den Link „ **Mehr anzeigen** “.

Welches Widget zeigt die Diagnoseprotokolle von Secure Private Access an?

Die Widgets **Diagnoseprotokolle** im Abschnitt **Protokollierung und Fehlerbehebung** zeigen eine Kreisdiagrammansicht aller Secure Private Access-Ereignisse im Zusammenhang mit Au-

thentifizierung, Anwendungsstart, App-Aufzählung sowie Protokolle im Zusammenhang mit der Gerätehaltung. Die Diagnoseprotokolle von Secure Private Access rufen Ereignisse von mehreren internen Komponenten ab, von denen jede ein Ereignis sendet, wenn ein Endbenutzer auf eine Anwendung zugreift. Diese Ereignisse sind in die Kategorien unterteilt: **Anmelden/Abmelden**, **App-Aufzählung**und **App-Zugriff**. Das Kreisdiagramm zeigt das allgemeine Erfolgs-/Misserfolgsverhältnis jeder Kategorie. Wenn Sie auf den farbigen Kreis in einem beliebigen Diagramm klicken, gelangen Sie zu den Diagnoseprotokollen, in denen Sie die entsprechenden Ereignisse finden. Wenn Sie den Gerätestatusdienst aktiviert haben, sind auch Gerätestatusprotokolle vorhanden. Sie können auch auf den Link **Mehr anzeigen** klicken, um die vollständigen Diagnoseprotokolle anzuzeigen.





Welche Details finde ich in den Diagnoseprotokollen von Secure Private Access?

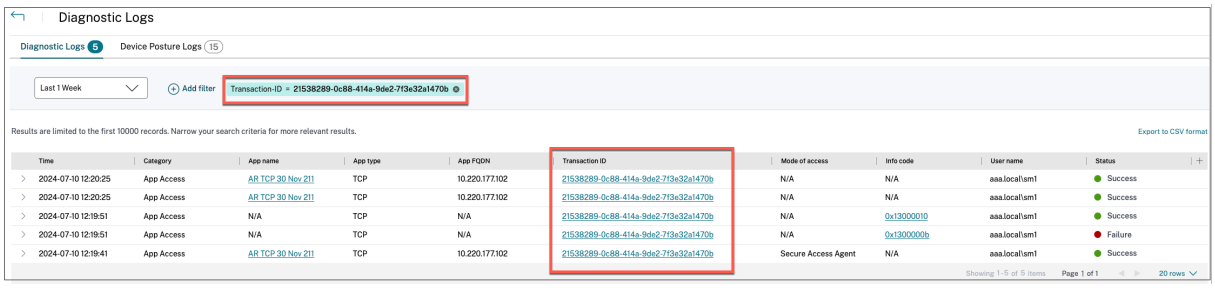
Das Dashboard „Secure Private Access-Benutzerprotokolle“bietet standardmäßig die folgenden Details.

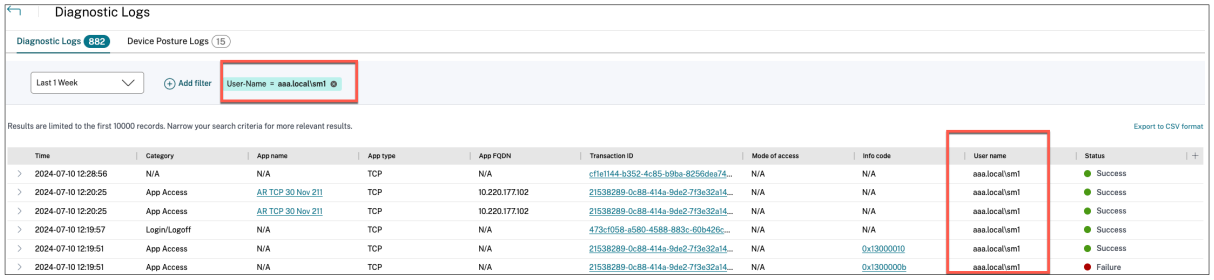
- **Zeitstempel** –Uhrzeit des Ereignisses in UTC.

- **Benutzername** –Benutzername des Endbenutzers, der auf die App zugreift.
- **App-Name** –Name der App/Apps, auf die zugegriffen wurde(n).
- **Richtlinieninfo** –Zeigt den Namen der Zugriffsrichtlinie(n) an, die während des Ereignisses ausgelöst wurden.
- **Status** –Zeigt den Status des Ereignisses an, Erfolg oder Fehler.
- **Infocode** –Jedes Fehlerereignis im Dashboard der Diagnoseprotokolle von Secure Private Access hat einen zugehörigen Infocode. Weitere Informationen finden Sie unter 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 mit der ausgeführten Operation verknüpft ist.
- **Vorgangstyp** –Zeigt den Vorgang an, für den das Protokoll generiert wird.
- **Kategorie** –Je nach Art der Veranstaltung stehen drei Kategorien zur Verfügung. Das ist App-Authentifizierung, App-Aufzählung oder App-Zugriff. Diese Optionen stehen Ihnen auch als Filteroptionen zur Verfügung. Mit diesen Optionen können Sie Protokolle je nach der Art des Problems filtern, mit dem Sie konfrontiert sind.
- **Transaktions-ID** –Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanforderung. Erfahren Sie, wie Sie eine Transaktions-IDverwenden. Die folgenden Details können durch Klicken auf die Schaltfläche + auf der rechten Seite des Dashboards abgerufen werden:
- **SPA-PoP-Standort** –Zeigt den Namen/die ID des PoP-Standorts des Secure Private Access-Dienstes an, der während des App-Zugriffs verwendet wurde. Siehe Sichere private Zugriffs-PoP-Standorte.

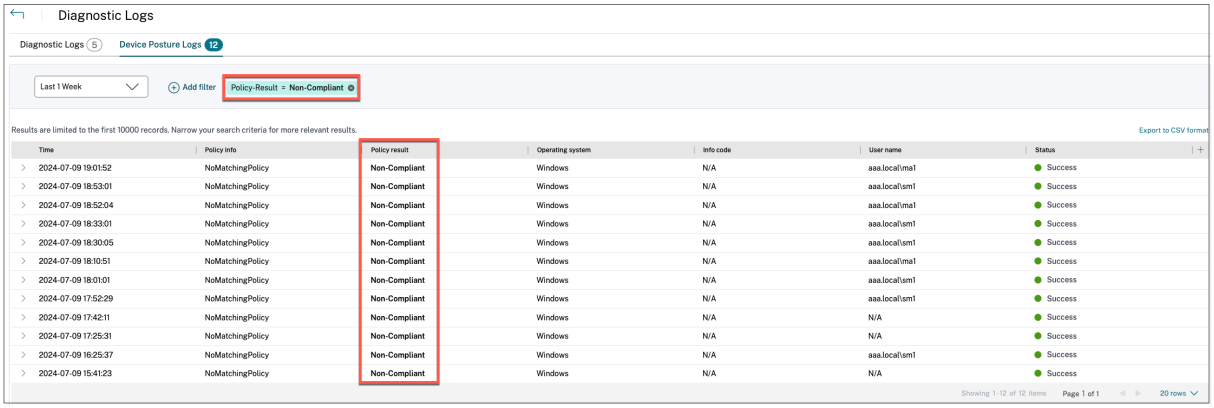
Wie filtere ich die Diagnoseprotokolle?

Mit der Option **Filter hinzufügen** können Sie Ihre Suche anhand verschiedener Kriterien wie App-Typ, Kategorie und Beschreibung verfeinern. Sie können beispielsweise im Suchfeld auf „Transaktions-ID =“(entspricht einem bestimmten Wert) klicken und „21538289-0c88-414a-9de2-7f3e32a1470b “eingeben, um nach allen Protokollen zu suchen, die mit dieser Transaktions-ID in Zusammenhang stehen. Einzelheiten zu den Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.





Sie können auch die verschiedenen Filteroptionen verwenden, um Ihre Suche in den Device Posture-Protokollen zu verfeinern.



Welche Ereignisse werden in den Diagnoseprotokollen von Secure Private Access erfasst?

Die Diagnoseprotokolle von Secure Private Access erfassen die folgenden Ereignisse:

- **Gerätestatus:** Gerätestatus des Endbenutzers. Diese Protokolle erfassen Informationen zu den Ergebnissen der Gerätehaltung. Ob das Gerät basierend auf Ihrer Gerätestatusrichtlinie als konform, nicht konform oder als Zugriffsverweigerung eingestuft wurde.
- **Anmelden/Abmelden**: Ereignisse zum Anmelde- oder Abmeldestatus des Endbenutzers beim Citrix Secure Access-Client und zur Authentifizierung beim Arbeitsbereich (interne oder externe Anbieter).
- **App-Aufzählung**: Im Secure Private Access-Dienst entscheiden von Administratoren konfigurierte Zugriffsrichtlinien, welcher Benutzer auf welche App zugreifen darf. Abgelehnte Anwendungen sind für Endbenutzer in der Citrix Workspace-App nicht sichtbar (nicht aufgezählt). Anhand dieser Ereignisse können Sie erkennen, welchen Anwendungen der Zugriff eines Benutzers basierend auf den im Secure Workspace Access-Dienst konfigurierten Zugriffsrichtlinien gestattet oder verweigert wurde.
- **App-Zugriff**: Ereignisse des Endbenutzeranwendungs-/Endpunktzugriffs, Zulassungs-/Verweigerungsstatus, Single-Sign-On-Status und Konnektivitätsstatus gemäß den konfigurierten Zugriffsrichtlinien für das ausgewählte Zeitintervall.

Wie verwende ich das Thema zur Fehlerbehebung bei Secure Private Access, um einen aufgetretenen Fehler zu beheben?

1. Holen Sie sich den Infocode für den Fehler, den Sie beheben möchten.
2. Suchen Sie den Infocode in der Fehlernachschlagetabelle.
3. Befolgen Sie die für diesen Infocode angegebenen Lösungsschritte.

Was ist ein Infocode? Wo finde ich sie?

Einige Protokollereignisse, z. B. Fehler, haben einen zugehörigen Infocode. Suchen Sie in der Fehlernachschlagetabelle nach diesem Infocode, um die Lösungsschritte oder weitere Informationen zu diesem Ereignis zu finden.

Was ist eine Transaktions-ID? Wie verwende ich es?

Bei Zugriffsfehlern/-problemen über den Citrix Enterprise Browser wird dem Endbenutzer eine Transaktions-ID angezeigt. Administratoren können diese Transaktions-ID von den Endbenutzern abrufen und diese Transaktions-ID verwenden, um die genauen Protokolle zu filtern, die das Problem verursacht haben, . So können sie das genaue Problem identifizieren. Sobald die Administratoren Ereignisse mit der Transaktions-ID filtern, werden nur die Ereignisse angezeigt, die sich auf das vorliegende Problem beziehen. Den Administratoren werden alle Einzelheiten darüber bereitgestellt, warum der Fehler oder das Problem aufgetreten ist. Administratoren können dann den Fehlercode in diesen Protokollen verwenden, um die Probleme weiter zu beheben.

