Citrix Secure Private Access™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Übersicht über die Secure Private Access-Dienstlösung 26
- Adaptive Sicherheit 26
- Anwendungszugriff 27
- Single Sign-On 27
- Browsersicherheit 27
- Gerätestatus 27
- Unterstützung für TCP- und UDP-Anwendungen 28
- Beispielanwendungsfälle 28
- Referenzartikel 29
- Referenzvideos 29
- Was ist neu in verwandten Produkten 29

Was ist neu 30
- 30 September 2026 30
- 03 September 2026 30
- 19 August 2026 31
- 05 August 2026 32
- 31 July 2026 32
- 24 June 2026 32
- 18 June 2026 33
- 09 June 2026 33
  - Wichtiger Hinweis 33
- 20 May 2026 35
- 28 April 2026 35
- 07 April 2026 35
- 04 March 2026 36
- 12 February 2026 36

© 1997–2026 Citrix Systems, Inc. All rights reserved.

05 February 2026 36
18 December 2025 37
16 December 2025 37
11 December 2025 37
30 October 2025 38
17 September 2025 38
13 August 2025 39
14 July 2025 39
03 June 2025 40
15 May 2025 40
24 April 2025 41
22 April 2025 42
20 February 2025 42
08 January 2025 43
07 January 2025 43
02 January 2025 44
03 December 2024 44
25 November 2024 44
14 November 2024 45
08 November 2024 45
07 November 2024 45
23 September 2024 45
15 August 2024 46
16 July 2024 46
11 June 2024 47
13 March 2024 47
12 February 2024 48
23 January 2024 48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

20 December 2023 48
16 October 2023 48
11 September 2023 49
30 August 2023 49
28 August 2023 49
22 August 2023 49
17 August 2023 50
07 June 2023 50
29 May 2023 50
10 April 2023 50
29 March 2023 51
07 March 2023 51
23 January 2023 51
22 December 2022 52
03 October 2022 52
09 September 2022 53
01 June 2022 54
04 April 2022 54
16 February 2022 57
11 October 2021 57
30 July 2021 57
09 June 2021 58
22 May 2021 58
01 May 2021 59
15 March 2021 59
11 November 2020 60
15 October 2020 60
08 October 2020 60

© 1997–2026 Citrix Systems, Inc. All rights reserved.

24 September 2020 60
07 July 2020 61
19 June 2020 61
08 May 2020 61
V2019.04.02 62
V2019.04.01 62
V2019.03.01 62
Integration mit Google Chrome Enterprise Premium 64
Lösungsübersicht 64
Erweiterte Sicherheitsfunktionen von Chrome Enterprise Premium 65
Citrix Secure Access-Steuerelemente für Chrome Enterprise 66
Voraussetzungen für eine erfolgreiche Integration 66
Citrix Secure Private Access – Unterstützte Bereitstellungsmodi 67
Rechtliches 67
Verwandte Themen 67
Voraussetzungen für die integrierte Lösung 68
Lizenzen, App-Versionen und Erweiterungen 68
Google Admin-Konsole 69
Secure Private Access-Dienst 69
Google Chrome 70
Benutzer verwalten 70
Obligatorisch – E-Mail-Adressfelder für Benutzer ausfüllen 71
Obligatorisch – E-Mail-Adressfelder für Benutzergruppen ausfüllen 71
Überlegungen zur Domänenzuordnung bei fehlender oder inkonsistenter E-Mail-Adresse 72
Benutzerverzeichnis, das in Citrix Secure Private Access konfiguriert ist, mit dem Google Cloud-Benutzerverzeichnis korrelieren 72
Active Directory 73
Microsoft Entra ID 73

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Okta 74
Google Cloud Identity (Google-Verzeichnis) 74
TLS-Inspektion umgehen 74
Administratorrollen und -berechtigungen 75
Berechtigungen für benutzerdefinierte Google-Administratorrollen 76
Rollen und Berechtigungen erstellen und zuweisen 78
Egress-Hub-Regionen konfigurieren 79
Das Panel „Egress-Regionen für SaaS-Anwendungen“ 79
Eine Region auswählen 81
Eine Region abwählen 81
Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen 83
Wie die Domänenzuordnung funktioniert 83
E-Mail-Adresskonstruktion 84
Einschränkungen 85
Verwaltete Profilidentität 85
Benutzerattributtyp einrichten 85
Open ID Connect mit Citrix Identity und Zugriffsverwaltung 86
Übersicht 87
Voraussetzungen 87
OIDC-Integrationsübersicht 88
Ein Google OIDC SSO-Profil erstellen 89
Einen Citrix OIDC-Client erstellen 90
Zuweisung des OIDC-SSO-Profils 91
Citrix OIDC-Client aktualisieren 91
OIDC-Client löschen 94
Endbenutzererfahrung 94
Citrix Secure Access-Erweiterung für Chrome Enterprise Premium 96
Protokolle der Secure Access-Erweiterung 97

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access-Steuerelemente für Chrome Enterprise 98
Unterstützte Steuerelemente 100
Benutzer und Gruppen in Richtlinien 101
Suchen nach Benutzern oder Gruppen 101
Synchronisierte Benutzer und Gruppen verwenden 102
Anti-Keylogging-Kontrolle 102
Voraussetzungen 103
Anti-Keylogging-Richtlinie konfigurieren 103
Steuerung des Zwischenablage-Containers 104
Voraussetzungen 104
Zwischenablage-Container-Steuerung aktivieren 104
Umfang der Zwischenablagefreigabe aktivieren 106
Domänensuffix für Webanwendungen 109
Voraussetzungen 109
DNS-Suffix konfigurieren 109
Steuerung der Sitzungsaufzeichnung 110
Architektur 111
Voraussetzungen 111
Systemanforderungen 112
Umgebung einrichten 112
Steuerung der Browser-Sitzungsreauthentifizierung 113
Voraussetzungen 114
Browser-Sitzungsreauthentifizierungssteuerung aktivieren 114
SSH-Steuerung 116
Vorteile dieser Integration 116
Anwendungsfälle 117
Systemanforderungen 117
Voraussetzungen 117

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access für SSH-Zugriff konfigurieren 117
SSH-Richtlinie konfigurieren 118
Remotedesktopsteuerung 118
Vorteile dieser Integration 119
Anwendungsfälle 119
Systemanforderungen 120
Voraussetzungen 120
Secure Private Access für RDP-Zugriff konfigurieren 120
Remotedesktop-Richtlinie konfigurieren 121
Fehlerbehebung bei CEP-Integrationsproblemen 121
Diagnoseprotokolle für die CEP-Fehlerbehebung 122
Bestätigen Sie, dass der Benutzer im richtigen Chrome-Profil angemeldet ist 123
Überprüfen Sie die installierte Secure Enterprise Browser-Erweiterung 124
Überprüfen Sie die ExtensionInstallForcelist-Richtlinie 124
Beheben von Problemen mit widersprüchlichen Richtlinien für die Erweiterungsinstallationsliste 124
Überprüfen der Secure Enterprise Browser-Erweiterungsrichtlinie 125
Benutzererweiterungskonfiguration in der Google Admin Console überprüfen 127
Überprüfen, ob Routen abgerufen werden 128
CEP-Integration in der Secure Private Access-Administratorkonsole validieren 129
Beheben von Problemen mit der Erreichbarkeit des Google Secure Gateway 129
Bestätigen der Anwendungsaufnahme in Routen 130
Fehlerbehebung beim Zugriff auf geroutete Anwendungen 130
Sicherstellen der Ausrichtung von IdP und Google Directory 132
Zugriffseinstellungen für die Gruppe in der Google Admin Console prüfen 132
Bekannte Probleme mit der CEP-Integration 132
Secure Private Access-Benutzeroberfläche 132
Konfiguration der adaptiven Zugriffsrichtlinie 133

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Chrome-Browser 133
Open ID Connect (OIDC) 134
Erste Schritte mit Citrix Secure Private Access 135
Systemanforderungen 135
Funktionsweise 135
Erste Schritte mit dem Citrix Secure Private Access-Dienst 136
Bereitstellungsmodelle für den Secure Private Access-Dienst 137
Standorte der Points of Presence (PoPs) für den Citrix Secure Private Access™ Dienst 139
Secure Private Access Management-PoPs 139
Secure Private Access Daten-PoPs 139
Secure Private Access-Onboarding und -Einrichtung 141
Benutzer für Secure Private Access onboarden 141
Store-URL in Citrix StoreFront Cloud konfigurieren 144
Google Chrome-Integration einrichten 144
IP-Adressen von SaaS-Anwendungen hinzufügen 147
Konfiguration von Richtlinien für die Zugriffsbegrenzung von Prinzipalen 147
Google-Integrationsdetails nach dem Onboarding aktualisieren 148
CEP für Google Directory Organisationseinheiten konfigurieren 150
Bekannte Überprüfungsfehler und -warnungen 153
Problem bei der Bereitstellung mit mehreren Benutzergruppen 156
Nächste Schritte 157
Datenregionalisierung 158
Unterstützte Bereitstellungen 159
Konfiguration 159
Einschränkungen 159
App-Konfiguration und -Verwaltung 161
Unternehmens-Web-Apps konfigurieren 161
Systemanforderungen 162

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Funktionsweise 162
Eine Web-App konfigurieren 162
Automatische Bereinigung von Routing-Einträgen beim Löschen von Anwendungen 175
SaaS-Apps konfigurieren 176
So werden SaaS-Apps mit dem Secure Private Access-Dienst unterstützt 176
Eine SaaS-App konfigurieren 177
Routing über Google Secure Gateway 189
Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung 189
SaaS-App-Server-spezifische Konfiguration 190
End-to-End-App-Konfiguration 206
Agentenloser Zugriff auf Unternehmens-Webanwendungen 206
Funktionsweise 206
Konfigurieren von Citrix Secure Private Access für den agentenlosen Zugriff auf Unternehmens-Webanwendungen 207
Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung 219
Device Posture-Dienst mit agentenlosen Zugriffs-Apps 220
Schritte zum Aktivieren des agentenlosen Zugriffs nur für konforme Geräte 220
Endbenutzererfahrung 224
Unterstützung für TCP/UDP-Anwendungen 224
Voraussetzungen 224
Secure Private Access für TCP/UDP-Anwendungen konfigurieren 225
Administratorkonfiguration – Clientbasierter Zugriff auf HTTP/HTTPS-Apps mit Citrix Secure Access 232
Voraussetzungen 232
Hinweise 233
Adaptiver Zugriff auf TCP/UDP- und HTTP(S)-Apps 233
So erstellen Sie eine adaptive Zugriffsrichtlinie 234
Registrierungen für Anmelde- und Abmeldeskriptkonfiguration 234

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beheben von IP-Adresskonflikten bei Anwendungsdomänen 235
Wichtige Hinweise 237
Always On vor der Windows-Anmeldung 238
Wie funktioniert Always On? 239
Active Directory- und Microsoft Entra ID Hybrid AD-Konfiguration 240
Secure Private Access-Konfiguration 244
Connector Appliance-Konfiguration 247
Always On nach der Windows-Anmeldung konfigurieren (Maschinen-/Benutzertunnel) 248
Einschränkungen 249
Referenzen 249
Reservierte CIDR-Adressen für die TCP- und UDP-Server 250
Reservierte CIDR-IP-Adressen konfigurieren 250
DNS-Suffixe zur Auflösung von FQDNs in IP-Adressen 250
Voraussetzungen 252
So fügen Sie DNS-Suffixe hinzu 252
Beispielanwendungsfall 253
Zugehörige Domänen mithilfe einer HAR-Datei ermitteln 256
Beispiel 256
Voraussetzungen 257
HAR-Datei importieren 257
Zugehörige Domänen verwalten 259
Validierung und Dateianforderungen 260
Portbasiertes Routing mithilfe von Routing-Ausnahmen – Vorschau 260
Anwendungsfälle für portbasiertes Routing 261
Beispiel zur Veranschaulichung von Port-basiertem Routing 267
Zertifikate in der Secure Private Access Konsole verwalten 268
Maschinenauthentifizierungszertifikate verwalten 269
Zertifikat hinzufügen 269

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein Zertifikat deaktivieren 270
Ein Zertifikat löschen 271
Priorität für das Zertifikat festlegen 271
SSL-Zertifikate verwalten 271
Zertifikat hinzufügen 271
Zertifikat suchen 272
Zertifikat ändern 273
Zertifikat löschen 273
Externe Benachrichtigung 274
Citrix Secure Access™ Client 274
Citrix Secure Access Client für Windows 274
Citrix Secure Access Client für macOS 274
Citrix Secure Access Client für iOS 274
Citrix Secure Access Client für Android 274
Citrix Secure Access Client für Linux 275
Best Practices für Web- und SaaS-Anwendungskonfigurationen 275
Anwendungszugriff innerhalb von Secure Private Access für veröffentlichte und nicht veröffentlichte Apps 275
Abgleich und Priorisierung von Zugriffsrichtlinien 276
Best Practices für die App-Konfiguration 278
IdP-Domänen müssen eine eigene Anwendung haben 278
Dieselben verwandten Domänen dürfen nicht Teil mehrerer Anwendungen sein 280
Deep-Link-URLs 283
Endbenutzererfahrung beim App-Zugriff erklärt 283
Zugriff auf eine Web-App über den Citrix Secure Access-Client 284
Zugriff auf eine TCP/UDP-App über den Citrix Secure Access-Client 284
Connector Appliance für Secure Private Access 285
Secure Private Access mit Connector Appliance konfigurieren 286

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validieren Ihrer Kerberos-Konfiguration 297
Überlegungen zu Skalierung und Größe 298
Web- und SaaS-Anwendungen 298
TCP-Anwendungen 298
Gemischter Datenverkehr (Web, SaaS, TCP) 299
Connector-Benachrichtigungen 299
Konfiguration und Verwaltung adaptiver Zugriffsrichtlinien 300
Funktionsweise 300
Zugriffsrichtlinie mit mehreren Regeln erstellen 301
Voraussetzungen 301
Suchen nach Benutzern oder Gruppen 306
Benutzer- und Gruppensynchronisierung überprüfen 307
Wichtige Punkte nach der Erstellung einer Richtlinie 308
Adaptiver Zugriff basierend auf Geräten 308
Adaptiver Zugriff basierend auf dem Standort 309
Adaptiver Zugriff basierend auf dem Gerätestatus 311
Sitzungsrichtlinien 312
Routing-Priorität 313
Unterstützte Citrix Secure Access™ Clients 313
Beispiel-Anwendungsfall 313
Direktes Routing innerhalb des Unternehmensnetzwerks mithilfe von Sitzungsrichtlinien konfigurieren 314
Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium 318
Chrome Enterprise Premium konfigurieren 318
Richtlinienanreicherung für Benutzergruppen ohne E-Mail 319
Secure Private Access Konfigurations-Parser für die CEP-Kompatibilitätsanalyse 320
So verwenden Sie das Tool 321
Konfigurationsänderungen vor der vollständigen Migration zu CEP 325

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Änderungen an der Single Sign-On-Konfiguration 325
Updates für Zugriffsrichtlinien und Sitzungsrichtlinien 326
Standardisierung von Aktionen über Anwendungen hinweg 326
Anwendungsanforderung für Richtlinienaktualisierungen 327
Aktualisierung der Webfilterrichtlinie (optional) 327
Weitere Richtlinienanpassungen (optional) 327
Bereinigung von Sicherheitsgruppen (optional) 328
CEP für die Organisation einführen (vollständige Migration) 328
Zusammenfassung des Migrationsprozesses 329
Herausforderungen beim E-Mail-Anreicherungsprozess 330
Bewährte Methoden 330
Fazit 330
Erweiterte Secure Private Access-Funktionen 331
Hybrider Datenpfad für den Secure Private Access Dienst 333
Wichtige Vorteile der Nutzung des hybriden Datenpfads 333
Funktionsweise des hybriden Datenpfads 333
Unterstützte Clients 334
Unterstützte NetScaler Gateway Builds 334
Konnektivitätsanforderungen 335
Zulassungsliste von URLs für ausgehende Verbindungen 335
Hybriden Datenpfad für Secure Private Access-Anwendungen einrichten 335
Mit einem Gateway verbinden, um eine Verbindung herzustellen 335
Registrieren Ihres NetScaler Gateways bei Citrix Cloud 337
Aktivieren des Routings des Datenverkehrs über das lokale NetScaler Gateway 339
Einschränkungen 341
Problem mit dem Secure Private Access-Registrierungsskript 342
Anwendungen, Domänen oder IP-Adressen in Ihrem Netzwerk ermitteln 344
Anwendungserkennung für interne Domänen in einer neuen Umgebung 345

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine Anwendung von der Seite App Discovery erstellen 348
Eine vorhandene Anwendung aktualisieren 349
Alle ausgewählten eingebetteten Domänen anzeigen 350
Bekannte Einschränkungen 351
Kontextbasiertes App-Routing und Auswahl des Ressourcenstandorts 352
Anwendungsfall: Kontextbasiertes Routing 352
Anwendungsfall: Auswahl des Ressourcenstandorts basierend auf dem Benutzerkontext 354
Schritte zum Ändern des Routing-Typs oder des Ressourcenstandorts 354
Anwendungsfall: Interne Unternehmensbenutzer direkt zu Back-End-Anwendungen leiten 357
Einblicke in das kontextbezogene Routing in Monitor 357
Nahtloser Zugriff auf lokale LAN-Ressourcen (Drucker, Dateiserver) 360
Wichtige Überlegungen 360
Funktion für den lokalen LAN-Zugriff aktivieren 361
Richtlinienmodellierungstool 363
Zugriff auf das Richtlinienmodellierungstool 364
Richtlinien für eine Gruppe von Benutzern oder Maschinen analysieren 364
Richtlinien für bestimmte Ziele analysieren 365
Zugriffsrichtlinien detailliert anzeigen 367
Anwendungen Import-Tool – Vorschau 369
So funktioniert der Import 370
Vorbereiten der CSV-Datei 370
Einzugebende Werte in der CSV-Datei 373
Schritte zur Migration von Anwendungen mit dem CSV-basierten Tool 376
Fehler beim Importieren oder Erstellen von Anwendungen bei Verwendung der CSV-Datei 381
Referenzen 382
Interne IP-Adresspools für Clients – Vorschau 382
Anwendungsfälle für interne IP-Adresspools für Clients 383
Einschränkungen des IP-Adresspools 383

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einen Intranet-IP-Adresspool erstellen 384
Einen IP-Adresspool löschen 386
Anzeigen der IP-Adressauslastungsdaten 387
Konsistente Verbindungen aufrechterhalten 388
Connector-Stickiness 389
Client-IP-Adressen-Persistenz – Vorschau 390
Voraussetzungen 391
Client-IP-Adresspersistenz für TCP/UDP-Anwendungen aktivieren 391
Aktive Sitzungen beenden und Benutzer/Maschinen zur Sperrliste hinzufügen 392
Anwendungsfälle 393
Voraussetzungen zum Blockieren von Benutzern bei Verwendung von Chrome Enterprise Premium 394
Benutzer/Computer zur Sperrliste hinzufügen 394
Endbenutzererfahrung, nachdem ein Benutzer/eine Maschine zur Sperrliste hinzugefügt wurde 396
Über die Cloud aufgerufene Anwendungen 396
Anwendungen, auf die über ein lokales NetScaler® Gateway zugegriffen wird (hybrider Datenpfad) 396
Timeouts für Benutzersitzungen 397
Timeout für die Web-App-Server 397
Timeouts für den Citrix Secure Access Client 397
Konfigurationsberichte 399
Einen Konfigurationsbericht generieren 399
ADFS-Integration mit Secure Private Access 400
Anspruchsanbieter-Vertrauensstellung in ADFS hinzufügen 401
ID der Anspruchsanbieter-Vertrauensstellung 404
Bezeichner der vertrauenden Seite 405
Relay-Status im IdP-initiierten Fluss aktivieren 406

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So aktivieren Sie den RelayState-Parameter auf Ihren ADFS-Servern 407
App-Konfiguration in Citrix Secure Private Access 407
IdP-initiierter Flow 407
SP-initiierter Flow 409
Citrix Secure Private Access Terraform-Provider 410
Hauptvorteile 411
Anwendungsfall 411
Systemanforderungen 411
Voraussetzungen 412
Berechtigungen 412
Installation 412
Terraform-Konfiguration 412
Fehlerbehebung 414
Einschränkungen 414
Wichtige Überlegungen 414
Referenzen 415
Sichtbarkeit und Überwachung 416
Monitor 416
Secure Private Access-Nutzungs-Dashboard 416
Secure Private Access-Anwendungs- und Sitzungsüberwachung 416
Connector Appliance-Zustandsüberwachung 417
Secure Private Access Nutzungs-Dashboard 417
Diagnoseprotokolle 418
Konnektorstatus 420
Top-Anwendungen nach Startanzahl 420
Top-Benutzer nach Anwendungsstartanzahl 421
Top-Zugriffsrichtlinien nach Durchsetzung 422
Top-erkannte Anwendungen 422

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erstellen einer App aus der Tabelle 423
Suchoperatoren 425
Secure Private Access-Anwendungen, -Sitzungen und -Trends 426
Anwendungen, Sitzungen und Trends 426
Zustandsüberwachung 427
Connector Appliance 427
Sitzungs- und Anwendungstrends 428
Sitzungen und Anwendungstrends 428
Sitzungsüberwachung 428
Anwendungstrends 429
Triage und Fehlerbehebung 430
Fehlerbehebung bei anwendungsbezogenen Problemen 430
Secure Private Access-Sitzungscodes in DaaS Monitor 430
Fehlerbehebung bei sitzungsbezogenen Problemen in Monitor 430
Fehlerbehebung bei Problemen im Zusammenhang mit dem Gerätestatus (Device Posture) 430
Fehlerbehebung bei authentifizierungsbezogenen Problemen 431
Fehlerbehebung mithilfe von Protokollen 431
Secure Private Access-Protokolle 431
Device Posture-Protokolle 431
Echtzeit-Sitzungsfehlerbehebung mit Monitor 432
Fehlercodes für Diagnoseprotokolle 432
App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist 436
App-Start fehlgeschlagen, da die Länge des App-FQDN überschritten wurde 436
Start der Web-App fehlgeschlagen, da keine Verbindung zur Backend-Web-App hergestellt werden konnte 437
Benutzerdetails nicht gefunden 437
Der Start der Web-/SaaS-App ist fehlgeschlagen, weil Benutzerattribute während der Vorbereitung des SAML-Tokens nicht gefunden wurden 437

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Start der Web-/SaaS-App ist fehlgeschlagen, weil die Anwendungs-FQDN nicht identifiziert werden konnte 438

Der Start der Web-/SaaS-App ist fehlgeschlagen, weil eine ungültige appId vom SAML-Dienstanbieter bereitgestellt wurde 438

Start der Web-/SaaS-App ist aufgrund einer ungültigen App-Zugriffsanforderung fehlgeschlagen 438

App-Start ist während der Richtlinienauswertung aufgrund eines internen Fehlers fehlgeschlagen 439

App-Start ist beim Parsen der Richtlinienauswertungsantwort fehlgeschlagen 439

Der App-Start ist während der Richtlinienauswertung mit einem ungültigen Ergebnis fehlgeschlagen 439

App-Start ist fehlgeschlagen aufgrund von ungültiger Ressourcenstandortkonfiguration 440

App-Start fehlgeschlagen, da der App-Name zu lang ist 441

App-Start ist während des Verbindungsaufbaus zum privaten TCP-Server aufgrund einer ungültigen App-ID fehlgeschlagen 441

App-Start wurde während der Richtlinienauswertung verweigert 441

App-Start ist fehlgeschlagen, da der Ziel-FQDN zu lang ist 441

App-Start aufgrund ungültiger Ziel-IP fehlgeschlagen 441

App-Start fehlgeschlagen, da keine Antwort von der Connector Appliance empfangen wurde 441

Anwendungsstart fehlgeschlagen aufgrund einer Anforderung an eine ungültige IP/einen ungültigen Hostnamen oder Port 442

Anwendungsstart fehlgeschlagen, da der Zielserver die Verbindung verweigerte 442

Anwendungsstart fehlgeschlagen, da das Ziel nicht gefunden wurde 442

Anwendungsstart fehlgeschlagen, da das Zielnetzwerk nicht erreichbar war 442

Anwendungsstart fehlgeschlagen aufgrund der Unfähigkeit, eine Verbindung zum Ziel herzustellen 442

Verbindung des Connectors zum Secure Private Access-Dienst fehlgeschlagen 443

Connector konnte die Proxy-Details nicht lesen 443

Konfigurierte Proxys sind nicht erreichbar 444

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connector Appliance kann FR (Edge-Knoten) nicht erreichen 444
Anwendungsstart fehlgeschlagen aufgrund eines internen Verbindungsfehlers 444
Start der Web-/SaaS-Anwendung fehlgeschlagen 445
Web-/SaaS-FormFill-SSO fehlgeschlagen aufgrund ungültiger Anwendungskonfiguration 445
Kerberos-SSO für Web/SaaS fehlgeschlagen 445
Web/SaaS-SSO aufgrund eines internen Serverfehlers fehlgeschlagen 446
Start der Web/SaaS-App fehlgeschlagen, da der konfigurierte Proxy nicht erreichbar ist 446
Start der Web/SaaS-App fehlgeschlagen, da die Authentifizierung mit dem konfigurierten Proxy fehlgeschlagen ist 446
Citrix Secure Access™ Client konnte SSO nicht durchführen 446
Sitzungscodes 447
Meldungscodes für die App-Aufzählung 447
Meldungscodes für den App-Start 449
Fehlercodes für den App-Start 450
Secure Private Access-Protokolle und -Ereignisse 453
Diagnose-Dashboard 453
Liste der Fehler 453
Audit-Protokolle 453
Systemprotokolle 453
Geräte-Posture-Protokolle 454
Diagnoseprotokolle 454
FAQ 454
Was sind Secure Private Access-Diagnoseprotokolle? 454
Wo finde ich Secure Private Access-Protokolle? 454
Welches Widget zeigt die Secure Private Access-Diagnoseprotokolle an? 454
Welche Details finde ich in den Diagnoseprotokollen von Secure Private Access? 455
Wie filtere ich die Diagnoseprotokolle? 456

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Welche Ereignisse werden in den Diagnoseprotokollen von Secure Private Access erfasst? 457
Liste der Fehler 458
Infocodes für Diagnoseprotokolle 458
Lösungsschritte 471
So erfassen Sie Client-Protokolle 501
FAQs 501
Referenzen 503
Audit- und Systemprotokolle 504
Gerätehaltungs-Protokolle und -Ereignisse 505
Gerätehaltungs-Dashboard in der Identity and Access Management-Konsole 506
Speicherort der Protokolle 507
Secure Private Access-Dashboard 507
Fehlerprotokolle der Gerätehaltung 508
Export von Gerätestatusdaten 508
Datenexporte und Integrationen von Drittanbietern 510
Sicherheitsinformations- und Ereignismanagement-Integration 510
Benutzerdefinierten Bericht mit OData-APIs erstellen 510
Systemprotokolle exportieren 511
Daten aus Kafka exportieren 511
Secure Private Access-Ereignisse 511
Device Posture-Dienstereignisse 511
Audit- und Systemprotokolle exportieren 512
Secure Private Access-Ereignisse mit der SystemLog-API exportieren 512
Sitzungsdaten mit OData exportieren 512
Rollenbasierte Zugriffssteuerung 514
Rollen und Berechtigungen 516
Rollenbasierten Zugriff für Administratoren aktivieren 518

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützung für Mehrsitzungs-Virtual-Desktop-Infrastruktur 520
Hauptmerkmale und Vorteile 520
Mehrsitzungs-VDI aktivieren 521
Citrix Secure Private Access für Mobilgeräte 523
Unterstützte Versionen und Plattformen 523
Unterstützte Funktionen 523
Voraussetzungen 524
Workflow für iOS- und Android-Benutzer mit Citrix Secure Access-Client 524
Verwandte Themen 525
Kerberos-Authentifizierung mit der iOS Kerberos-Erweiterung 525
iOS-Clientkonfiguration 525
Voraussetzungen 526
MDM-Registrierung auf dem iOS-Gerät überprüfen 526
MDM-Serverkonfiguration 526
Intune-Richtlinienkonfiguration 527
IIS-Konfiguration 530
Konfiguration auf der Domänencontrollerseite 532
Einstellung von Funktionen 534
Informationen zur Einstellung des clientlosen VPN-Zugriffs für den Web-App-Zugriff 535
Datengovernance 537
Datenresidenz 537
Datenerfassung 538
Datenübertragung 539
Datenkontrolle 539
Datenaufbewahrung 539
Datenexport 540
Definitionen 540
Produktzertifizierungen und Compliance 541

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zertifizierungen und Audits 541
Zertifikate und Auditberichte 542
index 543
Gateway Connector zu Connector Appliance migrieren 543
Übergeordnete Schritte zur Migration von Gateway Connector zu Connector Appliance 544
So installieren Sie Connector Appliance 544
FAQs 544
Routingtabellen zur Lösung von Konflikten, die aus denselben verwandten Domänen resultieren 545
Funktionsweise der Routingtabelle 545
Hauptroutingtabelle 546
Mini-Routentabelle 547
Routen zur Mini-Routentabelle hinzufügen 547
Einmaliges Anmelden beim Citrix Secure Access™ Client über die Citrix Workspace-App 549
Voraussetzungen 549
Funktionsanforderungen für Windows 550
ADFS-Integration mit Secure Private Access 550
Anspruchsanbieter-Vertrauen in ADFS hinzufügen 551
ID der Vertrauensstellung des Anspruchsanbieters 554
Bezeichner der vertrauenden Seite 555
Relay-Status im IdP-initiierten Fluss aktivieren 556
So aktivieren Sie den RelayState-Parameter auf Ihren ADFS-Servern 557
App-Konfiguration in Citrix Secure Private Access 557
IdP-initiierter Flow 557
SP-initiierter Flow 559
Citrix Secure Private Access™ 559
Hauptfunktionen von Citrix Secure Private Access 560
Secure Private Access REST-APIs 562
DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten 562

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Systemanforderungen 562
Funktionsaktivierung 563
Routing für DNS-Abfragen konfigurieren 563
G Suite konfigurieren 565
Jira konfigurieren 568
Citrix Gateway SaaS-Anwendung 568
O365 konfigurieren 577
Voraussetzungen 577
So funktioniert die Domänenföderation 579
Unterstützte Authentifizierungsmethoden für die Office 365-App 580
Konfigurieren der O365-App im Secure Private Access-Dienst 581
Konfigurieren der Domänenföderation von Microsoft Entra ID zu Citrix Workspace 582
Schritte zum Konfigurieren der Domänenföderation von Microsoft Entra ID zu Citrix Workspace 583
Automatisierte Domänenföderation von Microsoft Entra ID zu Citrix Workspace 585
Schritte zur automatischen Föderation einer Domäne 585
Multifaktor-Authentifizierung (MFA) unterdrücken 586
Konfigurieren einzelner Office-Suite-Anwendungen in Citrix Workspace 587
Drittanbieter-Apps, die in Microsoft Entra ID integriert sind 588
Referenzlinks 592
ERP Cloud konfigurieren 592
Citrix Gateway SaaS-Anwendung 592
ServiceNow konfigurieren 598
Tableau konfigurieren 607
Workday konfigurieren 609
Citrix Gateway SaaS-Anwendung 609
Zoom konfigurieren 611
Citrix Gateway SaaS-Anwendung 611

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Richtlinienerzwingung basierend auf dem Zugriffsmodus 614

Funktionsweise 614

Endbenutzererfahrung 615

Unterstützung für Server-zu-Client-Verbindungen – Vorschau 616

So funktioniert die Server-zu-Client-Verbindung 616

Eine Server-zu-Client-App erstellen 617

Voraussetzungen 617

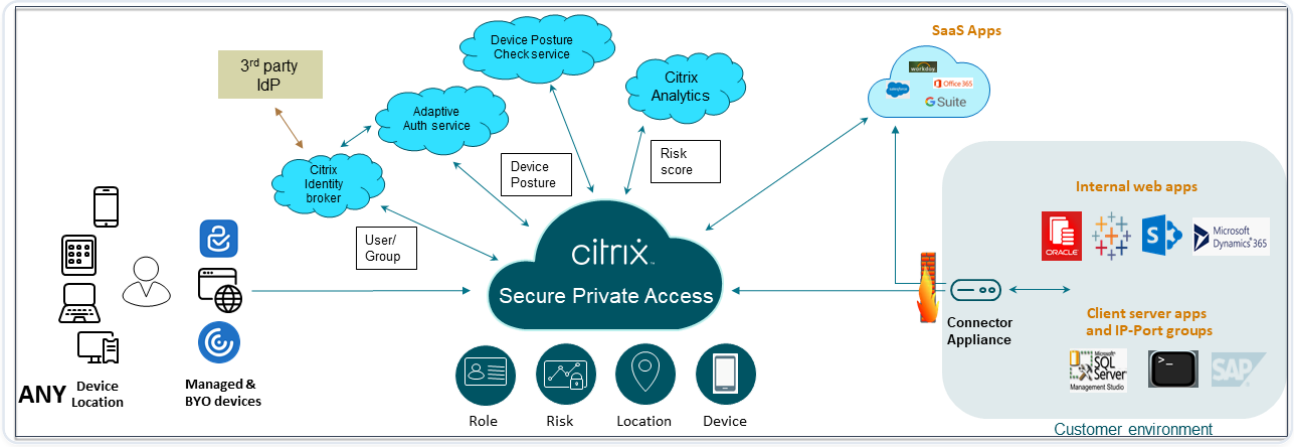
Führen Sie die folgenden Schritte aus, um Server-zu-Client-TCP/UDP-Apps zu konfigurieren 618

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Übersicht über die Secure Private Access-Dienstlösung

Herkömmliche VPN-Lösungen erfordern, dass Endbenutzergeräte verwaltet werden, bieten Zugriff auf Netzwerkebene und setzen statische Zugriffssteuerungsrichtlinien durch. Citrix Secure Private Access™ bietet der IT eine Reihe von Sicherheitskontrollen zum Schutz vor Bedrohungen durch BYO-Geräte und gibt Benutzern die Wahl, auf ihre von der IT genehmigten Anwendungen von jedem Gerät aus zuzugreifen, egal ob verwaltet oder BYO.

Citrix Secure Private Access bietet adaptive Authentifizierung, Single Sign-On-Unterstützung und erweiterte Sicherheitskontrollen für die Anwendungen. Secure Private Access bietet auch die Möglichkeit, das Endbenutzergerät vor dem 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 Authentifizierungsfluss für die aktuelle Anforderung. Die adaptive Authentifizierung kann den Gerätestatus, den geografischen Standort, das Netzwerksegment und die Benutzerorganisation/-abteilungszugehörigkeit identifizieren. Basierend auf den erhaltenen Informationen kann ein Administrator definieren, wie Benutzer für ihre von der IT genehmigten Apps authentifiziert werden sollen. Dies ermöglicht es Organisationen, denselben Authentifizierungsrichtlinien-Framework für jede Ressource zu implementieren, einschließlich öffentlicher SaaS-Apps, privater Web-Apps, privater Client-Server-Apps und Desktops as a Service (DaaS). Weitere Informationen finden Sie unter Adaptive Sicherheit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 eine lokal bereitgestellte Connector Appliance. Die Connector Appliance erstellt einen ausgehenden Steuerkanal 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. Weitere Informationen finden Sie unter Anwendungszugriff.

Single Sign-On

Mit der adaptiven Authentifizierung können Organisationen starke Authentifizierungsrichtlinien bereitstellen, um das Risiko kompromittierter Benutzerkonten zu reduzieren. Die Single Sign-On-Funktionen von Secure Private Access verwenden dieselben Richtlinien für die adaptive Authentifizierung für alle SaaS-, privaten Web- und Client-Server-Apps. Weitere Informationen finden Sie unter Single Sign-On.

Browsersicherheit

Secure Private Access ist in Google Chrome Enterprise Premium (CEP) integriert, das Funktionen wie Data Loss Prevention (DLP), Malware- und Phishing-Schutz sowie URL-Filterung umfasst. Der lokal auf dem Clientcomputer ausgeführte Google Chrome-Browser fungiert als sicherer Browser mit richtlinienbasierter Durchsetzung auf Benutzerebene über Chrome-verwaltete Profile. Weitere Informationen finden Sie unter Integration mit Google Chrome Enterprise Premium.

Gerätestatus

Der Gerätestatusdienst ermöglicht es einem Administrator, Richtlinien zu definieren, um den Status von Endpunktgeräten zu überprüfen, die versuchen, remote auf Unternehmensressourcen zuzugreifen. Basierend auf dem Compliance-Status eines Endpunkts kann der Gerätestatusdienst den Zugriff verweigern oder eingeschränkten/vollen Zugriff auf Unternehmensanwendungen und Desktops gewähren.

Wenn ein Endbenutzer eine Verbindung von seinem Store aus initiiert, sammelt der Device Posture-Client Informationen über die Endpunktparameter und teilt diese Informationen mit dem Device Posture-Dienst, um festzustellen, ob der Status des Endpunkts die Richtlinienanforderungen erfüllt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Unterstützung für TCP- und UDP-Anwendungen

Manchmal benötigen Remote-Benutzer Zugriff auf private Client-Server-Anwendungen, deren Frontend sich auf dem Endpunkt und deren Backend in einem Rechenzentrum befindet. Organisationen können zu Recht strenge Sicherheitsrichtlinien für diese internen und privaten Anwendungen durchsetzen, was es für Remote-Benutzer schwierig macht, auf diese Anwendungen zuzugreifen, ohne Sicherheitsprotokolle zu gefährden.

Der Secure Private Access-Dienst behebt die TCP- und UDP-Sicherheitslücken, indem er ZTNA ermöglicht, sicheren Zugriff auf diese Apps bereitzustellen. Benutzer können jetzt auf alle privaten Apps, einschließlich TCP-, UDP- und HTTPS-Apps, entweder über den Chrome-Browser oder eine native Client-Anwendung über den auf ihren Maschinen ausgeführten Citrix Secure Access™-Client zugreifen.

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

- Für Windows kann die Client-Version (22.3.1.5 und höher) von Downloads heruntergeladen werden.
- Für macOS kann die Client-Version (22.02.3 und höher) aus dem App Store heruntergeladen werden.

Weitere Informationen finden Sie unter Support für Client-Server-Apps.