Was sind alle Secure Private Access PoP-Standorte?

Nachfolgend finden Sie die Liste der Secure Private Access PoP-Standorte.

PoP-Name	Zone	Region
az-us-e	Azurblauer Osten	Virginia
az-us-w	Azure Westus	Kalifornien
az-us-sc	Azurblauer Südzentralus	Texas
az-aus-e	Azure AustralienOst	Neusüdwales
az-eu-n	Azurblaues Nordeuropa	Irland
az-eu-w	Azurblaues Westeuropa	Niederlande
az-jp-e	Azurblauer Japanost	Tokio, Saitama

PoP-Name	Zone	Region
az-bz-s	Azurblauer Brasiliensüd	Bundesstaat São Paulo
az-asia-se	Azurblaues Südostasien	Singapur
az-uae-n	Azurblauer UAEnorth	Dubai
az-in-s	Azurblaues Südindien	Chennai
az-asia-hk	Azurblaues Ostasien	Hongkong

Was kann ich tun, wenn ich meinen Fehler mithilfe des Infocodes und der Fehlernachschlagetabelle nicht beheben kann?

Wenden Sie sich an den Citrix-Support.

Referenzen

- **Hinzufügen einer Web-App**
  - Unterstützung für Enterprise-Web-Apps
  - Konfigurieren des direkten Zugriffs auf Web-Apps
- **Hinzufügen einer SaaS-App**
  - Unterstützung für Software-as-a-Service-App
  - SaaS-App-Server-spezifische Konfiguration
- **Konfigurieren von Client-Server-Apps**
  - Unterstützung für Client-Server-Apps
- **Erstellen von Zugriffsrichtlinien**
  - Erstellen von Zugriffsrichtlinien
- **Routentabellen**
  - Routentabellen

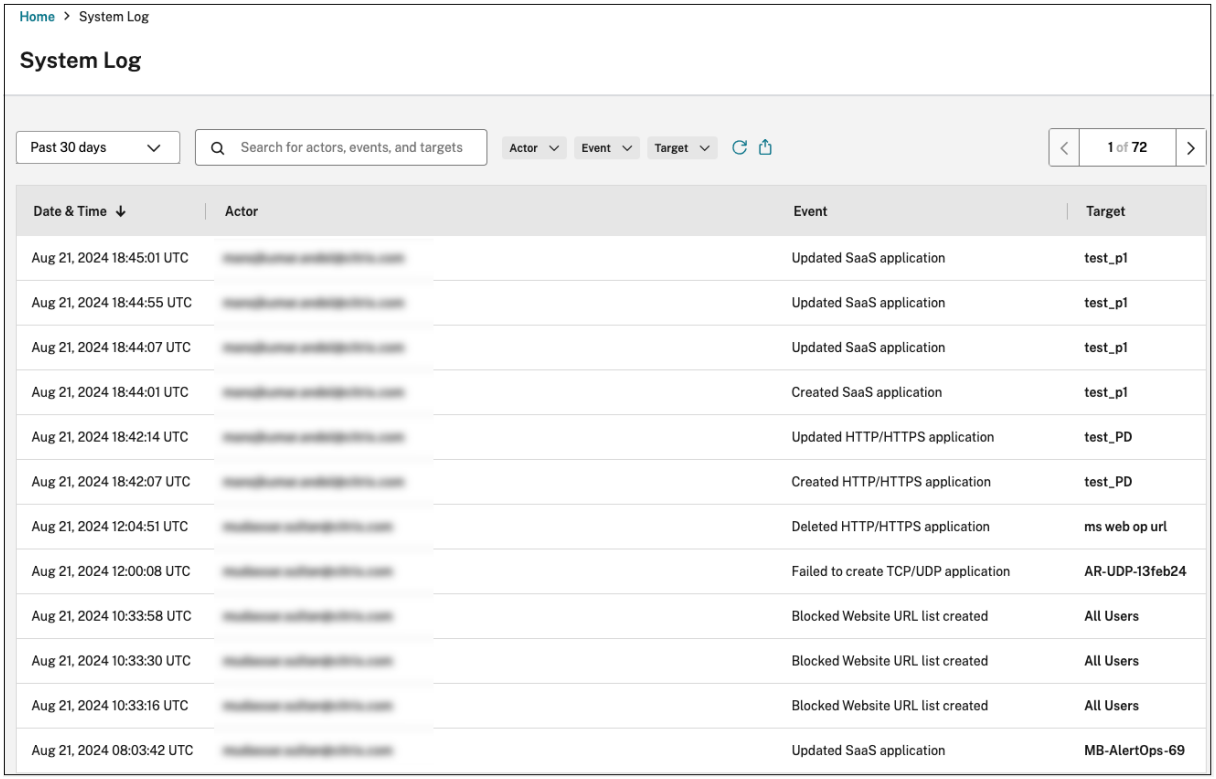
Auditprotokolle

October 21, 2024

Mit dem Secure Private Access-Dienst verbundene Ereignisse werden im **Citrix Cloud > Systemprotokoll**erfasst. Alle Ereignisse, die ein Administrator im Citrix Secure Workspace Access-Dienst ausführt, werden an Citrix Cloud gesendet und in den Systemprotokollen erfasst. Zu den Administratorereignissen können die folgenden gehören (sie sind jedoch nicht hierauf beschränkt):

- Erstellen oder Aktualisieren einer App
- Löschen einer App
- Konfigurieren oder Löschen einer adaptiven Zugriffsrichtlinie
- Connector-Upgrade
- Erstellung erlaubter oder blockierter Webseiten

Die folgende Abbildung zeigt die mit Secure Private Access verbundenen Ereignisse im **Systemprotokoll**.



Einzelheiten beispielsweise zum Exportieren von Ereignissen, Abrufen von Ereignissen für einen bestimmten Zeitraum, Weiterleiten von Protokollereignissen und Datenaufbewahrung finden Sie unter Systemprotokoll.

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

August 26, 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:

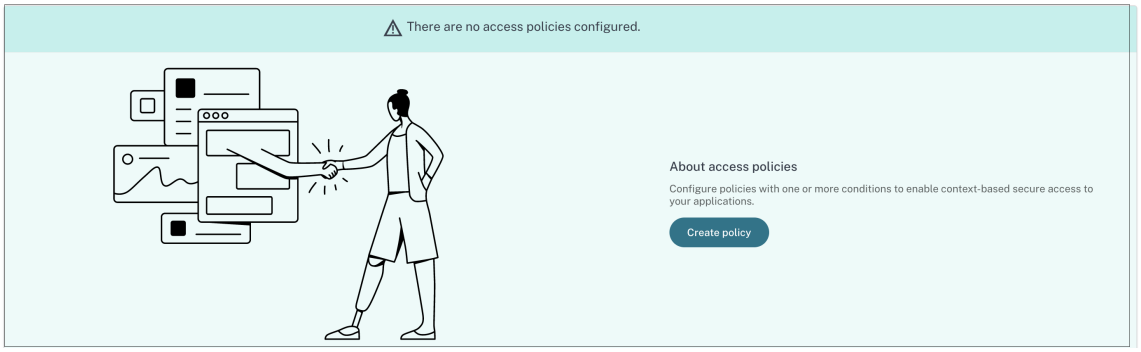
- Zugriff auf Zwischenablage einschränken
- Drucken einschränken
- Downloads einschränken
- Uploads einschränken
- Wasserzeichen anzeigen
- Schlüsselprotokollierung einschränken
- Bildschirmaufnahme einschränken

Weitere Informationen zu diesen Einschränkungen finden Sie unter Verfügbare Zugriffsbeschränkungen.

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

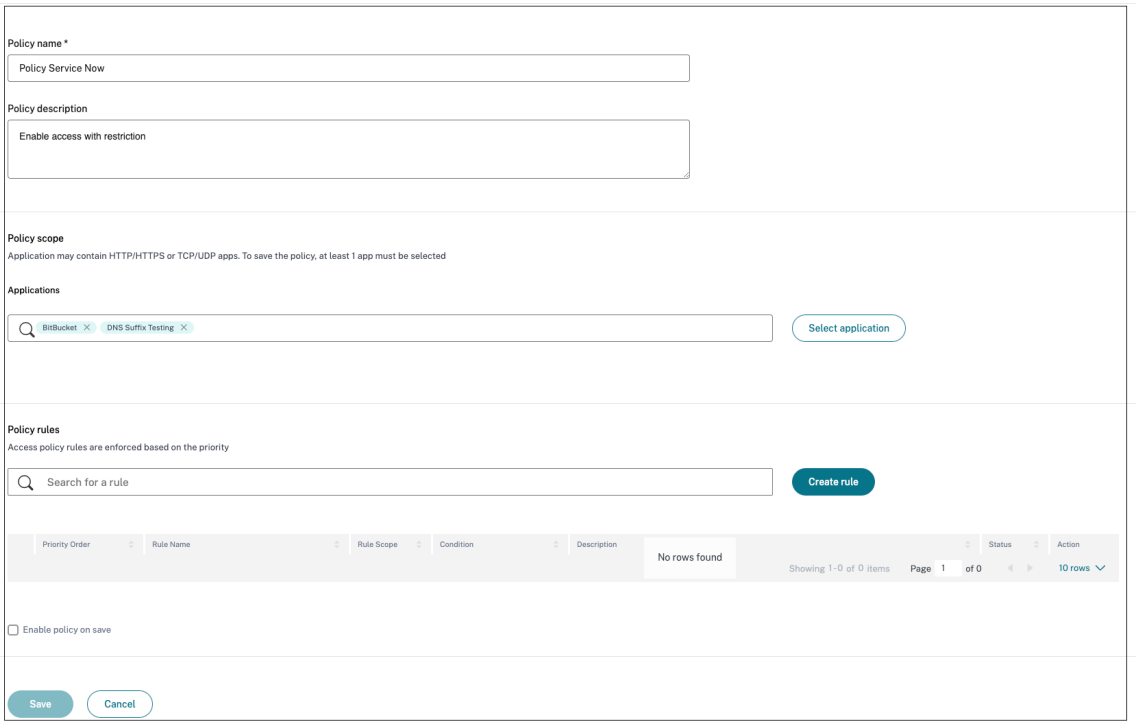
- Identität und Authentifizierung einrichten
- Konfigurierte Anwendungen