Beispielanwendungsfälle

- Zugriff auf interne Anwendungen (Web/TCP/UDP) mit einem Zero-Trust-Ansatz, ohne eingehenden Datenverkehr an der Firewall zu öffnen
- Umstellung auf einen Zero-Trust-Ansatz durch Erkennung von Anwendungen, auf die Benutzer zugreifen
- Zugriff auf SaaS-Anwendungen auf unternehmenseigene öffentliche IP-Adressen beschränken
- Verbesserte Sicherheit für Azure-verwaltete SaaS-Apps
- Verbesserte Sicherheit für Office 365
- Verbesserte Sicherheit für Okta-Apps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Referenzartikel

- Einführung in Secure Private Access
- Technisches Briefing
- Referenzarchitektur
- Onboarding und Einrichtung von Secure Private Access

Referenzvideos

- Zero Trust Network Access (ZTNA) für Apps
- Privater Web-App-Zugriff mit Citrix Secure Private 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 Private Access
- Bildschirmfreigabeschutz mit Citrix Secure Private Access
- Endbenutzererfahrung mit Citrix Secure Private Access
- ZTNA im Vergleich zur VPN-Anmeldeerfahrung mit Citrix Secure Private Access
- ZTNA im Vergleich zu VPN-Port-Scans mit Citrix Secure Private Access

Was ist neu in verwandten Produkten

- Citrix StoreFront Cloud: Was ist neu
- Citrix DaaS: Was ist neu
- Citrix Secure Access: Citrix Secure Access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Was ist neu

30 September 2026

- **Erweiterte Datenregionalisierung für Secure Private Access für neue Kunden**

  Secure Private Access leitet jetzt Verwaltungs- und Datenverkehr für neue Kunden an die richtigen regionalen Daten-POPs und Endpunkte weiter. Weitere Informationen finden Sie unter Datenregionalisierung.

- **Zugriffsmodusbasierte Richtlinienerzwingung**

  Die zugriffsmodusbasierte Richtlinienerzwingung ermöglicht Administratoren, einzuschränken, wie ein Benutzer eine Verbindung zu einer Anwendung herstellt. Die Verbindung kann über einen browserbasierten Client oder den Citrix Secure Access-Client erfolgen. Weitere Informationen finden Sie unter Zugriffsmodusbasierte Richtlinienerzwingung.

03 September 2026

- **Benutzer- und Gruppendetails in Zugriffsrichtlinien, angezeigt nach Domäne, Gesamtstruktur und IdP-Typ:**

  Wenn Sie nach Benutzern oder Gruppen nach Anzeigename, E-Mail-ID oder Benutzerprinzipalname suchen, werden die von Ihnen ausgewählten Benutzer und Gruppen in einem Raster angezeigt. Jede Zeile zeigt die Identitätsdetails an, wie Name, E-Mail-Adresse, IdP-Typ, OID und Domäne. Sie können gleichnamige Benutzer oder Gruppen über verschiedene Domänen, Gesamtstrukturen oder Identitätsanbieter (IdPs) hinweg klar unterscheiden. Details finden Sie unter Erstellen einer Zugriffsrichtlinie mit mehreren Regeln.

- **Verwandte Domänen mithilfe einer HAR-Datei ermitteln:**

  Secure Private Access ermöglicht Ihnen jetzt das Hochladen einer HAR-Datei, um die von einer Anwendung aufgerufenen Domänen automatisch zu ermitteln. Sie können die ermittelten Domänen überprüfen und diejenigen auswählen, die Sie der Konfiguration der verwandten Domänen der Anwendung hinzufügen möchten. Dies vereinfacht das Anwendungs-Onboarding, da die manuelle Identifizierung und Konfiguration verwandter Domänen reduziert

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wird. Weitere Informationen finden Sie unter Verwandte Domänen mithilfe einer HAR-Datei ermitteln.

- **Chrome Enterprise Premium (CEP)-Konfigurationen auf Organisationseinheiten von Google Directory anwenden:**

  Zusätzlich zu allen Benutzern und Google Directory-Benutzergruppen können Sie jetzt eine CEP-Konfiguration auf ausgewählte Organisationseinheiten von Google Directory anwenden. Weitere Informationen finden Sie unter CEP für Organisationseinheiten von Google Directory konfigurieren.

- **Unterstützung für bedingte Authentifizierung:**

  Single Sign-On (SSO) für Chrome Enterprise Premium (CEP), das Citrix Cloud als OpenID Connect (OIDC)-Authentifizierungsanbieter verwendet, unterstützt jetzt die bedingte Authentifizierung. Weitere Informationen finden Sie unter Open ID Connect mit Citrix Identity and Access Management.

- **Benutzerattributtyp einrichten:**

  Sie können jetzt Benutzerattribute über die Seite „Verwaltete Profilidentität“ in der Secure Private Access-Administratorkonsole einrichten. Weitere Informationen finden Sie unter Verwaltete Profilidentität.

- **Benutzer- und Gruppensynchronisierung überprüfen:**

  Bei der Auswahl von Benutzern oder Gruppen können Administratoren überprüfen, ob Einträge aus dem ausgewählten Benutzerverzeichnis mit Google Directory synchronisiert und dort korrekt konfiguriert sind. Secure Private Access-Richtlinien werden nur dann korrekt ausgewertet, wenn die Benutzer und Gruppen synchronisiert sind. Weitere Informationen finden Sie unter Benutzer- und Gruppensynchronisierung überprüfen.

- **Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung:**

  Wenn Sie eine Anwendung löschen, bereinigt Secure Private Access nun auch die Routing-Einträge. Weitere Informationen finden Sie unter Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung.

19 August 2026

- **Unterstützung von Google Cloud Identity für Chrome Enterprise Premium (CEP)**

  Google Cloud Identity kann jetzt als Identitätsanbieter mit CEP verwendet werden. Wenn Google Cloud Identity Ihr Identitätsanbieter ist, befinden sich Benutzer und Gruppen nativ im

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Cloud-Verzeichnis, sodass keine Verzeichnis-Korrelation erforderlich ist. Details finden Sie unter Voraussetzungen für die integrierte Lösung.

05 August 2026

- **Neue Routing-Methode für den Zugriff auf SaaS-Anwendungen:**

  Sie können den Routing-Typ einer SaaS-App jetzt entweder auf **Extern über Google Secure Gateway** festlegen, um den Datenverkehr über Google Secure Gateway zu leiten, oder auf **Extern**, um den Datenverkehr direkt vom Client zur App zu leiten. Details finden Sie unter Eine SaaS-App konfigurieren.

31 July 2026

- **Citrix Secure Access-Steuerelemente für Chrome Enterprise:**

  Citrix Secure Private Access unterstützt Sicherheitsrichtlinien, die von der Citrix Secure Access-Erweiterung für Google Chrome Enterprise Premium (CEP) bereitgestellt und durchgesetzt werden.

  Die folgenden Richtlinien werden von Secure Private Access unterstützt.

  - Anti-Keylogging
  - Zwischenablage-Container
  - Domänensuffix für Webanwendungen
  - Sitzungsaufzeichnung
  - Browser-Sitzungs-Reauthentifizierung

24 June 2026

- **Unterstützung für die Konfiguration von Egress-Hub-Regionen:**

  Secure Private Access ermöglicht Administratoren die Auswahl der Egress-Regionen, die Chrome Enterprise Premium für den SaaS-Anwendungsverkehr verwendet. Jede ausgewählte Region bietet einen dedizierten Satz von Egress-IP-Adressen, die Administratoren zu ihren Zulassungslisten für SaaS-Anwendungen hinzufügen können, um den über Google Secure Gateway geleiteten Datenverkehr zuzulassen. Diese Funktion ist sowohl für Cloud- als auch für Hybridbereitstellungen verfügbar. Weitere Informationen finden Sie unter Egress-Hub-Regionen konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Entfernung der Abhängigkeit von der citrix-schema-Synchronisierung für Google Directory:**

  Die Abhängigkeit von der Citrix-Schema-Synchronisierung für Google Directory in Chrome Enterprise Premium wurde entfernt. Die Google Directory-Synchronisierung kann nun mithilfe von Benutzer-E-Mail-IDs durchgeführt werden. Um diese Funktion zu aktivieren, wenden Sie sich an den Citrix Support.

- **SAML 2.0-Authentifizierungsunterstützung für OIDC:**

  SAML 2.0-Identitätsanbieter (IdPs) werden jetzt für OIDC unterstützt. Weitere Informationen zur OIDC-Integration mit Citrix Identity finden Sie unter OpenID Connect mit Citrix Identity.

18 June 2026

- **Primäre und sekundäre Ressourcenstandorte während des CSV-basierten Anwendungsimports definieren:**

Der Anwendungsimport über die CSV-Datei ermöglicht Administratoren nun, sowohl primäre als auch sekundäre Ressourcenstandorte während der Massenerstellung von Anwendungen zu definieren. Dies ermöglicht ein effizientes Onboarding für Unternehmensbereitstellungen, die an verschiedenen Standorten betrieben werden. Weitere Informationen finden Sie unter Anwendungsimport-Tool.

09 June 2026

Die folgenden Abschnitte enthalten weitere Informationen zur 09 June 2026 Version.

Wichtiger Hinweis

- **Citrix Secure Private Access™ Edge-Konfigurationsaktualisierung:**

  Im Rahmen der laufenden Leistungs- und Infrastrukturoptimierungen für Citrix Secure Private Access werden in Kürze bestimmte Citrix Secure Private Access Edge-Konfigurationsaktualisierungen bereitgestellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Diese Benachrichtigung ist **nur** für Kunden bestimmt, die möglicherweise spezifische FQDN-Zulassungslisten auf PoP-Ebene auf Firewall- oder Proxy-Ebene oder benutzerdefinierte Einträge außerhalb der dokumentierten Empfehlungen eingerichtet haben.

Was sich ändert:

Die Citrix Secure Private Access Edge-FQDNs werden auf ein neues Format aktualisiert, wie unten gezeigt:

Alte FQDN: `<pop>-rdvz.g.nssvc.net`

Neue FQDN: `<pop>-spa-rdvz.g.nssvc.net`

Beispiele:

`az-us-e-rdvz.g.nssvc.net` ändert sich zu `az-us-e-spa-rdvz.g.nssvc.net`

`az-eu-w-rdvz.g.nssvc.net` ändert sich zu `az-eu-w-spa-rdvz.g.nssvc.net`

Muss ich Maßnahmen ergreifen:

- **Keine Maßnahmen erforderlich:** Wenn Sie die empfohlene Wildcard-Domäne verwenden (zum Beispiel `*.nssvc.net`), sind sowohl die alten als auch die neuen Namen bereits abgedeckt, und es sind keine Maßnahmen erforderlich. Weitere Informationen finden Sie unter Connector Appliance for Secure Private Access.
- **Maßnahmen erforderlich:** Wenn Sie explizite FQDN-Zulassungslisten auf PoP-Ebene oder benutzerdefinierte Einträge verwenden, die außerhalb der dokumentierten Empfehlungen liegen, führen Sie die erforderlichen Maßnahmen durch.

Erforderliche Maßnahmen:

Kunden, die ausgehenden Datenverkehr zu bestimmten PoPs zulassen, müssen ihre Firewall-Regeln aktualisieren. Fügen Sie für jeden derzeit zugelassenen `<pop>-rdvz.g.nssvc.<suffix>`-Eintrag den entsprechenden `<pop>-spa-rdvz.g.nssvc.<suffix>`-Datensatz hinzu, um einen unterbrechungsfreien Dienst zu gewährleisten. Eine Liste der PoPs finden Sie unter Points of Presence (PoPs) locations for Citrix Secure Private Access service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

20 May 2026

- **Datenregionalisierung**

  Die Datenregionalisierung in Citrix Secure Private Access ermöglicht es Kunden, zu steuern, wo ihre Daten gespeichert werden, indem sie eine bevorzugte geografische Region auswählen. Kunden können die Region auswählen, in der ihre Daten gespeichert werden, mit Optionen wie Global, Europa (EU), APAC (Asien-Pazifik) und Nordamerika (NA). Alle Konfigurationsdaten im Ruhezustand verbleiben innerhalb der ausgewählten Region, wodurch sichergestellt wird, dass sie das festgelegte geografische Gebiet nicht verlassen. Weitere Informationen finden Sie unter Data regionalization.

28 April 2026

- **Vereinfachte Konfiguration des Secure Private Access-Dienstes**

  Die Konfiguration des Secure Private Access-Dienstes wurde zu einem einzigen, vereinheitlichten Workflow optimiert. Die Seite „Systemkonfiguration“ enthält jetzt ein Topologiediagramm, das die in einer Secure Private Access-Cloud-Bereitstellung verwendeten Komponenten zeigt. Administratoren können Connector Appliance und Google Chrome Enterprise Premium direkt von dieser Seite aus konfigurieren. Weitere Informationen finden Sie unter Secure Private Access onboarding and set up.

- **Obligatorische Google-Administratorberechtigungen für Telemetriezwecke**

  Ein neuer Satz von Berechtigungen muss dem Dienstkonto in der Google Admin Console zugewiesen werden. Diese Berechtigungen werden hauptsächlich für Telemetriezwecke verwendet (zum Beispiel DLP-Aktivitätsereignisse und Sicherheitswarnungen). Weitere Informationen finden Sie unter Setup Google Chrome integration.

- **Okta IdP-Unterstützung für CEP**

  Okta kann jetzt als Identitätsanbieter mit Chrome Enterprise Premium (CEP) verwendet werden. Weitere Informationen finden Sie unter „Citrix OIDC-Client erstellen“. Weitere Informationen finden Sie unter Create a Citrix OIDC client.

07 April 2026

- **Auflistung der fünf meistgenutzten Vorlagen zur Vereinfachung und Beschleunigung des App-Onboardings**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Abschnitt **Vorlage auswählen** auf der Anwendungskonfigurationsseite listet jetzt die fünf meistgenutzten Vorlagen zur Vereinfachung und Beschleunigung des App-Onboardings auf. Weitere Informationen finden Sie unter SaaS-App konfigurieren.

04 March 2026

- **Übergang der Secure Private Access Admin-UI-Domäne zu secureaccess.cloud.com**

  Die Secure Private Access Admin-UI-Domäne wurde jetzt auf `secureaccess.cloud.com` aktualisiert. Ihre aktuelle URL funktioniert weiterhin und wird automatisch auf die neue Domäne umgeleitet. Es sind keine Maßnahmen oder Konfigurationsänderungen erforderlich.

12 February 2026

- **Portbasiertes Routing mithilfe von Routing-Ausnahmen**

  Die Funktion für portbasiertes Routing ermöglicht Administratoren, den Datenverkehr für verschiedene Ports desselben Ziels für TCP/UDP-Anwendungen mithilfe von Routing-Ausnahmen unterschiedlich weiterzuleiten. Weitere Informationen finden Sie unter Portbasiertes Routing mithilfe von Routing-Ausnahmen.

05 February 2026

- **Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium**

  Der gestufte Migrationsansatz von Citrix Enterprise Browser zu Chrome Enterprise Premium ermöglicht es Unternehmen, die Geschäftskontinuität während der Übergangszeit aufrechtzuerhalten, indem beide Browserlösungen parallel ausgeführt werden. Mit der gestuften Migration können Kunden die Kompatibilität bestehender Anwendungen und Workflows mit Chrome Enterprise Premium überprüfen. Weitere Informationen finden Sie unter Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium.

- **Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen**

  Das Google-Verzeichnis erfordert eine verifizierte E-Mail-Adresse für alle Benutzer- und Gruppenobjekte. Dies ist jedoch nicht immer für Verzeichnisse verfügbar, die von Secure Private Access unterstützt werden, insbesondere Active Directory (AD) und Microsoft Entra ID. AD- und Microsoft Entra ID-Objekte verfügen möglicherweise nicht über eine E-Mail-Adresse oder haben eine, die auf eine interne oder spezielle Domäne verweist (z. B. @fabrikam.onmicrosoft.com), die das Google-Verzeichnis nicht überprüfen kann.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Da die E-Mail-Adresse normalerweise als gemeinsamer Bezeichner zwischen Secure Private Access und dem Google-Verzeichnis dient, werden Gruppen aus AD/Entra ohne eine verifizierte Google-E-Mail-Adresse in der Regel nicht für Secure Private Access-Richtlinien unterstützt. Die Funktion Domänenzuordnung löst dies, indem sie Administratoren ermöglicht, Richtlinien für Gruppen zu konfigurieren, auch wenn sie keine E-Mail-Adresse haben oder eine E-Mail-Adresse mit einer nicht verifizierten Domäne haben. Weitere Informationen finden Sie unter Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen.

18 December 2025

- **Sicherer Zugriff auf SSH- und RDP-Anwendungen im Browser**

  Citrix Secure Private Access ist in Chrome Enterprise Premium integriert, um sichere SSH- und RDP-Sitzungen direkt im Browser zu ermöglichen. Weitere Informationen finden Sie in den folgenden Themen:

  - Sicherer Zugriff auf SSH-Anwendungen im Browser
  - Sicherer Zugriff auf RDP-Anwendungen im Browser

16 December 2025

- **DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten**

  Administratoren können DNS-Abfragen für bestimmte Anwendungen direkt an ihre dedizierten Ressourcenstandorte weiterleiten. Dies ermöglicht eine genauere DNS-Auflösung, intelligentes Traffic-Management und eine bessere Benutzererfahrung. Weitere Informationen finden Sie unter DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten.

11 December 2025

- **Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium**

  Bestehende Secure Private Access-Dienstkunden können schrittweise von Citrix Enterprise Browser zu Chrome Enterprise Premium (CEP) migrieren. Dieser schrittweise Migrationsansatz ermöglicht es Unternehmen, die Geschäftskontinuität während der Übergangsphase aufrechtzuerhalten, indem beide Browserlösungen parallel betrieben werden. Mit der schrittweisen Migration können Kunden die Kompatibilität bestehender Anwendungen und Workflows mit Chrome Enterprise Premium überprüfen. Weitere Informationen finden Sie unter Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

30 October 2025

- **Allgemeine Verfügbarkeit der agentenlosen Zugriffsversion von Citrix Secure Private Access mit Chrome Enterprise-Lösung**

  Mit der Integration von Citrix Secure Private Access™ in Google Chrome Enterprise Premium können Endbenutzer jetzt sicher auf private Web- und SaaS-Anwendungen zugreifen, indem sie den Google Chrome-Browser als ihren Unternehmensbrowser verwenden, ohne einen Zero Trust Network Access (ZTNA)-Agenten zu benötigen, und einen pro-Anwendung-Zugriff mit Data Loss Prevention (DLP)-Kontrollen, Webfilterung und ZTNA-Richtliniendurchsetzung erreichen. Weitere Informationen finden Sie unter Integration von Citrix Secure Private Access mit Google Chrome Enterprise Premium.

  Empfehlungen für aktuelle Secure Private Access / Citrix Enterprise Browser-Kunden mit einem Produktionstenant

  Wir empfehlen bestehenden Produktionskunden, die agentenlose Zugriffsversion in einem separaten Tenant anstatt in ihrem Produktionstenant zu testen. Ein für Ende November 2025 geplantes Produktupdate wird Verbesserungen enthalten, die es bestehenden Secure Private Access-Kunden ermöglichen, die agentenlose Zugriffsfunktionalität zu nutzen, während ihre vorhandenen App-Konfigurationen und Zugriffsrichtlinien beibehalten werden. Die Version vom November 2025 wird auch eine Benutzeroberfläche bereitstellen, die es bestehenden Secure Private Access-Kunden ermöglicht, ihre App-Starts für aktuelle Web- und SaaS-Apps (derzeit über Citrix Enterprise Browser gestartet) für den Start im Chrome-Browser zu migrieren.

  Kunden, die diese Version vor dem Update vom November 2025 verwenden möchten, müssen ihre bestehenden Secure Private Access-Tenants auf einen sauberen Zustand zurücksetzen und die Kunden dann erneut für den Secure Private Access-Dienst onboarden. Führen Sie die folgenden Schritte aus:

  a. Löschen Sie alle Zugriffsrichtlinien, Apps und zugehörigen Domänen in der Secure Private Access-Konsole.
  b. Kehren Sie zur Secure Private Access-Kachel in der Citrix Cloud-Konsole zurück.
  c. Wählen Sie **Fully Cloud-delivered Service architecture** und klicken Sie dann auf **Weiter**. Einzelheiten finden Sie unter Secure Private Access-Onboarding und -Einrichtung.

17 September 2025

- **Secure Private Access-Unterstützung für iOS-Geräte**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access wird jetzt für mobile Geräte ab Secure Access Client Version 25.08.1 für iOS unterstützt. Mobile Benutzer können von ihren iOS-Geräten auf Unternehmensanwendungen zugreifen. Einzelheiten finden Sie unter Citrix Secure Private Access für mobile Geräte.

13 August 2025

- **Benutzerdefinierte Store-URLs für den Zugriff auf Apps über Citrix Enterprise Browser™**

  Die Funktion für benutzerdefinierte Store-URLs ermöglicht es Organisationen, Benutzern den Zugriff auf SaaS- und private Webanwendungen über eine gebrandete, unternehmenseigene Domäne (z. B. workspace.company.com) anstelle der Standarddomäne *.cloud.com zu ermöglichen.

- **Verbesserungen am Richtlinienmodellierungstool**

  Das Richtlinienmodellierungstool zeigt jetzt den Routing-Typ und den spezifischen Richtlinientyp an, die die Routing-Entscheidungen einer Anwendung beeinflussen. Diese Verbesserung hilft Administratoren bei der Fehlerbehebung von Routing-Problemen und bei der Überprüfung, ob Anwendungen den konfigurierten Richtlinien entsprechen. Einzelheiten finden Sie unter Richtlinienmodellierungstool.

14 July 2025

- **Überwachen und Beheben von Problemen mit agentenlosen Secure Private Access-Apps in Monitor**

  Administratoren und Helpdesk-Mitarbeiter können jetzt agentenlose App-Sitzungen und -Ereignisse von Secure Private Access in Monitor überwachen und Fehler beheben. Weitere Informationen finden Sie unter Secure Private Access-Integration mit Monitor.

- **Unterstützung von Server-zu-Client-Verbindungen für UDP-Anwendungen**

  Server-zu-Client-Verbindungen werden jetzt zusätzlich zu TCP-Anwendungen auch für UDP-Anwendungen unterstützt. Die Server am Ressourcenstandort des Kunden können eine UDP-Verbindung mit dem Remote-Client herstellen. Weitere Informationen finden Sie unter Unterstützung für Server-zu-Client-Verbindungen.

- **Neue rollenbasierte Zugriffssteuerungsrollen für Helpdesk-Personas**

  Die folgenden Rollen stehen Secure Private Access-Administratoren zusätzlich zu den Rollen „Administrator mit Vollzugriff“ und „Administrator mit Lesezugriff“ zur Verfügung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Vollständiger Monitor-Administrator
- Helpdesk-Administrator

Weitere Informationen finden Sie unter Rollenbasierte Zugriffssteuerung.

- **UDP-DNS-Abfragen an den anwendungsspezifischen Ressourcenstandort weiterleiten**

  Die UDP-DNS-Abfragen für bestimmte Hostnamen können jetzt direkt an den Ressourcenstandort weitergeleitet werden, an dem die entsprechende Anwendung gehostet wird. Dieses Routing verbessert die Anwendungsleistung, indem sichergestellt wird, dass DNS-Abfragen den relevantesten Ressourcenstandort erreichen. Zuvor wurden alle UDP-DNS-Abfragen standardmäßig an den geografisch nächstgelegenen Ressourcenstandort weitergeleitet, unabhängig vom tatsächlichen Standort der Anwendung.

  So funktioniert's:

  a. Das Routing von UDP-DNS-Abfragen an den anwendungsspezifischen Ressourcenstandort ist standardmäßig deaktiviert. Um diese Funktionalität zu aktivieren, wenden Sie sich an den Citrix Support.
  b. Sobald die Funktion aktiviert ist, wird die DNS-Abfrage an Secure Private Access weitergeleitet, um den spezifischen Ressourcenstandort zu identifizieren, der der Anwendung zugeordnet ist. Basierend auf der Antwort von Secure Private Access wird die DNS-Abfrage dann an den dedizierten Ressourcenstandort der Anwendung weitergeleitet.
  c. Falls kein anwendungsspezifischer Ressourcenstandort identifiziert wird, greift die Abfrage auf den nächstgelegenen verfügbaren Ressourcenstandort zurück.

03 June 2025

- **Zertifikate in der Secure Private Access-Konsole verwalten**

  Der Zertifikatsspeicher von Secure Private Access bietet Administratoren jetzt einen zentralen Ort zur effizienten Verwaltung von Zertifizierungsstellen- (CA) und Secure Sockets Layer- (SSL) Zertifikaten. Dieser dedizierte Speicher vereinfacht die Zertifikatsverwaltung, indem er Administratoren ermöglicht, nahtlos neue Zertifikate hinzuzufügen, bestehende zu ändern und nicht mehr benötigte zu entfernen. Einzelheiten finden Sie unter Zertifikate in der Secure Private Access-Konsole verwalten.

15 May 2025

- **Integration von Citrix Secure Private Access™ mit Google Chrome Enterprise Premium**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Integration von Citrix Secure Private Access mit Google Chrome Enterprise Premium ermöglicht es Kunden, Google Chrome Enterprise Premium als Enterprise-Browserlösung für den sicheren Zugriff auf private Web-Apps und SaaS-Anwendungen zusammen mit der von Citrix Secure Private Access bereitgestellten sicheren Konnektivität zu nutzen. Einzelheiten finden Sie unter Integration von Citrix Secure Private Access mit Google Chrome Enterprise Premium.

24 April 2025

- **Unterstützung für hybride Datenpfade**

  Der hybride Datenpfad für den Secure Private Access-Dienst nutzt sowohl lokale als auch Cloud-Infrastrukturen, um sicheren Zugriff auf Anwendungen zu ermöglichen. Organisationen können den hybriden Datenpfad verwenden, um den gesamten Datenverkehr über ein lokales NetScaler Gateway zu leiten. Einzelheiten finden Sie unter Hybrid-Datenpfad für den Secure Private Access-Dienst.

- **Anzeige kontextbezogener Routing-Einblicke in Monitor**

  Kontextbezogenes Routing kann zu dynamischen Änderungen der Anwendungsrouten führen. Beispielsweise könnte eine Anwendung über den Secure Private Access-Dienst geleitet werden, wenn der Benutzer sich außerhalb des Unternehmensnetzwerks befindet, aber direkt zur App, wenn der Benutzer intern ist. Administratoren Einblicke in diese Routing-Entscheidungen zu geben, ist entscheidend für die Behebung von Routing-Problemen. Einzelheiten finden Sie unter Kontextbezogene Routing-Einblicke in Monitor.

- **Backup-Ressourcenstandorte konfigurieren**

  Administratoren können die Hochverfügbarkeit von Anwendungen auch bei Störungen sicherstellen, indem sie einen sekundären Ressourcenstandort konfigurieren oder die Option „Erster verfügbarer“ verwenden. Einzelheiten finden Sie in den folgenden Themen:

  - Unterstützung für Enterprise-Web-Apps
  - Agentenloser Zugriff auf Enterprise-Web-Apps
  - Unterstützung für Software-as-a-Service-Apps
  - Unterstützung für Client-Server-Apps

- **IP-Adresspools sofort oder schrittweise im Laufe der Zeit löschen**

  Es wurde Unterstützung hinzugefügt, um IP-Adresspools sofort oder im Laufe der Zeit mithilfe einer der folgenden Optionen zu löschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **IP-Pool zwangsweise löschen:** Die Zuweisung von IP-Adressen an neue Benutzer wird beendet und ungenutzte IP-Adressen werden sofort freigegeben. Aktive Benutzersitzungen, die die gelöschten IP-Adressen verwenden, können beendet werden, was zu abrupten Schließungen und erzwungenen Abmeldungen führt. Benutzern mit beendeten Sitzungen werden erst dann neue IP-Adressen zugewiesen, wenn ein anderer IP-Adresspool erstellt wurde.
- **IP-Pool im Laufe der Zeit löschen:** Die Zuweisung von IP-Adressen an neue Benutzer wird beendet und ungenutzte IP-Adressen werden sofort freigegeben. Das System wartet, bis die aktiven Sitzungen abgemeldet oder abgelaufen sind, bevor der Pool vollständig gelöscht wird. Benutzern mit beendeten Sitzungen werden erst dann neue IP-Adressen zugewiesen, wenn ein anderer IP-Adresspool erstellt wurde.

Weitere Informationen finden Sie unter IP-Adresspool löschen.

22 April 2025

- **Anwendungen mithilfe der nsconfig-Datei importieren**

  Die Secure Private Access-Administratorkonsole enthält ein Dateiimport-Tool, das Administratoren ermöglicht, mehrere Anwendungen in großen Mengen in das System mithilfe der nsconfig-Datei zusätzlich zur CSV-Datei zu importieren. Dieses Tool ist besonders nützlich für Organisationen, die von einem herkömmlichen VPN zu einer fortschrittlicheren Lösung wie Secure Private Access wechseln. Weitere Informationen finden Sie unter Anwendungsimport-Tool.

  Die Funktion zum Importieren von Anwendungen mithilfe der nsconfig-Datei befindet sich in der Vorschau.

20 February 2025

- **Verbesserungen an der Admin-Audit-Logging-Funktion**

  Die Admin-Audit-Logging-Funktion wurde erweitert, um detaillierte Protokolle aller Administratoraktionen innerhalb des Secure Private Access-Dienstes zu erfassen. Weitere Informationen finden Sie unter Audit-Protokolle.

- **Benutzer basierend auf UPN und E-Mail-Adresse suchen und hinzufügen**

  Sie können jetzt Benutzer in Secure Private Access basierend auf der UPN und E-Mail-Adresse zusätzlich zum Anzeigenamen suchen und hinzufügen. Diese Suchoption ermöglicht es Administratoren, den richtigen Benutzer genau zu identifizieren und ihm Zugriff zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

gewähren, selbst wenn dieser mehrere Konten hat. Weitere Informationen finden Sie unter Zugriffsrichtlinie konfigurieren.

08 January 2025

- **Sitzungen dynamisch über Sitzungsrichtlinien weiterleiten**

  Administratoren können Sitzungsrichtlinien konfigurieren, um interne Unternehmensbenutzer direkt an Back-End-Anwendungen weiterzuleiten, ohne den Datenverkehr über Secure Private Access zu tunneln. Sitzungsrichtlinien bieten dynamisches Routing basierend auf Faktoren wie Netwerkstandort und Gerätehaltung. Weitere Informationen finden Sie unter Interne Unternehmensbenutzer direkt an Back-End-Anwendungen weiterleiten.

07 January 2025

- **Unterstützung für Connector-Stickiness**

  Secure Private Access unterstützt Connector-Stickiness. Connector-Stickiness stellt sicher, dass, nachdem ein Client eine Verbindung mit der Connector Appliance hergestellt hat, alle nachfolgenden Anfragen desselben Clients an dieselbe Quelle (Connector Appliance) geleitet werden. Weitere Informationen finden Sie unter Connector-Stickiness.

- **Unterstützung für Client-IP-Adress-Stickiness**

  Secure Private Access unterstützt Client-IP-Adress-Stickiness. Client-IP-Adress-Stickiness stellt sicher, dass Anfragen von einer bestimmten Client-IP-Adresse konsistent an denselben Back-End-Server weitergeleitet werden. Weitere Informationen finden Sie unter Client-IP-Adress-Stickiness.

  Die Funktion Client-IP-Adress-Stickiness befindet sich in der Vorschau.

- **Unterstützung für die Erstellung interner Client-IP-Adresspools**

  Es wurde Unterstützung für die Erstellung interner Client-IP-Adresspools hinzugefügt. Diese IP-Adresspools sind unerlässlich, um einem Benutzer und dem zugehörigen Gerät eine eindeutige IP-Adresse zuzuweisen, um die folgenden Anwendungsfälle zu unterstützen:

  - Server-zu-Client-Verbindungen
  - Unterstützung für Client-IP-Adress-Stickiness

  Weitere Informationen finden Sie unter Interne Client-IP-Adresspools.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Die Funktion für interne IP-Adresspools des Clients befindet sich in der Vorschauphase. Um diese Funktion zu aktivieren, wenden Sie sich an den Citrix Support.

- **Unterstützung für Server-zu-Client-Verbindungen**

  Secure Private Access unterstützt Server-zu-Client-Verbindungen, wobei die Server am Ressourcenstandort des Kunden eine TCP-Verbindung mit dem Remote-Client herstellen können. Um die Server-zu-Client-Verbindung zu ermöglichen, führt Secure Private Access die Server-zu-Client-App ein. Diese App kann mit den Client-Details (Port, Protokoll) und dem IP-CIDR-Bereich des Back-End-Servers konfiguriert werden. Weitere Informationen finden Sie unter Unterstützung für Server-zu-Client-Verbindungen.

  Die Unterstützung für Server-zu-Client-Apps befindet sich in der Vorschauphase.

02 January 2025

- **CSV-basiertes Importtool für Anwendungen**

  Die Secure Private Access-Administratorkonsole enthält ein CSV-basiertes Importtool, das Administratoren ermöglicht, mehrere Anwendungen mithilfe einer CSV-Datei in großen Mengen in das System zu importieren. Dieses Tool ist besonders nützlich für Organisationen, die von einem herkömmlichen VPN zu einer fortschrittlicheren Lösung wie Secure Private Access wechseln. Weitere Informationen finden Sie unter CSV-basiertes Importtool für Anwendungen.

03 December 2024

- **Secure Private Access-Unterstützung für Cloud-gehostete Multi-Session-VDIs**

  Der Citrix Secure Access-Client für Windows unterstützt jetzt die Verwendung von Secure Private Access, um Zero-Trust-Zugriff auf Unternehmensressourcen von Cloud-gehosteten Multi-Session-VDIs zu ermöglichen. Weitere Informationen finden Sie unter Unterstützung für Multi-Session Virtual Desktop Infrastructure.

25 November 2024

- **Secure Private Access-Sitzungscodes in DaaS Monitor**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Secure Private Access-Sitzungsbezogenen Codes werden jetzt in DaaS Monitor angezeigt. Eine Liste der Codes finden Sie unter Secure Private Access-Sitzungsbezogene Codes in Monitor.

14 November 2024

- **Verbesserungen am Richtlinienmodellierungstool**

  Administratoren können jetzt eine umfassende Liste der mit jeder Anwendung verknüpften Richtlinien anzeigen und die Drilldown-Funktion nutzen, um die spezifische Anwendungslogik der Richtlinie zu verstehen, warum eine bestimmte Richtlinie angewendet wurde und andere nicht. Weitere Informationen finden Sie unter Drilldown in Zugriffsrichtlinien.

08 November 2024

- **Integration von Secure Private Access mit Monitor**

  Secure Private Access ist in Monitor integriert, die Überwachungs- und Fehlerbehebungskonsole für Citrix DaaS. Administratoren und Helpdesk-Mitarbeiter können Web/SaaS- und TCP/UDP-App-Sitzungen und -Ereignisse über den DaaS Monitor überwachen und Fehler beheben. Weitere Informationen finden Sie unter Integration mit DaaS Monitor.

07 November 2024

- **Verbesserungen an der grafischen Benutzeroberfläche von Secure Private Access**

  Der Secure Private Access-Dienst bietet jetzt eine verbesserte grafische Benutzeroberfläche (GUI) für eine bessere Benutzererfahrung. Die primäre Menübaumstruktur wird durch eine Hover-Anzeigefunktion für eine einfachere Navigation ersetzt. Sekundäre Menüelemente werden beim Darüberfahren angezeigt und zeigen ein Untermenü für eine schnellere Auswahl.

  Sie können das gesamte Menü auch durch Klicken auf das Symbol reduzieren oder erweiternieren.

23 September 2024

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

  Die dynamische Domänenrouting-Konfiguration in der Zugriffsrichtlinie ermöglicht es Administratoren nun, den internen Routing-Typ pro URL basierend auf dem Benutzerkontext zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bearbeiten. Administratoren können die Ressourcenstandorte ändern, sodass die Benutzeranfragen an das optimale Rechenzentrum weitergeleitet werden, wodurch sichergestellt wird, dass Benutzeranfragen effizient bearbeitet und die Leistung optimiert wird. Weitere Informationen finden Sie unter Kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten.

15 August 2024

- **Option zur Konfiguration einer Zeitdauer für das Löschen der Einträge in der Liste der blockierten Benutzer**

  Administratoren können jetzt eine bestimmte Dauer (1 bis 99 Tage) für das Löschen der Einträge in der Liste der blockierten Benutzer festlegen. Weitere Informationen finden Sie unter Aktive Benutzersitzungen beenden und Benutzer zur Benutzerblockierungsliste hinzufügen.

- **Zusätzliche Sicherheitskontrollen**

  Die folgenden zusätzlichen Sicherheitskontrollen sind jetzt zur Einschränkung des Anwendungszugriffs verfügbar.

  - Mikrofon
  - Webcam
  - Benachrichtigungen
  - Pop-ups
  - Unsichere Inhalte

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

  Die Funktion für nicht genehmigte Websites (Webfilterung) ermöglicht Administratoren, den Zugriff auf den gesamten nicht genehmigten Datenverkehr standardmäßig zu blockieren oder ihn standardmäßig über den Citrix Enterprise Browser zuzulassen.

16 July 2024

- **Zusätzliche Sicherheitskontrollen**

  Die folgenden zusätzlichen Sicherheitskontrollen sind zur Einschränkung des Anwendungszugriffs verfügbar.

  - Download-Einschränkung nach Dateityp

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Upload-Einschränkung nach Dateityp
- Maskierung persönlicher Daten
- Druckerverwaltung
- Einschränkung der Zwischenablage für Sicherheitsgruppen

- **Anzeige eingebetteter Domänen auf der Seite zur App-Erkennung**

  Die Funktion zur App-Erkennung ermöglicht Administratoren das Erstellen neuer Anwendungen oder das Hinzufügen dieser Domänen zu einer bestehenden Anwendung, wenn eine Hauptdomäne oder eine eingebettete Domäne (HTTP/HTTPS) oder die Ziel-IP-Adresse (TCP/UDP) keiner Anwendung zugeordnet ist. Die Seite zur **App-Erkennung** zeigt sowohl die Hauptdomäne als auch die zugrunde liegenden eingebetteten Domänen in einer Baumstruktur an. Weitere Informationen finden Sie unter Domänen oder IP-Adressen ermitteln, auf die Endbenutzer zugreifen.

11 June 2024

- **Richtlinienmodellierungstool**

  Das Richtlinienmodellierungstool (**Zugriffsrichtlinien > Richtlinienmodellierung**) hilft Administratoren, Konfigurationsprobleme innerhalb der Administratorkonsole zu analysieren und zu beheben. Weitere Informationen finden Sie unter Richtlinienmodellierungstool.

- **Unterstützung für Filter im Diagramm der Diagnoselogdateien**

  Die Filteroption im Diagramm der **Diagnoselogdateien** hilft Administratoren, die Suche basierend auf verschiedenen Kriterien wie App-Typ, Kategorie und Beschreibung zu verfeinern, um die Analyse und Fehlerbehebung von Protokollen zu erleichtern. Weitere Informationen finden Sie unter Diagnoselogdateien.

13 March 2024

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen finden Sie unter Aktive Benutzersitzungen beenden und Benutzer zur Liste der deaktivierten Benutzer hinzufügen.

12 February 2024

- **Allgemeine Verfügbarkeit der Browser- und Antivirenscans**

  Die Browser- und Antivirenscans, die vom Device Posture-Dienst unterstützt werden, sind jetzt allgemein verfügbar. Weitere Informationen finden Sie unter Vom Geräte-Posture unterstützte Scans.

23 January 2024

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

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

20 December 2023

- **Allgemeine Verfügbarkeit von Secure Private Access On-Premises**

  Citrix Secure Private Access On-Premises ist jetzt allgemein verfügbar. Weitere Informationen finden Sie unter „Neuerungen“.

16 October 2023

- **Vorschaufunktionen der Secure Private Access On-Premises-Lösung**

  Die Secure Private Access On-Premises-Lösung bietet jetzt Folgendes:

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

  Weitere Informationen finden Sie unter Secure Private Access On-Premises.

- **Vorschaufunktionen des Device Posture-Dienstes**

  Der Device Posture-Dienst unterstützt jetzt die folgenden Prüfungen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Device Posture-Dienst wird jetzt auf den IGEL-Plattformen unterstützt.
- Der Device Posture-Dienst unterstützt jetzt Geolocation- und Netwerkstandort-Prüfungen.

Weitere Informationen finden Sie unter Device Posture.

11 September 2023

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

  Die Device Posture-Integration mit Microsoft Intune ist jetzt allgemein verfügbar. Weitere Informationen finden Sie unter Microsoft Intune integration with Device Posture.

30 August 2023

- **Citrix Endpoint Analysis Client für den Device Posture-Dienst verwalten**

  Der EPA-Client kann zusammen mit NetScaler und Device Posture verwendet werden. Einige Konfigurationsänderungen sind erforderlich, um den EPA-Client bei Verwendung mit NetScaler und Device Posture zu verwalten. Weitere Informationen finden Sie unter Manage Citrix Endpoint Analysis Client for Device Posture service.

28 August 2023

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

  Der Device Posture-Dienst wird jetzt auf iOS-Plattformen unterstützt. Weitere Informationen finden Sie unter Device Posture.

  Diese Funktion befindet sich in der Vorschau.

22 August 2023

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

  Der Citrix Device Posture-Dienst kann jetzt kontextbezogenen Zugriff (Smart Access) auf Citrix DaaS- und Secure Private Access-Ressourcen ermöglichen, indem das Zertifikat des Endgeräts mit einer Unternehmenszertifizierungsstelle abgeglichen wird, um festzustellen, ob dem Endgerät vertraut werden kann. Weitere Informationen finden Sie unter Gerätezertifikatsprüfung mit dem Device Posture-Dienst.

  Diese Funktion befindet sich in der Vorschauphase.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

17 August 2023

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

  Device Posture-Dienstereignisse und Überwachungsprotokolle sind jetzt im DaaS Monitor durchsuchbar. Weitere Informationen finden Sie unter Device Posture-Ereignisse im Citrix DaaS Monitor.

07 June 2023

- **Tool zur Konfiguration von Secure Private Access für lokale Umgebungen**

  Eine vereinfachte Benutzeroberfläche ist jetzt verfügbar, um die Secure Private Access-Lösung für lokale Umgebungen zu konfigurieren. Das Konfigurationstool kann auf einem Citrix Virtual Apps and Desktops™ Delivery Controller ausgeführt werden, um schnell eine SaaS- oder Webanwendung zu erstellen. Darüber hinaus können Sie dieses Tool verwenden, um Anwendungsbeschränkungen, Datenverkehrsrouting und NetScaler Gateway-Einstellungen festzulegen.

29 May 2023

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

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

10 April 2023

- **Anwendungsermittlung**

  Die Funktion zur Anwendungsermittlung hilft einem Administrator, Einblick in die internen privaten Anwendungen wie Web-Apps und Client-Server-Apps (TCP- und UDP-basierte Apps) in seiner Organisation und die Benutzer, die auf diese Anwendungen zugreifen, zu erhalten. Administratoren können die Apps ermitteln, indem sie den Bereich der Domänen (Platzhalterdomänen) oder IP-Subnetze angeben. Weitere Informationen finden Sie unter Anwendungsermittlung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

29 March 2023

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

  Als Citrix StoreFront- und NetScaler Gateway-Kunde können Sie jetzt nahtlos auf Web- und SaaS-Anwendungen sowie auf Citrix Virtual Apps und virtuelle Desktops zugreifen, indem Sie die Citrix Secure Private Access-Lösung für lokale Bereitstellungen verwenden. Weitere Informationen finden Sie unter Secure Private Access für lokale Bereitstellungen.

07 March 2023

- **DNS-Suffixe konfigurieren**

  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 vollständig qualifizierten 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 über den entsprechenden FQDN unter der DNS-Suffixdomäne auf die Anwendungen zugreifen können.

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

23 January 2023

- **Geräte-Posture-Dienst**

  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. Weitere Informationen finden Sie unter Geräte-Posture.

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

  Zusätzlich zu den nativen Scans, die vom Device Posture-Dienst angeboten werden, kann der Device Posture-Dienst auch in andere Drittanbieterlösungen integriert werden. Device Posture

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ist in Microsoft Endpoint Manager (MEM) unter Windows und macOS integriert. Weitere Informationen finden Sie unter Integration von Microsoft Endpoint Manager mit Device Posture.

22 December 2022

- **Unterstützung für Single Sign-On 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 der Benutzer bereits über die Citrix Workspace-App angemeldet ist. Diese SSO-Funktionalität verbessert die Benutzererfahrung, indem mehrere Authentifizierungen vermieden werden. Weitere Informationen finden Sie unter Unterstützung für Single Sign-On für die Workspace-URL.

- **Zugriff auf Apps mithilfe von Zugriffsrichtlinien aktivieren**

  Um Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren jetzt Zugriffsrichtlinien mit einer passenden Benutzerabonnementliste erstellen, damit die Apps für Endbenutzer verfügbar sind. Zuvor mussten Administratoren Benutzer als Abonnenten hinzufügen, um den Zugriff zu ermöglichen. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.

03 October 2022

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

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

- **Unterstützung für UDP-Apps**

  Der Secure Private Access-Dienst unterstützt jetzt den Zugriff auf UDP-Apps. Weitere Informationen finden Sie unter Vorschaufunktionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

09 September 2022

- **Adaptiver Zugriff basierend auf dem Benutzerrisikowert**

  Administratoren können jetzt eine adaptive Zugriffsrichtlinie mit dem Benutzerrisikowert konfigurieren, der von Citrix Analytics for Security (CAS) bereitgestellt wird. Weitere Informationen finden Sie unter Adaptiver Zugriff basierend auf dem Benutzerrisikowert.

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

  Administratoren können die adaptive Zugriffsrichtlinie jetzt 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 Netwerkstandort des Benutzers. Weitere Informationen finden Sie unter Adaptiver Zugriff basierend auf dem Standort.

- **Verbesserter Generator für adaptive Zugriffsrichtlinien**

  Der Zugriff auf die Apps ist jetzt erst möglich, nachdem die konfigurierten Bedingungen erfüllt sind. Ein App-Abonnement allein gewährt Ihren Kunden keinen Zugriff auf die Anwendungen. Administratoren müssen zusätzlich zum App-Abonnement Zugriffsrichtlinien hinzufügen, um den Zugriff auf die Apps zu ermöglichen. Außerdem ist die Angabe von Benutzern oder Gruppen eine obligatorische Bedingung in den Zugriffsrichtlinien, die erfüllt sein muss, um auf die Apps zugreifen zu können. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.

- **Dateiuploads in SaaS-/Web-Apps einschränken**

  Diese Funktion ermöglicht es den Kundenadministratoren, zu steuern (zuzulassen oder einzuschränken), wer Dateien in ihre geschäftskritischen Anwendungen hochladen darf. Dadurch können nur autorisierte Benutzer Dateien in die Anwendungen hochladen. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.

- **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. Weitere Informationen finden Sie unter Dashboard.

- **Einstellung der Bibliothek**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Secure Private Access-Anwendungen sind jetzt nicht mehr in der Citrix Cloud™-Bibliothek sichtbar. Alle konfigurierten Secure Private Access-Anwendungen befinden sich im Abschnitt „Anwendungen“ innerhalb der Secure Private Access-Dienstkachel. Dies hilft Administratoren, die Anwendungen einfach zu navigieren, zu bearbeiten und zu konfigurieren.

- **Überwachungsprotokolle für Secure Private Access**

  Die Ereignisse des Citrix Secure Private Access-Dienstes werden jetzt im **Citrix Cloud > Systemprotokoll** erfasst. Weitere Informationen finden Sie unter Überwachungsprotokolle.

- **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, über den Administratoren auf die Ereignisse zugreifen und diese herunterladen können. Diese Ereignisse können über ein PowerShell-Skript aufgerufen werden. Weitere Informationen finden Sie unter Diagnoseprotokolle für den Zugriff auf Enterprise-Web- und SaaS-Apps.

- **Handbuch zur Fehlerbehebung**

  Administratoren können das Handbuch zur Fehlerbehebung verwenden, um konfigurationsbezogene Probleme zu lösen. Weitere Informationen finden Sie unter Beheben von Problemen mit Apps.

01 June 2022

- **Dienst für adaptive Authentifizierung**

  Die adaptive Authentifizierung ist jetzt allgemein verfügbar (GA). Ausführliche Informationen zur adaptiven Authentifizierung finden Sie unter Dienst für adaptive Authentifizierung.

04 April 2022

- **Änderungen beim Rebranding**

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

- **Administratorgeführter Workflow für einfaches Onboarding und Einrichtung**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access bietet jetzt eine neue, optimierte Administratorerfahrung mit einem Schritt-für-Schritt-Prozess zur Konfiguration des Zero Trust Network Access für SaaS-Anwendungen, interne Webanwendungen und TCP-Anwendungen. Es umfasst die Konfiguration der adaptiven Authentifizierung, Anwendungen einschließlich Benutzerabonnement, adaptive Zugriffsrichtlinien und andere innerhalb einer einzigen Administratorkonsole. Weitere Informationen finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichtung.

Diese Funktion ist jetzt allgemein verfügbar (GA).

- **Secure Private Access-Dashboard**

  Das Secure Private Access-Dashboard bietet Administratoren vollständige Transparenz über ihre Top-Apps, Top-Benutzer, den Integritätsstatus der Konnektoren, die Bandbreitennutzung und alles an einem einzigen Ort zur Nutzung. Diese Daten werden von Citrix Analytics abgerufen. Weitere Informationen finden Sie unter Secure Private Access-Dashboard.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

- **Direkter Zugriff auf Unternehmens-Web-Apps**

  Kunden können jetzt Zero Trust Network Access (ZTNA) für interne Web-Apps direkt über native Webbrowser wie Chrome, Firefox, Safari und Microsoft Edge aktivieren. Weitere Informationen finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

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

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

  Diese Funktion ist jetzt allgemein verfügbar (GA).

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zugriff auf die Apps bereitzustellen, 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 (Geo-Standort oder Netwerkstandort)
- Gerätehaltung (Gerätehaltungsprüfung)
- Risiko (Benutzerrisikobewertung)

Weitere Informationen finden Sie unter Adaptiver Zugriff und Sicherheitskontrollen für Enterprise Web-, TCP- und SaaS-Anwendungen.

Diese Funktion ist jetzt allgemein verfügbar (GA).

- **Audit-Protokolle für Secure Private Access**

  Die ereignisbezogenen Ereignisse des Citrix Secure Private Access-Dienstes werden jetzt in **Citrix Cloud > Systemprotokoll** erfasst. Weitere Informationen finden Sie unter Audit-Protokolle.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

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

  Die Citrix Secure Private Access-Ereignisse sind jetzt in Citrix Analytics integriert. Citrix Analytics bietet einen öffentlichen Endpunkt, der Administratoren den Zugriff und das Herunterladen der Ereignisse ermöglicht. Auf diese Ereignisse kann über ein PowerShell-Skript zugegriffen werden. Weitere Informationen finden Sie unter Diagnoseprotokolle für den Zugriff auf Enterprise Web- und SaaS-Anwendungen.

  Diese Funktion ist jetzt allgemein verfügbar (GA).

- **Adaptiver Authentifizierungsdienst**

  Citrix Cloud-Kunden können jetzt Citrix Workspace verwenden, um Adaptive Authentication für Citrix Virtual Apps and Desktops bereitzustellen. Adaptive Authentication ist ein Citrix Cloud-Dienst, der eine erweiterte Authentifizierung für Kunden und Benutzer ermöglicht, die sich bei Citrix Workspace anmelden. Der Adaptive Authentication-Dienst ist ein von Citrix verwalteter und in Citrix Cloud gehosteter ADC. Weitere Informationen finden Sie unter Adaptiver Authentifizierungsdienst.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diese Funktion befindet sich in der Vorschau.

16 February 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 eliminieren, um Remote-Benutzern Zugriff auf alle privaten Apps zu ermöglichen.

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

11 October 2021

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

  Die Citrix Gateway-Dienstkachel wurde nun zu einem einzigen Secure Private Access in Citrix Cloud zusammengeführt.

  - Alle Secure Private Access-Kunden, einschließlich Citrix Workspace Essentials™ und Citrix Workspace Standard, können jetzt eine einzige Secure Private Access-Kachel verwenden, um SaaS- und Enterprise-Web-Apps, erweiterte Sicherheitskontrollen, kontextbezogene Richtlinien sowie Webfilterrichtlinien zu konfigurieren.
  - Alle Citrix DaaS-Kunden können den Citrix Gateway-Dienst weiterhin als HDX-Proxy über die Workspace-Konfiguration aktivieren. Der Shortcut zum Aktivieren des Citrix Gateway-Dienstes über die Gateway-Dienstkachel wurde jedoch entfernt. Sie können den Citrix Gateway-Dienst unter **StoreFront Cloud > Access > External Connectivity** aktivieren. Weitere Informationen finden Sie unter Externe Konnektivität. An der Funktionalität ändert sich ansonsten nichts.

30 July 2021

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 aus dem Citrix Workspace-Portal ausgeblendet wird, gibt der Citrix Gateway-Dienst diese App während der Enumeration nicht zurück. Benutzer können jedoch weiterhin auf die ausgeblendete App zugreifen.

09 June 2021

- **Routingtabelle zum Definieren der Regeln für die Weiterleitung des App-Datenverkehrs**

  Administratoren können jetzt die Routingtabelle 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 External, Internal, Internal-Bypass Proxy oder External via Gateway Connector definieren, je nachdem, wie sie den Datenfluss definieren möchten.

22 May 2021

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

  Die Funktion für kontextbezogenen Zugriff des Citrix Secure Private Access-Dienstes bietet einen umfassenden Zero-Trust-Zugriffsansatz, der sicheren Zugriff auf die Anwendungen ermöglicht. Der kontextbezogene Zugriff ermöglicht es Administratoren, einen detaillierten Zugriff auf die Apps zu gewähren, auf die Benutzer basierend auf dem Kontext zugreifen können. Der Begriff „Kontext“ bezieht sich hier auf Benutzer, Benutzergruppen und die Plattform (Mobilgerät oder Desktop-Computer), von der aus der Benutzer auf die Anwendung zugreift.

- **Rebranding der Benutzeroberfläche des Citrix Gateway Connectors**

  Die Benutzeroberfläche des Citrix Cloud Gateway Connector™ wurde gemäß den Citrix Branding-Richtlinien neu gestaltet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

01 May 2021

- **Löschung von Kundendaten aus dem Datenspeicher des Citrix Secure Private Access-Dienstes**

  Kundendaten, einschließlich Sicherungen, werden nach 90 Tagen nach Ablauf der Dienstberechtigung aus dem Datenspeicher des Citrix Secure Private Access-Dienstes gelöscht.

- **Vereinfachte Schritte zur Föderation einer Domäne von Azure AD zu Citrix Workspace**

  Die Schritte zur Föderation einer Domäne von Azure AD zur Citrix Workspace-App wurden für ein schnelleres Onboarding in Citrix Workspace vereinfacht. Die Domänenföderation kann jetzt in der Benutzeroberfläche des Citrix Gateway-Dienstes auf der Seite „Single Sign-On“ durchgeführt werden.

- **Verbesserung des Konnektivitätstest-Tools**

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

15 March 2021

- **Plattformverbesserungen**

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

- **Verbesserte Leistung von Web-Apps**

  Die Leistung von Web-Apps wurde verbessert, wenn die Webanwendungen über den Systembrowser mit clientlosem VPN aufgerufen werden.

- **Aktivierung des Citrix Gateway Connectors zur Verwendung von TLS1.2-Cipher-Suites der Klasse A oder höher**

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11 November 2020

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

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

15 October 2020

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

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

08 October 2020

- **Sitzungs-Timeouts für die Citrix Secure Private Access-Browsererweiterung konfigurieren**

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

- **RBAC-Steuerung für die Admin-Einstellungen der Citrix Secure Private Access Browsererweiterung**

  Die RBAC-Steuerung wird jetzt für die Admin-Einstellungen der Citrix Secure Private Access Browsererweiterung erzwungen.

24 September 2020

- **VPN-losen Zugriff auf Unternehmens-Web-Apps über einen lokalen Browser ermöglichen**

  Sie können jetzt die Browsererweiterung **Citrix Secure Private Access** verwenden, um VPN-losen Zugriff auf Unternehmens-Web-Apps über einen lokalen Browser zu ermöglichen. Die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Browsererweiterung **Citrix Secure Private Access** wird sowohl von Google Chrome als auch von Microsoft Edge unterstützt.

07 July 2020

- **Kerberos-Konfiguration auf Citrix Gateway Connector validieren**

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

19 June 2020

- **Schreibgeschützter Zugriff für Administratoren des Citrix Gateway-Dienstes und des Citrix Secure Private Access-Dienstes**

  Sicherheitsadministratoren, die den Citrix Gateway-Dienst verwenden, können jetzt detaillierte Kontrollen bereitstellen, wie 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 Private Access-Dienst können nur die Einstellungen für den Inhaltszugriff anzeigen.

08 May 2020

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

  - **Netzwerkverfolgung:** Sie können jetzt die Funktion **Trace** verwenden, um Probleme bei der Registrierung des Citrix Gateway Connectors zu beheben. Sie können die Trace-Datei herunterladen und zur Fehlerbehebung mit den Administratoren teilen.
  - **Konnektivitätstests:** Sie können jetzt die Funktion **Konnektivitätstest** verwenden, um zu bestätigen, dass keine Fehler in der Gateway Connector-Konfiguration vorliegen und der Gateway Connector in der Lage ist, eine Verbindung zu den URLs herzustellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2019.04.02

- **Unterstützung der Kerberos-Authentifizierung für Citrix Gateway Connector zu ausgehendem Proxy**

  Die Kerberos-Authentifizierung wird jetzt für den Datenverkehr vom Citrix Gateway Connector zum ausgehenden Proxy unterstützt. Der Gateway Connector verwendet die konfigurierten Proxy-Anmeldeinformationen, um sich beim ausgehenden Proxy zu authentifizieren.

V2019.04.01

- **Der Datenverkehr von Web-/SaaS-Apps kann jetzt über einen im Unternehmensnetzwerk gehosteten Gateway-Connector geleitet werden, wodurch eine Zwei-Faktor-Authentifizierung vermieden wird.** Wenn ein Kunde eine SaaS-App veröffentlicht hat, die außerhalb des Unternehmensnetzwerks gehostet wird, wird jetzt die Unterstützung hinzugefügt, um den Datenverkehr für diese App über einen lokalen Gateway-Connector zu authentifizieren.

  Stellen Sie sich zum Beispiel vor, ein Kunde hat eine Okta-geschützte SaaS-App (wie Workday). Der Kunde möchte möglicherweise, dass, obwohl der tatsächliche Workday-Datenverkehr nicht über den Citrix Gateway-Dienst geleitet wird, der Authentifizierungsverkehr zum Okta-Server über den Citrix Gateway-Dienst über einen lokalen Gateway-Connector geleitet wird. Dies hilft einem Kunden, eine Zwei-Faktor-Authentifizierung vom Okta-Server zu vermeiden, da der Benutzer sich vom Unternehmensnetzwerk aus mit dem Okta-Server verbindet.

- **Deaktivieren von Filter-Websitelisten und Website-Kategorisierung**. Filter-Websitelisten und Website-Kategorisierung können deaktiviert werden, wenn der Administrator diese Funktionen für einen bestimmten Kunden nicht anwenden möchte.

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

V2019.03.01

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Eine neue Kategorie „Bösartig und gefährlich“ wird in den Kategorien „Zugriffssteuerung Webfilterung“ hinzugefügt.** Eine neue Kategorie namens **Bösartig und gefährlich** in den Kategorien **Zugriffssteuerung Webfilterung** wird unter der Gruppe **Malware und Spam** hinzugefügt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integration mit Google Chrome Enterprise Premium

Die folgenden Abschnitte enthalten Details zur integrierten Lösung.

Lösungsübersicht

Citrix-Kunden können den weltweit beliebtesten und sichersten Webbrowser, Chrome, mit einer vertrauten Erfahrung nutzen, um nativ auf autorisierte Unternehmens-Webanwendungen zuzugreifen. Citrix Secure Private Access erzwingt den Zugriff mit den geringsten Berechtigungen pro Anwendung basierend auf vom Administrator definierten Richtlinien, die zentral über die Secure Private Access-Konsole verwaltet werden. Administratoren können Unternehmensanwendungsdomänen und Zero-Trust-Zugriffsrichtlinien einfach auf der Secure Private Access-Konsole konfigurieren. Sie können Richtlinien modellieren, um Sicherheitsergebnisse zu validieren und zu testen und das richtige Maß an Benutzerzugriff und Endbenutzererfahrung zu liefern.

Der Vorteil dieser Integration besteht darin, den agentenlosen Zugriff vom Chrome-Browser auf private Web- und SaaS-Anwendungen durch automatisierte Datenverkehrssteuerung über die Citrix Secure Private Access-Infrastruktur zu ermöglichen. Wenn Benutzer über Chrome auf Anwendungen zugreifen, sendet das System ihren Datenverkehr automatisch über das Google Secure Gateway an Citrix Secure Private Access. Dies gewährleistet einen sicheren und kontrollierten Netzwerkzugriff, ohne dass zusätzliche Software auf den Benutzergeräten installiert werden muss. Es vereinfacht auch die Bereitstellung, reduziert den IT-Verwaltungsaufwand, verbessert die Benutzererfahrung und optimiert den IT-Betrieb.

Die integrierte Lösung umfasst die folgenden Komponenten:

- Google Chrome Enterprise Premium (CEP), das Funktionen wie Data Loss Prevention (DLP), Malware- und Phishing-Schutz, URL-Filterung und die Google-Administrationskonsole umfasst.
    - Der Google Chrome-Browser, der lokal auf dem Clientcomputer ausgeführt wird, fungiert als sicherer Browser mit richtlinienbasierter Durchsetzung auf Benutzerebene über Chrome-verwaltete Profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Die Google Chrome Enterprise Premium-Konsole, die über das Google Cloud-Portal aufgerufen wird, bietet die Administrations-, Verwaltungs- und Überwachungskonsole für die Chrome Enterprise Premium-Sicherheitsrichtlinien.

- Citrix Secure Private Access, das den Zugriff auf die Cloud-Infrastruktur, die ZTNA-Richtlinien-Engine und in der Kundenumgebung bereitgestellte Connector Appliances umfasst.
- Citrix-Konsole, einschließlich der Secure Private Access-Konsole für Zero-Trust-Zugriffsrichtlinien für private Anwendungen und Citrix Monitor zur Überwachung und Fehlerbehebung.

Der Citrix Secure Private Access-Dienst erzwingt alle vom Administrator konfigurierten Zugriffsrichtlinien und stellt sicher, dass Benutzern nur der Zugriff auf bestimmte Webanwendungen gewährt wird.

Erweiterte Sicherheitsfunktionen von Chrome Enterprise Premium

Im Folgenden sind einige der erweiterten Sicherheitsfunktionen aufgeführt, die von Chrome Enterprise Premium angeboten werden:

- **Data Loss Prevention (DLP)**: Implementieren Sie granulare Kontrollen und Richtlinien, um zu verhindern, dass sensible Daten verloren gehen oder versehentlich weitergegeben werden.
- **Malware-Tiefenscan**: Verwenden Sie fortschrittliche Scan-Techniken, um unbekannte oder risikoreiche Dateien zu erkennen und unter Quarantäne zu stellen, die Ausführung bösartigen Codes zu verhindern und vor Zero-Day-Angriffen zu schützen.
- **Phishing-Schutz**: Schützen Sie Benutzer vor dem Besuch schädlicher Websites, indem Sie Phishing-Versuche identifizieren und blockieren und so den Diebstahl von Anmeldeinformationen und persönlichen Daten verhindern.
- **URL-Kategorisierung und -Filterung**: Beschränken Sie den Zugriff auf Websites basierend auf ihrer Inhaltskategorie und verhindern Sie so, dass Benutzer auf unangemessene oder bösartige Inhalte zugreifen.
- **Einblicke und Analysen zur Webnutzung**: Bieten Sie detaillierte Berichte und Analysen zum Web-Traffic, die es Administratoren ermöglichen, Benutzeraktivitäten zu überwachen, potenzielle Sicherheitsbedrohungen zu identifizieren und die Netzwerkbandbreite zu optimieren.

Weitere Informationen finden Sie unter Übersicht über Chrome Enterprise Premium.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access-Steuerelemente für Chrome Enterprise

Die folgenden mehrwertschaffenden Funktionen werden mit der Integration von Secure Private Access und Chrome Enterprise Premium unterstützt.

- **RDP** – Ermöglichen Sie sichere RDP-Sitzungen direkt im Browser. Weitere Informationen finden Sie unter Remote Desktop-Steuerung.
- **SSH** – Ermöglichen Sie sicheren Zugriff auf SSH-Apps im Browser. Weitere Informationen finden Sie unter SSH-Steuerung.
- **Anti-Keylogging** – Verhindern Sie Keylogger beim Zugriff auf Ressourcen in CEP. Weitere Informationen finden Sie unter Anti-Keylogging-Steuerung.
- **Zwischenablage-Container** – Beschränken oder erlauben Sie die gemeinsame Nutzung der Zwischenablage zwischen dem Browser und virtualisierten Anwendungen. Weitere Informationen finden Sie unter Zwischenablage-Container-Steuerung.
- **Sitzungsaufzeichnung** – Zeichnen Sie Benutzersitzungen innerhalb des Browsers auf. Weitere Informationen finden Sie unter Sitzungsaufzeichnungssteuerung
- **Browser-Sitzungsreauthentifizierung** – Erzwingt die periodische Reauthentifizierung von Browser-Sitzungen nach einem konfigurierten Zeitintervall. Weitere Informationen finden Sie unter Browser-Sitzungsreauthentifizierungssteuerung.
- **Domänensuffix** – Optimieren Sie die Benutzererfahrung, indem Sie die Domäne an kurze URLs anhängen. Weitere Informationen finden Sie unter Domänensuffix für Webanwendungen.

Voraussetzungen für eine erfolgreiche Integration

Um eine optimale Integration zwischen der Citrix Workspace™-App und Chrome Enterprise Premium zu gewährleisten, müssen die folgenden Voraussetzungen erfüllt sein. Der erfolgreiche Abschluss dieser Voraussetzungen führt zu einer effizienteren und nahtloseren Erfahrung beim Starten von Anwendungen über die Citrix Workspace-App oder die webbasierte Benutzeroberfläche.

Die Voraussetzungen werden grob in die folgenden Kategorien eingeteilt.

- Lizenzen, App-Versionen und Erweiterungen
- Google Admin-Konsole
- Secure Private Access-Dienst
- Chrome-Browser

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Benutzerverzeichnis, das in Citrix Workspace konfiguriert ist, mit dem Google Cloud-Benutzerverzeichnis synchronisieren

Citrix Secure Private Access – Unterstützte Bereitstellungsmodi

Die integrierte Lösung unterstützt die folgenden Bereitstellungsmodi von Citrix Secure Private Access:

- **Citrix Secure Private Access-Dienst**: In diesem Bereitstellungsmodus werden alle Komponenten, einschließlich der Steuerungsebene und der Gateway-Infrastruktur, in Citrix Cloud gehostet. Weitere Informationen finden Sie unter Citrix Secure Private Access.
- **Hybride Bereitstellung von Citrix Secure Private Access**: Diese Bereitstellung ermöglicht es Kunden, eine Zero Trust Network Access (ZTNA)-Lösung unter Verwendung von lokalen StoreFront- und NetScaler Gateway-Komponenten zu implementieren und Citrix Cloud für die Verwaltung der Konfigurations-, Administrations- und Überwachungsfunktionen zu nutzen. Dies bedeutet, dass Kunden vorhandene lokale NetScaler Gateways nutzen können, um die Benutzerdatenverkehrsführung zu steuern, während sie die in Citrix Cloud gehostete Benutzeroberfläche für die Verwaltung von Konfigurationen und Richtlinien verwenden und auch Citrix Monitor, das in Citrix Cloud gehostet wird, für Überwachungs- und Fehlerbehebungsfunktionen nutzen können. Weitere Informationen finden Sie unter Hybride Bereitstellung von Citrix Secure Private Access.

WICHTIG:

Für Chrome Enterprise Premium (CEP) werden nur HTTPS-Unternehmens-Web- und SaaS-Apps unterstützt. HTTP-Unternehmens-Web- und SaaS-Apps werden nicht unterstützt.

Rechtliches

Chrome Enterprise Premium wird von Google LLC bereitgestellt, und Ihre Nutzung unterliegt den Nutzungsbedingungen von Google und den dienstspezifischen Bedingungen.

Verwandte Themen

- Onboarding und Einrichtung von Secure Private Access
- Details zur Google-Integration nach dem Onboarding aktualisieren
- App-Konfiguration und -Verwaltung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tech Brief: Citrix Secure Access mit Chrome Enterprise

Voraussetzungen für die integrierte Lösung

Um eine optimale Integration zwischen der Citrix Workspace™-Anwendung und Chrome Enterprise Premium zu gewährleisten, müssen die folgenden Voraussetzungen erfüllt sein. Der erfolgreiche Abschluss dieser Voraussetzungen führt zu einer effizienteren und nahtloseren Erfahrung beim Starten von Anwendungen über die Citrix Workspace-App oder die webbasierte Benutzeroberfläche.

Die Voraussetzungen werden grob in die folgenden Kategorien eingeteilt.

- Lizenzen, App-Versionen und Erweiterungen
- Google Admin-Konsole
- Secure Private Access-Dienst
- Chrome-Browser
- Benutzer verwalten
- Benutzerverzeichnis korrelieren
- TLS-Inspektion umgehen

Lizenzen, App-Versionen und Erweiterungen

- **Chrome Enterprise Premium-Lizenz**: Stellen Sie sicher, dass Sie über eine aktive Chrome Enterprise Premium-Lizenz verfügen, die über das Citrix Cloud Platform License (CPL)-Programm erhältlich ist.
- **Citrix Workspace-App (CWA)-Versionen**:
  - Windows: 2025.07 und höher
  - macOS: 2025.08 und höher
  - ChromeOS: 25.7.0.25 und höher

> **HINWEIS:**
>
> Die Citrix Workspace-App ist eine optionale Anforderung für diese Lösung.

- **Citrix Endpoint Analysis (EPA)-Clientversionen:**
  - Windows: 25.9.1.9 und höher

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- macOS: 25.10.3 und höher

HINWEIS:

Wir empfehlen, den Windows EPA-Client im Administratormodus zu installieren, um periodische Geräte-Posture-Scans zu unterstützen. Darüber hinaus müssen periodische Geräte-Posture-Scans auf der Seite Gerätestatus-**Einstellungen** aktiviert werden. Weitere Informationen finden Sie unter Periodisches Scannen von Geräten.

- **Chrome-Browserversion**: Endpunkte müssen die neueste Google Chrome-Version verwenden.
- **Betriebssysteme**: Windows, macOS und ChromeOS.

Google Admin-Konsole

- **Google-Kunden-ID**: Rufen Sie Ihre Google-Kunden-ID aus der Google Admin-Konsole ab. Diese ID ist erforderlich, um Google-Dienste und -Integrationen zu konfigurieren. Ihre Kunden-ID kann über **Konto > Kontoeinstellungen** in der Google Admin-Konsole abgerufen werden.
- **Benutzerdefinierte Rolle in der Google Admin-Konsole erstellen**: Um Kunden in Chrome Enterprise Premium (CEP) aufzunehmen und die Google Chrome-Integration zu aktivieren, müssen Administratoren eine benutzerdefinierte Rolle erstellen und die entsprechenden Berechtigungen in der Google Admin-Konsole zuweisen. Weitere Informationen finden Sie unter Administratorrollen und -berechtigungen.
- **DevTools-Erweiterungen einschränken**: Chrome DevTools für zwangsinstallierte Erweiterungen müssen deaktiviert werden, um die Offenlegung sensibler Daten zu verhindern. Dies ist die Standardoption in der Google Admin-Konsole.

Secure Private Access-Dienst

- **Einschränkungen für IPv6-Endpunkte**: Der Citrix Secure Private Access-Dienst kann bei Integration mit Google Cloud-Endpunkten Datenverkehr von Endbenutzergeräten mit IPv6-Adressen empfangen. Derzeit unterstützen die Zugriffsrichtlinien für Secure Private Access Geo Location und Netwerkstandort kein IPv6.

  Folglich können Zugriffsrichtlinien mit Geo Location- oder Netwerkstandort-Bedingungen für Endbenutzergeräte mit einer IPv6-Adresse fehlschlagen. Andere Zugriffsrichtlinien, die solche Bedingungen nicht nutzen, funktionieren sowohl für IPv4- als auch für IPv6-fähige Endbenutzergeräte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zugriffsbeschränkungen werden jetzt in der Google Admin-Konsole für CEP konfiguriert**: Zugriffsbeschränkungen, die zuvor in der Secure Private Access-Konsole konfiguriert wurden, gelten nur für den Citrix Enterprise Browser. Wenn Google Chrome der Unternehmensbrowser ist, müssen Zugriffsbeschränkungen als Richtlinien und Regeln in der Google Admin-Konsole konfiguriert werden.

  - Richtlinien werden in der **Google Admin-Konsole > Geräte > Chrome > Einstellungen** konfiguriert. Diese Einstellungen ermöglichen Ihnen die Verwaltung von Browsereinstellungen, wie z. B. das Blockieren von JavaScript und die Zulassungsliste für Drucker.
  - Regeln werden in der **Google Admin-Konsole > Regeln** konfiguriert. Diese Regeln sind erweiterte Einstellungen im Zusammenhang mit DLP, wie z. B. das Hinzufügen eines Wasserzeichens, das Blockieren des Downloads von Dateien mit Sozialversicherungsnummern und die URL-Filterung.

  Einzelheiten zum Erstellen von Richtlinien und Regeln in der Google Workspace Admin-Konsole finden Sie in den folgenden Themen:

  - Chrome Enterprise-Connector-Richtlinien für Chrome Enterprise festlegen
  - Datenschutzregeln

Google Chrome

Verwaltete Chrome-Profile: Alle Endbenutzer müssen über ein verwaltetes Profil auf Chrome zugreifen. Verwaltete Profile stellen sicher, dass Chrome-Richtlinien, -Erweiterungen und -Sicherheitseinstellungen auf Benutzergeräten erzwungen werden.

Benutzer verwalten

Für eine nahtlose Integration muss eine Korrelation zwischen den in Citrix Secure Private Access konfigurierten Benutzern und Google Identity (Verzeichnis) bestehen. Dies stellt sicher, dass nur autorisierte Benutzer auf ihre zugewiesenen Anwendungen zugreifen können. Die folgenden Benutzerverzeichnisse werden für die Integration unterstützt:

- Active Directory
- Microsoft Entra ID (früher bekannt als Azure Active Directory)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Obligatorisch – E-Mail-Adressfelder für Benutzer ausfüllen

Google Identity erfordert, dass das E-Mail-Adressfeld ausgefüllt wird. Zu diesem Zweck muss ein Benutzerobjekt im Verzeichnis, das von Secure Private Access verwendet wird, eines der folgenden Merkmale aufweisen:

- Eine E-Mail-Adresse mit einem Domänenteil, der in der Google Admin-Konsole konfiguriert und verifiziert ist. Zum Beispiel wird `Alice` mit der E-Mail-Adresse `alice@example.com` in Google Identity als `alice@example.com` zugeordnet.
- Eine E-Mail-Adresse mit einem Domänenteil, der nicht in der Google Admin-Konsole konfiguriert ist. Zum Beispiel hat `Bob` die E-Mail-Adresse `bob@example.internal.net`, die in Google nicht konfiguriert ist. In diesem Fall wird er in Google Identity als `bob@example.com` zugeordnet, wobei `example.com` eine verifizierte Domäne ist.
- Ein weiteres Verzeichnisfeld, das bei fehlender E-Mail-Adresse für Domänenzuordnungszwecke verwendet werden kann. Ein typischer Ansatz ist die Nutzung des User Principal Name (UPN), mit oder ohne Domänensubstitution. Zum Beispiel hat `Charlie` einen UPN `charlie@ADdomain.com` und wird in Google Identity als `charlie@example.com` zugeordnet.

Es gibt erhebliche Einschränkungen für Benutzer, deren E-Mail-Adresse im Secure Private Access-Verzeichnis und im Google-Verzeichnis nicht übereinstimmt. Weitere Informationen finden Sie im Abschnitt Überlegungen zur Domänenzuordnung.