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

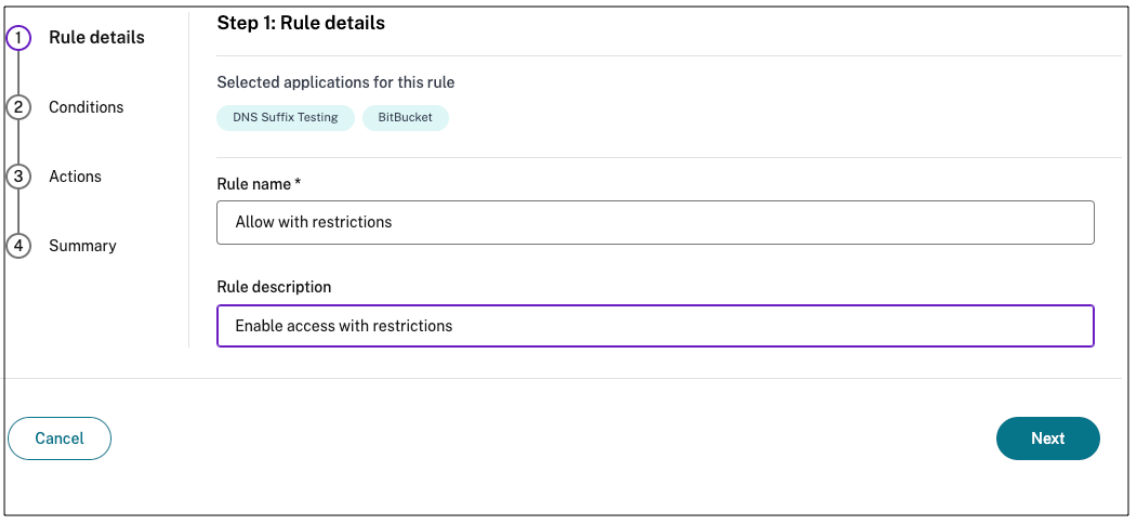


Für Erstbenutzer werden **auf der Zielseite Zugriffsrichtlinien** keine Richtlinien angezeigt. Sobald Sie eine Richtlinie erstellt haben, können Sie sie hier sehen.

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.

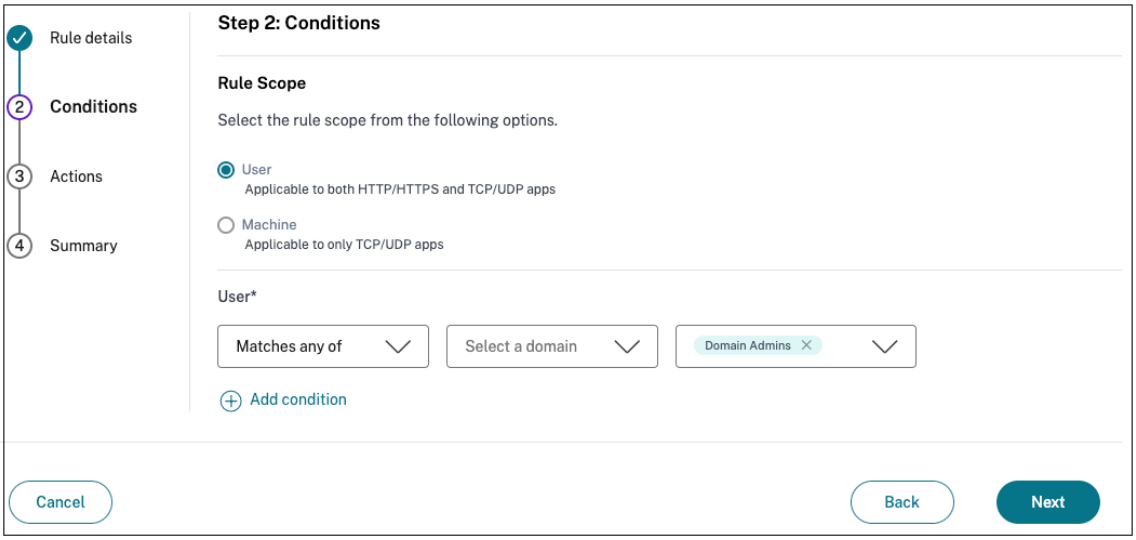


5. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein, und klicken Sie dann auf **Weiter**.



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.

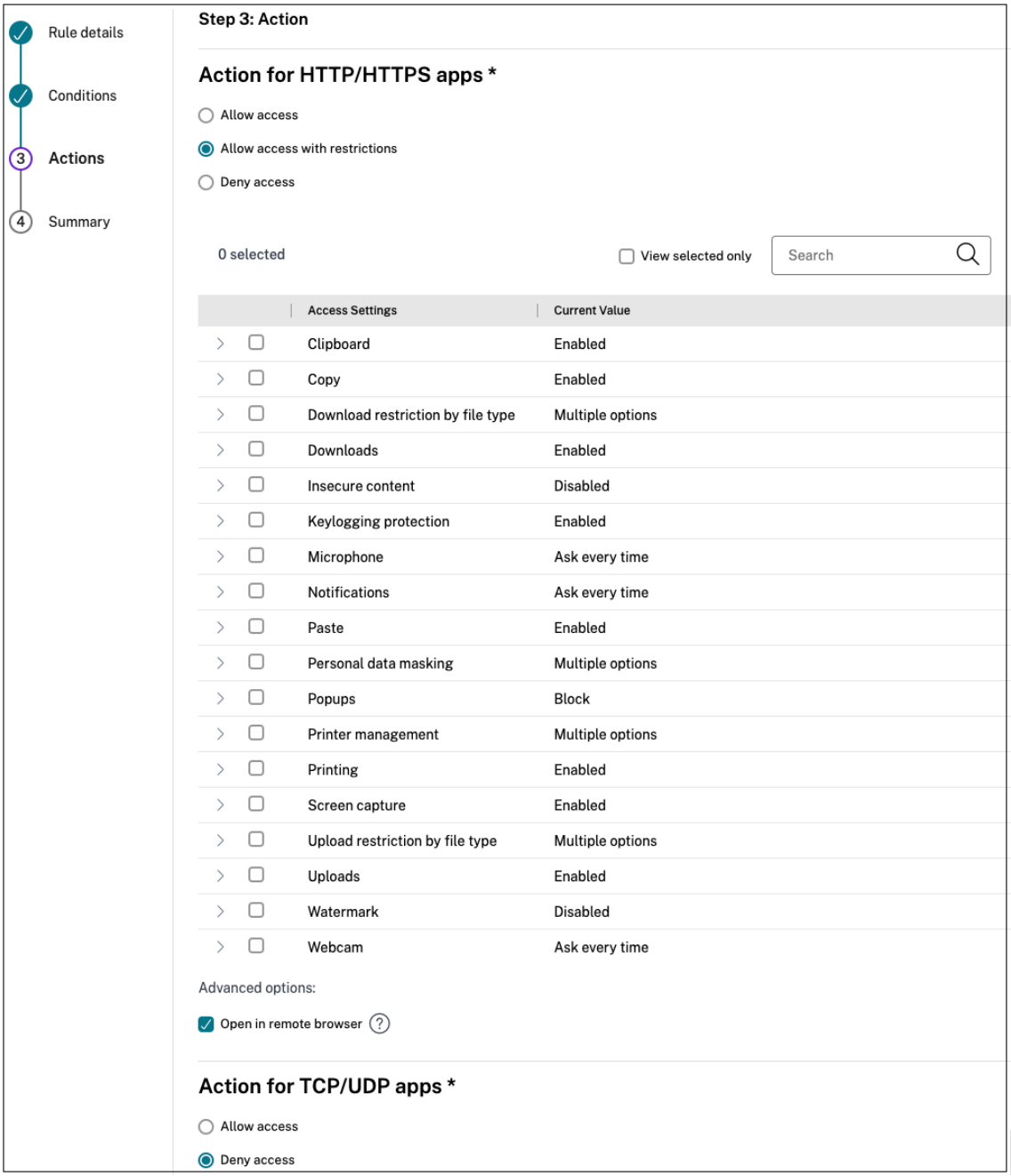
    - Für HTTP/HTTPS-Apps können Sie Folgendes auswählen:

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

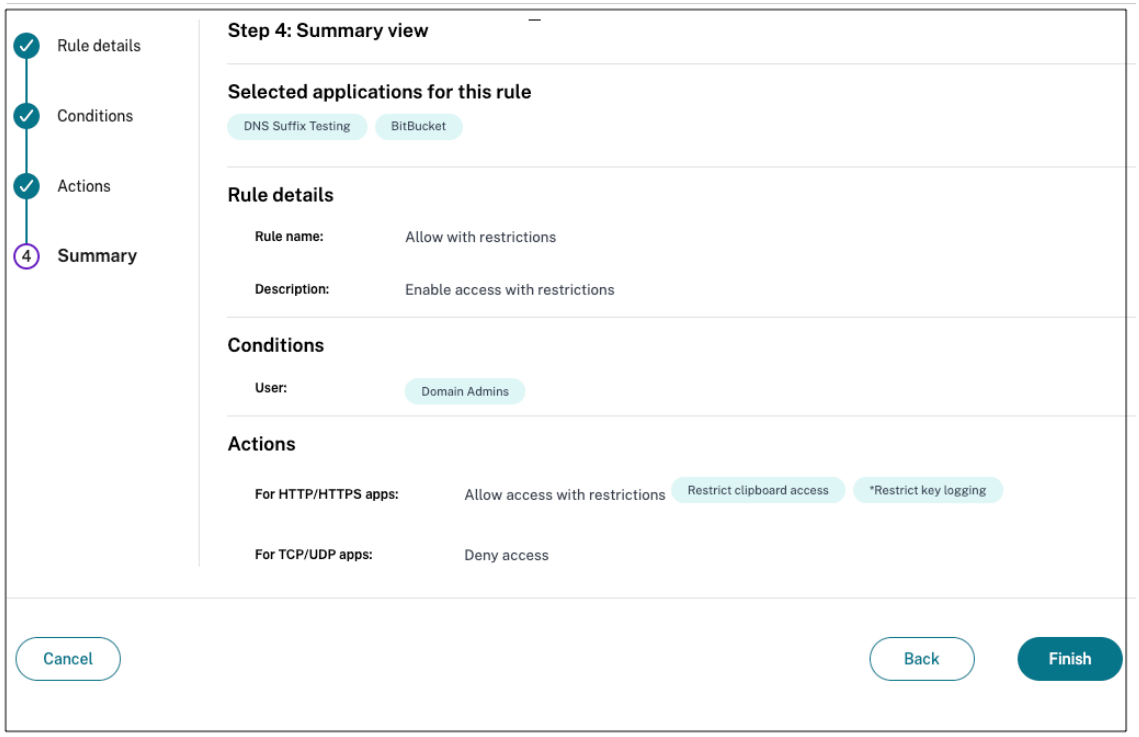
        > **Hinweis:**
        >
        > Wenn Sie **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie die Einschränkungen auswählen, die Sie für die Apps erzwingen möchten. Einzelheiten zu den Einschränkungen finden Sie unter Verfügbare Optionen für Zugriffsbeschränkungen . Sie können auch angeben, 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