Obligatorisch – E-Mail-Adressfelder für Benutzergruppen ausfüllen

Ähnlich wie bei Benutzern muss ein Gruppenobjekt im Verzeichnis, das von Secure Private Access verwendet wird, eines der folgenden Merkmale aufweisen:

- Eine E-Mail-Adresse mit einem Domänenteil, der in der Google Admin-Konsole konfiguriert und verifiziert ist.
- Eine E-Mail-Adresse mit einem Domänenteil, der nicht in der Google Admin-Konsole konfiguriert ist.
- Ein weiteres Verzeichnisfeld, das bei fehlender E-Mail-Adresse für Domänenzuordnungszwecke verwendet werden kann. Ein typischer Ansatz ist die Nutzung des Common Name (CN) und das Anhängen der entsprechenden Domäne im Google-Verzeichnis. Zum Beispiel wird eine Gruppe mit dem CN `group1` in Google Identity als `group1@example.com` zugeordnet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Überlegungen zur Domänenzuordnung bei fehlender oder inkonsistenter E-Mail-Adresse

Benutzer:

Falls die E-Mail-Adresse eines Benutzers im Secure Private Access-Verzeichnis fehlt oder zwischen diesem und der Google Identity inkonsistent ist, gelten die folgenden Überlegungen:

- Ein Benutzer ohne E-Mail-Adresse steht nicht zur Auswahl, wenn Secure Private Access-Richtlinien in der Secure Private Access-Konsole konfiguriert werden.
- Die Secure Private Access-Richtlinien für einen Benutzer mit einer E-Mail-Adresse, die zwischen dem Secure Private Access-Verzeichnis und dem Google-Verzeichnis nicht übereinstimmt, funktionieren nicht.
- Das Starten einer Web- oder SaaS-Anwendung aus Cloud-Stores (mithilfe der Citrix Workspace-App oder eines Webbrowsers) wird für diese Benutzer nicht unterstützt.

Gruppen:

Falls die E-Mail-Adresse einer Gruppe im Secure Private Access-Verzeichnis fehlt oder zwischen diesem und der Google Identity inkonsistent ist, ist eine entsprechende Domänenzuordnungskonfiguration erforderlich, um sicherzustellen, dass die Secure Private Access-Gruppenrichtlinien korrekt funktionieren.

Benutzerverzeichnis, das in Citrix Secure Private Access konfiguriert ist, mit dem Google Cloud-Benutzerverzeichnis korrelieren

Sie müssen das in Citrix Secure Private Access konfigurierte Benutzerverzeichnis mit dem Google Cloud-Verzeichnis korrelieren. Insbesondere werden die folgenden Benutzerverzeichnisse unterstützt:

- Active Directory
- Microsoft Entra ID (früher bekannt als Azure Active Directory)
- Okta

Beachten Sie, dass die Korrelation des Benutzerverzeichnisses regelmäßig erfolgen muss, um sicherzustellen, dass der Anwendungszugriff ordnungsgemäß erzwungen wird. Für die Korrelation ist nur ein minimaler Satz von Attributen erforderlich.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Active Directory

Für Active Directory müssen Name, E-Mail-Adresse, Object Globally Unique Identifier (objectGUID) und Security Identifier (SID) korreliert werden. Das Kennwort und alle anderen Attribute müssen nicht mit dem Google Cloud-Verzeichnis korreliert werden.

Details zur Korrelation Ihres AD mit Google Cloud, um benutzerdefinierte AD-Felder unter dem benutzerdefinierten Schema `citrix-schema` einzuschließen, finden Sie unter Google Cloud Identity als Identitätsanbieter mit Citrix Cloud verbinden und Bereitstellung von Active Directory-Benutzerkonten.

Microsoft Entra ID

Sie müssen Ihre Microsoft Entra ID mit dem Google Cloud-Benutzerverzeichnis für die Benutzer- und Gruppenverwaltung über beide Google- und Microsoft-Cloud-Plattformen hinweg synchronisieren. Details finden Sie unter Microsoft Entra ID (ehemals Azure AD) Benutzerbereitstellung und Single Sign-On.

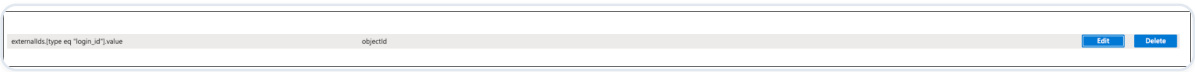
Bei der Konfiguration der Synchronisierung müssen Sie die folgenden Anforderungen berücksichtigen:

- **E-Mail-Adresse:** Das Feld für die E-Mail-Adresse muss für alle Benutzer und Gruppen ausgefüllt sein. Einzelheiten finden Sie unter Benutzer verwalten.
- **Zuordnung des objectId-Attributs:** Das objectId-Attribut von Entra ID-Benutzern muss dem Google-Verzeichnis zugeordnet werden.

  Nehmen Sie diese Zuordnung in der G-Suite Connector-Konfiguration vor:

  a. Klicken Sie im linken Menü auf **Verwalten > Bereitstellung**.
  b. Klicken Sie im neuen Menü auf **Verwalten > Attributzuordnung**.
  c. Klicken Sie auf **Microsoft Entra ID-Benutzer bereitstellen**.
  d. Suchen Sie die entsprechende Zeile für objectId.

  - Klicken Sie auf **Bearbeiten** und wählen Sie unter **Zielattribut externalIds**..value.
  - Überprüfen Sie, ob die resultierende Konfiguration mit dem folgenden Screenshot übereinstimmt.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Single Sign-On:** Die Konfiguration für Single Sign-On (SSO) ist optional. Sie können ein separates Kennwort im Google-Verzeichnis konfigurieren, SSO mit Entra ID konfigurieren oder SSO mit Open ID Connect mit Citrix Identity konfigurieren.

Okta

Sie können Okta als Identitätsquelle verwenden, indem Sie Benutzer und Gruppen von Okta in das Google Cloud-Benutzerverzeichnis (Cloud Identity / Google Workspace) bereitstellen. Nach der Bereitstellung folgt die Korrelation mit Secure Private Access demselben Modell wie bei den anderen unterstützten Verzeichnissen. Es ist nur ein minimaler Satz von Attributen erforderlich, und das Feld für die E-Mail-Adresse muss für alle Benutzer und Gruppen ausgefüllt sein.

Einzelheiten zur Bereitstellung von Okta in Google finden Sie unter Okta-Benutzerbereitstellung und Single Sign-On. Sie können derselben Anleitung folgen, um SSO für Okta zu konfigurieren, oder Open ID Connect mit Citrix Workspace konsultieren.

Google Cloud Identity (Google-Verzeichnis)

Wenn Google Cloud Identity bereits Ihr Identitätsanbieter ist, befinden sich die Benutzer und Gruppen nativ im Google Cloud-Verzeichnis. Es ist keine Verzeichnis-Korrelation oder -Synchronisierung erforderlich, da es kein separates externes Verzeichnis gibt, das mit Google abgeglichen werden müsste. Google ist die Identitätsquelle sowohl für Citrix Workspace als auch für Chrome-verwaltete Profile.

HINWEIS:

Die Integration des Device Posture-Dienstes für Chrome Enterprise Premium basiert auf dem OpenID Connect (OIDC)-Fluss, bei dem das Google Cloud-Verzeichnis als Relying Party gegenüber Citrix Workspace fungiert. Dieser Fluss wird nicht unterstützt, wenn Google Cloud Identity selbst der zugrunde liegende IdP ist. Daher ist die Integration des Device Posture-Dienstes in dieser Konfiguration nicht verfügbar.

TLS-Inspektion umgehen

Um sicherzustellen, dass Chrome Enterprise Premium-Endpunkte in Netzwerken mit TLS-Inspektion (oder SSL-Inspektion) ordnungsgemäß funktionieren, müssen Sie die folgenden Hostnamen von der Inspektion ausschließen.

- `ingress.cloudproxy.app`
- `securegateway.goog`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `*.securegateway.goog`

Dieser Ausschluss ist unerlässlich, da viele TLS-Inspektionslösungen (wie SSE-Anbieter oder Proxyserver) die von Chrome Enterprise Premium verwendete HTTP CONNECT-Methode nicht vollständig unterstützen, was dazu führen kann, dass der Datenverkehr abrupt unterbrochen wird.

Darüber hinaus wird empfohlen, die folgenden Hostnamen von der TLS-Inspektion auszuschließen, um potenzielle Leistungsprobleme und Verbindungsverzögerungen für Endbenutzer zu vermeiden.

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

Administratorrollen und -berechtigungen

Das Citrix-Dienstkonto wird von Secure Private Access verwendet, um Benutzer in Chrome Enterprise Premium (CEP) aufzunehmen und die CEP-Integration zu ermöglichen. Daher müssen Sie dem Dienstkonto in der Google Admin-Konsole eine Rolle mit den erforderlichen Berechtigungen zuweisen.

In der Google Admin-Konsole sind zwei Arten von Rollen verfügbar:

Systemrollen: Dies sind die von Google bereitgestellten Standardrollen. Mit Ausnahme der Super-Admin-Rolle enthalten die übrigen Systemrollen nicht alle notwendigen Berechtigungen, die für die CEP-Integration mit Secure Private Access erforderlich sind.

Benutzerdefinierte Rollen: Diese können eine beliebige Untermenge von Admin-API-Berechtigungen enthalten. Sie müssen eine benutzerdefinierte Rolle erstellen, die alle für die CEP-Integration mit Secure Private Access erforderlichen Berechtigungen enthält.

Für diese Aufgabe müssen Sie als Super-Administrator in der Google Admin-Konsole angemeldet sein.

HINWEIS:

Super-Administratorrollen können keinen Dienstkonten zugewiesen werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Berechtigungen für benutzerdefinierte Google-Administratorrollen

Für die CEP- und Secure Private Access-Integration muss das Citrix-Dienstkonto in der Google Admin-Konsole eine benutzerdefinierte Rolle mit den folgenden spezifischen Berechtigungen haben:

ERFORDERLICHE ADMINISTRATORBERECHTIGUNG	WARUM IST DIESE BERECHTIGUNG ERFORDERLICH?
Kunden verwalten > Kunden lesen	Um den benutzerfreundlichen Namen der Google-Kundenorganisation zu lesen.
Organisationseinheiten > Lesen	Um zu überprüfen, ob die konfigurierten Organisationseinheiten im Google Directory verfügbar sind.
Services > Chrome Management > Settings > Manage User Settings **Hinweis:** Stellen Sie sicher, dass Sie das übergeordnete Privileg **Manage User Settings** und die Unterprivilegien (**Manage Application Settings** und **Manage Web Settings**) auswählen.	Zum Hinzufügen der erforderlichen Erweiterungen und deren Konfiguration, die für die CEP- und SPA-Integration in den Benutzerprofilen notwendig sind.
Services > Chrome Management > Settings Managed Browsers > Read	Zum Lesen der verwalteten Chrome-Profile und der verwalteten Browser.
License Management > Read	Zum Abfragen der Gesamtzahl der für die Organisation bereitgestellten Chrome Enterprise Premium zugewiesenen Lizenzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERFORDERLICHE ADMINISTRATORBERECHTIGUNG	WARUM IST DIESE BERECHTIGUNG ERFORDERLICH?
Berichte	Zum Lesen der Benutzer, die ihre zugewiesenen Lizenzen aktiv nutzen. Zum Lesen der Aktivitätsereignisse, wenn die Data Loss Prevention (DLP)-Regeln ausgelöst werden. Zum Lesen der Fehlerereignisse.
Gruppen > Lesen	Um zu überprüfen, ob die konfigurierten Integrationsgruppen im Google-Verzeichnis verfügbar sind.
Dienste > Benachrichtigungscenter > Vollzugriff > Lesezugriff	Zum Lesen der Sicherheitswarnungen für Data Loss Prevention und der Anmeldefehlerereignisse.
Geräte und Einstellungen verwalten	Zum Lesen von Gerätemetadaten, um sie in der Ansicht „Netzwerktopologie überwachen“ anzuzeigen.
Benutzer > Lesen	Um zu überprüfen, ob die konfigurierten Integrationsbenutzer im Google-Verzeichnis verfügbar sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Es ist auch erforderlich, die entsprechenden OAuth-Bereiche für diese Administratorberechtigungen zu gewähren.
- Alle Administratorberechtigungen finden Sie jetzt im Abschnitt **Administratorberechtigungen**. Dies umfasst Berechtigungen, die zuvor in den Abschnitten **Administrator-Konsolenberechtigungen** und **Administrator-API-Berechtigungen** aufgeführt waren. Diese Änderung hat keine Auswirkungen auf die Zuweisung von Berechtigungen, und bestehende Berechtigungen funktionieren weiterhin wie zuvor.
- Stellen Sie sicher, dass Sie die Berechtigung der obersten Ebene **Benutzereinstellungen verwalten** und die Unterberechtigungen (**Anwendungseinstellungen verwalten** und **Webeinstellungen verwalten**) auswählen. Die Auswahl nur der Unterberechtigungen ist nicht ausreichend.
- Citrix Secure Private Access stellt Konfigurationen für Ihr Google-Konto mithilfe des konfigurierten Citrix-Dienstkontos bereit. Nachdem die Integration von Citrix Secure Private Access und Google CEP abgeschlossen ist, öffnen Sie die Google Admin-Konsole und navigieren Sie zu **Chrome-Browser > Apps & Erweiterungen**. Beachten Sie, dass mehrere Browsererweiterungen auf der Stammorganisationsebene konfiguriert wurden. Diese werden von den untergeordneten Organisationseinheiten geerbt. Wenn Benutzer Google Chrome-Profile mit diesem Tenant einbinden, werden diese Erweiterungen automatisch bereitgestellt.

Rollen und Berechtigungen erstellen und zuweisen

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Administratorrolle zu erstellen und Berechtigungen zuzuweisen:

1. Gehen Sie in der Google Admin-Konsole zu **Konten** > **Administratorrollen**.
2. Klicken Sie auf **Neue Rolle erstellen** und geben Sie einen Namen und eine Beschreibung für die Rolle ein.
3. Fügen Sie alle für die Google Chrome-Integration erforderlichen Berechtigungen zu dieser benutzerdefinierten Rolle hinzu. Eine Liste der erforderlichen Berechtigungen finden Sie unter Google-Berechtigungen für benutzerdefinierte Administratorrollen.

   Weitere Informationen zu Rollen und Berechtigungen finden Sie in der Google-Dokumentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Speichern Sie die benutzerdefinierte Rolle.

Egress-Hub-Regionen konfigurieren

Secure Private Access ermöglicht Administratoren die Auswahl der Egress-Regionen, die Chrome Enterprise Premium für den SaaS-Anwendungsverkehr verwendet. Jede ausgewählte Region bietet einen dedizierten Satz von Egress-IP-Adressen, die Administratoren zu ihren Zulassungslisten für SaaS-Anwendungen hinzufügen können, um den über Google Secure Gateway geleiteten Datenverkehr zuzulassen. Diese Funktion ist sowohl für Cloud- als auch für Hybrid-Bereitstellungen verfügbar.

Sie können das Panel **Egress-Regionen für SaaS-Anwendungen** über einen der folgenden Pfade aufrufen.

- Klicken Sie auf die Schaltfläche **Egress-Regionen verwalten** auf der Chrome Enterprise Premium-Einrichtungskarte.

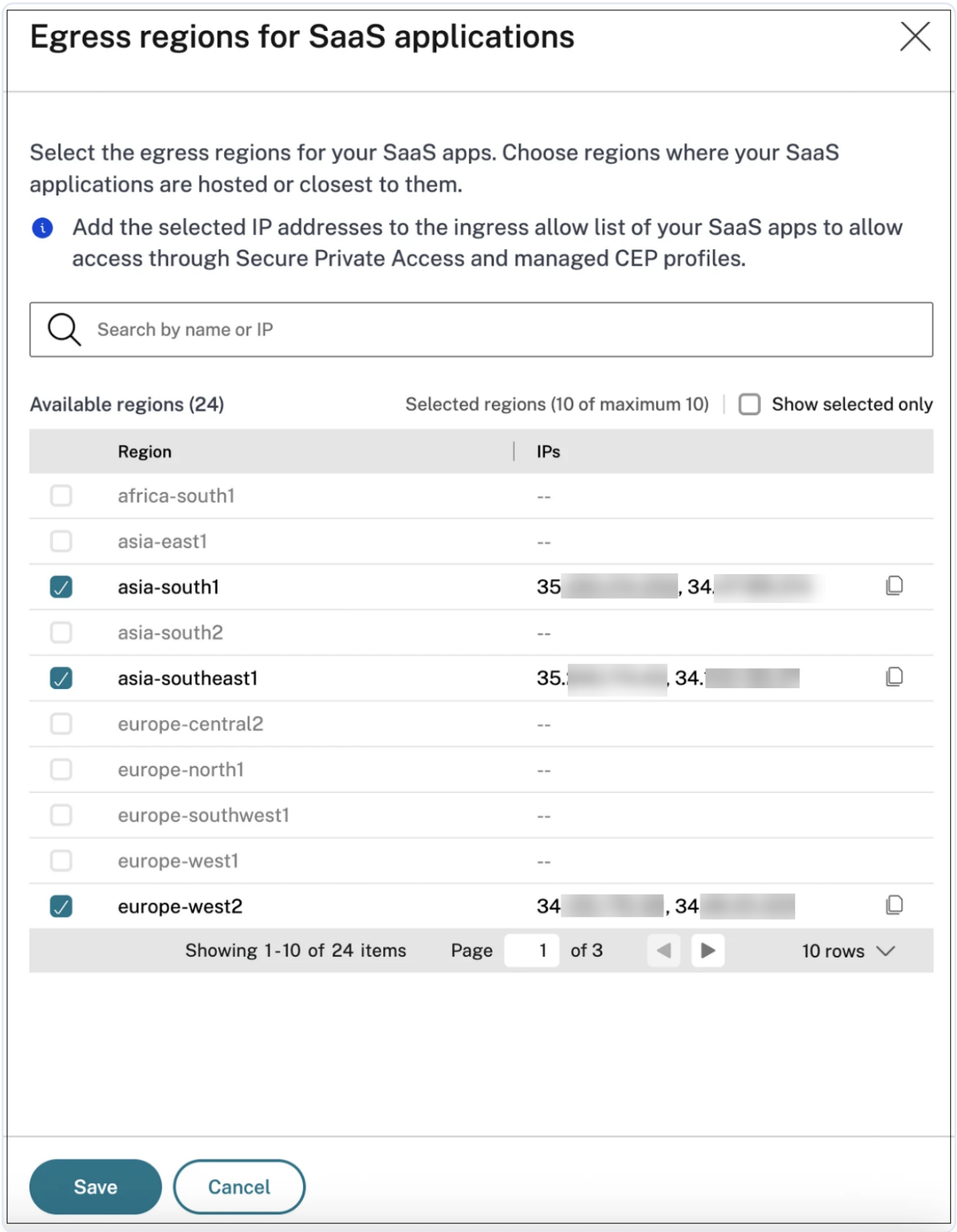


- Klicken Sie auf **Bearbeiten** unter **Browsereinstellungen > Browser konfigurieren > Egress-Regionen für SaaS-Anwendungen**.

Das Panel „Egress-Regionen für SaaS-Anwendungen“

Das Panel **Egress-Regionen für SaaS-Anwendungen** zeigt die verfügbaren Egress-Regionen und die mit jeder ausgewählten Region verbundenen IP-Adressen an. Sie können nach Regionen nach Namen oder IP-Adresse suchen und dann die IP-Adressen einer Region kopieren, um sie zu den Zulassungslisten Ihrer SaaS-Anwendungen hinzuzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



IP-Adressen werden erst verfügbar, nachdem Sie eine Region ausgewählt, Ihre Änderungen gespeichert und Google die Bereitstellung abgeschlossen hat. Bis die Bereitstellung abgeschlossen ist, zeigen neu ausgewählte Regionen keine IP-Adressen an. Die Bereitstellung dauert in der Regel einige Minuten, wobei die genaue Zeit variieren kann.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine Region auswählen

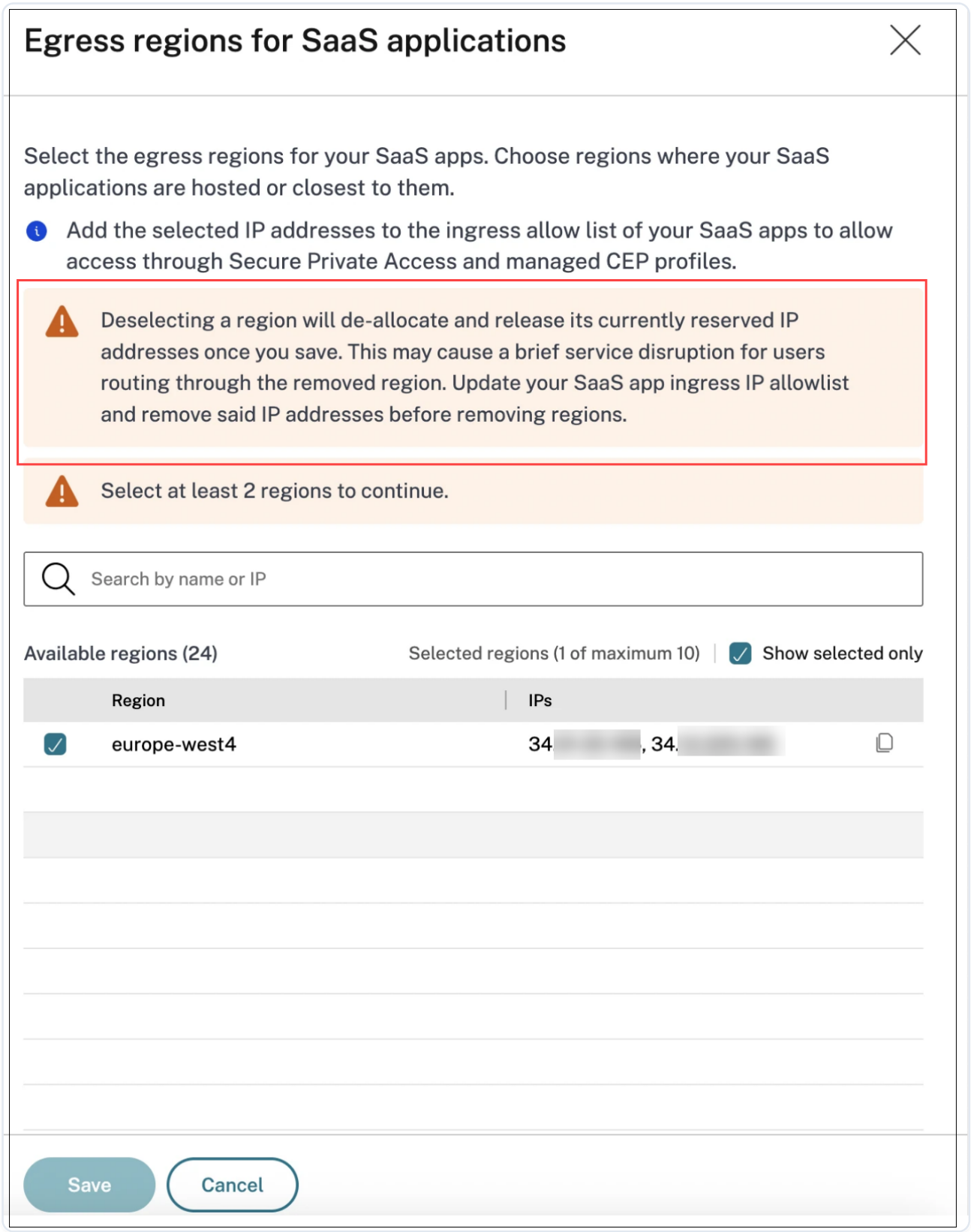
Wählen Sie die Regionen aus, in denen Ihre SaaS-Anwendungen gehostet werden, oder die Regionen, die diesen am nächsten liegen. Um Redundanz bei einem regionalen Ausfall zu gewährleisten, wählen Sie mindestens zwei Regionen aus. Sie können bis zu 10 Regionen auswählen.

Nachdem Google die ausgewählten Regionen bereitgestellt hat und die zugehörigen IP-Adressen verfügbar sind, fügen Sie diese IP-Adressen den Ingress-Zulassungslisten Ihrer SaaS-Anwendungen hinzu.

Eine Region abwählen

Das Abwählen einer Region zeigt eine Warnmeldung an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sie müssen Ihre Zulassungslisten für SaaS-Anwendungen aktualisieren, bevor Sie die Änderungen speichern. Wenn Sie **Abbrechen** auswählen, werden alle Änderungen verworfen.

Wenn Sie später dieselbe Region abwählen und erneut auswählen, weist Google einen neuen Satz von Egress-IP-Adressen zu. Diese IP-Adressen unterscheiden sich in der Regel von den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zuvor zugewiesenen, daher müssen Sie Ihre Zulassungslisten für SaaS-Anwendungen entsprechend aktualisieren.

Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen

Das Google-Verzeichnis erfordert eine verifizierte E-Mail-Adresse für alle Benutzer- und Gruppenobjekte. Dies ist jedoch nicht immer für Verzeichnisse verfügbar, die von Secure Private Access unterstützt werden, insbesondere Active Directory (AD) und Microsoft Entra ID. AD- und Microsoft Entra ID-Objekte verfügen möglicherweise über keine E-Mail-Adresse oder haben eine, die auf eine interne oder spezielle Domäne verweist (zum Beispiel @fabrikam.onmicrosoft.com), die das Google-Verzeichnis nicht verifizieren kann.

Da die E-Mail-Adresse normalerweise als gemeinsamer Bezeichner zwischen Secure Private Access und dem Google-Verzeichnis dient, werden Gruppen aus AD/Entra ohne verifizierte Google-E-Mail-Adresse typischerweise für Secure Private Access-Richtlinien nicht unterstützt. Die Funktion Domänenzuordnung löst dies, indem sie Administratoren ermöglicht, Richtlinien für Gruppen zu konfigurieren, selbst wenn diese keine E-Mail-Adresse haben oder eine E-Mail-Adresse mit einer nicht verifizierten Domäne besitzen.

Wie die Domänenzuordnung funktioniert

- Betrachten Sie eine Gruppe in Ihrem AD ohne E-Mail-Adresse.

  AD-Gruppe ohne E-Mail(/en-us/citrix-secure-private-access/media/group-without-email.png)

- Diese Gruppe wird im Google-Verzeichnis mit einer E-Mail-Adresse repliziert, die aus dem allgemeinen Gruppennamen (beachten Sie, dass Leerzeichen in einer E-Mail-Adresse nicht unterstützt werden und daher weggelassen werden) und einer verifizierten Google-Domäne `@groups.fabrikam.com` synthetisiert wird. Die effektive Google-Gruppen-E-Mail-Adresse, `noemailgroup@groups.fabrikam.com`, existiert nicht im Quellverzeichnis.

  Gruppenreplikation(/en-us/citrix-secure-private-access/media/replication-group-without-email.png)

- Der Administrator kann die Domänenzuordnung für Gruppen ohne E-Mail-Adresse konfigurieren.

  a. Navigieren Sie in der Secure Private Access-Administratorkonsole zu **Browsereinstellungen > Domänenzuordnung**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Schalten Sie den Schalter **Leere Domäne einschließen** auf EIN, um die Zuordnung von Gruppen ohne E-Mail-Adressen zu ermöglichen.

c. Geben Sie im Feld **Google-Domänen > Domänen** die Zieldomäne der Gruppe ein (`groups.fabrikam.com` in diesem Beispiel). Durch Hinzufügen der Zieldomäne der Gruppe ermöglichen Sie dem Administrator, Gruppen ohne E-Mail der entsprechenden Google-Domänen-E-Mail (`groups.fabrikam.com`) zuzuordnen, wenn Richtlinien konfiguriert werden.

Beim Zuweisen von Gruppen zu einer Richtlinie wird, wenn Sie nach der Gruppe ohne E-Mail-Adresse suchen (`noemailgroup`), eine E-Mail-Adresse basierend auf Ihrer Domänenzuordnungskonfiguration synthetisiert und `noemailgroup@groups.fabrikam.com` wird verfügbar. Diese Konvertierung basiert auf einer vorab festgelegten Konvertierungslogik. Einzelheiten finden Sie unter E-Mail-Adresskonstruktion.

Benutzerauswahl(/en-us/citrix-secure-private-access/media/conversion-group-without-email.png)

E-Mail-Adresskonstruktion

- Für Gruppen ohne vorhandene E-Mail-Adresse:
  - Der lokale Teil der E-Mail-Adresse wird mit der Kleinbuchstabenversion des Group Common Name (cn) gefüllt, wobei Leerzeichen weggelassen werden.
  - Der Domänenteil der E-Mail-Adresse wird mit der Kleinbuchstabenversion der Google-Domäne (google-domain) gefüllt.
  - Domänenauswahl (wenn mehrere Google-Domänen vorhanden sind): Wenn eine Gruppe mit mehreren Google-Domänen verknüpft ist, kann der Administrator die entsprechende Domäne für die E-Mail-Adresse auswählen.
- Für Gruppen mit einer vorhandenen onmicrosoft.com- oder anderweitigen E-Mail-Adresse in einer nicht verifizierten Domäne:
  - Lokaler Teil der E-Mail-Adresse: Der lokale Teil der E-Mail-Adresse wird mit der Kleinbuchstabenversion des lokalen Teils der vorhandenen E-Mail-Adresse gefüllt.
  - Domänenauswahl (wenn mehrere Google-Domänen vorhanden sind): Wenn eine Gruppe mit mehreren Google-Domänen verknüpft ist, kann der Administrator die entsprechende Domäne für die E-Mail-Adresse auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einschränkungen

Die Domänenzuordnungsfunktion unterstützt nur Gruppen mit alphanumerischen Zeichen, Bindestrichen, Unterstrichen und Leerzeichen.

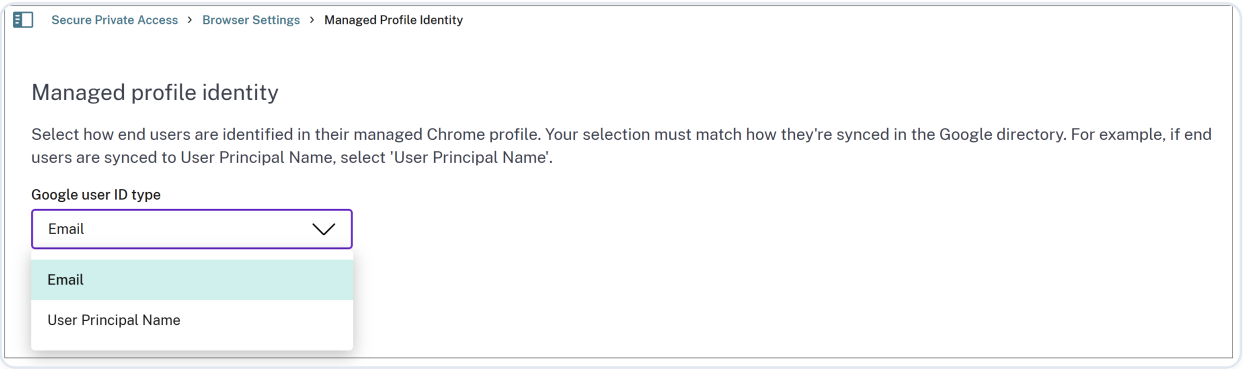
Verwaltete Profilidentität

Das Google-Verzeichnis identifiziert jedes Benutzerkonto anhand einer primären E-Mail-Adresse. Wenn Ihre Organisation Benutzer aus Active Directory oder Microsoft Entra ID mit dem Google-Verzeichnis synchronisiert, wählen Sie aus, welches Quellattribut diese Adresse wird. Die meisten Organisationen ordnen die E-Mail-Adresse zu. Organisationen, die das E-Mail-Attribut nicht für jeden Benutzer ausfüllen, können stattdessen den Benutzerprinzipalnamen (UPN) zuordnen, da der UPN immer in Active Directory vorhanden ist.

Secure Private Access muss jeden Benutzer anhand desselben Attributs suchen, das Ihre Verzeichnissynchronisierung als primäre Adresse verwendet hat, da es sonst den Benutzer nicht seinem Konto im Google-Verzeichnis zuordnen kann. Sie können das Attribut auf der Seite „Verwaltete Profilidentität“ in der Secure Private Access-Administratorkonsole festlegen.

Benutzerattributtyp einrichten

1. Navigieren Sie in der Secure Private Access-Administratorkonsole zu **Browsereinstellungen > Verwaltete Profilidentität**.
2. Wählen Sie unter **Google-Benutzer-ID-Typ** das Attribut aus, das Secure Private Access zur Identifizierung von CEP-Endbenutzern verwendet.



   - **E-Mail** – Secure Private Access identifiziert Endbenutzer anhand ihrer E-Mail-Adresse. Dies ist der Standardwert und der, der von bestehenden Bereitstellungen verwendet wird.
   - **Benutzerprinzipalname** – Secure Private Access identifiziert Endbenutzer anhand ihres Benutzerprinzipalnamens (UPN).

3. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Überprüfen Sie im Bestätigungsfenster **Google-Benutzer-ID-Typ aktualisieren?** die Meldung und klicken Sie auf **Aktualisieren**.

Eine Bestätigungsmeldung wird angezeigt, wenn die Einstellung gespeichert wurde.

HINWEIS:

- Die Einstellung **Google-Benutzer-ID-Typ** gilt nur für Benutzer. Google-Gruppen haben keinen Benutzerprinzipalnamen, daher bleibt die Gruppenidentität unberührt. Wenn Ihre Gruppen im Quellverzeichnis keine E-Mail-Adresse haben, siehe Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen.
- Die Einstellung wird mandantenweit angewendet. Sie können kein anderes Identitätsattribut für einzelne Benutzer auswählen.

Open ID Connect mit Citrix Identity und Zugriffsverwaltung

Sie können Single Sign-On (SSO) für Chrome Enterprise Premium (CEP) mithilfe des OpenID Connect (OIDC)-Authentifizierungsanbieters für Citrix Cloud konfigurieren. Die OIDC-Integration mit Citrix Identity bietet die folgenden Vorteile:

- **Integration des Device Posture service:** Durch die Integration des Device Posture service mit Google Chrome Enterprise Premium können Sie Gerätekonformitätsprüfungen auf Chrome-Browser-basierte Zugriffsszenarien ausweiten. Diese Integration ermöglicht es Organisationen, Gerätestatusrichtlinien durchzusetzen, wenn Benutzer über ihre verwalteten Google Chrome-Profile auf Anwendungen zugreifen. Um den Device Posture service für diese Integration zu nutzen, empfehlen wir die Konfiguration regelmäßiger Gerätestatus-Scans.

  HINWEIS:

  Diese Integration funktioniert nicht, wenn der Device Posture service im Modus für mehrere Stores konfiguriert ist.

  Weitere Informationen zum Device Posture service finden Sie unter Übersicht über den Gerätestatus.

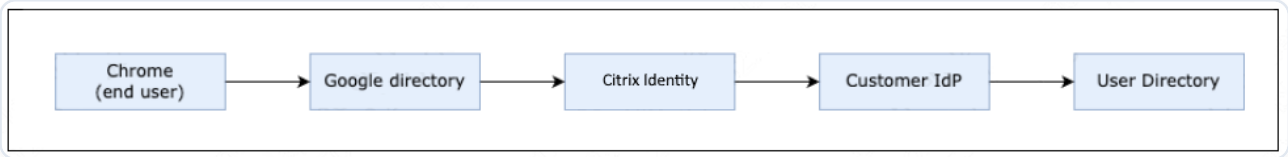
- **Einheitliches Anmeldeerlebnis:** Während Sie SSO für Chrome für die meisten gängigen Identitätsanbieter konfigurieren können, einschließlich, aber nicht beschränkt auf Active

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Directory (AD) und Microsoft Entra (ehemals Azure AD), können Sie sich für ein einheitliches Anmeldeerlebnis sowohl für Cloud-Stores als auch für CEP entscheiden.

Übersicht

OIDC ermöglicht SSO unter Verwendung von Citrix Identity als OIDC-Authentifizierungsanbieter. Die an OIDC beteiligten Komponenten sind im folgenden Diagramm dargestellt:



Google Chrome versucht beim Erstellen eines verwalteten Profils immer, sich gegenüber dem Google-Verzeichnis zu authentifizieren. Mit OIDC wird das Google-Verzeichnis im Wesentlichen zu einer Relying Party (RP) gegenüber Citrix Identity, das ein OIDC Connect Provider ist. Im Gegenzug ermöglicht Citrix Identity Folgendes:

- Gerätestatusfunktionen
- Ein gemeinsames und einheitliches Anmeldeerlebnis für Chrome und Cloud-Stores.

Voraussetzungen

Bevor Sie die OIDC-Authentifizierung mit Citrix Identity konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie haben administrativen Zugriff auf die Google Admin-Konsole.
- Sie haben die Verzeichnissynchronisierung konfiguriert und durchgeführt. Weitere Informationen finden Sie unter Benutzerverzeichnis, das in Citrix Identity konfiguriert ist, mit dem Google Cloud-Benutzerverzeichnis synchronisieren.
- Der Benutzeridentitätsanbieter (IdP) ist in Citrix Cloud Identity and Access Management eingerichtet und konfiguriert. Die folgenden Identitätsanbieter werden unterstützt:
  - Active Directory (AD) – Standard-On-Premises-Active Directory-Integration
  - Active Directory mit Token – AD-Integration mit tokenbasierter Authentifizierung
  - Microsoft Entra ID – Cloudbasierter Identitätsdienst (ehemals Azure AD)
  - Okta
  - SAML 2.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Single Sign-On (SSO) für Chrome Enterprise Premium (CEP), das Citrix Cloud als OpenID Connect (OIDC)-Authentifizierungsanbieter verwendet, unterstützt jetzt die bedingte Authentifizierung.

- Weitere Informationen zu Citrix Cloud Identity and Access Management finden Sie unter Identitäts- und Zugriffsverwaltung.
- Sie haben konfiguriert, wie Abonnenten sich bei ihren Stores authentifizieren, indem Sie einen der zuvor genannten Identitätsanbieter ausgewählt haben. Anweisungen zur Konfiguration der Store-Authentifizierung finden Sie unter Authentifizierung konfigurieren.
- Sie haben die Ersteinrichtung und das Onboarding von Secure Private Access bereits abgeschlossen. Weitere Informationen finden Sie unter Secure Private Access Onboarding und Einrichtung.