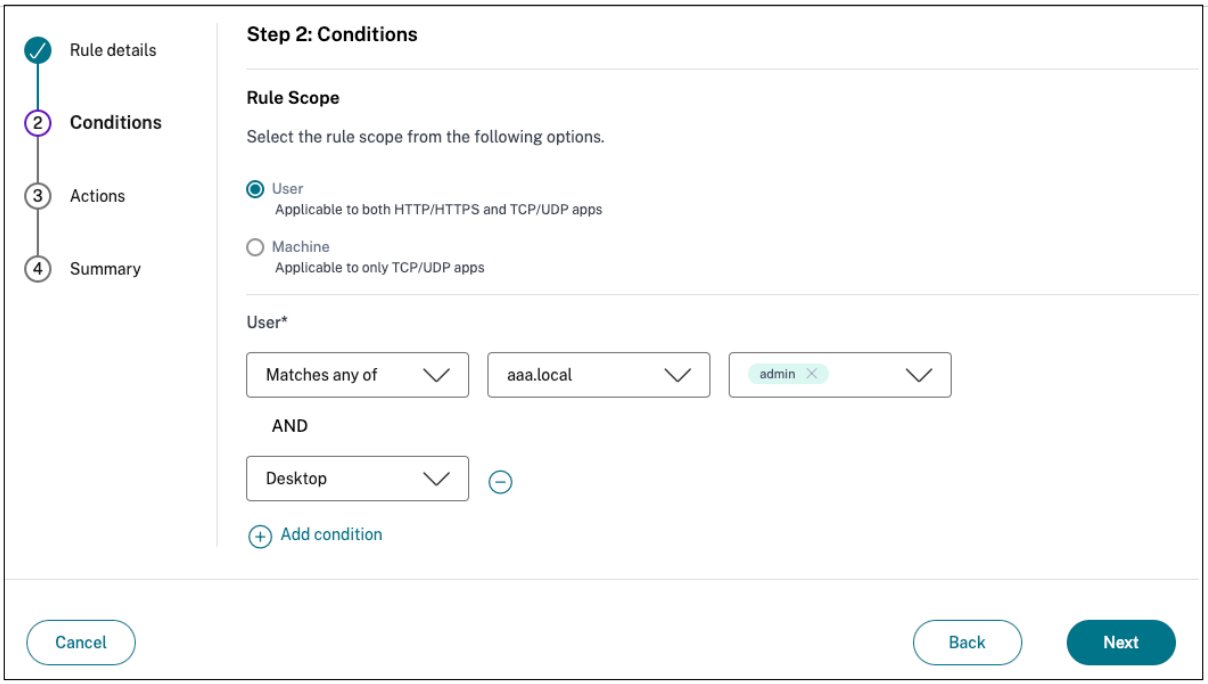
Wenn Sie die Aktion **Zugriff mit Einschränkungen zulassen**auswählen, müssen Sie mindestens eine der Sicherheitseinschränkungen auswählen. Diese Sicherheitseinschränkungen sind im System vordefiniert. Administratoren können keine anderen Kombinationen ändern oder hinzufügen. Einzelheiten finden Sie unter Verfügbare Optionen für Zugriffsbeschränkungen

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.

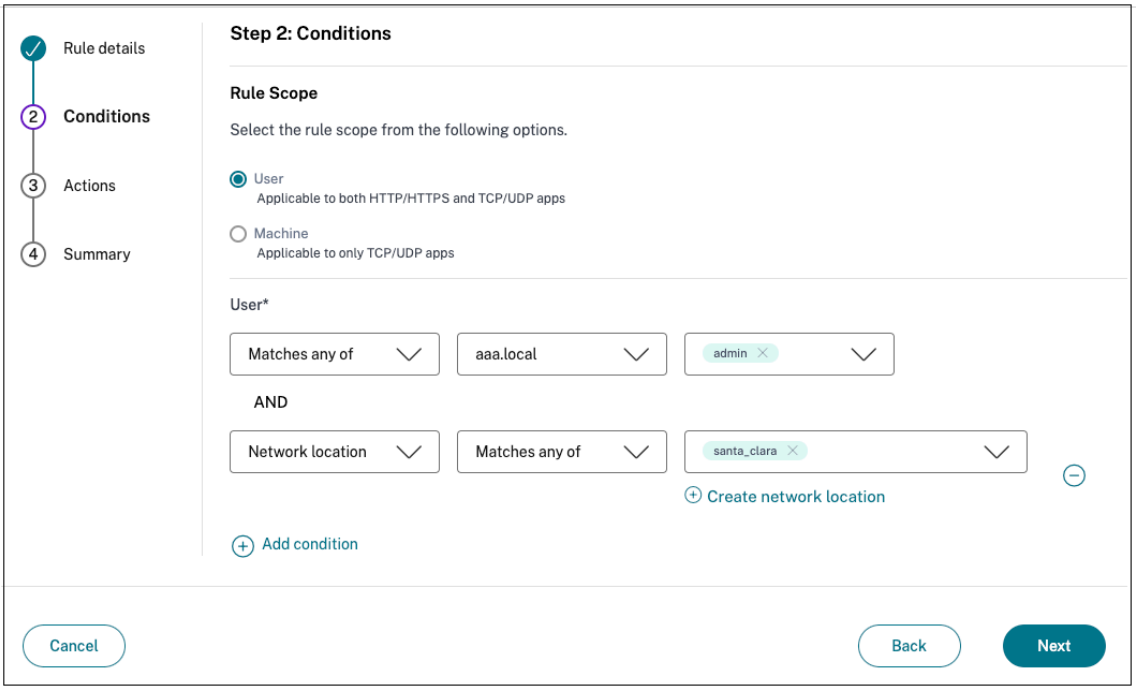
Um eine adaptive Zugriffsrichtlinie basierend auf dem Standort zu konfigurieren, verwenden Sie das Verfahren [Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen mit den folgenden Änderungen.

- 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

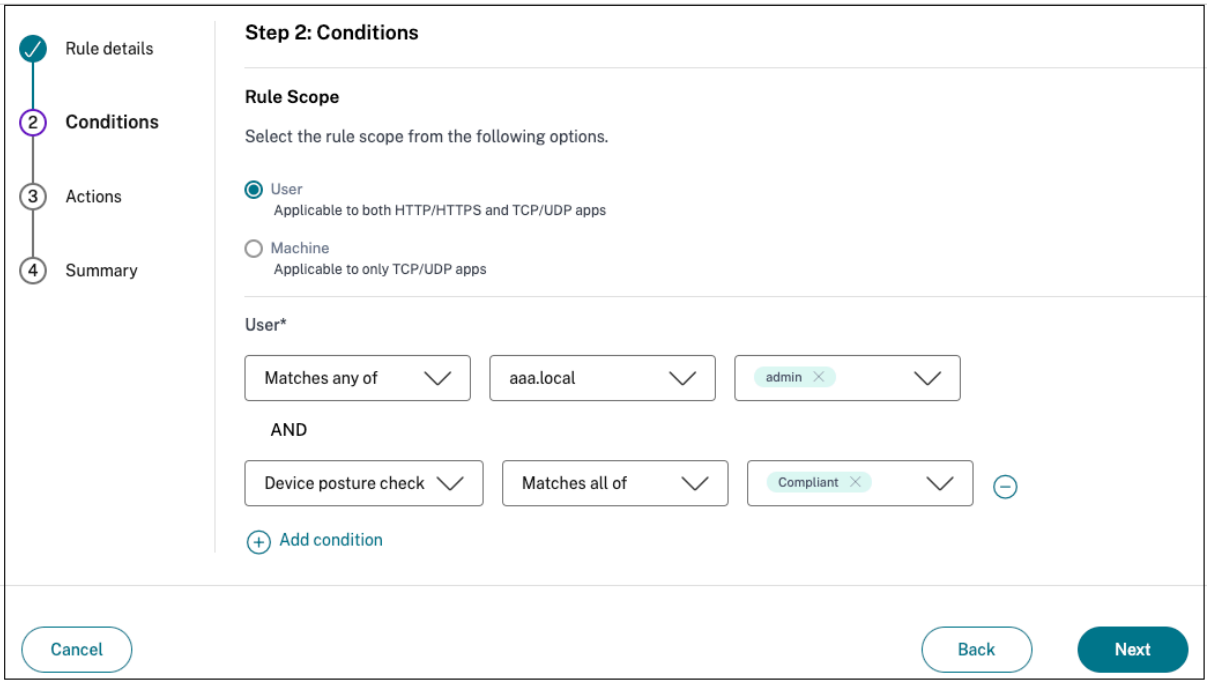
Sie können den Secure Private Access Service so konfigurieren, dass er die Zugriffskontrolle mithilfe von Device Posture Tags erzwingt. Nachdem sich ein Gerät nach der Überprüfung der Gerätehaltung anmelden darf, kann das Gerät als konform oder nicht konform eingestuft werden. Diese Informationen sind 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.

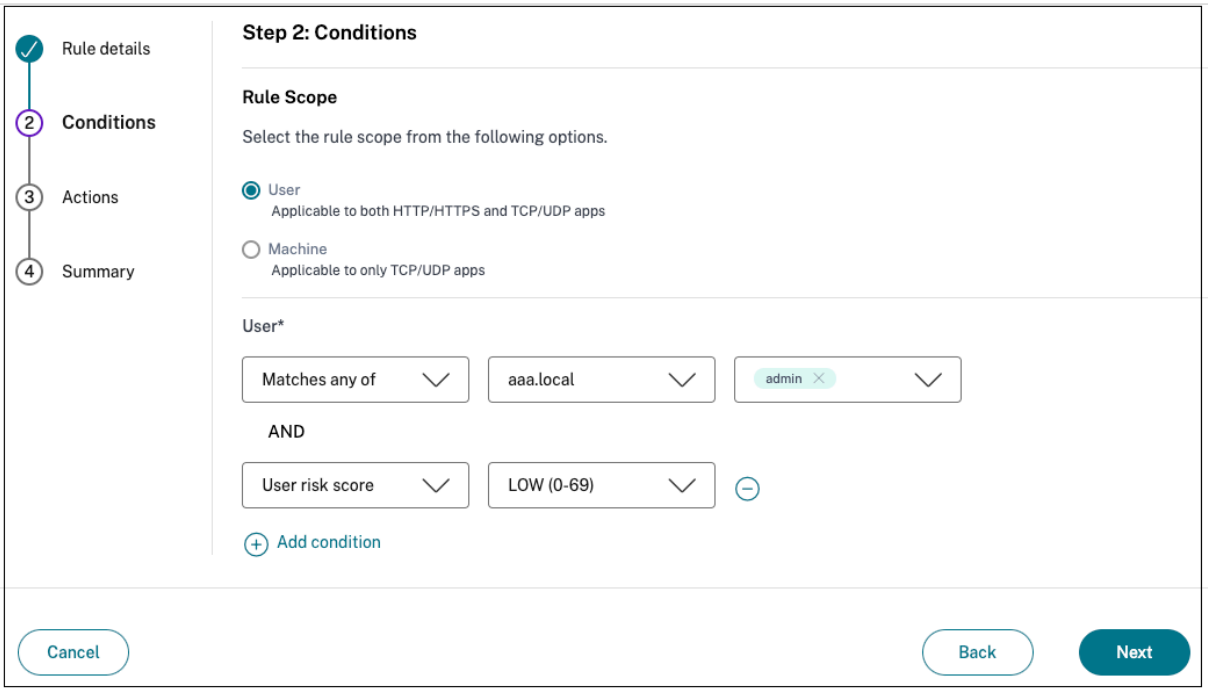
Um eine adaptive Zugriffsrichtlinie mit Risikobewertung zu konfigurieren, verwenden Sie das Verfahren Adaptive Zugriffsrichtlinie mit mehreren Regeln erstellen mit den folgenden Änderungen.

- 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**



Routentabellen zur Lösung von Konflikten, die aus denselben verwandten Domänen resultieren

October 21, 2024

Mit der Anwendungsdomänenfunktion des Citrix Secure Private Access-Dienstes können Kunden Routing-Entscheidungen treffen, die eine externe oder interne Weiterleitung verwandter Anwendungsdomänen über Connector Appliances ermöglichen.

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

So funktioniert die Routentabelle

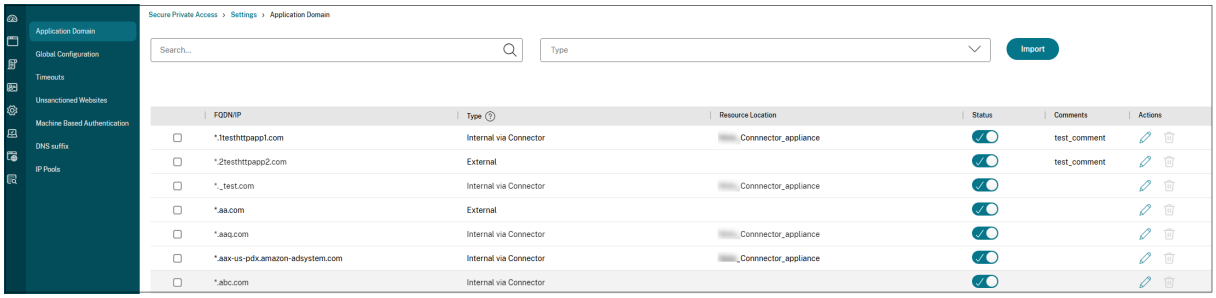
Die Administratoren können für die Apps folgende Routentypen festlegen, je nachdem, wie sie den Verkehrsfluss definieren möchten.

- **Intern –Proxy umgehen** –Der Domänenverkehr wird über Citrix Cloud Connector geleitet und umgeht dabei den auf dem Connector Appliance konfigurierten Webproxy des Kunden.
- **Intern über Connector** –Die Apps sind extern, aber der Datenverkehr muss über das Connector-Gerät zum externen Netzwerk fließen.
- **Extern** –Der Datenverkehr fließt direkt ins Internet.

> **Hinweis:**
>
> - Routeneinträge haben keinen Einfluss auf die Sicherheitsrichtlinien, die für die Apps konfiguriert sind.
> - Wenn Administratoren einen Eintrag in der Routentabelle nicht verwenden möchten oder die entsprechenden Apps nicht wie vorgesehen funktionieren, können Administratoren den Eintrag einfach deaktivieren, anstatt ihn zu löschen.
> - Alle Connector Appliances für einen bestimmten Kunden erhalten die SSO-Einstellungen, unabhängig vom App-Typ. Bisher war die SSO-Einstellung für eine bestimmte App an einen Ressourcenstandort gebunden.

Hauptroutentabelle

Die Hauptroutingtabelle in der Secure Private Access-Konsole (**Einstellungen > Anwendungsdomänen**) ist ein schreibgeschütztes Dashboard, das Ihnen alle Details zu den konfigurierten Domänen in allen Anwendungen anzeigt. Damit können für jede Domäne folgende Informationen angezeigt werden:



In der Hauptroutentabelle können Sie für jede Domäne die folgenden Informationen anzeigen:

- **FQDN/IP:** FQDN oder die IP-Adresse, für die die Art der Verkehrsweiterleitung konfiguriert werden soll.
- **Typ**: App-Typ. **Intern**, **Intern –Proxy umgehen**oder **Extern** , je nach Auswahl beim Hinzufügen der App.

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

- **Ressourcenstandort:** Ressourcenstandort für Routing vom Typ **Intern**. Wenn ein Ressourcenstandort nicht zugeordnet ist, wird bei der jeweiligen App in der Spalte **Ressourcenstandort** ein dreieckiges Symbol angezeigt. Wenn Sie mit der Maus über das Symbol fahren, wird die folgende Meldung angezeigt.

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

- **Status:** Über den Kippschalter in der Spalte **Status** kann die Route für einen Routeneintrag deaktiviert werden, ohne die App zu löschen. Wenn der Kippschalter ausgeschaltet ist, wird die Routeneingabe nicht wirksam. Wenn FQDNs mit exakter Übereinstimmung vorhanden sind, können Administratoren außerdem auswählen, welche Route aktiviert oder deaktiviert werden soll.
- **Kommentare:** Zeigt Kommentare an, falls vorhanden.
- **Aktionen:** Das Bearbeiten-Symbol wird verwendet, um einen Ressourcenstandort hinzuzufügen oder den Typ der Routeneingabe zu ändern. Mit dem Löschsymbol können Sie die Route löschen.

Mini-Routentabelle

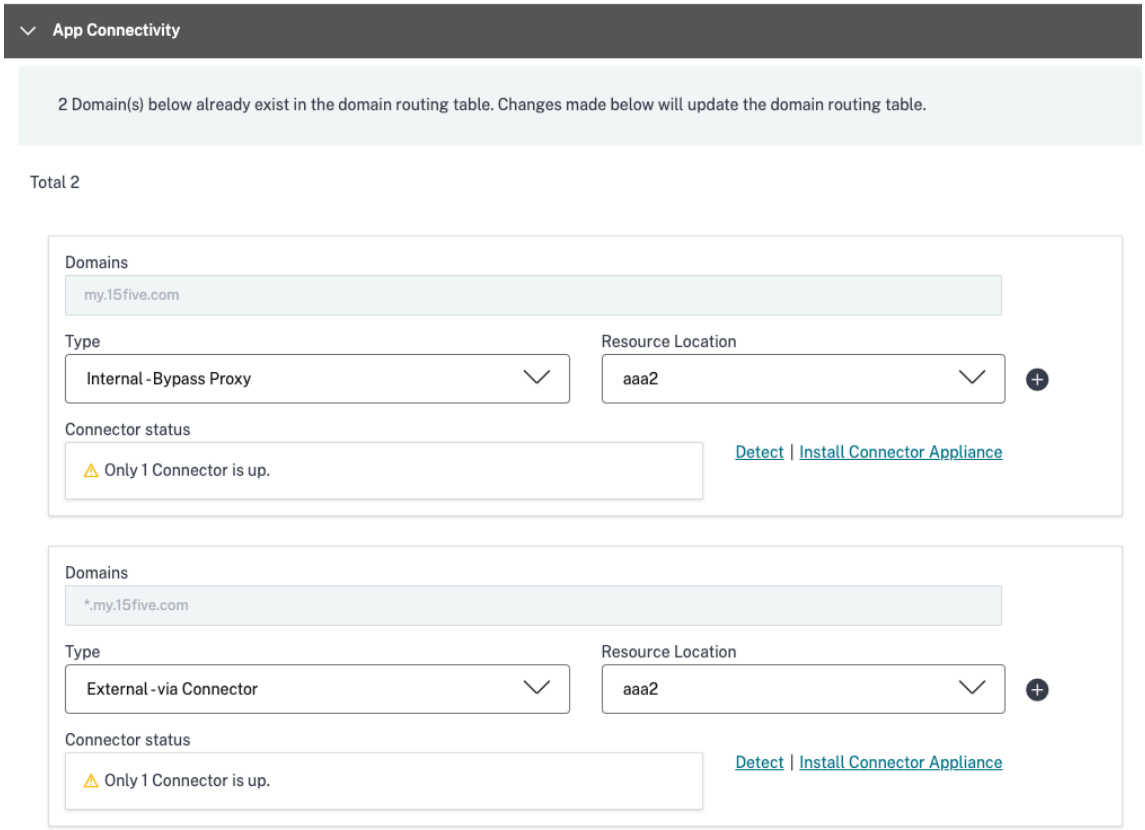
Um während der App-Konfiguration Routing-Entscheidungen treffen zu können, steht eine Miniversion der Anwendungsdomänentabelle zur Verfügung. Die Mini-Routentabelle ist im Abschnitt **App-**

Konnektivität in der Benutzeroberfläche des Citrix Secure Private Access-Dienstes verfügbar.

So fügen Sie Routen zur Miniroutentabelle hinzu

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

1. Führen Sie hierzu die folgenden Schritte aus:
    - Wählen Sie eine Vorlage.
    - Geben Sie App-Details ein.
    - Wählen Sie, sofern zutreffend, erweiterte Sicherheitsdetails.
    - Wählen Sie ggf. die Single-Sign-On-Methode aus.
2. Klicken Sie auf **App-Konnektivität**. –Eine Miniversion der Anwendungsdomänentabelle ist verfügbar, um die Routing-Entscheidungen während der App-Konfiguration zu treffen.



- **Domänen:** Die Spalte „Domänen“zeigt eine oder mehrere Zeilen für eine bestimmte App an. In der ersten Zeile wird die eigentliche App-URL angezeigt, die der Administrator beim Hinzufügen der App-Details eingegeben hat. Die anderen Zeilen sind alle zugehörigen

Domänen, die beim Hinzufügen der App-Details eingegeben werden. Wenn die App-URL und die zugehörigen Domänen identisch sind, werden sie in einer Zeile angezeigt.

In einer Zeile wird die SAML-Assertion-URL angezeigt, wenn SAML SSO ausgewählt ist.

- **Typ:** Wählen Sie eine der folgenden Optionen.
  - **Intern –Proxy umgehen** –Der Domänenverkehr wird über Citrix Cloud Connector geleitet und umgeht dabei den auf dem Connector Appliance konfigurierten Webproxy des Kunden.
  - **Intern über Connector** –Die Apps sind extern, aber der Datenverkehr muss über das Connector-Gerät zum externen Netzwerk fließen.
  - **Extern** –Der Datenverkehr fließt direkt ins Internet.
- **Ressourcenstandort:** Wird automatisch ausgefüllt, wenn Sie den Typ „Intern“für eine App auswählen. Ändern Sie es, wenn ein anderer Ressourcenstandort gewünscht wird.
- **Connector Appliance-Status:** Wird zusammen mit dem Ressourcenstandort automatisch ausgefüllt, wenn Sie den Typ „Intern“für eine App auswählen.