OIDC-Integrationsübersicht

Um die Anmeldung mit verwalteten Google Chrome-Profilen in Ihren konfigurierten Citrix Identitätsanbieter zu integrieren, muss ein Google OIDC SSO-Profil einem Citrix OIDC-Client zugeordnet werden. Gehen Sie dazu wie folgt vor:

1. Erstellen Sie in der Google Admin-Konsole ein neues SSO-Profil, indem Sie einen Profilnamen eingeben. Die anderen Felder können Sie vorerst leer lassen. Details zum Erstellen eines neuen SSO-Profils und einer Weiterleitungs-URL finden Sie unter Ein Google OIDC SSO-Profil erstellen.
2. Nachdem das SSO-Profil erstellt wurde, kopieren Sie die für dieses Profil generierte Weiterleitungs-URL.
3. Erstellen Sie in der Secure Private Access-Konsole den Citrix OIDC-Client und fügen Sie die Weiterleitungs-URL (aus dem Google SSO-Profil) in das Feld **Weiterleitungs-URL** ein. Details zum Erstellen eines Citrix OIDC-Clients finden Sie unter Einen Citrix OIDC-Client erstellen.
4. Sobald der OIDC-Client erstellt ist, notieren Sie sich die Client-ID, das Client-Geheimnis und die Aussteller-URL, die in der Secure Private Access-Konsole angezeigt werden.
5. Kehren Sie zur Google Admin-Konsole zurück und aktualisieren Sie das SSO-Profil mit der Client-ID, dem Client-Geheimnis und der Aussteller-URL aus der Secure Private Access-Konsole.

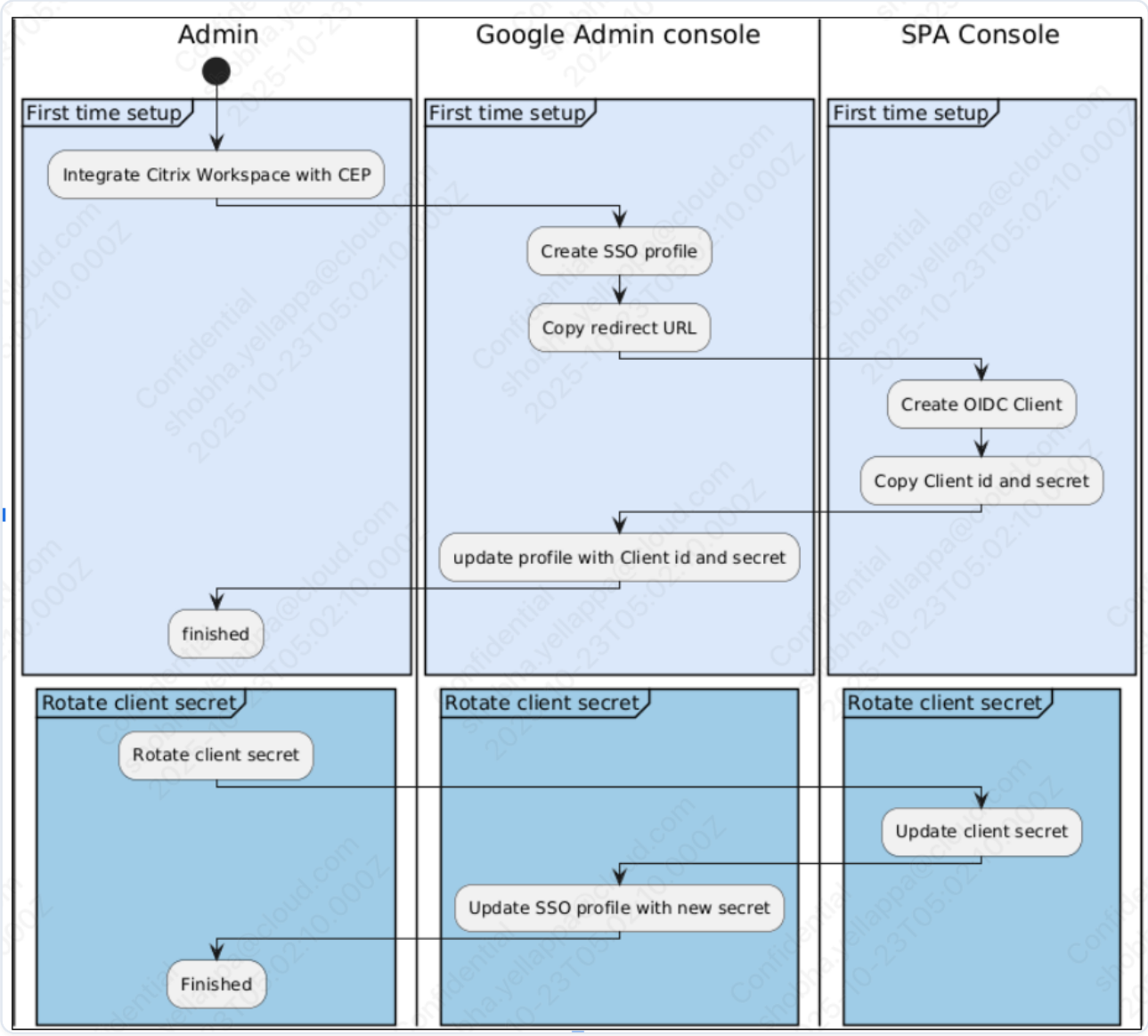
© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Wählen Sie unter **SSO-Profilzuweisungen verwalten** das Google SSO-Profil aus, das Sie zur Vervollständigung der Integration konfiguriert haben.

HINWEIS:

Nach der Erstellung des OIDC-Clients können Sie das Client-Geheimnis in der Secure Private Access-Konsole rotieren und das SSO-Profil in der Google Admin-Konsole aktualisieren.

Das folgende Diagramm veranschaulicht den OIDC-Integrationsworkflow:



Ein Google OIDC SSO-Profil erstellen

Führen Sie die folgenden Schritte in der Google Admin-Konsole aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Gehen Sie zu **Sicherheit > Authentifizierung > SSO mit Drittanbieter-IdP** und wählen Sie dann **OIDC-Profil hinzufügen**.
2. Geben Sie einen Namen für das Profil an.
3. Weisen Sie der Client-ID und dem Client-Geheimnis einen Dummy-Wert zu oder lassen Sie diese leer. Diese Felder werden später aktualisiert.
4. Geben Sie unter **Aussteller-URL** `https://accounts.cloud.com/core` ein.
5. Klicken Sie auf **Speichern**.

OIDC-SSO-Profil erstellen(/en-us/citrix-secure-private-access/media/spa-cep-create-oidc-profile.png)

Klicken Sie nach dem Erstellen des Profils darauf, um die Umleitungs-URI zu erhalten, die zum Erstellen des OIDC-Clients benötigt wird.

OIDC-Umleitungs-URI(/en-us/citrix-secure-private-access/media/spa-cep-redirect-uri.png)

Einen Citrix OIDC-Client erstellen

Führen Sie die folgenden Schritte in der Secure Private Access-Administratorkonsole aus:

1. Klicken Sie im Navigationsbereich auf **Browsereinstellungen > Open ID Connect (OIDC)**.

   HINWEIS:

   Die Option **Open ID Connect (OIDC)** im Menü **Browsereinstellungen** ist erst verfügbar, nachdem der Onboarding-Prozess abgeschlossen ist.

2. Geben Sie unter **E-Mail des Besitzers** die E-Mail-Adresse des Benutzers ein. Diese E-Mail-Adresse ist erforderlich, um Benachrichtigungen zu senden, wenn das OIDC-Client-Geheimnis abläuft.
3. Geben Sie unter **Umleitungs-URL** die Umleitungs-URI ein, die in der Google Admin-Konsole generiert wurde, als Sie das Google OIDC-SSO-Profil erstellt haben. Der Identitätsanbieter antwortet auf Benutzerauthentifizierungsanfragen über diese URL.
4. Wählen Sie den Identitätsanbieter aus, der in Ihrer Umgebung konfiguriert ist.
5. Klicken Sie auf **Erstellen**.

   Einen OIDC-Client erstellen(/en-us/citrix-secure-private-access/media/spa-cep-create-oidc-client.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie erfolgreich einen OIDC-Client erstellt haben, wird ein Pop-up-Fenster mit der Client-ID, dem Client-Geheimnis und der Aussteller-URL angezeigt. Sie müssen diese Details in Ihre Google Admin-Konsolenkonfiguration kopieren. Sie können die Anmeldeinformationen mit einer der folgenden Methoden abrufen:

- Kopieren der Werte direkt aus dem Pop-up-Fenster
- Herunterladen der Details als CSV-Datei zur sicheren Speicherung

WICHTIG:

Das Client-Geheimnis ist nur während dieses anfänglichen Einrichtungsschritts sichtbar. Sie müssen das Client-Geheimnis abrufen, bevor Sie das Pop-up-Fenster schließen oder mit dem nächsten Schritt fortfahren. Sobald das Fenster geschlossen ist, kann das Client-Geheimnis nicht erneut angezeigt werden, und Sie müssen das Geheimnis rotieren, um ein neues zu erhalten.

6. Klicken Sie auf **Schließen**.

Zuweisung des OIDC-SSO-Profils

Sobald der OIDC-Client erstellt und das Google OIDC-SSO-Profil mit der Client-ID und dem Geheimnis aktualisiert wurde, muss das OIDC-SSO-Profil den Benutzern und Gruppen zugewiesen werden, damit SSO wirksam wird.

1. Gehen Sie in der Google Admin-Konsole zu **Sicherheit > Authentifizierung > SSO mit IdP von Drittanbietern**.
2. Klicken Sie unter **SSO-Profilzuweisungen verwalten** auf **Verwalten**.
3. Wählen Sie im linken Navigationsbereich die Stammorganisationseinheit (OU) und Ihr SSO-Profil aus, um SSO für alle Benutzer Ihrer Organisation zu aktivieren. Alternativ können Sie das SSO-Profil bestimmten Gruppen oder OUs zuweisen.

Citrix OIDC-Client aktualisieren

Das Citrix OIDC-Client-Geheimnis hat eine Standardlebensdauer von zwei Jahren. Sie können die OIDC-Sicherheit aufrechterhalten oder auf einen potenziellen Sicherheitsvorfall reagieren, indem Sie das Client-Geheimnis rotieren. Die Rotation des Client-Geheimnisses ist eine kritische Sicherheitsmaßnahme, die durchgeführt werden muss, wenn ein vorhandenes Geheimnis kurz vor dem Ablauf steht oder als Teil der proaktiven Sicherheitswartung. Jedes Mal, wenn Sie ein Client-Geheimnis rotieren, wird ein neues Geheimnis generiert. Das alte Geheimnis bleibt bis zu seinem

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ursprünglichen Ablaufdatum gültig, um einen reibungslosen Übergang ohne SSO-Authentifizierungsausfall zu gewährleisten. Stellen Sie sicher, dass Sie Ihre Google Admin-Konsolenkonfiguration nach jeder Rotation so schnell wie möglich mit dem neuen Client-Geheimnis aktualisieren.

Führen Sie die folgenden Schritte aus, um die Client-Geheimnisse zu rotieren

1. Klicken Sie in der Admin-Konsole auf die Seite **Einstellungen > Open ID Connect (OIDC)-Client**.
2. Klicken Sie auf **Client-Geheimnis rotieren**, um ein neues Geheimnis zu generieren. Eine Bestätigungsmeldung wird angezeigt.
3. Aktivieren Sie den Umschalter, um der Bestätigungsmeldung zuzustimmen, und klicken Sie dann auf **Rotieren**.

   HINWEIS:

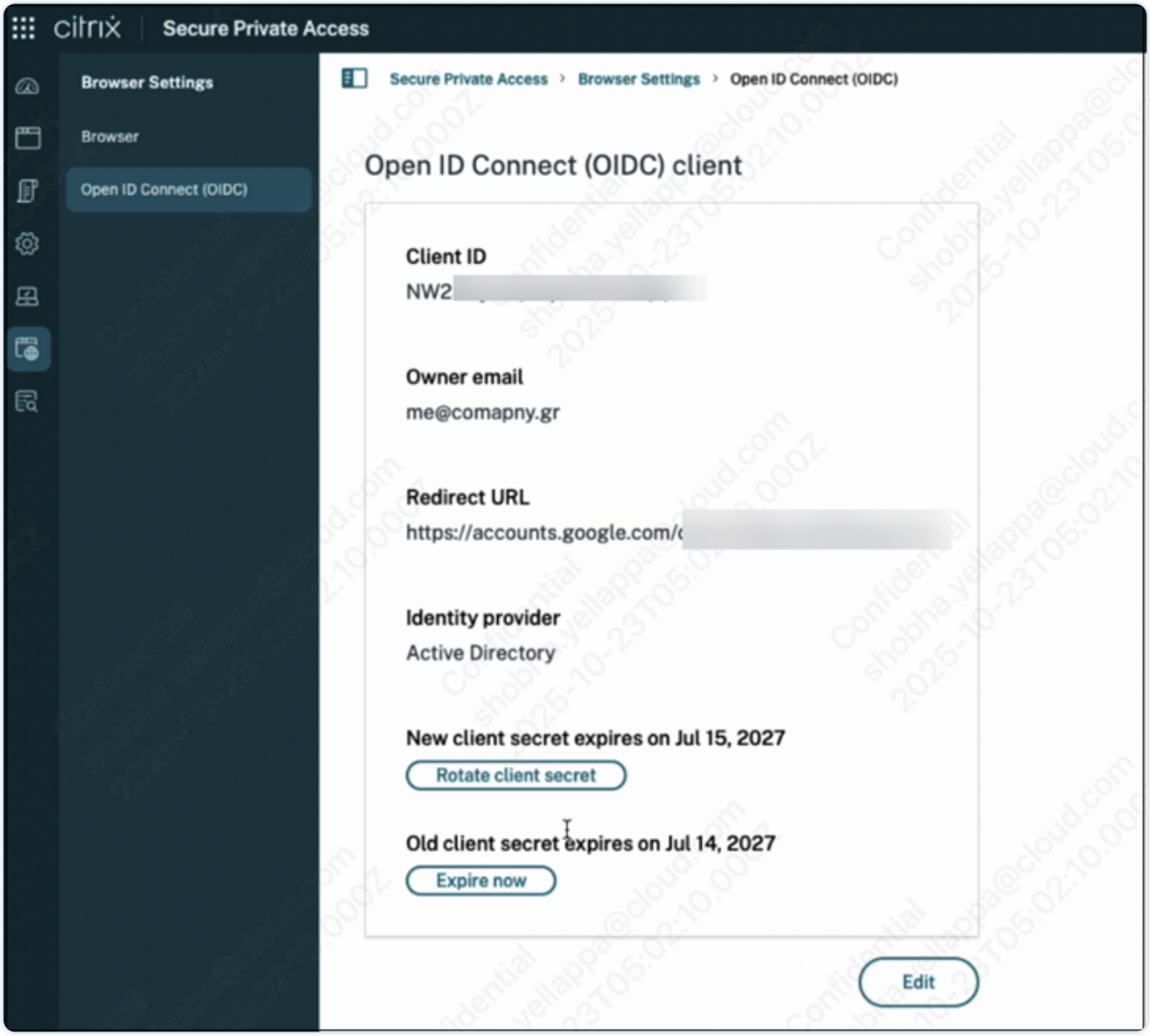
   - Das alte Client-Geheimnis bleibt bis zu seinem Ablauf gültig. Dadurch können Sie Google Workspace ohne Authentifizierungsausfall aktualisieren.
   - Wenn Sie aus Sicherheitsgründen sofort ablaufen lassen möchten, klicken Sie auf **Jetzt ablaufen lassen**.
   - Die Client-ID bleibt während dieses Vorgangs unverändert.

4. Klicken Sie auf **Schließen**.
5. Aktualisieren Sie das neue Geheimnis sofort in Ihrer Google Workspace-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Sie müssen das neue Client-Geheimnis in Ihrer Google OIDC SSO-Profilkonfiguration aktualisieren, bevor das vorherige Geheimnis abläuft, um eine unterbrechungsfreie OIDC-Authentifizierung aufrechtzuerhalten. Wenn das Geheimnis nicht rechtzeitig aktualisiert wird, wird die Authentifizierung unterbrochen, was zu Zugriffsproblemen für Benutzer und Dienste führen kann.
- Eine regelmäßige Rotation von Client-Geheimnissen wird empfohlen, um Risiken durch unbefugten Zugriff zu mindern und die Integrität des Authentifizierungssystems aufrechtzuerhalten.
- Sobald Sie das Geheimnis des Google OIDC SSO-Profils aktualisiert haben, wird empfohlen, das alte Geheimnis ablaufen zu lassen.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

OIDC-Client löschen

Ein Client-Geheimnis kann nach Ablauf nicht mehr rotiert werden. Wenn das Client-Geheimnis abläuft, bevor es rotiert wird, wird es ungültig. In diesem Fall müssen Sie den vorhandenen Client löschen und einen neuen erstellen.

Führen Sie die folgenden Schritte in der Secure Private Admin-Konsole aus.

1. Klicken Sie auf **Bearbeiten** auf der Seite des Open ID Connect (OIDC)-Clients.
2. Klicken Sie auf **Client löschen**.

   Eine Bestätigungsmeldung wird angezeigt.
3. Schieben Sie den Schalter auf EIN und klicken Sie dann auf **Client löschen**.

Endbenutzererfahrung

Benutzer können über Secure Private Access mithilfe der folgenden Methoden auf Anwendungen zugreifen. Jede Zugriffsmethode bietet eine andere Benutzererfahrung, wodurch Organisationen den am besten geeigneten Ansatz basierend auf ihrer gewünschten Benutzererfahrung und Bereitstellungsstrategie wählen können.

- **Citrix Workspace-App** – Die native Desktop-Anwendung, die die sicherste und funktionsreichste Zugriffserfahrung mit vollständiger Richtliniendurchsetzung und Single Sign-On-Funktionen bietet.
- **Store-URL in einem Webbrowser** – Benutzer können ihren Store in einem Webbrowser öffnen:
  - Nicht-Chrome-Browser (wie Firefox, Safari oder Edge)
  - Chrome mit nicht verwaltetem Profil (persönlicher Chrome-Browser ohne Unternehmensrichtlinien)
  - Chrome mit verwaltetem Profil (unternehmensverwalteter Chrome-Browser mit Chrome Enterprise Premium-Richtlinien)
- **Verwaltetes Chrome-Profil** – Benutzer greifen direkt auf Anwendungen zu, indem sie Lesezeichen verwenden oder die Anwendungs-URL manuell in die Adressleiste eines verwalteten Chrome-Profils eingeben.

Die folgende Tabelle fasst die Endbenutzererfahrung zusammen, wenn die Anwendungen mit verschiedenen Methoden aufgerufen werden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	DIREKT	STORE-URL IN EINEM WEBBROWSER	CITRIX WORKSPACE-APP
Nicht-Chrome-Browser	Zugriff für SaaS-Anwendungen verweigert (vorausgesetzt, die SaaS-Anwendungen wurden mit der entsprechenden IP-Adressen-Zulassungsliste konfiguriert).	Anwendungen werden in der Benutzeroberfläche aufgelistet.	Nicht zutreffend
	Private Apps sind nicht erreichbar.	Die Anwendungen werden im entsprechenden verwalteten Chrome-Profil gestartet.	
		Ein Assistent zur Profilerstellung wird gestartet, wenn das entsprechende verwaltete Profil noch nicht erstellt wurde.	
Chrome (nicht verwaltetes Profil)	Zugriff für SaaS-Apps verweigert (vorausgesetzt, die SaaS-Apps wurden mit der entsprechenden IP-Adressen-Zulassungsliste konfiguriert).	Die Anwendungen werden im entsprechenden verwalteten Chrome-Profil gestartet.	Nicht zutreffend
	Private Apps sind nicht erreichbar.	Ein Assistent zur Profilerstellung wird gestartet, wenn das entsprechende	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	DIREKT	STORE-URL IN EINEM WEBBROWSER	CITRIX WORKSPACE-APP
		verwaltete Profil noch nicht erstellt wurde.	
Chrome (verwaltetes Profil)	Apps werden je nach Secure Private Access-Konfiguration zugelassen oder verweigert.	Die aufgezählte App wird in einem neuen Tab gestartet.	Nicht zutreffend
Citrix Workspace-App	Nicht zutreffend	Nicht zutreffend	Apps werden in der Benutzeroberfläche aufgelistet.
			Die Anwendungen werden im entsprechenden verwalteten Chrome-Profil gestartet.
			Ein Assistent zur Profilerstellung wird gestartet, wenn das entsprechende verwaltete Profil noch nicht erstellt wurde.

Citrix Secure Access-Erweiterung für Chrome Enterprise Premium

Die Citrix Secure Access-Erweiterung für Chrome Enterprise Premium (CEP) ermöglicht den sicheren, clientlosen Zugriff auf interne und externe Anwendungen direkt über den Chrome-Browser. Sie kombiniert die Funktionen von Citrix Secure Private Access und Chrome Enterprise, um Sicherheit auf Unternehmensniveau, Zero-Trust-Zugriff, kontextbezogene Kontrollen und eine moderne Benutzererfahrung zu bieten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Organisationen können diese Erweiterung nutzen, um sicheren Zugriff auf SaaS-Anwendungen, interne Web-Apps, SSH-Server und RDP-Systeme zu ermöglichen, ohne dass VPNs oder native Client-Installationen erforderlich sind.

Die Secure Access-Browsererweiterung wird automatisch installiert, wenn Sie Secure Private Access in Chrome Enterprise Premium integrieren. Anweisungen zur Einrichtung finden Sie unter Google Chrome-Integration einrichten. Nach der Installation können Sie über das Symbol in der oberen rechten Ecke Ihres Chrome-Browsers auf die Erweiterung zugreifen.

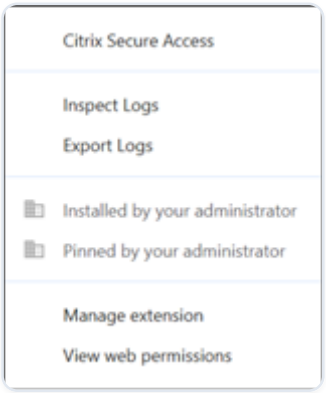


Protokolle der Secure Access-Erweiterung

Die Protokolle der Secure Access-Browsererweiterung sind für die Überwachung und Fehlerbehebung unerlässlich. Endbenutzer können Protokolle überprüfen und herunterladen, um sie bei Problemen mit Administratoren oder Support-Teams zu teilen.

So überprüfen oder laden Sie Protokolle herunter:

1. Klicken Sie mit der rechten Maustaste auf das Symbol der Browsererweiterung.
    - Klicken Sie auf **Protokolle prüfen**, um die Protokolle zu überprüfen.
    - Klicken Sie auf **Protokolle exportieren**, um die Protokolle herunterzuladen.



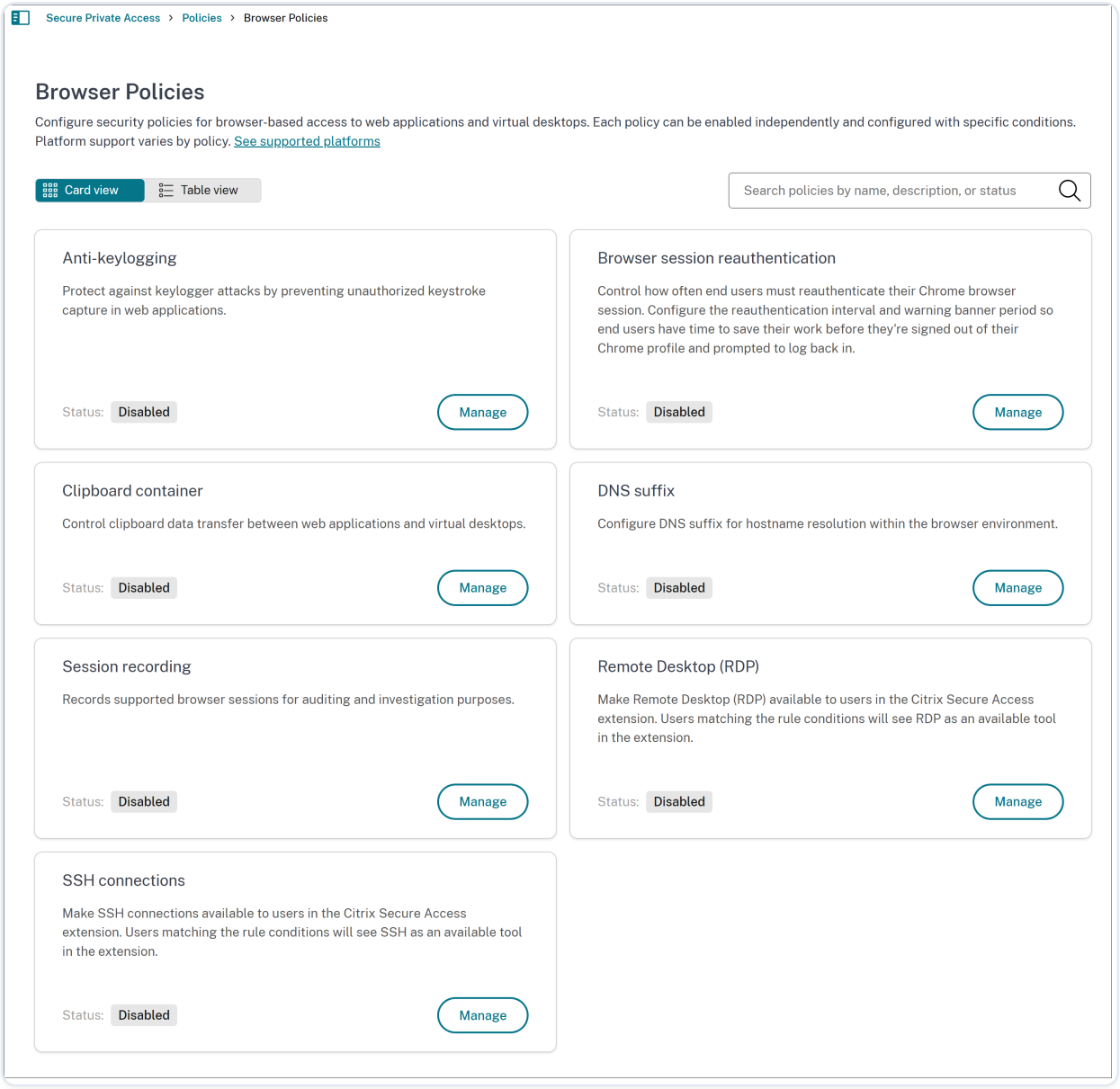
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access-Steuerelemente für Chrome Enterprise

Citrix Secure Private Access unterstützt Sicherheitsrichtlinien, die von der Citrix Secure Access-Erweiterung für Google Chrome Enterprise Premium (CEP) bereitgestellt und erzwungen werden. Weitere Informationen finden Sie unter Unterstützte Steuerelemente.

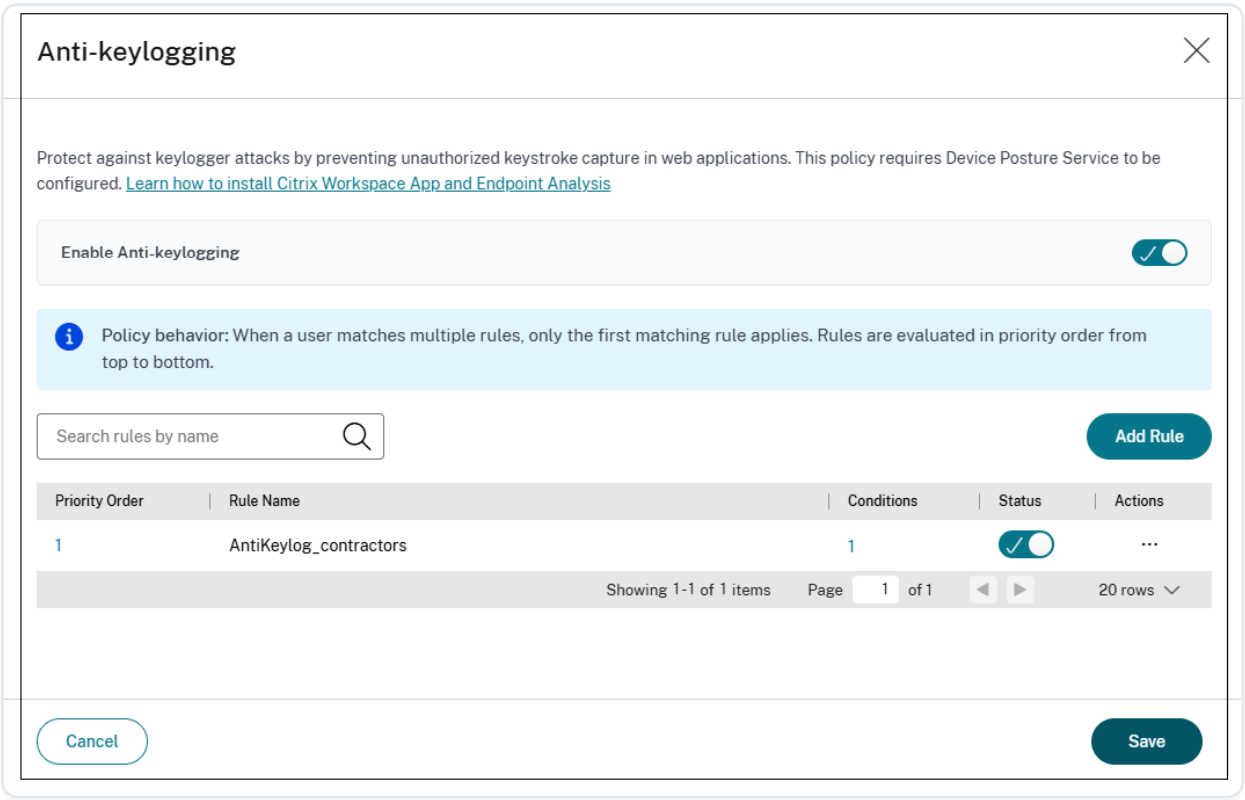
Sie können diese Richtlinien über die Secure Private Access-Administratorkonsole konfigurieren.

1. Gehen Sie zu **Richtlinien > Browserrichtlinien**, und klicken Sie dann auf **Browserrichtlinie erstellen**.
2. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Verwalten**.



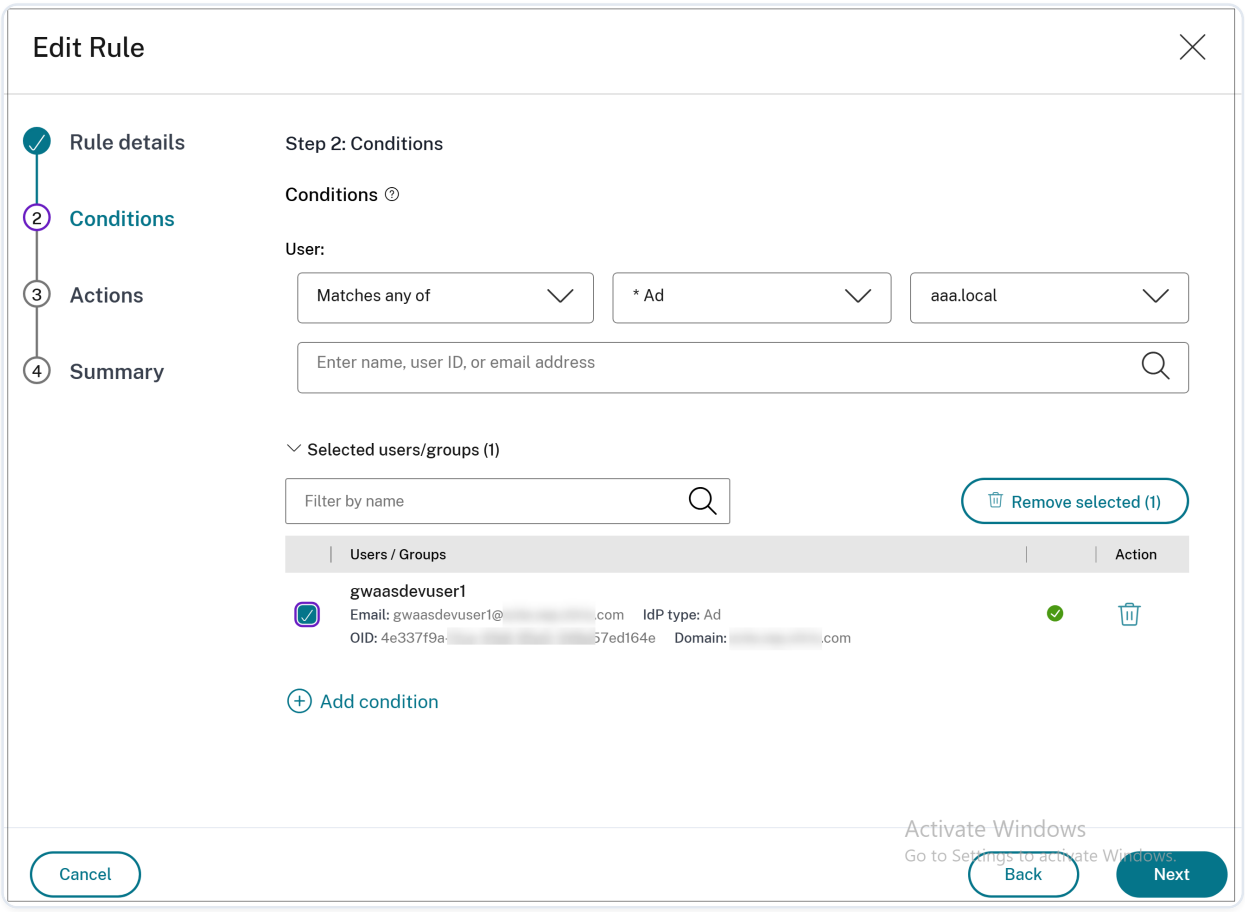
3. Fügen Sie Regeln für die Richtlinie hinzu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Fügen Sie eine Bedingung für den **Zugriffsmodus** hinzu, um Browsersteuerungen auf Browsersitzungen zu beschränken. Bei Browserrichtlinien ist der Wert typischerweise **Browser**. Weitere Informationen zu Zugriffsmodi finden Sie unter Richtlinienerzwingung basierend auf dem Zugriffsmodus.
5. Wählen Sie die Bedingungen aus, für die die Richtlinie ausgewertet werden muss.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Bei der Auswahl von Benutzern oder Gruppen können Administratoren überprüfen, ob Einträge aus dem ausgewählten Benutzerverzeichnis mit Google Directory synchronisiert und dort korrekt konfiguriert sind. Secure Private Access-Richtlinien werden nur dann korrekt ausgewertet, wenn sie synchronisierte Benutzer und Gruppen verwenden. Andernfalls können Warnungen angezeigt werden. Weitere Informationen finden Sie unter Benutzer- und Gruppensynchronisierung überprüfen.

Detaillierte Konfigurationsschritte finden Sie in der Dokumentation für jedes Steuerelement.

Unterstützte Steuerelemente

Citrix unterstützt die folgenden Secure Access-Steuerelemente mit der Integration von Secure Private Access und Chrome Enterprise Premium:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STEUERELEMENT	FUNKTION
Anti-Keylogging	Verschleiert Tastenanschläge, um zu verhindern, dass Keylogger-Malware auf dem Endpunkt Benutzereingaben erfasst.
Zwischenablage-Container	Steuert, was Benutzer zwischen dem Browser und anderen Apps kopieren und einfügen können.
DNS-Suffix	Vervollständigt automatisch kurze interne URLs (z. B. „wiki/“) zu vollständigen Adressen.
Sitzungsaufzeichnung	Zeichnet Browser-Sitzungsaktivitäten für Audit und Compliance auf.
Browser-Sitzungs-Reauthentifizierung	Erzwingt eine periodische Reauthentifizierung von Browser-Sitzungen nach einem konfigurierten Zeitintervall.
SSH-Verbindungen	Ermöglicht Benutzern, SSH-Verbindungen direkt in einem Browser-Tab herzustellen, ohne einen Terminal-Client zu benötigen.
Remotedesktop (RDP)	Ermöglicht Benutzern, Remotedesktop-Sitzungen direkt in einem Browser-Tab zu starten, ohne einen RDP-Client zu benötigen.

Benutzer und Gruppen in Richtlinien

Die folgenden Abschnitte enthalten weitere Informationen zu Benutzern und Gruppen:

Suchen nach Benutzern oder Gruppen

Die von Ihnen ausgewählten Benutzer und Gruppen werden in einem Raster angezeigt. Jede Zeile im Raster zeigt die folgenden Identitätsdetails an, damit Sie identisch benannte Benutzer oder Gruppen über verschiedene Domänen, Gesamtstrukturen oder Identitätsanbieter (IdPs) hinweg eindeutig unterscheiden können:

- **Name** – Der Anzeigename des Benutzers oder der Gruppe.
- **E-Mail** – Die mit der Identität verknüpfte E-Mail-Adresse.
- **IDP-Typ** – Der Identitätsanbieter, z. B. Azure AD, Active Directory, Okta oder Google.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **OID** – Die Objekt-ID oder Sicherheitskennung der Identität.
- **Domäne** – Die Domäne, zu der der Benutzer oder die Gruppe gehört.

Sie können das Raster nach Namen filtern, einzelne Zeilen entfernen oder mehrere Einträge auswählen und diese gemeinsam über **Ausgewählte entfernen** löschen.

Synchronisierte Benutzer und Gruppen verwenden

Bei der Auswahl von Benutzern oder Gruppen können Administratoren überprüfen, ob Einträge aus dem ausgewählten Benutzerverzeichnis mit dem Google-Verzeichnis synchronisiert und korrekt konfiguriert sind. Secure Private Access-Richtlinien werden nur dann korrekt ausgewertet, wenn sie synchronisierte Benutzer und Gruppen verwenden. Andernfalls können die folgenden Warnungen angezeigt werden:

- **Fehlende Mandantenkontoberechtigungen.**

  Abhilfe: Weisen Sie in der Google Admin-Konsole dem Mandanten-Dienstkonto die Berechtigungen **Benutzer > Lesen** und **Gruppen > Lesen** zu. SPA benötigt diese Berechtigungen, um zu überprüfen, ob ein Benutzer oder eine Gruppe existiert.

- **Benutzer oder Gruppe nicht synchronisiert.**

  Abhilfe: Der gesuchte oder ausgewählte Benutzer oder die Gruppe ist nicht mit dem Google-Verzeichnis synchronisiert. Synchronisieren Sie die Verzeichnisentität mit dem Google-Verzeichnis, bevor Sie sie in einer SPA-Richtlinie verwenden.

- **Unzureichende Gruppenzugriffseinstellungen.**

  Abhilfe: Öffnen Sie in der Google Admin-Konsole die Zugriffseinstellungen für die ausgewählte Gruppe und stellen Sie sicher, dass unter **Wer Mitglieder anzeigen kann** mindestens die Option **Gruppenmitglieder** ausgewählt ist.

HINWEIS:

Diese Funktion ist erst verfügbar, nachdem die Google Chrome-Integration erfolgreich abgeschlossen wurde.

Anti-Keylogging-Kontrolle

Cyberkriminelle verwenden bösartige Software wie Keylogger, um sensible Informationen wie Passwörter, Kreditkartennummern und vertrauliche Unternehmensdaten zu stehlen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Citrix Secure Access Browsererweiterung für Chrome Enterprise Premium (CEP) unterstützt Anti-Keylogging, um Ihre Daten zu schützen. Diese Funktion verschlüsselt Tastenanschläge, sodass, wenn ein bösartiges Programm versucht, die eingegebene Eingabe zu erfassen, es nur unlesbare Zeichen aufzeichnet, während der tatsächliche Text sicher an Ihre Arbeitsanwendungen übermittelt wird.

Unterstützte Bereitstellungen: Citrix Secure Private Access Service und Hybridbereitstellungen.

Unterstützte Plattformen: Windows 11 und höher.

HINWEIS:

Anti-Keylogging wird für native RDP-Sitzungen nicht unterstützt.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie Anti-Keylogging aktivieren:

- CWA Version 2603 und höher ist installiert.
- Die Integration zwischen Citrix Secure Access und Chrome Enterprise Premium (CEP) ist abgeschlossen.

Anti-Keylogging-Richtlinie konfigurieren

1. Melden Sie sich bei der Secure Private Access Admin-Konsole an.
2. Gehen Sie zu **Policies > Browser Policies** und klicken Sie dann auf **Create browser policy**.
3. Wählen Sie **Anti-keylogging** und klicken Sie dann auf **Manage**.
4. Klicken Sie auf **Regel hinzufügen**, um Regeln für die Benutzer hinzuzufügen, um Anti-Keylogging zu aktivieren.
    a. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.
    b. Wählen Sie Bedingungen basierend auf Ihren Anforderungen aus, z. B. Benutzer oder Gruppe. Sie können auch Bedingungen wie **Geo-Standort**, **Netwerkstandort** und **Geräte-Posture-Check** hinzufügen.
    c. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Anzahl der Regeln, die für die Anti-Keylogging-Richtlinie konfiguriert sind, wird auf der Registerkarte **Browserrichtlinien > Anti-Keylogging** angezeigt.

Steuerung des Zwischenablage-Containers

Bereitstellungen, die Chrome für den Webzugriff und VDI für native Anwendungen verwenden, können die Funktion des Zwischenablage-Containers nutzen, um die Datenfreigabe zwischen dem Browser und VDI-Sitzungen zu steuern. Zwischenablagedaten werden direkt zwischen Citrix-Sitzungen übertragen, ohne in die Zwischenablage des lokalen Endpunkts geschrieben zu werden. Dies verbessert die Sicherheit und bietet den Benutzern gleichzeitig Flexibilität bei der Arbeit in beiden Umgebungen.

Unterstützte Bereitstellungen: Secure Private Access Service und Hybridbereitstellungen.

Unterstützte Plattformen: Windows.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die Integration zwischen Citrix Secure Access und Chrome Enterprise Premium (CEP) ist abgeschlossen.
- Citrix Workspace-App 2603.10 oder höher.
- Windows VDA mit 2607 LTSR oder höher (GA-Version für Clipboard Sharing Scope). Weitere Informationen finden Sie unter Clipboard Sharing Scope.
- Windows VDA mit 2507 LTSR (Vorschauversion für Clipboard Sharing Scope), aktivieren Sie Folgendes:
  - Funktion **Cross clipboard container with DaaS**. Weitere Informationen finden Sie unter Cross clipboard container with DaaS. Diese Funktion ist derzeit als Vorschau in DaaS verfügbar.
  - Registrierung **Clipboard Sharing Scope**. Weitere Informationen finden Sie unter Enable the Clipboard Sharing Scope registry.

Zwischenablage-Container-Steuerung aktivieren

1. Melden Sie sich bei der Secure Private Access-Administrationskonsole an.
2. Gehen Sie zu **Policies > Browser Policies** und klicken Sie dann auf **Create browser policy**.
3. Wählen Sie **Clipboard container** aus, und klicken Sie dann auf **Verwalten**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Klicken Sie auf **Regel hinzufügen**, um Regeln für die Zwischenablagefreigabe zwischen VDA und Browser hinzuzufügen.

   a. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.

   b. Wählen Sie Bedingungen basierend auf Ihren Anforderungen aus, z. B. Benutzer oder Gruppe. Sie können auch Bedingungen wie **Geo-location**, **Netwerkstandort** und **Device posture check** hinzufügen.

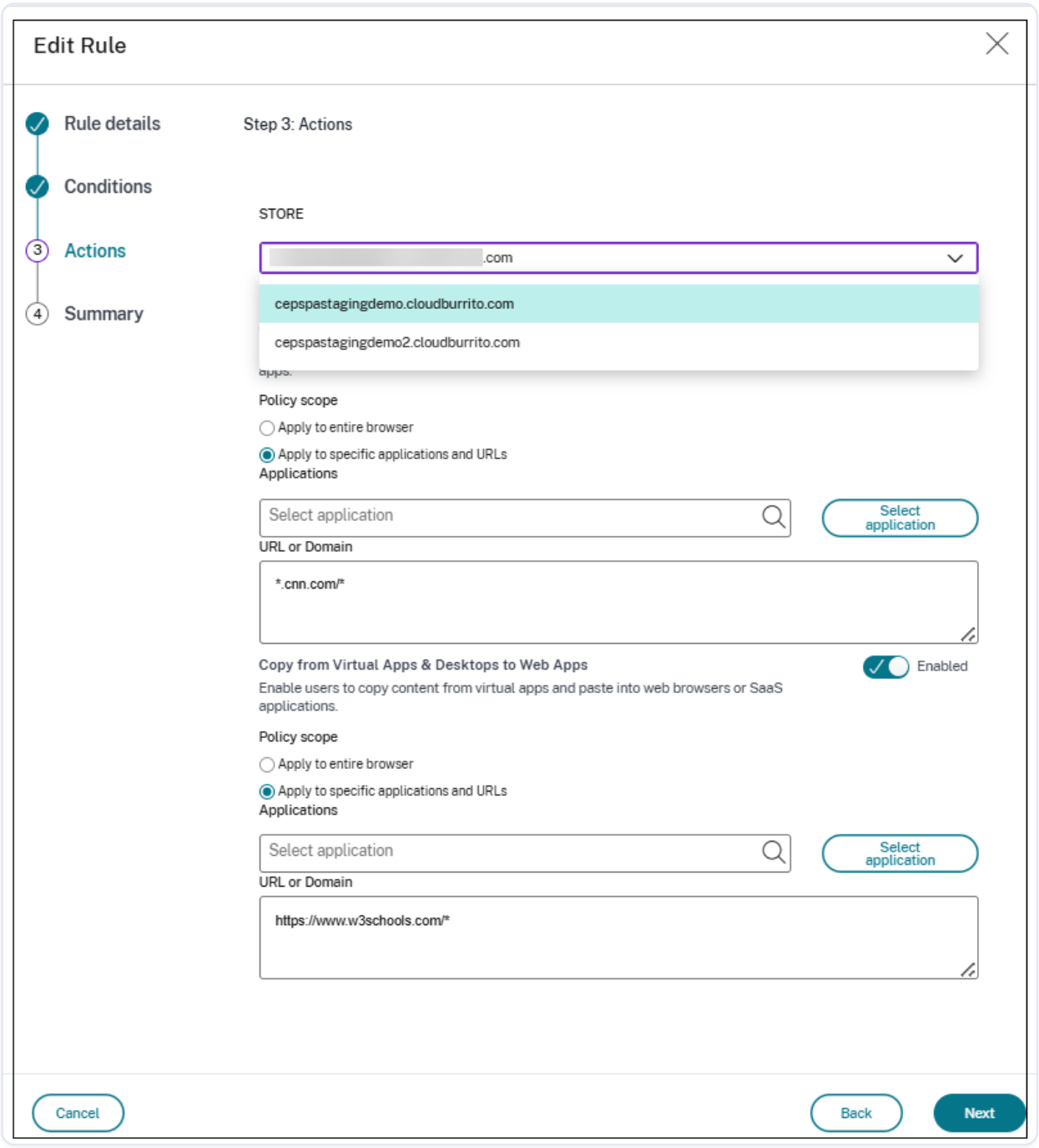
   c. Klicken Sie auf **Weiter**.

   d. Definieren Sie die URL und die Secure Private Access-Anwendungen, um die Zwischenablagefreigabe zu ermöglichen.

   e. Wählen Sie den Richtlinienbereich aus.

   - **Auf gesamten Browser anwenden** — Die Richtlinie steuert alle Zwischenablageaktivitäten im verwalteten Profil.
   - **Auf bestimmte Anwendungen und URLs anwenden** — Die Richtlinie ist auf ausgewählte Anwendungen und die eingegebenen URL-/Domänenmuster beschränkt.
     - **Anwendung auswählen** — Wählen Sie die spezifischen veröffentlichten Anwendungen mithilfe der Anwendungsauswahl aus.
     - **URL oder Domäne** – Geben Sie die URL oder die Domänen der spezifischen Anwendung ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Klicken Sie auf **Speichern**.

   Die Anzahl der für die Zwischenablagecontainer-Richtlinie konfigurierten Regeln wird auf der Registerkarte **Browserrichtlinien > Zwischenablagecontainer** angezeigt.

Umfang der Zwischenablagefreigabe aktivieren

Für VDA-Version 2607:

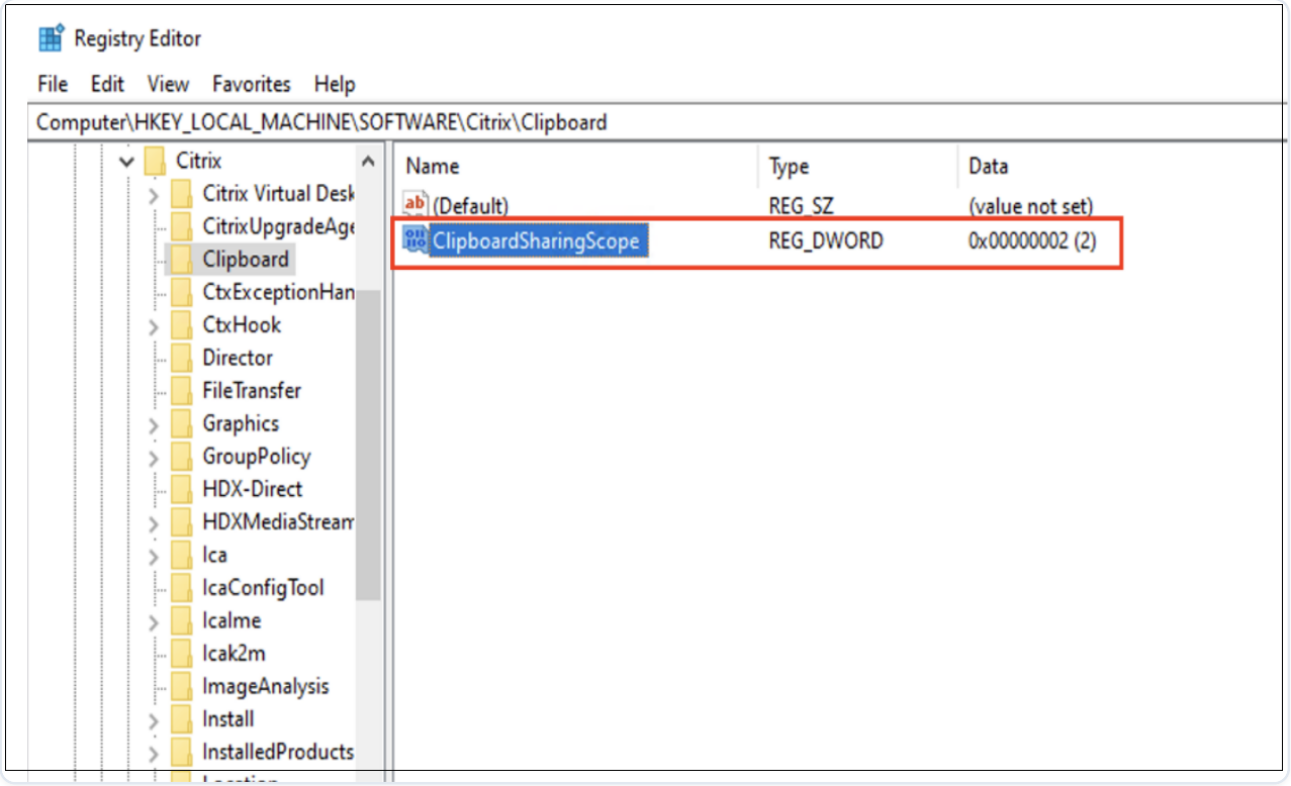
Siehe Funktionsweise.

Für VDA-Version 2507:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aktivieren Sie diesen Registrierungseintrag **Clipboard Sharing Scope**.

1. Öffnen Sie den Windows-Registrierungs-Editor mit regedit.exe.
2. Navigieren Sie zu HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\.
3. Erstellen Sie einen REG_DWORD-Wert mit dem Namen `ClipboardSharingScope`.

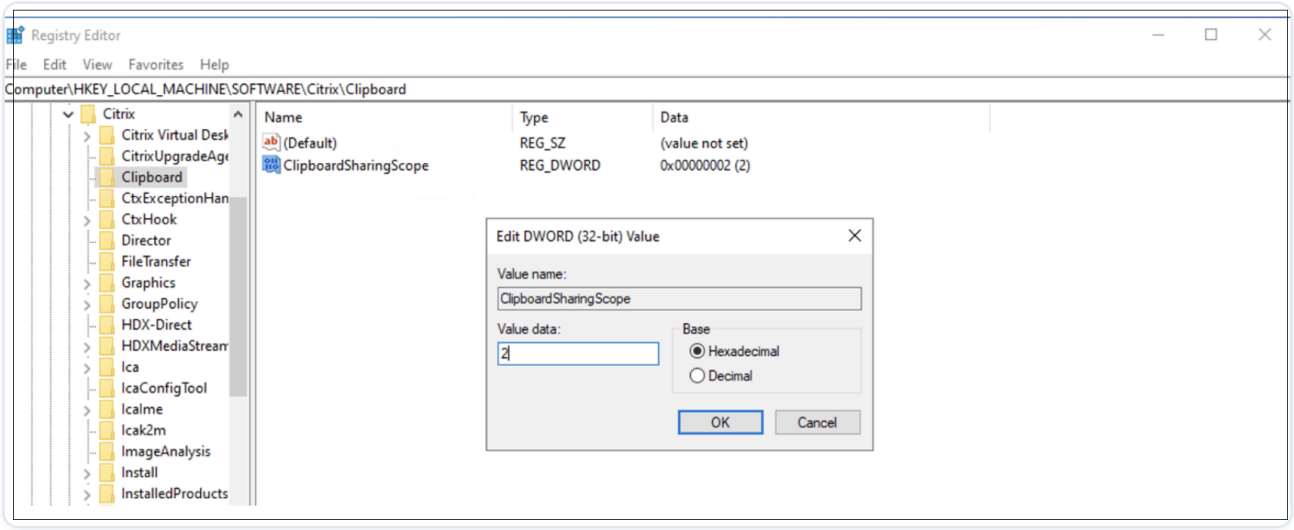


Die `ClipboardSharingScope`-Richtlinie steuert, wo VDA-Zwischenablagedaten freigegeben werden können. Bis die neue DDC-Richtlinie verfügbar ist, kann diese Einstellung über den vorhergehenden Registrierungsschlüssel konfiguriert werden.

UNTERSTÜTZTER WERT	BEREICH	BESCHREIBUNG
0	Unbegrenzt	Zwischenablagedaten werden in die Zwischenablage des Clientsystems kopiert und können vom Client, VDA und CEP aufgerufen werden.
1	Nur VDA	Auf die Zwischenablagedaten kann nur der VDA zugreifen. Die Zwischenablage des Clientsystems und CEP können nicht auf den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UNTERSTÜTZTER WERT	BEREICH	BESCHREIBUNG
		Zwischenablageinhalt zugreifen.
2	Nur CEP	Auf die Zwischenablagedaten kann nur CEP zugreifen. Die Zwischenablage des Clientsystems und der VDA können nicht auf den Zwischenablageinhalt zugreifen.
3	VDA und CEP	Auf die Zwischenablagedaten können sowohl der VDA als auch CEP zugreifen. Die Zwischenablage des Clientsystems kann nicht auf den Zwischenablageinhalt zugreifen.



HINWEIS:

- Die Modi „Nur CEP (2)“ und „VDA und CEP (3)“ sind für die Zusammenarbeit mit der Funktion „Zwischenablagecontainer“ in der CEP-Erweiterung konzipiert.
- Wenn die Richtlinie für den Zwischenablagecontainer aktiviert ist, dürfen nur vom Administrator konfigurierte URLs Zwischenablagedaten mit der VDI austauschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
>-  Content copied from the approved web applications can be pasted into
the VDI.

>-  Content copied from the VDI can be pasted only into administrator-
configured, paste-allowed URLs.