Nicht genehmigte Websites

October 21, 2024

Anwendungen (Intranet oder Internet), die nicht in Secure Private Access konfiguriert sind, gelten als „nicht genehmigte Websites“. Standardmäßig verweigert Secure Workspace 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 in der Administratorkonsole über die Registerkarte **Einstellungen > Nicht genehmigte Websites** den Zugriff über den Citrix Enterprise Browser zulassen oder verweigern. Um browserbasierte Angriffe zu verhindern, können Administratoren den Zugriff auch auf eine Remote Browser Isolated (RBI)-Umgebung umleiten. Wenn ein Administrator die Umleitung von URLs zu RBI konfiguriert hat, werden die folgenden Aktionen ausgeführt.

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

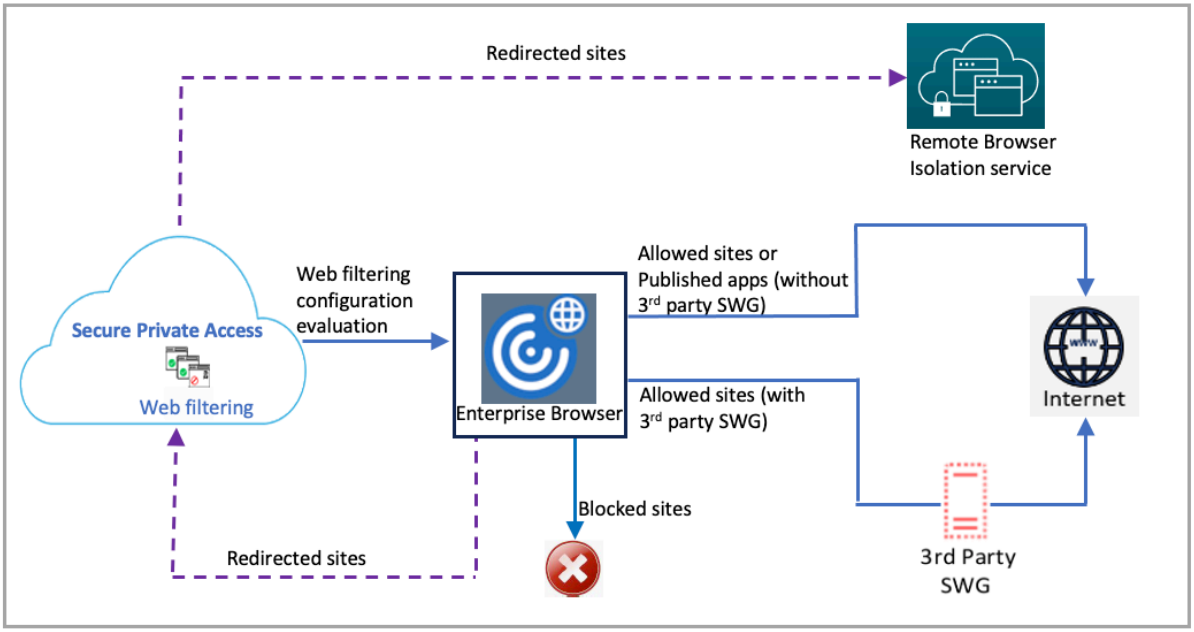
Sie können Platzhalter wie `*.example.com`verwenden, um den Zugriff auf alle Domänen dieser Website und alle Seiten innerhalb dieser Domäne zu steuern.

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

So funktionieren nicht genehmigte Websites

1. Durch eine URL-Analyse wird ermittelt, ob es sich bei der URL um eine Citrix-Dienst-URL handelt.
2. Anschließend wird die URL überprüft, um festzustellen, ob es sich um die URL einer Enterprise-Web- oder SaaS-App handelt.
3. Anschließend wird die URL überprüft, um festzustellen, ob es sich um eine blockierte URL handelt, ob eine Weiterleitung zu einer sicheren Browser-Sitzung erforderlich ist oder ob der Zugriff auf die URL zugelassen werden kann.

Die folgende Abbildung erläutert den Endbenutzer-Datenverkehrsfluss.



Wenn eine Anfrage eintrifft, werden die folgenden Prüfungen durchgeführt und entsprechende Aktionen ausgeführt:

1. Stimmt die Anfrage mit der globalen Zulassungsliste überein?
    a) Bei einer Übereinstimmung kann der Nutzer auf die angefragte Webseite zugreifen.
    b) Bei Nichtübereinstimmung werden Website-Listen geprüft.
2. Stimmt die Anfrage mit der konfigurierten Websiteliste überein?
    a) Bei einer Übereinstimmung bestimmt die folgende Sequenz die Aktion.

i. Blockieren

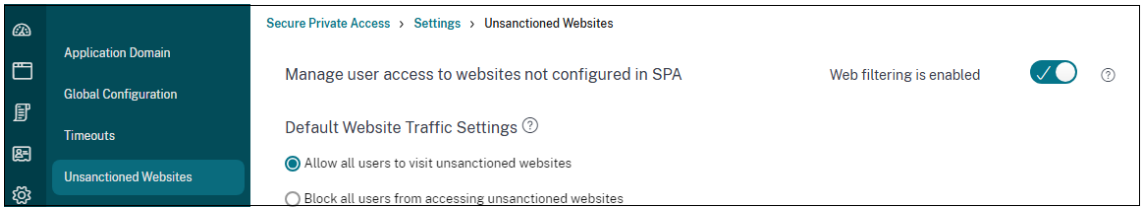
ii. Umleiten

iii. Zulassen

b) Bei keiner Übereinstimmung wird die Standardaktion (ALLOW) angewendet. Die Standardaktion kann nicht geändert werden.

Konfigurieren Sie Regeln für nicht genehmigte Websites

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 erlaubt.
> - Sie können die Einstellung auf **ändern, um allen Benutzern den Zugriff auf nicht genehmigte Websites zu verbieten, oder auf** , um allen Benutzern den Zugriff auf beliebige Internet-URLs über den Citrix Enterprise Browser zu verbieten.

```
1  ![Konfigurieren von Regeln](/en-us/citrix-secure-private-access/media/
       spa-enable-website-list-filtering.png)
2
3  Sie können die Einstellungen für bestimmte URLs auch ändern, indem Sie
       sie zu blockierten oder zugelassenen Websites hinzufügen oder zur
       Remote Browser Isolation-Liste umleiten.
4
5  Wenn Sie beispielsweise den Zugriff auf alle nicht genehmigten URLs
       standardmäßig blockiert haben und den Zugriff nur auf einige
       bestimmte Internet-URLs zulassen möchten, können Sie dies mit den
       folgenden Schritten erreichen:
6
7  1.  Klicken Sie auf die Registerkarte **Zugelassene Websites** und dann
        auf **Eine Website zulassen**.
8  1.  Fügen Sie die Website-Adresse hinzu, der der Zugriff gestattet
       werden muss. Sie können die Website-Adresse entweder manuell hinzufü
       gen oder eine CSV-Datei mit der Website-Adresse per Drag & Drop
       verschieben.
9  1.  Klicken Sie auf **URL hinzufügen** und dann auf **Speichern**.
10
11     Die URL wird zur Liste der zulässigen Websites hinzugefügt.
```


> **Hinweis:**
>
> Ein Kunde (Organisation) des kostenpflichtigen Remote Browser Isolation Standard-Dienstes erhält standardmäßig 5.000 Nutzungsstunden pro Jahr. Für mehr 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.

Wichtige Hinweise

Wenn die Benutzer keinen Zugriff auf eine SaaS-App haben, können sie die Anwendung nicht über den Citrix Enterprise Browser starten. Sie können jedoch möglicherweise weiterhin auf die App zugreifen, indem sie die URL direkt in den Citrix Enterprise Browser eingeben.

- Wenn der Zugriff auf eine App durch eine Richtlinie verweigert wird, wird die Anwendungs-URL zur Sperrliste hinzugefügt, sofern die Funktion **Webfilterung** aktiviert ist. Dadurch wird sichergestellt, dass alle Versuche, auf die App zuzugreifen, sei es über den Citrix Enterprise Browser oder direkt über die URL, blockiert werden.
- Bei nicht veröffentlichten Apps wird der Zugriff auf diese Apps verweigert, auch wenn das Routing konfiguriert ist. Die URL der nicht veröffentlichten App wird der Sperrliste hinzugefügt, wenn die Funktion **Webfilterung** aktiviert ist, wodurch sämtliche Zugriffsversuche verhindert werden.

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.

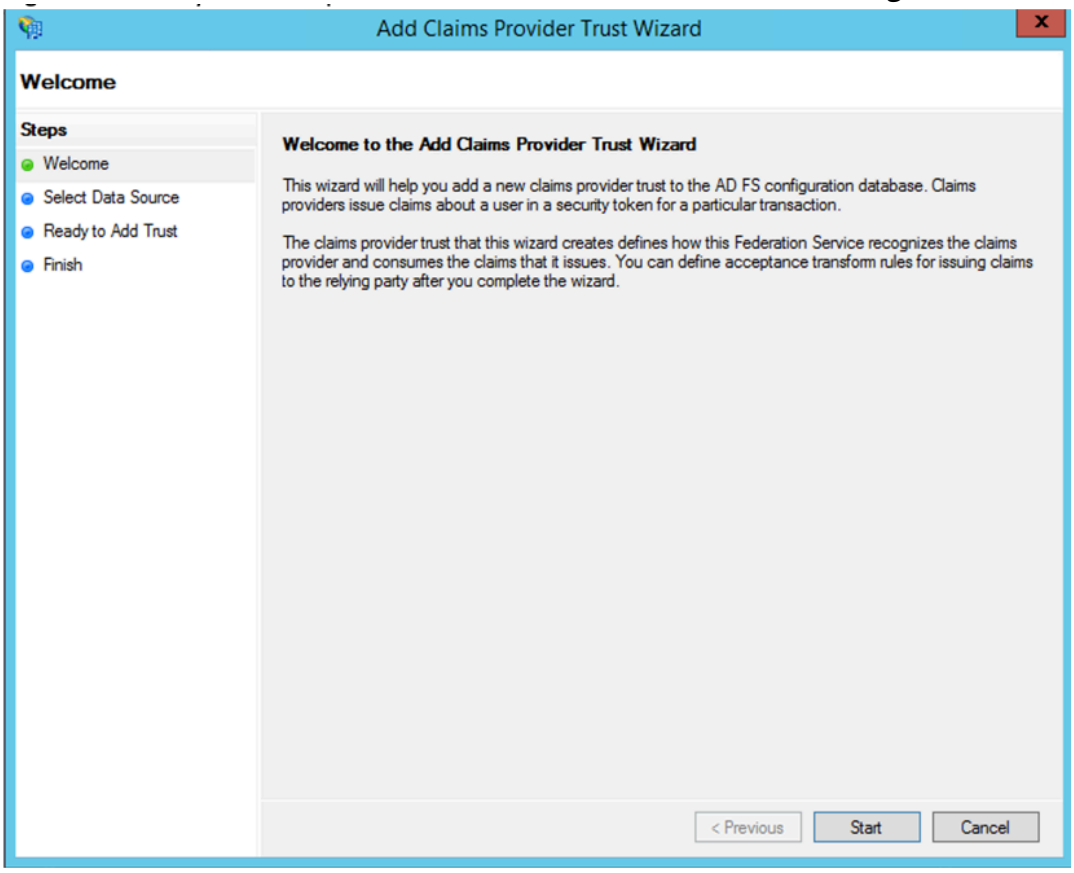
Um ADFS so einzurichten, dass Ansprüche von Citrix Secure Private Access akzeptiert werden, müssen Sie die folgenden Schritte ausführen:

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

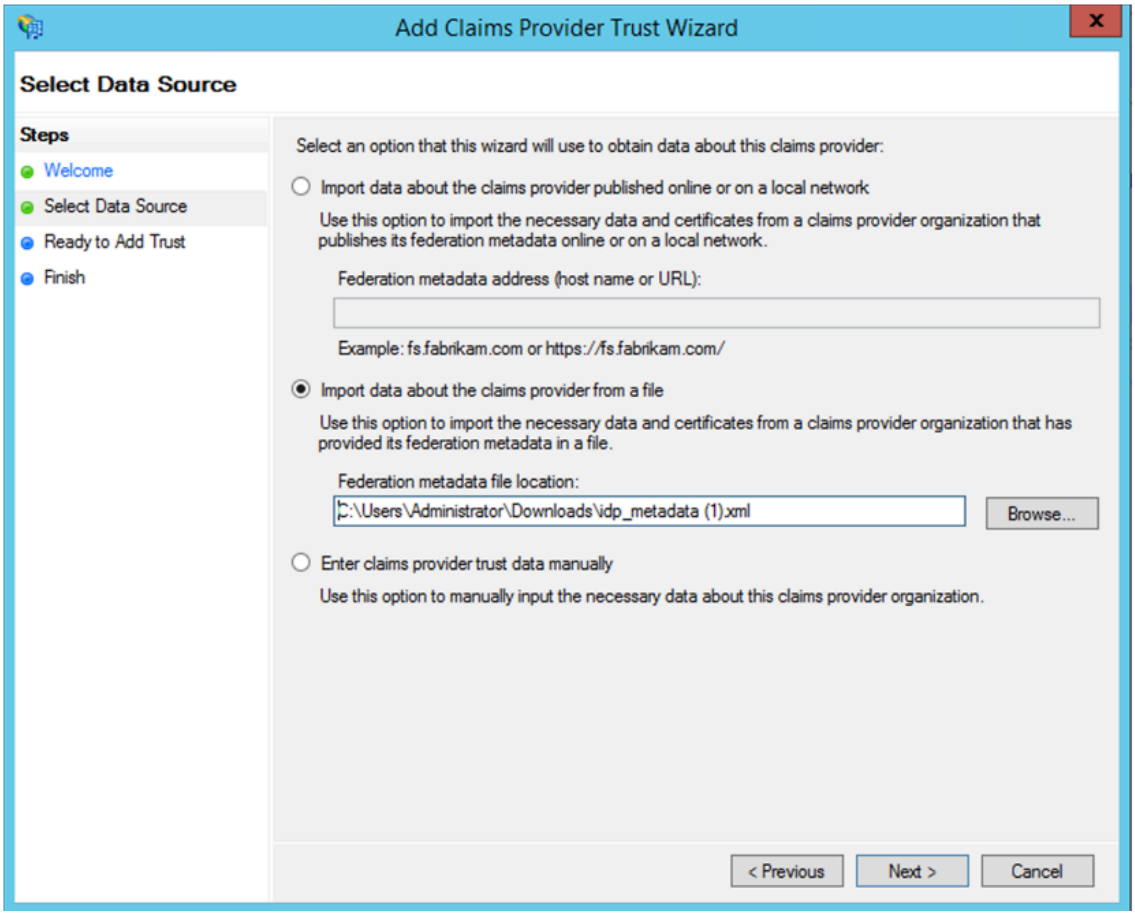
1. Öffnen Sie die ADFS-Managementkonsole. Gehen Sie zu **ADFS > Trust Beziehung > Claim Provider Trust**.

   a) Klicken Sie mit der rechten Maustaste und **wählen Sie Vertrauensstellung**für

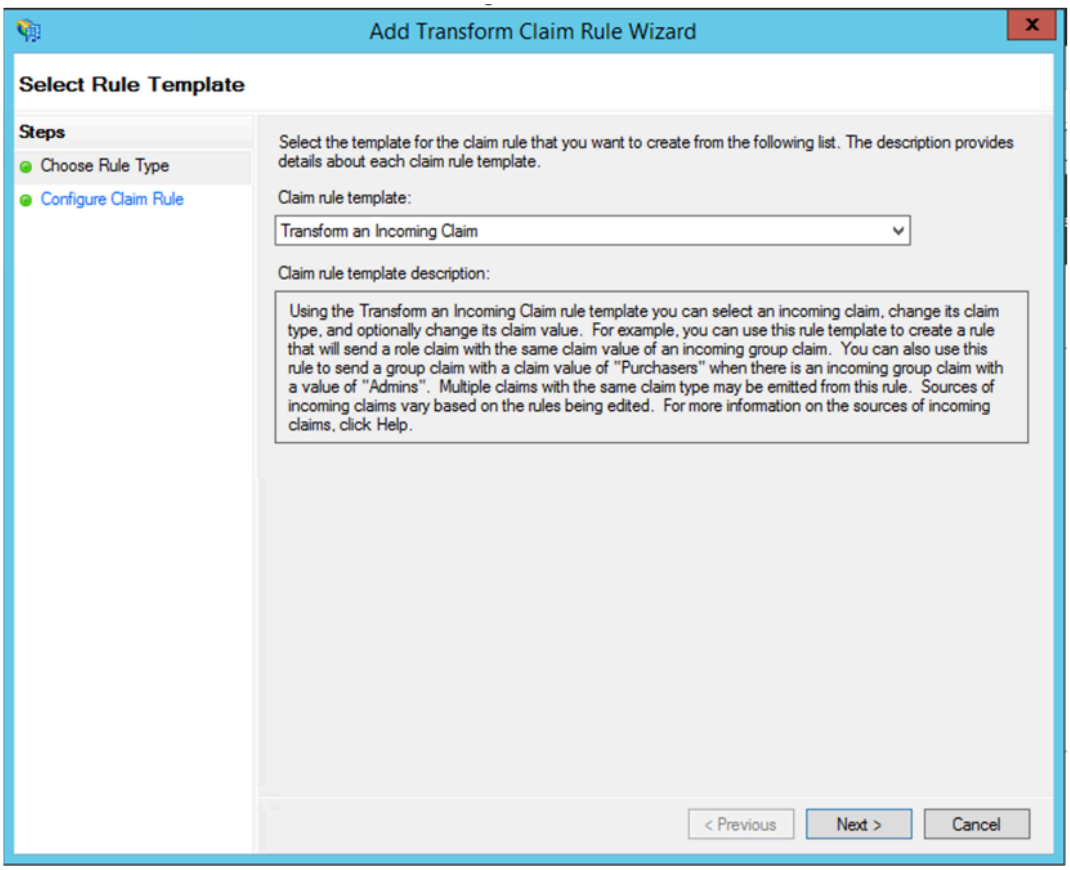


   b) Fügen Sie in Secure Private Access eine App hinzu, die für die Verbindung zu ADFS verwendet wird. Einzelheiten finden Sie unter App-Konfiguration auf Citrix Secure Private Access.

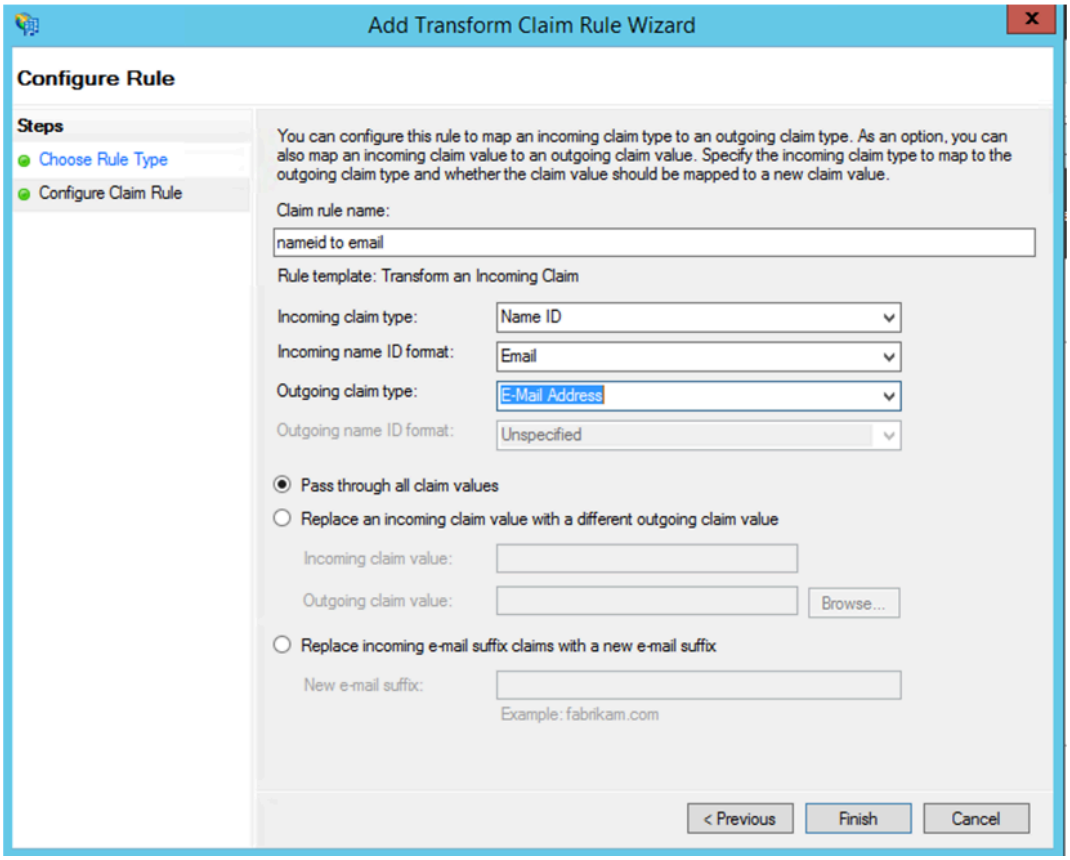
> **Hinweis:**
>
> Fügen Sie zuerst die App hinzu und aus dem SSO-Konfigurationsbereich der App können Sie die SAML-Metadatendatei herunterladen und dann die Metadatendatei in ADFS importieren.