>-  If a user attempts to paste VDI clipboard content into a website that
is not included in the policy, the paste operation is blocked and an error
message appears.
```

Domänensuffix für Webanwendungen

In Szenarien, in denen Benutzer kurze, interne Hostnamen im Browser eingeben (zum Beispiel `sw` oder `server001`), hängt die Domänensuffix-Funktion automatisch das DNS-Suffix an und wandelt diese mithilfe von Browser-verwalteten DNS-Suffix-Richtlinien in vollqualifizierte Domänennamen (FQDNs) um, anstatt sich auf die DNS-Suffix-Konfiguration des Betriebssystems zu verlassen.

Die DNS-Suffix-Funktion wird sowohl auf **Windows**- als auch auf **macOS**-Plattformen unterstützt und gilt konsistent für gängige URL-Eingabeformate, einschließlich:

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

Unterstützte Bereitstellungen: Secure Private Access Service und Hybridbereitstellungen.

Unterstützte Plattformen: Windows und macOS.

Voraussetzungen

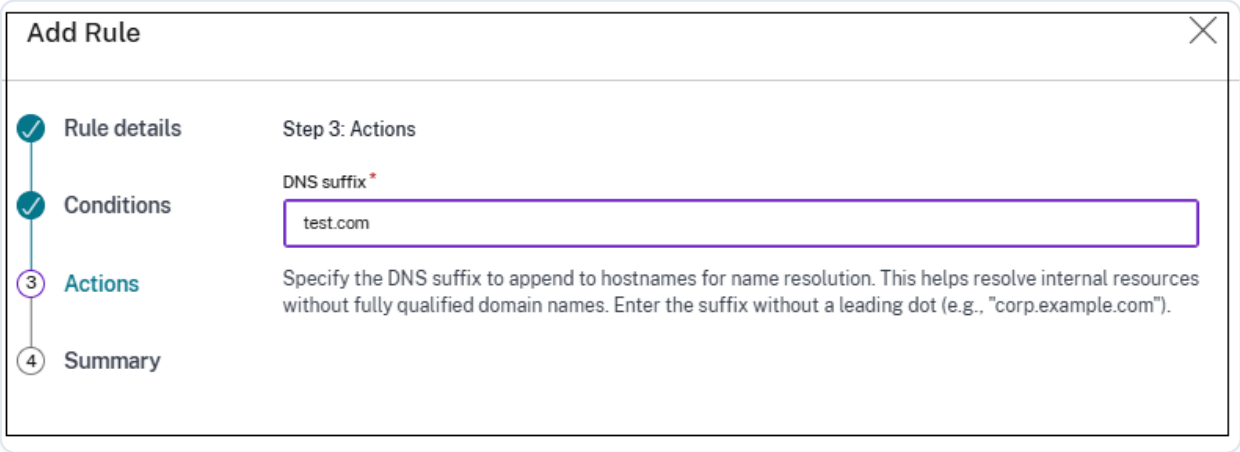
Stellen Sie sicher, dass die Integration von Citrix Secure Access mit Chrome Enterprise konfiguriert ist. Weitere Informationen finden Sie unter Integration mit Google Chrome Enterprise Premium.

DNS-Suffix konfigurieren

1. Melden Sie sich bei der Secure Private Access Admin-Konsole an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. a. Gehen Sie zu **Richtlinien > Browserrichtlinien**, und klicken Sie dann auf **Browserrichtlinie erstellen**.
3. Wählen Sie **DNS-Suffix**, und klicken Sie dann auf **Verwalten**.
4. Klicken Sie auf **Regel hinzufügen**, um Regeln für die Domäne hinzuzufügen, die Ihrer URL hinzugefügt werden soll.
   a. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.
   b. Wählen Sie Bedingungen basierend auf Ihren Anforderungen, z. B. Benutzer oder Gruppe. Sie können auch Bedingungen hinzufügen wie **Geo-Standort**, **Netwerkstandort** und **Geräte-Posture-Check**.
   c. Klicken Sie auf **Weiter**.
   d. Definieren Sie die Domäne, die Sie für den Zugriff anhängen möchten.



5. Klicken Sie auf **Speichern**.

   Die Anzahl der Regeln, die für die DNS-Suffix-Richtlinie konfiguriert sind, wird auf der Registerkarte **Browserrichtlinien > DNS-Suffix** angezeigt.

Steuerung der Sitzungsaufzeichnung

Die Sitzungsaufzeichnung zeichnet Sitzungen zur Wiederherstellung und Wiedergabe auf, katalogisiert und archiviert sie.

Die Sitzungsaufzeichnung bietet die folgenden Hauptvorteile:

- Bietet flexible Richtlinien, um Aufzeichnungen von Anwendungs- und Desktopsitzungen automatisch auszulösen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

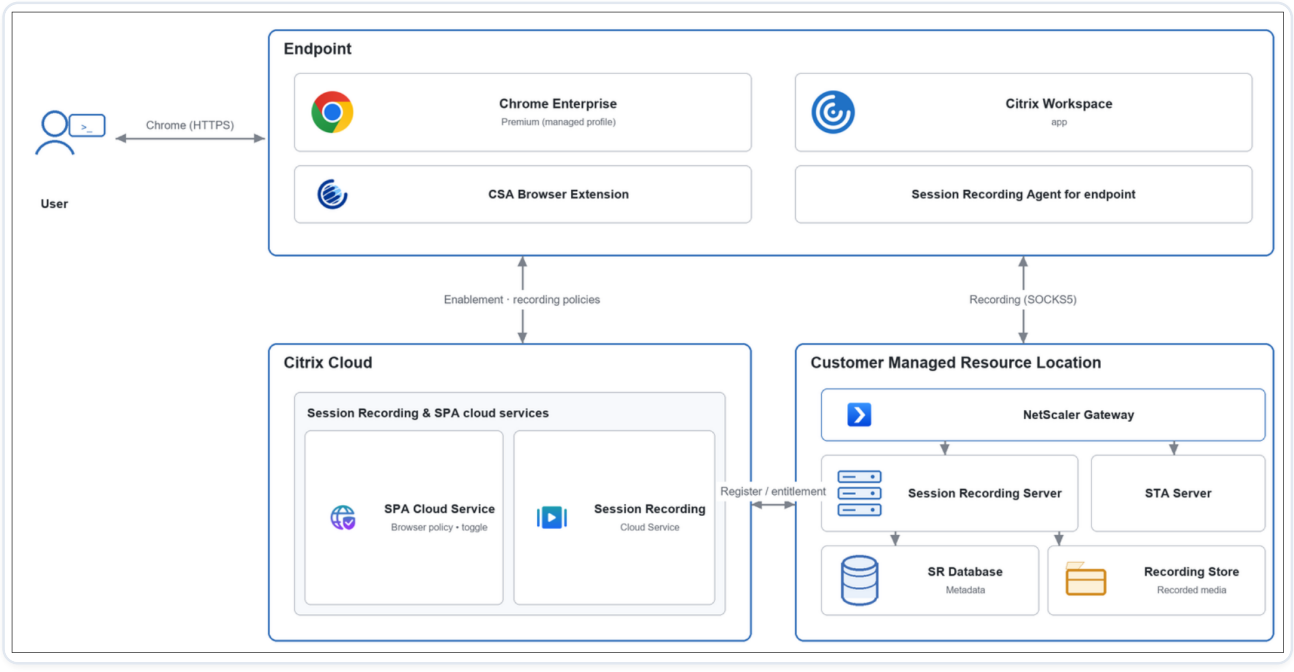
- Ermöglicht IT-Mitarbeitern die Überwachung und Untersuchung von Benutzeraktivitäten und unterstützt interne Kontrollen für die Einhaltung gesetzlicher Vorschriften und die Sicherheitsüberwachung.
- Unterstützt den technischen Support, indem es die Problemidentifizierung beschleunigt und die Lösungszeit verkürzt.

Weitere Informationen finden Sie unter Vorteile.

Architektur

Die Sitzungsaufzeichnungslösung umfasst drei Ebenen:

- Der Endpunkt mit dem verwalteten Chrome-Profil, der Citrix Secure Access-Erweiterung und dem Session Recording Agent für Endpunkte.
- Die Citrix Cloud-Steuerungsebene, die die Cloud-Dienste Secure Private Access und Session Recording beherbergt.
- Der vom Kunden verwaltete Ressourcenstandort, der NetScaler Gateway, den STA-Server, den Session Recording-Server sowie dessen Datenbank und Aufzeichnungsspeicher umfasst.



Voraussetzungen

- Citrix Workspace-App für Windows 2603.10 oder höher
- Endpoint Analysis (EPA)-Version: 26.5.1.7 und höher

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Systemanforderungen

- Citrix Secure Private Access, bereitgestellt entweder im Dienst- oder Hybridmodus in Kombination mit Chrome Enterprise Premium (mit verwaltetem Profil).
- Session Recording Cloud-Dienst mit Session Recording Server 2511 oder höher. Weitere Informationen finden Sie unter Erste Schritte.
- Windows 64-Bit- oder 32-Bit-Endpunkte mit den folgenden Komponenten:
  - Citrix Endpoint Analysis (EPA)-Plug-in 26.5.1.7 oder höher.
  - Citrix Workspace-App für Windows, Version 2603.10 oder höher, mit installiertem Session Recording Endpoint Agent

Umgebung einrichten

Führen Sie die folgenden Schritte aus, um die Endpunktaufzeichnung für Chrome Enterprise-Sitzungen zu aktivieren und zu validieren.

Session Recording-Site konfigurieren

Befolgen Sie die Schritte, die unter Endpunktaufzeichnungsrichtlinien konfigurieren dokumentiert sind.

HINWEIS:

NetScaler Gateway ist für die Endpunktaufzeichnung erforderlich. Es leitet den Aufzeichnungsverkehr in beiden Secure Private Access-Bereitstellungstypen über den STA an den Session Recording Server weiter. Selbst beim Secure Private Access-Dienst, bei dem NetScaler den Benutzer-zu-Anwendungszugriff nicht verwaltet, müssen Sie eine Gateway-URL für den Aufzeichnungsverkehr angeben.

Session Recording-Browserrichtlinie in Secure Private Access konfigurieren

1. Melden Sie sich bei der Secure Private Access-Administratorkonsole an.
2. Gehen Sie zu **Richtlinien > Browserrichtlinien**, und klicken Sie dann auf **Browserrichtlinie erstellen**.
3. Wählen Sie **Sitzungsaufzeichnung** aus, und klicken Sie dann auf **Verwalten**.
4. Klicken Sie auf **Regel hinzufügen**, geben Sie einen Namen für die Regel ein, und klicken Sie dann auf **Weiter**.
5. Legen Sie die Bedingungen fest (Benutzer und Gruppen). (Optional) Fügen Sie **Geo-Standort**, **Netwerkstandort** und **Geräte-Posture-Prüfung** hinzu, und klicken Sie dann auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Klicken Sie auf **Speichern**. Die Regelanzahl wird auf der Registerkarte **Browserrichtlinien > Sitzungsaufzeichnung** angezeigt.

Installieren Sie die Workspace-App mit dem Sitzungsaufzeichnungs-Agent für Endpunkte

Befolgen Sie die Schritte, die in Sitzungsaufzeichnungs-Add-on-Support dokumentiert sind.

Aufgezeichnete Sitzungen wiedergeben

Aufzeichnungen können in der Sitzungsaufzeichnungskonsole angezeigt werden.

- Alle Fenster, die dem Chrome-Arbeitsprofil des Benutzers zugeordnet sind, werden aufgezeichnet.
- Mehrere Fenster über einen oder mehrere Monitore hinweg werden aufgezeichnet.
- Fenster, die nicht im Fokus stehen oder von einer anderen Anwendung verdeckt werden, werden weiterhin vollständig aufgezeichnet.
- Minimierte Fenster und Fenster, bei denen der Anti-Screen-Capture aktiviert ist, erscheinen während der Wiedergabe als schwarze Rechtecke.

Best Practices

- **Behalten Sie eine globale Site bei**. Verwenden Sie eine einzige globale Endpunkt-Aufzeichnungs-Site und dokumentieren Sie die Konfiguration. Eine Änderung kann unbeabsichtigt die konfigurierten Richtlinien der anderen Sites deaktivieren.
- **Regionen ausrichten**. Halten Sie die URL des Session Recording Cloud-Dienstes, den Cloud-Client und das Backend in derselben Citrix Cloud-Region, um Latenz- und Datenresidenzprobleme zu vermeiden.
- **Speicher planen**. Die Aufzeichnung von Web-/SaaS-Anwendungen im Vollbildmodus kann speicherintensiv sein. Dimensionieren Sie den Server, die Session Recording-Datenbank und den Aufzeichnungsspeicher entsprechend und überwachen Sie den Speicherverbrauch genau.
- **Berechtigungen und Rollen zuerst überprüfen**. Nicht übereinstimmende Citrix DaaS- und Citrix Secure Private Access-Berechtigungen sind die häufigste Ursache für Bereitstellungsfehler. Vergewissern Sie sich, dass ein einzelner aktiver Kundendatensatz vorhanden ist und dass die erforderlichen Administratorrollen zugewiesen sind, bevor Sie Richtlinien aktivieren.

Steuerung der Browser-Sitzungsreauthentifizierung

Citrix Secure Private Access ermöglicht Administratoren, Sitzungs-Timeout-Richtlinien für Chrome Enterprise Premium (CEP)-Browsersitzungen zu erzwingen. Benutzer müssen sich nach einer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

konfigurierten Sitzungsdauer erneut authentifizieren, unabhängig von der Browseraktivität. Dies stärkt die Zero-Trust-Zugriffskontrollen für Anwendungen, auf die über das Google Chrome-Arbeitsprofil zugegriffen wird.

Sobald eine Sitzung abläuft, müssen sich Benutzer mit Unternehmensanmeldeinformationen und Multi-Faktor-Authentifizierung (MFA) erneut authentifizieren. Eine erfolgreiche erneute Authentifizierung stellt die zuletzt aktive Seite wieder her und startet den Sitzungs-Timer neu.

Unterstützte Bereitstellungen: Secure Private Access-Dienst und hybride Bereitstellungen.

Unterstützte Plattformen: Windows, macOS, Linux, ChromeOS.

Voraussetzungen

Stellen Sie sicher, dass die folgende Voraussetzung erfüllt ist:

- Die Integration zwischen Citrix Secure Access und Chrome Enterprise Premium (CEP) ist abgeschlossen.

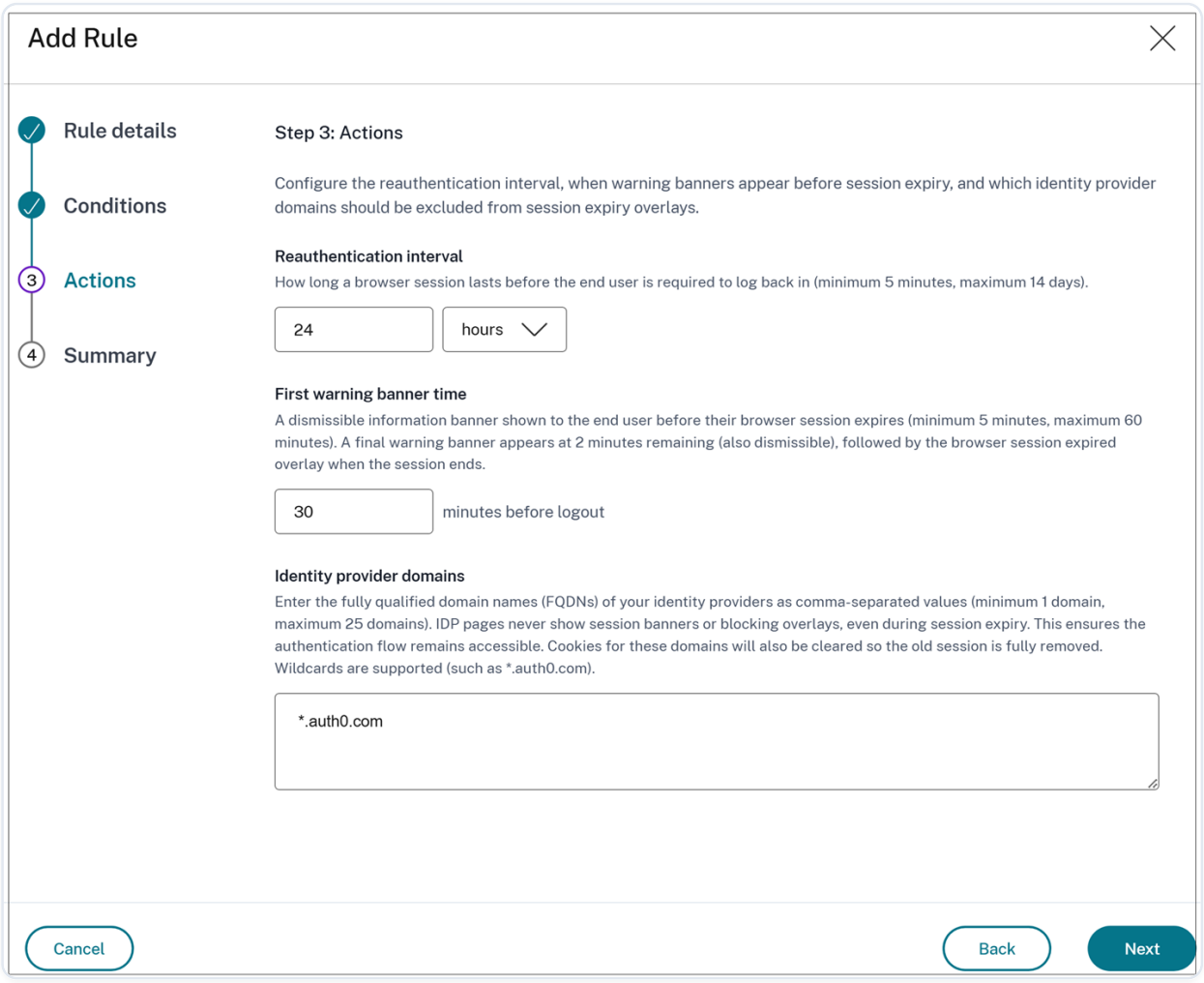
Browser-Sitzungsreauthentifizierungssteuerung aktivieren

1. Melden Sie sich bei der Secure Private Access-Administratorkonsole an.
2. Gehen Sie zu **Richtlinien > Browserrichtlinien** und klicken Sie dann auf **Browserrichtlinie erstellen**.
3. Wählen Sie **Browser-Sitzungsreauthentifizierung** aus und klicken Sie dann auf **Verwalten**.
4. Klicken Sie auf **Regel hinzufügen**, um Regeln zum Aktivieren der Browser-Sitzungsreauthentifizierung hinzuzufügen.
    a. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.
    b. Wählen Sie Bedingungen basierend auf Ihren Anforderungen aus, z. B. Benutzer oder Gruppe. Sie können auch Bedingungen wie **Geo-Standort**, **Netwerkstandort** und **Geräte-Posture-Check** hinzufügen.
    c. Klicken Sie auf **Weiter**.
    d. Konfigurieren Sie Folgendes:
        - **Intervall für erneute Authentifizierung**: Die Dauer einer Browsersitzung, bevor der Benutzer sich erneut authentifizieren muss. Das Intervall kann zwischen 5 Minuten und 14 Tagen eingestellt und in Minuten, Stunden oder Tagen konfiguriert werden.
        - **Zeitpunkt des ersten Warnbanners**: Ein ausblendbares Warnbanner, das dem Benutzer angezeigt wird, bevor seine Browsersitzung abläuft. Der Wert kann zwischen 5 und 60

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Minuten vor dem Ablauf festgelegt werden. Ein zweites Warnbanner erscheint, wenn noch 2 Minuten verbleiben, gefolgt von einem Overlay für abgelaufene Sitzungen, wenn die Sitzung endet.

- **Identitätsanbieter-Domänen**: Die vollqualifizierten Domänennamen (FQDNs) Ihrer Identitätsanbieter als kommagetrennte Werte. Sie können zwischen 1 und 25 Domänen angeben. Sitzungsbanner und blockierende Overlays werden auf IdP-Seiten unterdrückt, um sicherzustellen, dass der Authentifizierungsfluss ununterbrochen bleibt. Cookies für diese Domänen werden gelöscht, wenn die Sitzung abläuft, um sicherzustellen, dass die alte Sitzung vollständig entfernt wird. Platzhalter werden unterstützt (zum Beispiel *.auth0.com).



5. Klicken Sie auf **Weiter** und dann auf **Speichern**.

Die Anzahl der Regeln, die für die Zwischenablage-Containerrichtlinie konfiguriert sind, wird auf der Registerkarte **Browserrichtlinien > Browser-Sitzungs-Reauthentifizierung** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSH-Steuerung

Citrix Secure Private Access ist in Chrome Enterprise Premium integriert, um sichere SSH-Sitzungen direkt im Browser zu ermöglichen. Diese Integration verbessert die Sicherheit und optimiert den Zugriff für Administratoren und Benutzer.

Organisationen benötigen eine sichere Fernverwaltung von SSH-basierten Systemen. Herkömmliche Methoden, die eigenständige SSH-Clients verwenden, bergen Risiken, da sie Endpunkte unkontrollierten Umgebungen aussetzen und keine robuste Durchsetzung der Data Loss Prevention (DLP) bieten, was die Einhaltung von Vorschriften erschwert.

Die SSH-Sitzungen werden nun im Chrome-Browser anstatt in eigenständigen SSH-Clients gestartet, was die Abhängigkeit von lokalen Installationen reduziert und die Compliance verbessert.

HINWEIS:

- Diese Funktion ist für die in Chrome Enterprise Premium integrierte Secure Private Access-Einrichtung für Hybrid- und Cloud-Bereitstellungen anwendbar. Einzelheiten finden Sie in den folgenden Themen:
- Sie müssen über Administratorrechte verfügen, um Secure Private Access- und Chrome Enterprise Premium-Richtlinien zu konfigurieren.
- Verbindungen zu FreeBSD-Servern werden nicht unterstützt.

Vorteile dieser Integration

Diese Integration bietet die folgenden Hauptvorteile:

- **Verbesserte Sicherheit:** Eliminiert die Abhängigkeit von nicht verwalteten SSH-Clients und reduziert die Exposition gegenüber Sicherheitsrisiken.
- **Vereinfachter Zugriff:** Bietet browser-nativen Zugriff, wodurch die Notwendigkeit zusätzlicher Softwareinstallationen entfällt.
- **Compliance:** Setzt unternehmensweite DLP-Richtlinien direkt im Browser durch und hilft so, regulatorische Anforderungen zu erfüllen.
- **Betriebliche Effizienz:** Reduziert den IT-Aufwand, der mit der Endpunktverwaltung und Client-Bereitstellung verbunden ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsfälle

Diese Funktion unterstützt verschiedene Anwendungsfälle, wie zum Beispiel:

- **Gesundheits-Kioske:** Ermöglicht sicheren SSH-Zugriff zur Gerätefehlerbehebung, ohne native Clients installieren zu müssen.
- **IT-Administration:** Ermöglicht Administratoren den sicheren Zugriff auf Linux-Server von verwalteten Chrome-Browsern mit erzwungenen DLP-Richtlinien.
- **Auftragnehmerzugriff:** Bietet temporären SSH-Zugriff für Drittanbieter, ohne die Sicherheitslage des Unternehmens zu gefährden.

Systemanforderungen

Stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

- Neueste Version von Chrome Enterprise Premium.
- Citrix Secure Private Access ist für die Integration konfiguriert.
- Zugriffsrichtlinien, die SSH-Datenverkehr zulassen, müssen in der Secure Private Access-Administrationskonsole erstellt werden.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen für die Aktivierung des sicheren Zugriffs auf SSH-Anwendungen erfüllt sind:

- Citrix Secure Private Access ist mit der Google Chrome Enterprise Premium-Integration konfiguriert. Weitere Informationen finden Sie unter Integration mit Google Chrome Enterprise Premium.
- Der Endbenutzer hat den neuesten Google Chrome-Browser mit der Citrix Secure Access-Browsererweiterung installiert.
- Die bereitstellungsspezifischen Voraussetzungen finden Sie in den folgenden Themen:
  - Cloud-Bereitstellung – Erste Schritte mit Citrix Secure Private Access
  - Hybride Bereitstellung – Systemanforderungen und Voraussetzungen

Secure Private Access für SSH-Zugriff konfigurieren

1. Melden Sie sich bei Citrix Cloud an und klicken Sie dann auf **Secure Private Access**.
2. Klicken Sie in der Administratorkonsole auf **Applications > App Configuration** und dann auf **Add an app**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Konfigurieren Sie die SSH-App als TCP/UDP-App in Secure Private Access.
    - Die App kann eine genaue IP-Adresse oder einen Bereich, einen FQDN oder einen Hostnamen des Servers haben.
    - SSH wird über Standard- und Nicht-Standardports unterstützt.
4. Weisen Sie den relevanten Benutzergruppen Zugriff zu.

Detaillierte Informationen zum Erstellen einer TCP/UDP-App finden Sie in den folgenden Themen.

- Cloud-Bereitstellung – Unterstützung für TCP/UDP-Apps
- Hybride Bereitstellung – Unterstützung für TCP/UDP-Apps

SSH-Richtlinie konfigurieren

1. Melden Sie sich bei der Secure Private Access-Administratorkonsole an.
2. Gehen Sie zu **Policies > Browser Policies** und klicken Sie dann auf **Create browser policy**.
3. Wählen Sie **SSH** aus und klicken Sie dann auf **Manage**.
4. Klicken Sie auf **Regel hinzufügen**, um Regeln für die Benutzer hinzuzufügen, damit SSH aktiviert werden kann.
5. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.
6. Wählen Sie Bedingungen basierend auf Ihren Anforderungen aus, z. B. Benutzer oder Gruppe.
    1. Sie können auch Bedingungen wie **Geo-Standort, Netwerkstandort** und **Geräte-Posture-Check** hinzufügen.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Speichern**.

Die Anzahl der Regeln, die für die Anti-Keylogging-Richtlinie konfiguriert sind, wird auf der Registerkarte **Browserrichtlinien > SSH** angezeigt.

Remotedesktopsteuerung

Citrix Secure Private Access ist in Chrome Enterprise Premium integriert, um sichere RDP-Sitzungen direkt im Browser zu ermöglichen. Diese Integration verbessert die Sicherheit und optimiert den Zugriff für Administratoren und Benutzer.

Herkömmlicher Remotedesktopzugriff basiert oft auf nativen RDP-Clients, denen in der Regel eine browserbasierte DLP-Durchsetzung fehlt. Dieser Mangel kann Sicherheitsrisiken erhöhen, insbesondere in nicht verwalteten Umgebungen, und die Compliance erschweren. Unternehmen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

benötigen eine sichere, konforme und vereinfachte Lösung für den Fernzugriff, die diese Bedenken berücksichtigt.

Diese Integration ermöglicht es Administratoren, DLP-Kontrollen auf Unternehmensebene durchzusetzen, wie z. B. die Steuerung der Zwischenablage und die Verhinderung von Screenshots.

HINWEIS:

- Diese Funktion ist für die in Chrome Enterprise Premium integrierte Secure Private Access-Einrichtung für Hybrid- und Cloud-Bereitstellungen anwendbar. Einzelheiten finden Sie in den folgenden Themen:
- Sie müssen über Administratorrechte verfügen, um Secure Private Access- und Chrome Enterprise Premium-Richtlinien zu konfigurieren.

Nicht unterstützte Funktionen:

Die folgenden Funktionen werden nicht unterstützt:

- Freigabe der Zwischenablage
- Audio-/Webcam-/Smartcard-/USB-Umleitung
- Zwei-Faktor- und biometrische Authentifizierung

Vorteile dieser Integration

Diese Integration bietet die folgenden Hauptvorteile:

- **Sicherheit:** Verhindert Datenlecks während Remotesitzungen durch die Durchsetzung granularer DLP-Richtlinien.
- **Compliance:** Hilft, regulatorische Anforderungen für sensible Umgebungen durch robuste Sicherheitskontrollen zu erfüllen.
- **Benutzerfreundlichkeit:** Eliminiert die Notwendigkeit der Installation separater RDP-Clients, was den Benutzerzugriff und die Bereitstellung vereinfacht.
- **Flexibilität:** Unterstützt sicheren RDP-Zugriff von verwalteten Chrome-Browsern und bietet eine konsistente und sichere Erfahrung.

Anwendungsfälle

Diese Funktion unterstützt verschiedene Anwendungsfälle, wie zum Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Unternehmensauftragnehmer:** Bietet sicheren Remote-Desktop-Zugriff für Drittanbieter, ohne die interne Sicherheit zu gefährden.
- **Gesundheitspersonal:** Ermöglicht sicheren Zugriff auf Windows-Systeme von Kiosken oder gemeinsam genutzten Arbeitsplätzen in Gesundheitseinrichtungen.
- **IT-Support:** Ermöglicht IT-Mitarbeitern die Fehlerbehebung bei Remote-Desktops, ohne zusätzliche Softwareinstallationen zu erfordern.

Systemanforderungen

Stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

- Neueste Version von Chrome Enterprise Premium.
- Citrix Secure Private Access ist für die Integration konfiguriert.
- Zugriffsrichtlinien, um RDP-Datenverkehr zuzulassen, müssen in der Secure Private Access Admin-Konsole erstellt werden.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen für die Aktivierung des sicheren Zugriffs auf RDP-Anwendungen erfüllt sind:

- Citrix Secure Private Access ist mit der Google Chrome Enterprise Premium-Integration konfiguriert. Weitere Informationen finden Sie unter Integration mit Google Chrome Enterprise Premium.
- Der Endbenutzer hat den neuesten Google Chrome-Browser mit der Citrix Secure Access-Browsererweiterung installiert.
- Die Bereitstellungsspezifischen Voraussetzungen finden Sie in den folgenden Themen:
  - Cloud-Bereitstellung – Erste Schritte mit Citrix Secure Private Access
  - Hybride Bereitstellung – Systemanforderungen und Voraussetzungen

Secure Private Access für RDP-Zugriff konfigurieren

1. Melden Sie sich bei Citrix Cloud an und klicken Sie dann auf **Secure Private Access**.
2. Klicken Sie in der Administratorkonsole auf **Applications > App Configuration** und dann auf **Add an app**.
3. Konfigurieren Sie die RDP-App als TCP/UDP-App in Secure Private Access.
   - Die App kann eine genaue IP-Adresse oder einen Bereich, FQDN oder Hostnamen des Servers haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RDP wird über Standard- und Nicht-Standardports unterstützt.

4. Weisen Sie relevanten Benutzergruppen Zugriff zu.

Detaillierte Informationen zum Erstellen einer TCP/UDP-App finden Sie in den folgenden Themen.

- Cloud-Bereitstellung – Unterstützung für TCP/UDP-Apps
- Hybride Bereitstellung – Unterstützung für TCP/UDP-Apps

Remotedesktop-Richtlinie konfigurieren

1. Melden Sie sich bei der Secure Private Access-Administrationskonsole an.
2. Gehen Sie zu **Richtlinien > Browserrichtlinien**, und klicken Sie dann auf **Browserrichtlinie erstellen**.
3. Wählen Sie **Remotedesktop** aus, und klicken Sie dann auf **Verwalten**.
4. Klicken Sie auf **Regel hinzufügen**, um Regeln für Benutzer hinzuzufügen, die Remotedesktop aktivieren sollen.
5. Geben Sie den Namen für die Regel ein und klicken Sie auf **Weiter**.
6. Wählen Sie Bedingungen basierend auf Ihren Anforderungen aus, z. B. Benutzer oder Gruppe.
   1. Sie können auch Bedingungen wie **Geo-Standort, Netwerkstandort** und **Geräte-Posture-Check** hinzufügen.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Speichern**.

Die Anzahl der für die Anti-Keylogging-Richtlinie konfigurierten Regeln wird auf der Registerkarte **Browserrichtlinien > Remotedesktop** angezeigt.

Fehlerbehebung bei CEP-Integrationsproblemen

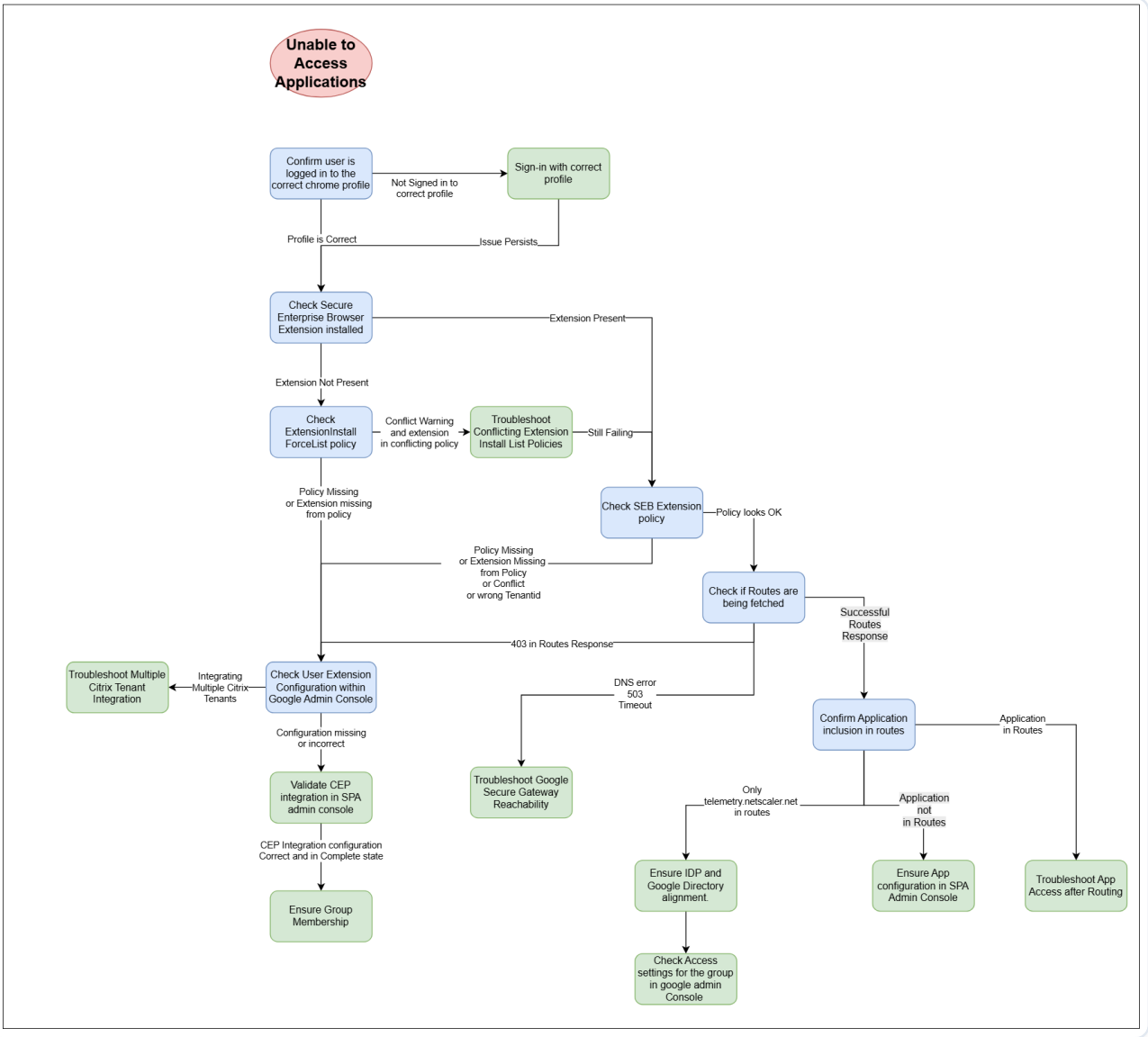
Dieser Artikel bietet einen Workflow zur Fehlerbehebung für Kundenadministratoren, die die Integration von Chrome Enterprise Premium (CEP) mit Citrix Secure Private Access abgeschlossen haben und nicht auf Anwendungen zugreifen können.

Grundlegende Annahmen:

- Der Kundenadministrator hat die Verzeichnissynchronisierung mit Google Directory abgeschlossen.
- Der Kunde hat das Chrome Enterprise-Onboarding in Secure Private Access erfolgreich abgeschlossen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anwendungen und Zugriffsrichtlinien sind in der Secure Private Access-Administratorkonsole konfiguriert, um dem Benutzer oder einer Gruppe, der der Benutzer angehört, den Zugriff auf die relevanten Anwendungen zu ermöglichen.
- Der Benutzer meldet sich bei der integrierten Domäne an.
- Der Browser verfügt über eine Internetverbindung.



Diagnoseprotokolle für die CEP-Fehlerbehebung

Um die Untersuchung zu optimieren, sammeln Sie die folgenden Diagnoseinformationen, bevor Sie einen Supportfall öffnen, und fügen Sie diese jeder Einreichung bei.

1. Chrome-Richtlinien exportieren.
    a. Öffnen Sie Chrome und navigieren Sie zu chrome://policy/.
    b. Klicken Sie auf **Weitere Aktionen** und wählen Sie dann **Als JSON exportieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Fügen Sie die exportierte Datei Ihrem Supportfall bei.

2. Ausführliche Protokollierung für die Secure Enterprise Browser-Erweiterung aktivieren.

   a. Klicken Sie auf das Ellipsensymbol neben der Secure Enterprise Browser-Erweiterung.

   b. Klicken Sie auf die Optionen und legen Sie dann die **Protokollierungsstufe** auf **Alle** fest.

   c. Chrome schließen und erneut öffnen.

   d. Gehen Sie zurück zu den Erweiterungsoptionen (Ellipsensymbol) und klicken Sie dann auf **Protokoll herunterladen**.

3. Erweiterungsprotokoll erfassen.

   a. Chrome schließen und erneut öffnen.

   b. Wiederholen Sie Schritt 2, um auf die **Erweiterungs**optionen zuzugreifen, und klicken Sie dann auf **Protokoll herunterladen**.

   c. Fügen Sie die heruntergeladene Datei Ihrem Supportfall an.

4. Ein Netzwerkprotokoll erfassen.

   a. Navigieren Sie in Chrome zu chrome://net-export/ und klicken Sie auf **Protokollierung auf Datenträger starten** (der Standarddateiname ist chrome-net-export-log.json).

   b. Greifen Sie auf einige SaaS- und Webanwendungen zu, kehren Sie dann zu chrome://net-export/ zurück und klicken Sie auf **Protokollierung beenden**.

   c. Fügen Sie die resultierende Datei Ihrem Supportfall an.

Bestätigen Sie, dass der Benutzer im richtigen Chrome-Profil angemeldet ist

So überprüfen Sie dies: Klicken Sie oben rechts im Chrome-Browser auf das Profilsymbol. Es muss der richtige Benutzer und die richtige Domäne für das Profil angezeigt werden, über das Sie auf Ihre Anwendungen zugreifen möchten.

Stellen Sie außerdem sicher, dass das Profil nicht **Angehalten** oder **Zum Anmelden klicken** anzeigt. Ist dies der Fall, müssen Sie sich erneut authentifizieren.

- **Profil ist korrekt und authentifiziert:** Fahren Sie fort mit Überprüfen Sie die installierte Secure Enterprise Browser-Erweiterung.
- **Profil ist falsch oder nicht authentifiziert:** Melden Sie sich mit dem richtigen Profil an oder authentifizieren Sie sich erneut. Stellen Sie sicher, dass das Domänensuffix der E-Mail-Adresse des Benutzers mit der Domäne des Google Admin-Kontos übereinstimmt, das mit Secure Private Access installiert ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Überprüfen Sie die installierte Secure Enterprise Browser-Erweiterung

So überprüfen Sie: In der oberen rechten Ecke des Chrome-Browsers muss ein grünes Schildsymbol vorhanden sein, das der Secure Enterprise Browser-Erweiterung entspricht. Möglicherweise müssen Sie auf das Puzzleteil klicken, um alle Erweiterungen anzuzeigen.

- **Erweiterung vorhanden:** Fahren Sie fort mit Überprüfen Sie die Secure Enterprise Browser-Erweiterungsrichtlinie.
- **Erweiterung nicht vorhanden:** Fahren Sie fort mit Überprüfen Sie die ExtensionInstallForcelist-Richtlinie.

Überprüfen Sie die ExtensionInstallForcelist-Richtlinie

So überprüfen Sie: Navigieren Sie zu chrome://policy und suchen Sie unter **Chrome-Richtlinien** nach einer Richtlinie namens **ExtensionInstallForcelist**. Klicken Sie am Ende der entsprechenden Zeile auf **Mehr anzeigen**, um die Details der Richtlinie anzuzeigen.

Innerhalb dieser Erzwingungsliste sollten Sie eine Erweiterung mit der ID: `ekajlcmdfcigmdbphhifahdfjbkciflj` sehen. Dies entspricht der Secure Enterprise Browser-Erweiterung.

Es ist möglich, dass Ihnen eine Warnung angezeigt wird, die darauf hinweist, dass zwei widersprüchliche Richtlinien vorhanden sind.

- **Konfliktwarnung und Erweiterung in widersprüchlicher Richtlinie:** Fahren Sie fort mit Beheben von Problemen mit widersprüchlichen Richtlinien für die Erweiterungsinstallationsliste.
- **Richtlinie fehlt:** Das vollständige Fehlen der Richtlinie deutet darauf hin, dass der Benutzer nicht für die Verwendung des Secure Enterprise Browsers konfiguriert ist, und Sie müssen Die Benutzererweiterungskonfiguration in der Google Admin Console überprüfen.
- **Erweiterung fehlt in der Richtlinie:** Fahren Sie fort mit Die Benutzererweiterungskonfiguration in der Google Admin Console überprüfen.

Beheben von Problemen mit widersprüchlichen Richtlinien für die Erweiterungsinstallationsliste

Konfliktierende Richtlinien sind nicht unbedingt ein Hindernis für die Unterstützung von CEP mit Secure Private Access. Die effektive Richtlinie muss jedoch die Installation der folgenden drei Erweiterungen erzwingen:

- Secure Enterprise Browser (`ekajlcmdfcigmdbphhifahdfjbkciflj`)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Access (`loifegnemklkgbmonigcdkmniboielgl`)
- Endpoint Verification (`callobklhcbilhphinckomhgkigmfocg`)

Um Konflikte bei Erweiterungsrichtlinien für Secure Private Access zu beheben, führen Sie die folgenden Schritte basierend auf dem Chrome Policy Hierarchy Guide aus.

1. **Konflikt identifizieren:** Navigieren Sie zu `chrome://policy`. Suchen Sie **ExtensionInstallForcelist** und überprüfen Sie den **Status** und die **Quelle**.
2. **Rangfolge analysieren:** Beachten Sie, dass Richtlinien auf Maschinenebene (GPO) im Allgemeinen Vorrang vor Richtlinien auf Cloud-/Benutzerebene haben.
3. **Harmonisieren:** Stellen Sie sicher, dass die Richtlinie mit der höchsten Priorität alle drei erforderlichen Erweiterungs-IDs enthält (es ist in Ordnung, wenn zusätzliche Erweiterungen enthalten sind). Alternativ können Sie die Funktion zur Richtlinienzusammenführung verwenden, wenn der Browser und das Profil von derselben Google Workspace-Organisation verwaltet werden.
4. **Überprüfen:** Klicken Sie auf **Richtlinien neu laden**. Die Spalten **Gilt für** und **Ebene** müssen bestätigen, dass die erforderlichen Erweiterungen **obligatorisch** und auf der effektiven Ebene aktiv sind.

Wenn das Problem auch nach der Korrektur der Richtlinie für die Erweiterungsinstallationsliste weiterhin besteht, fahren Sie mit Überprüfen der Secure Enterprise Browser-Erweiterungsrichtlinie fort.

Überprüfen der Secure Enterprise Browser-Erweiterungsrichtlinie

So überprüfen Sie: Navigieren Sie zu chrome://policy und suchen Sie unter **Secure Enterprise Browser** nach einer Richtlinie namens **securityGateway**. Klicken Sie auf **Mehr anzeigen**, um die vollständige Richtlinienkonfiguration anzuzeigen. Ihr Wert sollte das folgende Format haben:

```
{

  "authentication": {},

  "context": {

    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"

  },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "externalHelper": {
    "id": "com.citrix.device_posture_context_provider",
    "metadata": {
      "action": "device/metadata",
      "input": [
        {
          "key": "tenantId",
          "stringValue": "<tenant_id>"
        }
      ]
    }
  },
  ...
}
```

Stellen Sie sicher, dass das Feld `tenant_id` einen Wert hat, der Ihrer Citrix Cloud Tenant-ID entspricht. Wenn dieser Wert abweicht, könnte es sein, dass ein zweiter Tenant für die Integration mit diesem Google-Konto konfiguriert ist.

- **Richtlinie fehlt oder ist leer:** Das vollständige Fehlen der Richtlinie deutet darauf hin, dass die Secure Enterprise Browser-Erweiterung nicht nur von Secure Private Access, sondern auch vom Kunden konfiguriert wird und der Benutzer die leere Erweiterungskonfiguration aus einer früheren oder manuellen Konfiguration übernimmt. Sie müssen Benutzererweiterungskonfiguration in der Google Admin Console überprüfen.
- **Richtlinie ist mit falscher Citrix Tenant-ID gefüllt:** Wenn die Richtlinie vorhanden ist, der Wert aber nicht mit dem Beispiel übereinstimmt, ist entweder die Tenant-ID anders oder es gibt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zwei konfliktierende Richtlinien. Fahren Sie mit Benutzererweiterungskonfiguration in der Google Admin Console überprüfen fort.

- **Die Richtlinie ist korrekt:** Fahren Sie fort mit Überprüfen, ob Routen abgerufen werden.

Benutzererweiterungskonfiguration in der Google Admin Console überprüfen

So überprüfen Sie dies: Navigieren Sie zu https://admin.google.com. Gehen Sie von hier aus zu **Chrome Browser > Apps & Extensions**. In dieser Ansicht müssen Sie alle angewendeten Richtlinienkonfigurationen finden.

Klicken Sie auf die Registerkarte **Übersicht** (sofern vorhanden) und wählen Sie die App **Secure Enterprise Browser** aus. Links, unter **Installationsrichtlinie**, muss Folgendes stehen: **Erzwungen installiert und angeheftet in \<primäre Domäne\>**, wobei \<primäre Domäne\> der obersten Organisationseinheit Ihrer Google Admin Console entspricht.

Wenn Sie sich durchklicken, um die **Bereitstellungseinstellungen** der Erweiterung anzuzeigen, suchen Sie nach der Konfiguration **Richtlinie für Erweiterungen**. Diese muss so aussehen, wie im Abschnitt Richtlinie für Secure Enterprise Browser-Erweiterung überprüfen beschrieben.

- **Einzelne Richtlinie, die korrekt erscheint:** Wenn die Richtlinie für die übergeordnete Organisationseinheit korrekt aussieht, müssen Sie sicherstellen, dass der Benutzer, mit dem Sie testen, zu dem betreffenden Konto gehört und dass es keine andere Konfiguration auf einer untergeordneten Organisationseinheit oder Gruppenebene gibt, die die Richtlinie der übergeordneten Organisationseinheit überschreiben könnte. Wenn die Mitgliedschaft bestätigt ist, das Problem aber weiterhin besteht, wenden Sie sich an den Citrix Support.
- **Richtlinie fehlt:** Das vollständige Fehlen der Richtlinie deutet darauf hin, dass dieses Google-Konto nicht für die Verwendung von Secure Enterprise Browser konfiguriert ist und Sie die CEP-Integration in der Secure Private Access-Administratorkonsole validieren müssen.
- **Mehrere Richtlinien – Mehrere Citrix-Konten:** Wenn Sie mehrere Konfigurationen für die Secure Enterprise Browser-Erweiterung sehen, könnte dies eine Ursache für eine falsche Konfiguration der zugehörigen Richtlinie sein. Das Verknüpfen mehrerer Citrix-Konten mit demselben Google-Konto ist nicht verboten, kann aber dazu führen, dass die Integration nicht funktioniert.
- **Mehrere Richtlinien – Einzelnes Citrix-Konto:** Wenn Sie nur einen Citrix-Mandanten integrieren, müssen Sie sicherstellen, dass keine anderen Administratorfunktionen in Ihrer Organisation diese Erweiterung konfigurieren. Wenn Sie sicher sind, dass niemand sonst Richtlinienkonfigurationen für diese Erweiterung bereitstellt, können Sie die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Richtlinienkonfigurationen entfernen, die nicht dem Citrix-Mandanten entsprechen, mit dem Sie über die Secure Private Access Admin Console integriert haben.

Wenn Sie die überflüssigen Erweiterungskonfigurationen entfernen und nach dem Neustart des Browsers immer noch nicht auf Ihre Anwendungen zugreifen können, wenden Sie sich an den Citrix Support.

Überprüfen, ob Routen abgerufen werden

So überprüfen Sie dies: Navigieren Sie zu chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj oder klicken Sie mit der rechten Maustaste auf die Secure Enterprise Browser-Erweiterung und wählen Sie **Optionen** aus.

Legen Sie die Protokollstufe auf **ALLE** fest und klicken Sie auf **PROTOKOLL ANZEIGEN**. Sobald das Protokoll angezeigt wird, schließen Sie den Browser und wiederholen Sie den Vorgang, um zur Protokollseite zu gelangen. Dadurch wird sichergestellt, dass Sie den vollständigen Satz an Protokollen zur Fehlerbehebung abgerufen haben.

Suchen Sie im Protokoll nach einer Protokollzeile, die Folgendes enthält:

```
Calling 'https://api.prod.securegateway.goog/api/v1/routes'
```

Darauf muss eine Antwort wie die folgende folgen:

```
[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog',...
```

.

- **Kontextbezogene Routen zeigen einen 403-Statuscode in den Protokollen an:** Dieser 403-Fehler kann von einer abfangenden Firewall wie Zscaler, Umbrella usw. zurückgegeben werden.
  - Stellen Sie in diesem Fall sicher, dass der für das Google Security Gateway bestimmte Datenverkehr gemäß den Voraussetzungen für die integrierte Lösung zugelassen ist.
  - Andernfalls handelt es sich wahrscheinlich um ein Authentifizierungsproblem mit dem Benutzerprofil und könnte eine unvollständige Integration von Secure Private Access mit CEP bedeuten. Fahren Sie fort mit CEP-Integration in der Secure Private Access-Administratorkonsole validieren.
- **Kontextbezogene Routen zeigen Timeout, einen DNS-Fehler oder einen 503-Fehler an:** Fahren Sie fort mit Beheben von Problemen mit der Erreichbarkeit des Google Secure Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Kontextbezogene Routen erscheinen erfolgreich (200 OK):** Fahren Sie fort mit Bestätigen der Anwendungsaufnahme in Routen.

CEP-Integration in der Secure Private Access-Administratorkonsole validieren

Besuchen Sie den Abschnitt **Browsereinstellungen** innerhalb von Secure Private Access in der Citrix Cloud-Konsole.

Überprüfen Sie in diesem Abschnitt Folgendes:

- **Der Integrationsstatus von Google Chrome** muss als **Abgeschlossen** angezeigt werden. Wenn Sie feststellen, dass er fehlgeschlagen ist, stellen Sie sicher, dass Sie die erforderlichen Schritte für die CEP-Integration gemäß der Dokumentation abgeschlossen haben, und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.
- **Die Kunden-ID** muss einen Wert haben, der dem Google-Konto entspricht, mit dem Sie integrieren. Sie finden den Wert in Ihrer Google Admin Console unter **Konto > Kontoeinstellungen**.

Wenn alle oben genannten Werte korrekt sind, Sie aber immer noch nicht die richtige Erweiterungskonfiguration in Ihrem Chrome-Browser erhalten, wenden Sie sich an den Citrix Support.

Beheben von Problemen mit der Erreichbarkeit des Google Secure Gateway

So überprüfen Sie dies: Kopieren Sie die URL `https://api.prod.securegateway.goog/api/v1/routes` und navigieren Sie in der Adressleiste des Browsers zu dieser URL. Sie müssen eine HTTP 401-Fehlerantwort erhalten. Dies ist ein erwartetes Verhalten und zeigt an, dass eine Netzwerkverbindung zum Google Secure Gateway erfolgreich hergestellt werden kann.

- **DNS-Auflösungsfehler:** Dies deutet darauf hin, dass Ihr Unternehmen möglicherweise eine restriktive DNS-Auflösungskonfiguration eingerichtet hat, die die Auflösung des FQDN des Google Security Gateways verhindert. Dies ist jedoch eine Voraussetzung für die Nutzung dieser Funktion, und der entsprechende FQDN muss auflösbar sein.
- **Die Anforderung hängt oder es wird eine Timeout-Fehlerseite angezeigt:** Dies deutet stark darauf hin, dass eine Firewall zwischen dem Browser und dem Internet den für das Google Security Gateway bestimmten Datenverkehr blockiert. Befolgen Sie die Voraussetzungen für die integrierte Lösung, um sicherzustellen, dass die erforderlichen Internetstandorte von Ihrem Netzwerk aus erreichbar sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie immer noch nicht die richtigen Routen erhalten, wenden Sie sich an den Citrix Support.

Bestätigen der Anwendungsaufnahme in Routen

Eine erfolgreiche Routenantwort enthält FQDNs, die Anwendungen entsprechen, die von Ihrem Secure Private Access-Administrator konfiguriert wurden. Zum Beispiel:

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog',
endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'},
{hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname:
'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}.
```

Enthält diese Zeile die Anwendung, auf die Sie zugreifen möchten?

- **Die unzugängliche Anwendung ist in der Routenantwort enthalten:** Fahren Sie fort mit Fehlerbehebung beim Zugriff auf geroutete Anwendungen.
- **Nur telemetry.netscalergateway.net ist in der Routenantwort enthalten:** Versuchen Sie, eine zusätzliche Anwendung und eine inklusive Anwendungsrichtlinie zu konfigurieren. Wenn Sie sie immer noch nicht in den Routen sehen, deutet dies stark auf ein Problem mit der Gruppenmitgliedschaft oder eine Fehlausrichtung der Gruppen zwischen Ihrem in Citrix konfigurierten IdP und dem Google Directory hin. Fahren Sie fort mit Sicherstellen der IdP- und Google Directory-Ausrichtung.
- **Die unzugängliche Anwendung ist nicht in der Routenantwort enthalten:** Dies deutet darauf hin, dass die Anwendung in der Secure Private Access Administratorkonsole nicht korrekt konfiguriert ist. Überprüfen Sie, ob die Anwendung existiert und eine zugehörige Richtlinie (entweder zum Zulassen oder Verweigern des Zugriffs) hat. Wenn Sie sicher sind, dass die Anwendung konfiguriert ist, sie aber immer noch in den vorhergehenden Routen fehlt, wenden Sie sich an den Citrix Support.

Fehlerbehebung beim Zugriff auf geroutete Anwendungen

Wenn Sie versuchen, auf Ihre Anwendung zuzugreifen (die in der Routenliste angezeigt wird), welches Verhalten wird beobachtet?

- **Sie erhalten einen Domänenauflösungsfehler (ERR_NAME_NOT_FOUND)**

  Dies deutet höchstwahrscheinlich darauf hin, dass die Anwendung nicht korrekt konfiguriert ist oder die kontextbezogenen Routen nicht korrekt empfangen werden.

- **Eine cremefarbene Seite mit der Meldung „Zugriff verweigert“**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dies deutet darauf hin, dass die Richtlinienkonfiguration in der Secure Private Access Konsole nicht so konfiguriert ist, dass sie den aktuellen Benutzer einschließt.

- **Eine cremefarbene Seite mit der Meldung „Hoppla! Etwas ist schiefgelaufen.“**

  Die häufigste Ursache für diese Fehlerseite ist, dass der Connector die Zielanwendung nicht erreichen kann. In diesem Fall beheben Sie den Connector-Zugriff auf interne Anwendungen gemäß der Citrix-Dokumentation. Häufige Probleme sind:

  - Interne DNS-Erreichbarkeit
  - Backend-Dienst ist ausgefallen
  - Firewall-Regeln

- **Eine weiße Seite mit der Meldung „Dienst nicht verfügbar“ in großer roter Schrift**

  Dies kann ein vorübergehender Fehler sein und sich nach einigen Minuten von selbst beheben.

  Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

- **Zeitüberschreitung**

  - Stellen Sie zunächst sicher, dass `via.prod.securegateway.goog` erreichbar ist, indem Sie es in die Adressleiste von Chrome eingeben. Sie müssen eine 401-Antwort erhalten. Wenn ein Timeout auftritt, blockiert eine zwischengeschaltete Firewall oder ein Proxy den Zugriff und muss behoben werden, bevor auf Anwendungen zugegriffen werden kann.
  - Eine weitere mögliche Ursache für ein Anwendungs-Timeout ist eine Firewall, die den Datenverkehr zum Internet und insbesondere zum Google Security Gateway blockiert. Dies ist häufig in Szenarien der Fall, in denen ein Kunde einen expliziten Proxy benötigt, um das Internet zu erreichen. Die Secure Private Access-Integration mit Chrome Enterprise Premium unterstützt diese Proxy-Konfiguration nicht.

- **Zertifikatsfehler**

  Die Anwendung verwendet möglicherweise ein privates CA-Zertifikat, und der Browser könnte daher einen „Fehler bei nicht vertrauenswürdigem Zertifikat“ anzeigen. Über die Chrome Enterprise Premium-Konfiguration kann der Kunde seine vertrauenswürdige Stamm-CA an den Browser übertragen. Weitere Informationen finden Sie unter Chrome Enterprise Premium zum Verwalten von Stammzertifikatkonfigurationen verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sicherstellen der Ausrichtung von IdP und Google Directory

Für die Secure Private Access-Integration mit Chrome Enterprise Premium muss die Synchronisierung Ihres Verzeichnisses mit Google Directory bestimmte Spezifikationen erfüllen, die in den Voraussetzungen für die integrierte Lösung beschrieben sind.

Wenn die E-Mails der Benutzer und Benutzergruppen korrekt sind und mit den in Ihrem Quellverzeichnis konfigurierten übereinstimmen, fahren Sie mit Zugriffseinstellungen für die Gruppe in der Google Admin Console prüfen fort.

Zugriffseinstellungen für die Gruppe in der Google Admin Console prüfen

Navigieren Sie in der Google Admin Console zu **Verzeichnis > Gruppen** und wählen Sie die Gruppe aus, für die Sie Ihre Zugriffsrichtlinie konfiguriert haben und für die Ihre Anwendung nicht geladen wird.

Wählen Sie dort **Zugriffseinstellungen** aus und stellen Sie sicher, dass in der Zeile **Wer Mitglieder anzeigen kann** die Option **Gruppenmitglieder** aktiviert ist. Diese Konfiguration muss für alle Gruppen gelten, für die Sie Richtlinien in Secure Private Access erstellen möchten.

Wenn diese Option bereits aktiviert ist, wenden Sie sich an den Citrix Support.

Bekannte Probleme mit der CEP-Integration

Die folgenden bekannten Probleme bestehen in der Secure Private Access-Integration mit Chrome Enterprise Premium.