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



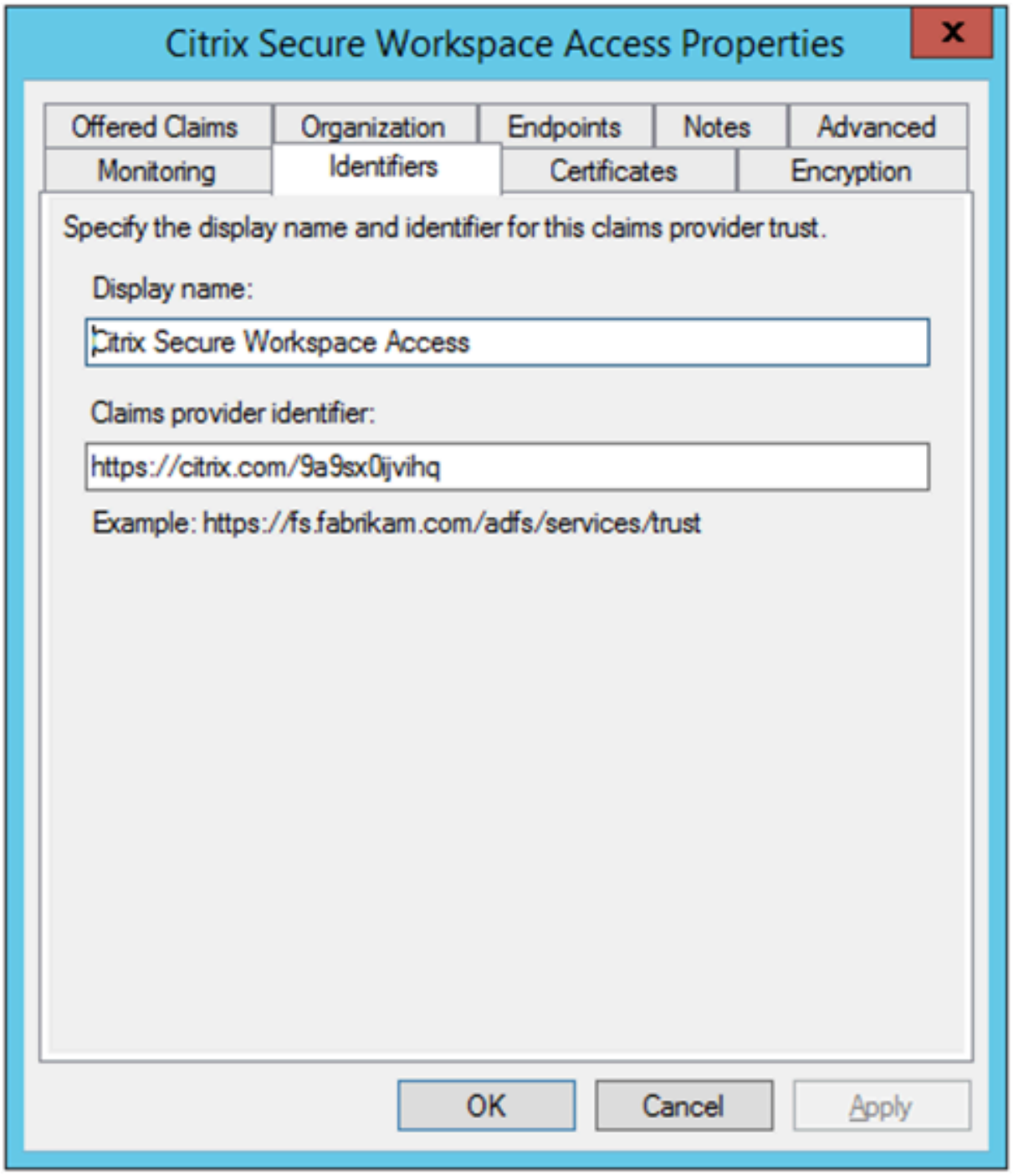
c) Vervollständigen Sie die Einstellungen wie in der folgenden Abbildung gezeigt. Wenn Ihr ADFS andere Ansprüche akzeptiert, verwenden Sie diese Ansprüche und konfigurieren Sie SSO in Secure Private Access ebenfalls entsprechend.



Sie haben jetzt die Anspruchsanbietervertrauensstellung konfiguriert, die bestätigt, dass ADFS jetzt Citrix Secure Private Access for SAML vertraut.

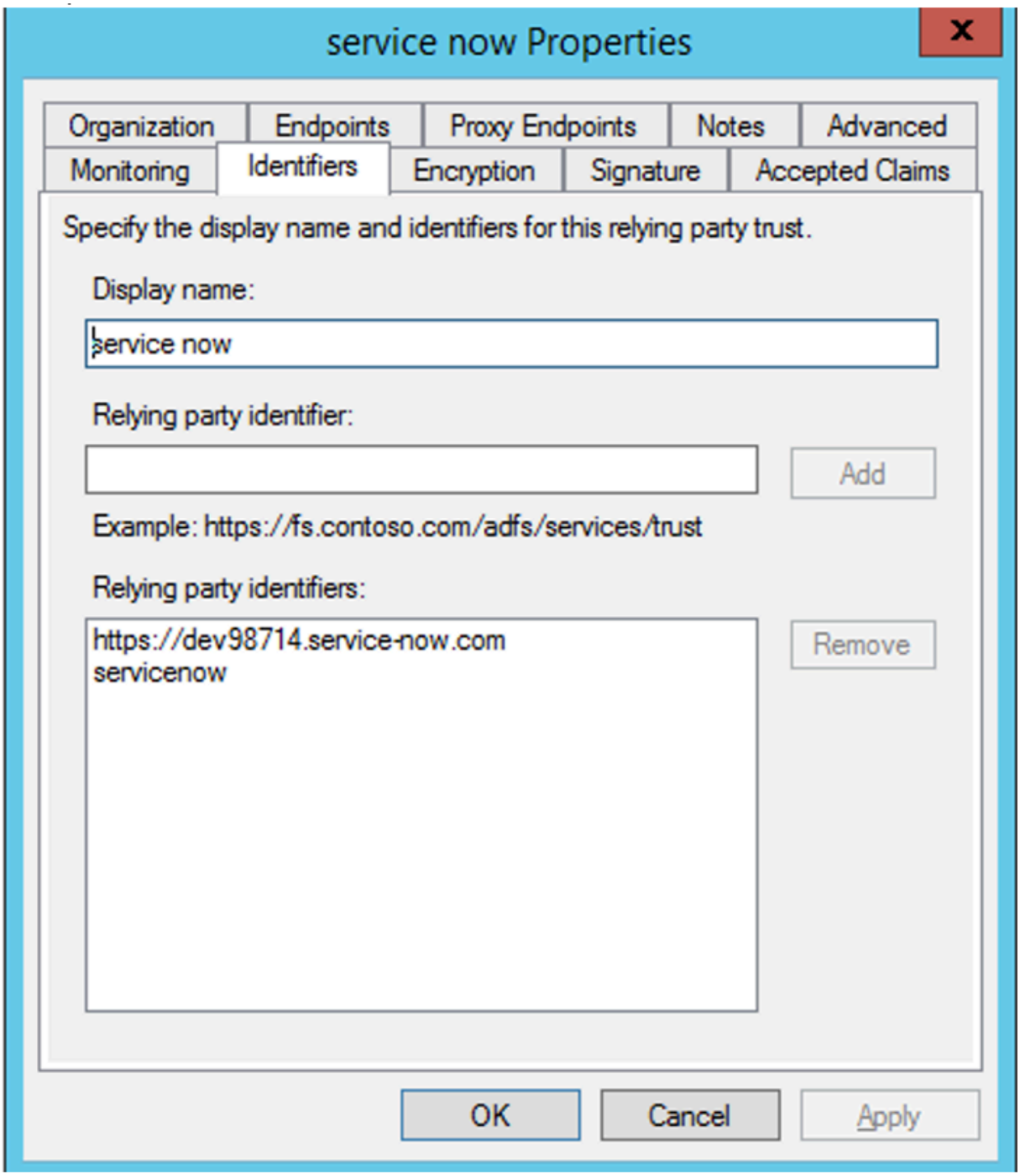
Vertrauensnummer des Anbieters

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.

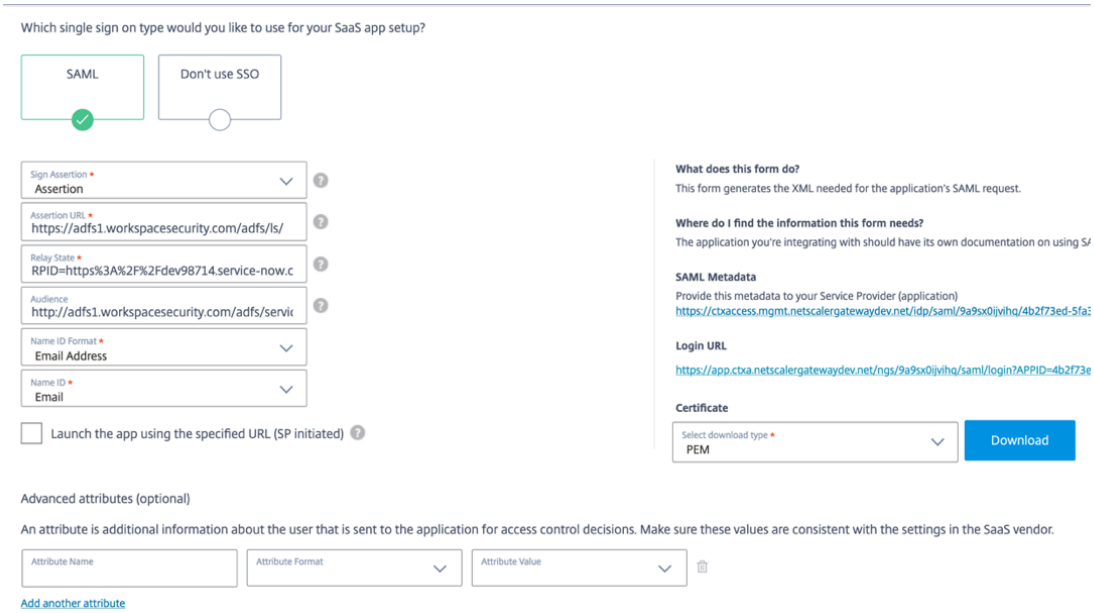
  Beispiel: https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

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**.

Veraltete Funktionen

August 26, 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.