Secure Private Access-Benutzeroberfläche

- **Problem:** Die Sitzungsrichtlinienkonfiguration erlaubt Benutzern derzeit nur das Hinzufügen von zwei Simulationsbedingungen, obwohl drei Bedingungen verfügbar sind. Dies schränkt die Flexibilität bei der Richtlinienerstellung ein.

  Problemumgehung: Erstellen Sie zwei separate Sitzungsrichtlinien; eine mit zwei der Simulationsbedingungen und eine weitere Richtlinie mit der verbleibenden Bedingung.

- **Problem:** Die TCP/UDP-Server-zu-Client-Konfigurationsoption ist in der Benutzeroberfläche der Anwendungskonfiguration nicht in allen Kundenumgebungen verfügbar. Dies schränkt die Möglichkeit ein, das Server-zu-Client-Verkehrsverhalten zu definieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfiguration der adaptiven Zugriffsrichtlinie

- **Problem:** Die Erstellung von Zugriffsrichtlinien schlägt fehl, wenn Okta-Gruppen in den Regeln angegeben sind. Dieses Problem betrifft nur Gruppen, die im Okta-Verzeichnis vorhanden sind.

  Problemumgehung: Sie können Okta als Identitätsanbieter, aber nicht als Verzeichnis verwenden. Um Okta als IdP zu verwenden, müssen Sie zuerst Ihr lokales AD mit Okta integrieren. Einzelheiten finden Sie unter Okta als Identitätsanbieter mit Citrix Cloud verbinden.

Google Chrome-Browser

- **Problem:** Wenn die Google-Profilauswahl geöffnet ist und der Benutzer versucht, eine App von CWA oder einem Nicht-Chrome-Browser zu starten, wenn kein vorhandenes Profil vorhanden ist, wird der Workflow zur Profilerstellung nicht ausgelöst.

  Problemumgehung: Schließen Sie die Profilauswahl und starten Sie die App neu.

- **Problem:** Das Anmelden bei CWA mit einem verwalteten Chrome-Profil und das Starten einer App führt den Benutzer nach der Profilerstellung nicht zur ursprünglichen internen App-URL.

  Problemumgehung: Starten Sie die App nach der Profilerstellung neu.

- **Problem:** Benutzer, die Teil einer Gruppe sind, werden nicht automatisch synchronisiert, wenn eine Gruppe aus der Google Admin-Konsole synchronisiert wird. Die Einstellung `whoCanViewGroupMembership` wird während der Synchronisierung explizit auf `ALL_MANAGERS_CAN_VIEW` überschrieben. Daher ist die eingeschränkte Sichtbarkeit zu erwarten.

  Problemumgehung: Aktualisieren Sie die Google-Gruppenberechtigung manuell in der Google Admin-Konsole oder über die API. Einzelheiten finden Sie unter `<https://developers.google.com/workspace/admin/groups-settings/manage>`.

- **Problem:** Benutzer werden aufgefordert, sich mit einem Benutzernamen und Kennwort über ein Proxy-Pop-up zu authentifizieren, wenn sie über ein verwaltetes Chrome-Profil auf veröffentlichte SaaS-/Webanwendungen zugreifen. Dies tritt typischerweise nach einer Zeit der Inaktivität auf:

  Ursachen:

  - Ein Proxy-Token ist nicht verfügbar oder das Proxy-Token ist verfügbar, aber anschließend abgelaufen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die SEB-Erweiterung erfordert aufgrund einer verzögerten Initialisierung eine erneute Initialisierung.

Problemumgehung: Starten Sie die Chrome-Sitzung in einem neuen Fenster neu.

- **Problem:** Benutzer können zeitweise „Service Unavailable“-Fehler erhalten, wenn sie über verwaltete Chrome-Profile oder die Citrix Workspace App auf externe SaaS-Anwendungen zugreifen. Dieses Problem ist auf ein ungelöstes Backend-Problem in der Google-Infrastruktur zurückzuführen.

  Problemumgehung: Wenden Sie sich an das Google-Team, um Unterstützung zu erhalten.

Open ID Connect (OIDC)

Problem: Wenn ein Kunde mehr als eine Microsoft Entra ID-Verbindung zum selben Azure-Mandanten hat, können die Entra ID IdPs während der OIDC-Clientkonfiguration nicht zuverlässig unterschieden werden. Dieses Problem betrifft nur die Zuverlässigkeit der IdP-Auswahl. Die OIDC-Clientkonfiguration und das Authentifizierungsverhalten bleiben davon unberührt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erste Schritte mit Citrix Secure Private Access

Dieses Dokument führt Sie durch die ersten Schritte beim Onboarding und der erstmaligen Einrichtung der Bereitstellung von SaaS-Anwendungen. Dieses Dokument richtet sich an Anwendungsadministratoren.

Systemanforderungen

- **Unterstützung von Betriebssystemen:** Die Citrix Workspace-App wird unterstützt auf:
  - Windows 7, 8, 10 und 11
  - macOS – 10.11 und höher
- **Browser-Unterstützung:** Greifen Sie über die Cloud Store-URL mit den neuesten Versionen von Edge, Chrome, Firefox oder Safari auf Apps zu.
- **Unterstützung der Citrix Workspace™-App:** Greifen Sie mit der Citrix Workspace-App für jede der Desktop-Plattformen (Windows, Mac) auf Stores zu.
- Wenn Benutzer über eine benutzerdefinierte URL auf ihren Store zugreifen, müssen sie die folgenden Mindestversionen verwenden:
  - Citrix Workspace-App für Windows: 2503.10 oder höher
  - Citrix Workspace-App für Mac: 2505.10 oder höher
  - Citrix Secure Access-App für Mac: 26.04.1.1 und höher
  - Citrix Secure Access-App für iOS: 26.04.1 und höher

Funktionsweise

Citrix Secure Private Access hilft IT- und Sicherheitsadministratoren, den autorisierten Endbenutzerzugriff auf genehmigte SaaS- und unternehmensgehostete Web-Apps zu steuern. Benutzeridentitäten und -attribute werden verwendet, um Zugriffsrechte zu bestimmen, und Zugriffssteuerungsrichtlinien legen die für die Ausführung von Operationen erforderlichen Rechte fest. Sobald ein Benutzer authentifiziert ist, autorisiert die Zugriffssteuerung die entsprechende

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zugriffsebene und die zulässigen Aktionen, die mit den Anmeldeinformationen dieses Benutzers verbunden sind.

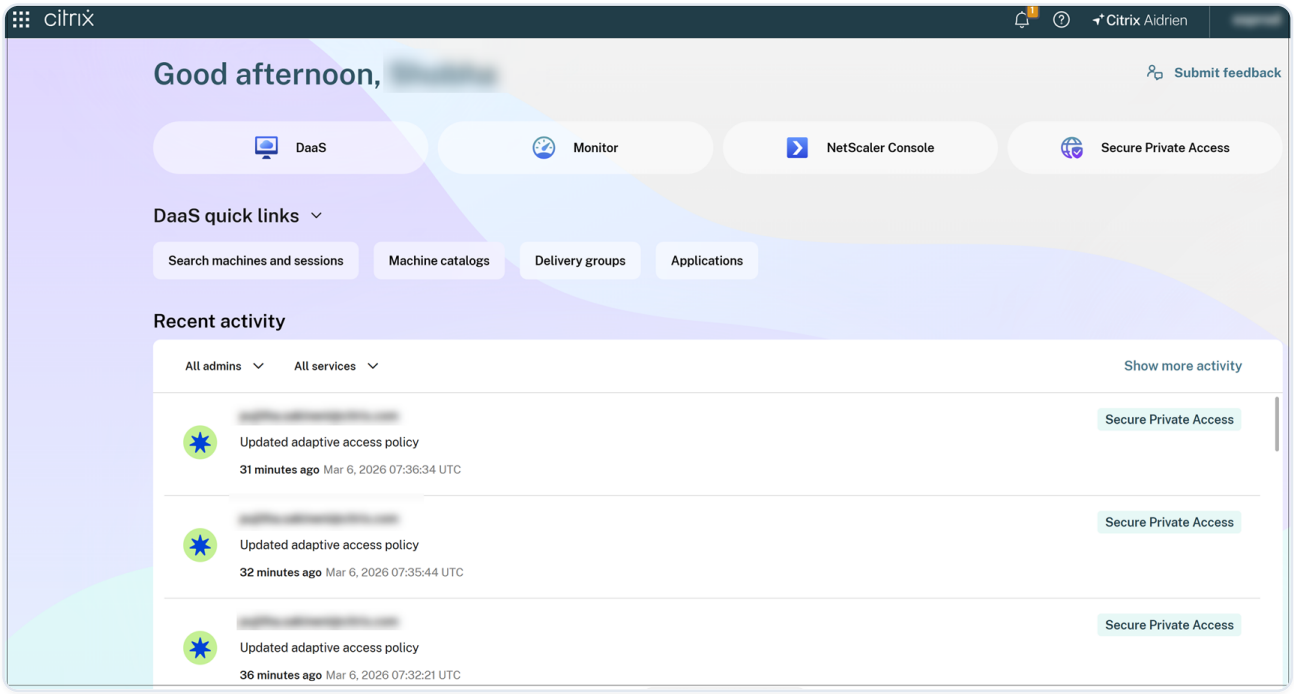
Citrix Secure Private Access kombiniert Elemente mehrerer Citrix Cloud™-Dienste, um Endbenutzern und Administratoren eine integrierte Erfahrung zu bieten.

FUNKTIONALITÄT	DIENST/KOMPONENTE, DER/DIE DIE FUNKTIONALITÄT BEREITSTELLT
Konsistente Benutzeroberfläche für den Zugriff auf Apps	StoreFront Cloud
SSO für SaaS- und Web-Apps	Citrix Gateway Service Standard
Webfilterung und -kategorisierung	Webfilterdienst
Erweiterte Sicherheitsrichtlinien für SaaS	Cloud-App-Steuerung
Sicheres Browsen	Remote Browser Isolation-Dienst
Transparenz bei Website-Zugriffen und riskantem Verhalten	Citrix Analytics

Erste Schritte mit dem Citrix Secure Private Access-Dienst

1. Registrieren Sie sich für Citrix Cloud.
2. Beantragen Sie die Berechtigung für den Secure Private Access-Dienst.
3. Nachdem die Berechtigung erteilt wurde, wird der Secure Private Access-Dienst für Ihr Konto bereitgestellt.
4. Greifen Sie auf die Admin-Benutzeroberfläche des Secure Private Access-Dienstes zu.
5. Konfigurieren Sie den Store, den Endbenutzer verwenden, um ihre Apps in StoreFront Cloud anzuzeigen und zu starten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Hinweis:

- Damit Ihre Endbenutzer den Store nutzen und auf die Apps zugreifen können, müssen sie die Citrix Workspace-App herunterladen und verwenden oder die Store-URL in ihrem Webbrowser öffnen. Sie müssen einige SaaS-Apps in Ihrem Store veröffentlicht haben, um die Citrix Secure Private Access-Lösung zu testen. Die Workspace-App kann unter Downloads heruntergeladen werden. Wählen Sie in der Liste **Downloads suchen** die Option **Citrix Workspace-App** aus.
- Wenn Sie eine ausgehende Firewall konfiguriert haben, stellen Sie sicher, dass der Zugriff auf die folgenden Domänen zugelassen ist.
  - *.cloud.com
  - *.nssvc.net
  - *.netscalergateway.net

  Weitere Details finden Sie unter Cloud Connector-Proxy- und Firewallkonfiguration und Anforderungen an die Internetkonnektivität.

Bereitstellungsmodelle für den Secure Private Access-Dienst

Der Secure Private Access-Dienst steht Kunden in zwei Architekturvarianten zur Verfügung.

- **Hybride Dienstarchitektur:** Die hybride Dienstarchitektur ermöglicht Ihnen die Verwendung Ihrer lokalen StoreFront- und NetScaler Gateway-Komponenten, wodurch sichergestellt wird, dass der gesamte Benutzerdatenverkehr unter Ihrer Kontrolle bleibt. Außerdem werden die

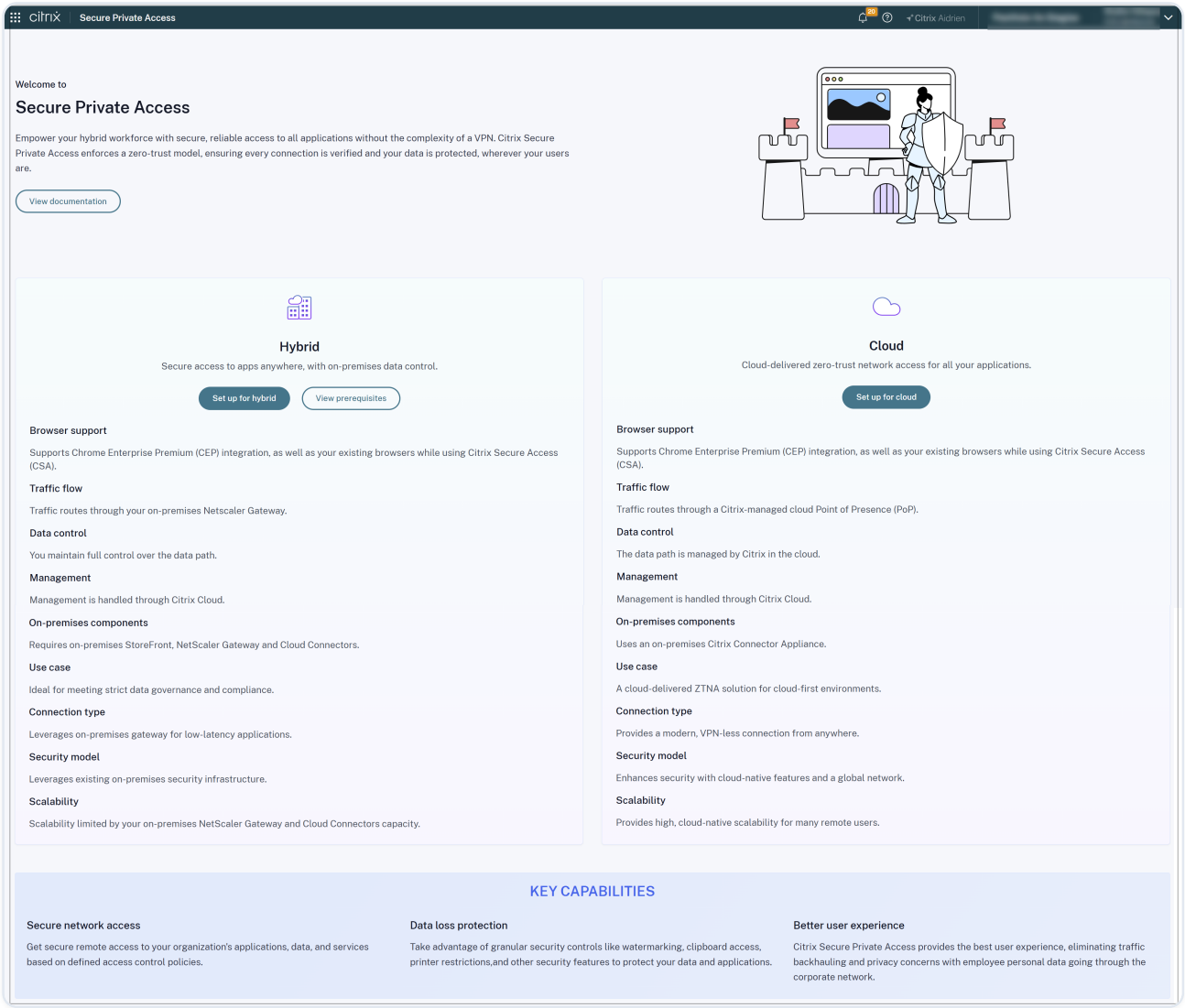
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Komponenten für die Standortverwaltung von Citrix gehostet und verwaltet. Weitere Informationen finden Sie unter Hybride Bereitstellung.

- **Cloud-native Dienstarchitektur:** Die Cloud-native Dienstarchitektur ist eine Cloud-basierte ZTNA-Lösung, die adaptiven Zugriff auf von der IT genehmigte Anwendungen bietet, unabhängig davon, ob sie lokal oder in der Cloud bereitgestellt werden. Weitere Informationen finden Sie unter Citrix Secure Private Access.

Sie können diese Optionen in der Verwaltungskonsole des Secure Private Access-Dienstes auswählen.

1. Melden Sie sich bei Citrix Cloud™ an und klicken Sie dann auf **Secure Private Access**.
2. Wählen Sie je nach Bedarf **Einrichtung für Hybrid** oder **Einrichtung für Cloud**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standorte der Points of Presence (PoPs) für den Citrix Secure Private Access™ Dienst

Citrix fügt weltweit weitere PoPs hinzu, um Geschäftskontinuität und qualitativ hochwertigen Service für die Kunden von Citrix Secure Private Access zu gewährleisten.

Secure Private Access Management-PoPs

Im Folgenden finden Sie eine Liste der Secure Private Access Management-PoP-Standorte.

POP-NAME	ZONE	REGION
az-eu-w-mgmt	Azure Westeuropa	Niederlande
az-in-s-mgmt	Azure Südindien	Chennai
az-us-e-mgmt	Azure Ost-USA	Virginia

Secure Private Access Daten-PoPs

Im Folgenden ist die Liste der Secure Private Access Daten-PoP-Standorte aufgeführt.

POP-NAME	ZONE	REGION
az-us-e	Azure US-Osten	Virginia
az-us-w	Azure US-Westen	Kalifornien
az-us-sc	Azure US-Süd-Mitte	Texas
az-aus-e	Azure Ostaustralien	New South Wales
az-eu-n	Azure Nordeuropa	Irland
az-eu-w	Azure Westeuropa	Niederlande
az-jp-e	Azure Japan, Osten	Tokio, Saitama
az-bz-s	Azure Brasilien, Süden	Bundesstaat São Paulo
az-asia-se	Azure Südostasien	Singapur
az-uae-n	Azure VAE Nord	Dubai

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POP-NAME	ZONE	REGION
az-in-s	Azure Südindien	Chennai
az-asia-hk	Azure Ostasien	Hongkong
az-nw-e	Azure Norwegen Ost	Norwegen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access-Onboarding und -Einrichtung

Die Secure Private Access™-Administratorkonsole ermöglicht Administratoren das Onboarding und die Verwaltung von SaaS-, Web- und TCP/UDP-Anwendungen sowie das Definieren detaillierter Zugriffsrichtlinien, die festlegen, wie Benutzer mit diesen Anwendungen interagieren.

Citrix Secure Private Access ist in Google Chrome Enterprise Premium integriert, wodurch Kunden sicher auf private Web- und SaaS-Anwendungen zugreifen können, indem sie Google Chrome Enterprise Premium als ihren Unternehmensbrowser verwenden.

Die übergeordneten Schritte zum Onboarding und zur Einrichtung von Secure Private Access sind:

1. Benutzer für Secure Private Access onboarden
2. Store-URL in Citrix® StoreFront Cloud konfigurieren
3. Google Chrome-Integration einrichten.
4. Connector Appliance konfigurieren
5. Apps für Ihre Benutzer hinzufügen.
6. Berechtigungen für den App-Zugriff durch Erstellen der erforderlichen Zugriffsrichtlinien zuweisen.

WICHTIG:

Sie können Google Chrome als Ihren Unternehmensbrowser festlegen. Weitere Informationen finden Sie in den folgenden Themen.

- Google Chrome als Unternehmensbrowser festlegen
- Überlegungen vor dem Browserwechsel

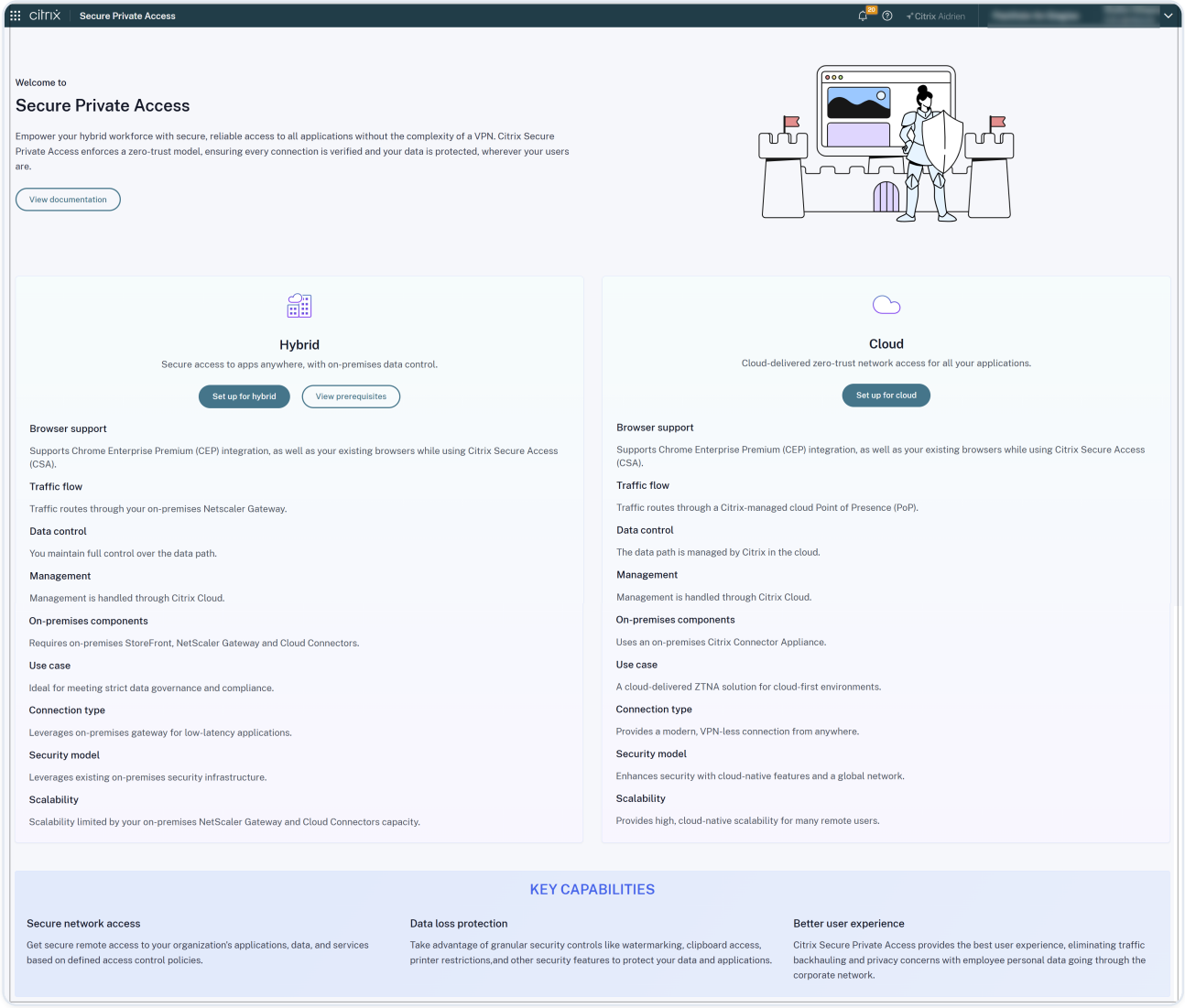
Benutzer für Secure Private Access onboarden

Führen Sie die folgenden Schritte aus, um Ihre Benutzer in Secure Private Access zu integrieren.

1. Melden Sie sich bei Citrix Cloud™ an und klicken Sie dann auf **Secure Private Access**.

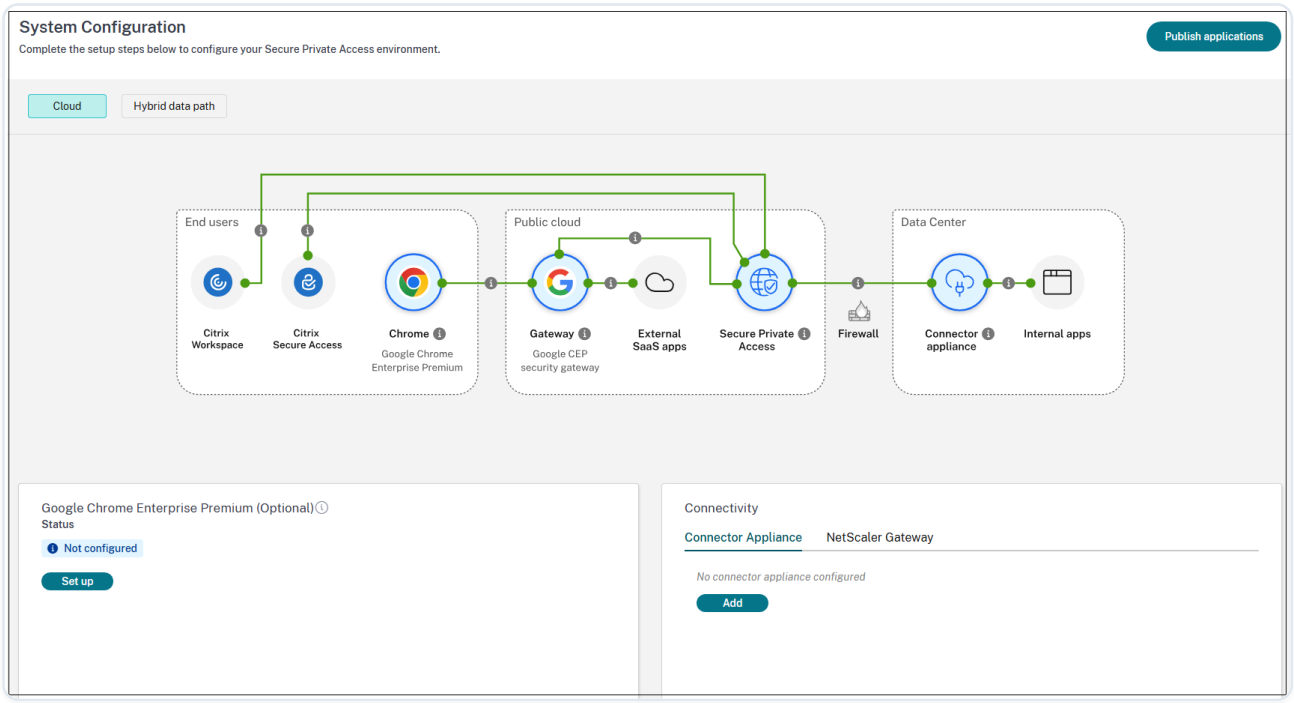
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie **Setup for cloud** aus und klicken Sie dann auf **Continue**.



Das Topologiediagramm zeigt die Komponenten, die in Secure Private Access Cloud-Bereitstellungen verwendet werden. Sie können auf das Hilfesymbol klicken, um eine kurze Beschreibung jeder Komponente im Ablauf anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Für neue Kunden** öffnet die Auswahl des Secure Private Access-Dienstes in der Citrix Cloud-Konsole die Einrichtungsseite, auf der sie Connector Appliance und CEP konfigurieren können.
  - Um Connector Appliance zu konfigurieren, klicken Sie im Bereich **Connector Appliance Configuration** auf **Add**. Weitere Informationen finden Sie unter Configure Connector Appliance.
  - Um Google Chrome Enterprise Premium (CEP) zu konfigurieren, klicken Sie im Bereich **Google Chrome Enterprise Premium** auf **Set up** und folgen Sie den Anweisungen auf dem Bildschirm. Weitere Informationen finden Sie unter Setup Google Chrome integration.

  Sobald die Einrichtung abgeschlossen ist, werden die Administratoren bei späteren Besuchen zum Secure Private Access-Dashboard weitergeleitet, wenn sie in der Citrix Cloud-Konsole auf Secure Private Access klicken.
- **Für bestehende Kunden** prüft das System:
  - Verfügbarkeit der Connector Appliance
  - Status von Chrome Enterprise Premium

  Connector Appliance-Prüfung: Das System prüft, ob eine oder mehrere Connector Appliances konfiguriert sind und wie viele verfügbar sind. Diese Prüfung hilft Administratoren zu verstehen, dass die Konfiguration einer Connector Appliance für Benutzer obligatorisch ist, um sich erfolgreich mit internen Unternehmensanwendungen (Web, TCP/UDP) zu verbinden. Die Connector Appliance ermöglicht die Endbenutzerkonnektivität über den nativen Citrix Secure Access-Client und unterstützt jeden Browser der Wahl des Kunden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Chrome Enterprise Premium-Konfigurationsprüfung: Die Chrome Enterprise Premium-Konfigurationsprüfung hilft Administratoren festzustellen, ob die Integration zwischen Citrix Secure Private Access und Chrome Enterprise Premium aktiviert ist. Diese Integration ermöglicht Endbenutzern den sicheren Zugriff auf Unternehmens-Webanwendungen über den Chrome-Browser, ohne dass der native Citrix Secure Access-Client erforderlich ist.

HINWEIS:

Die Einrichtung von Google Chrome Enterprise Premium ist optional und kann übersprungen werden.

Store-URL in Citrix StoreFront Cloud konfigurieren

Sie können den Secure Private Access-Dienst in Citrix® StoreFront Cloud integrieren. Sie stellen Ihren Benutzern eine Store-URL zur Verfügung, die sie in einem Webbrowser oder der Citrix Workspace™-App öffnen können. Der Store bietet eine einheitliche Benutzererfahrung für die konfigurierten SaaS-Apps, Web-Apps, virtuellen Apps und andere konfigurierte Ressourcen.

Standardmäßig wird ein Store mit der URL `customerid.cloud.com` erstellt. Sie können diese URL ändern oder eine eigene benutzerdefinierte URL hinzufügen, z. B. `store.company.com`. Informationen zum Konfigurieren der Stores finden Sie unter Zugriff auf Stores konfigurieren.

Google Chrome-Integration einrichten

Führen Sie auf der Seite „Google Chrome-Integration“ die folgenden Schritte aus:

1. Kopieren Sie die automatisch generierte E-Mail-Adresse des Dienstkontos und fügen Sie sie in das entsprechende Feld in der Google Admin-Konsole ein.
    a. Gehen Sie in der Google Admin-Konsole zu **Administratorrollen**.
    b. Wählen Sie die Rolle aus, die für den Secure Private Access-Dienst erstellt wurde, und wenden Sie die empfohlenen Berechtigungen an. Eine Liste der Berechtigungen finden Sie unter Administratorrollen und Berechtigungen.
    c. Wählen Sie unter **Administratoren** die Option **Dienstkonten zuweisen**.
    d. Fügen Sie das Citrix-Dienstkonto (`tenant-sa-<random-string>.iam.gserviceaccount.com`) ein und wählen Sie **Hinzufügen**. Wählen Sie dann **Rolle zuweisen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zu Rollen finden Sie unter Informationen zu Administratorrollen.

e. Navigieren Sie in der Google Admin-Konsole zu **Verzeichnis > Benutzer**.

f. Klicken Sie auf **Neuen Benutzer hinzufügen** und erstellen Sie einen neuen Benutzer (Vorname: Citrix Service, Nachname: Account, Primäre E-Mail: caccount). Behalten Sie die E-Mail-Adresse des neu erstellten Benutzers bei.

g. Nachdem der neue Benutzer erstellt wurde, wählen Sie ihn aus und gehen Sie zu **Benutzerdetails**. Wählen Sie unter **Administratorrollen und -berechtigungen** dieselbe Rolle aus und weisen Sie sie diesem Benutzer zu.

h. Gehen Sie zu **Sicherheit > Zugriffs- und Datenkontrolle > API-Steuerelemente** und klicken Sie auf **Domainweite Delegierung verwalten**.

i. Klicken Sie unter **API-Clients** auf **Neu hinzufügen** und geben Sie die Client-ID und die OAuth-Bereiche mit den entsprechenden Informationen ein, die auf der Seite „Google Chrome-Integration“ bereitgestellt werden.

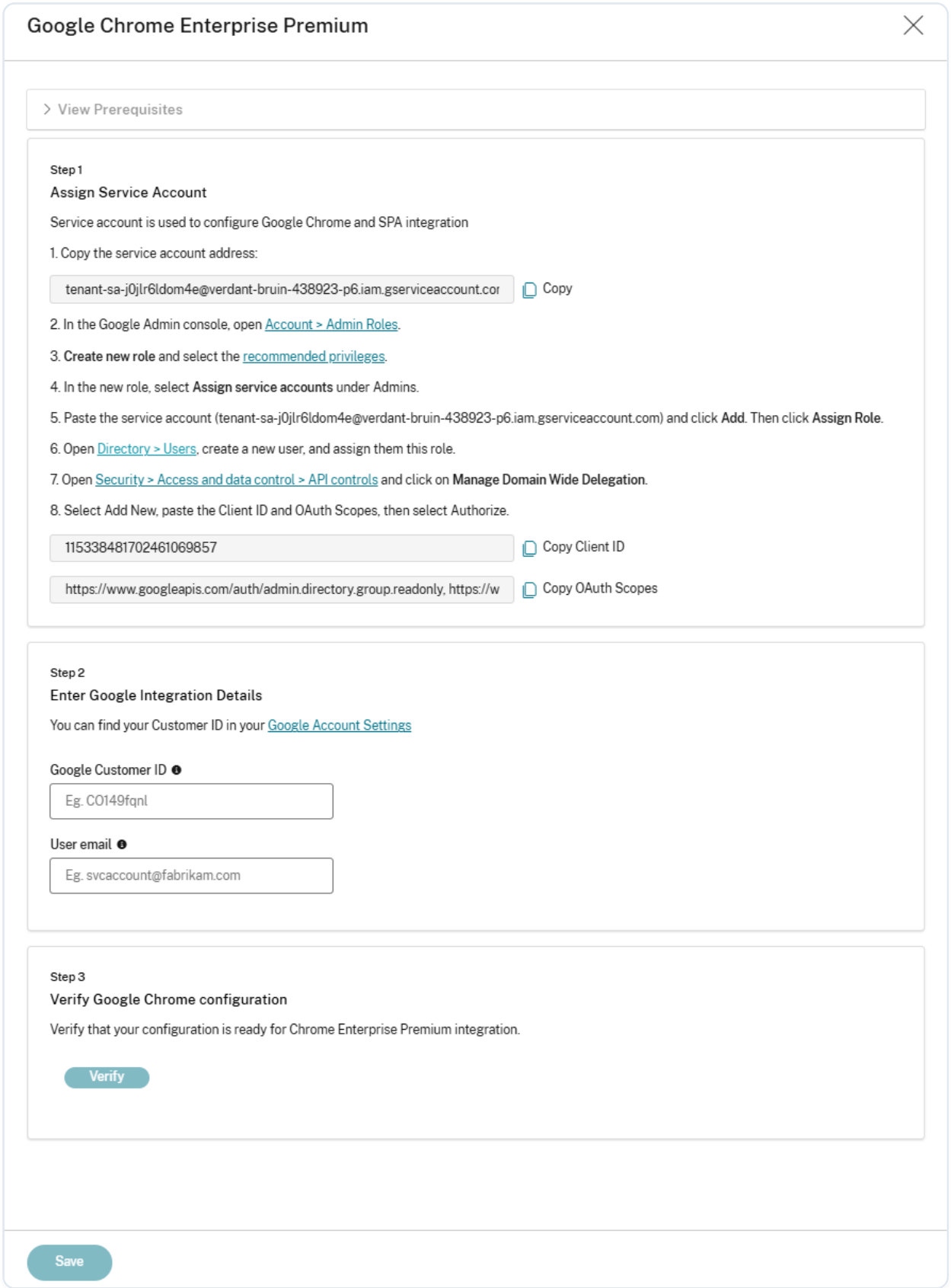
j. Kopieren Sie die Google-Kunden-ID, die in den **Google-Kontoeinstellungen** in der Google Admin-Konsole verfügbar ist, in das Feld **Google-Kunden-ID** auf der Seite **Google Chrome-Integration**.

k. Füllen Sie das **Benutzer-E-Mail-Feld** auf der Seite „Google Chrome-Integration“ mit der E-Mail-Adresse des zuvor erstellten Benutzers aus.

2. Klicken Sie auf **CEP-Verifizierung ausführen**, um Ihre Google Workspace-Konfiguration zu überprüfen und sicherzustellen, dass sie für die Chrome Enterprise Premium-Integration bereit ist, bevor Sie mit dem nächsten Schritt fortfahren.

   - Wenn die Überprüfung einen Fehler oder eine Warnung zurückgibt, finden Sie unter Bekannte Überprüfungsfehler und Warnungen Anleitungen zur Fehlerbehebung.
   - Sobald die CEP-Verifizierung erfolgreich ist, verbindet sich der Secure Private Access-Dienst erfolgreich mit der Google-Kunden-ID und ein Secure Gateway wird erstellt.
   - Nach erfolgreicher Erstellung des Secure Gateways zeigt das System die ihm zugewiesenen Ausgangs-IP-Adressen an. Administratoren können die Ausgangsregionen auswählen, die Chrome Enterprise Premium für den SaaS-Anwendungsverkehr verwendet. Weitere Informationen finden Sie unter Ausgangs-Hub-Regionen konfigurieren.
   - Wenn ein Benutzer versucht, auf eine SaaS-Anwendung zuzugreifen, geht die Anfrage nicht direkt an den SaaS-Anbieter. Stattdessen wird der Datenverkehr zuerst über das Secure Gateway geleitet, das als Partner-Konnektor fungiert. Dieses Gateway fungiert als Vermittler, der den gesamten Datenverkehr prüft und sichert, bevor er die Zielanwendung erreicht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Sie können die Integrationsdetails auch aktualisieren, nachdem der Kunde in CEP integriert wurde. Weitere Informationen finden Sie unter Google-Integrationsdetails nach der Integration aktualisieren.
- Sie können die CEP-Konfiguration während des Onboardings auf ausgewählte Organisationseinheiten des Google-Verzeichnisses anwenden, zusätzlich zu allen Benutzern und Benutzergruppen. Weitere Informationen finden Sie unter CEP für Google Directory-Organisationseinheiten konfigurieren.

- Weitere Informationen zur Integration von Secure Private Access mit Google Chrome Enterprise Premium finden Sie unter Integration mit Google Chrome Enterprise Premium.

IP-Adressen von SaaS-Anwendungen hinzufügen

Nachdem Kunden in Secure Private Access und Chrome Enterprise Premium integriert wurden, müssen Sie die Liste der von Ihren SaaS-Anwendungen verwendeten IP-Adressen zulassen. Dieser Schritt ist entscheidend, um sicherzustellen, dass:

- Benutzer auf SaaS-Anwendungen zugreifen können, ohne Konnektivitätsprobleme oder Blockaden durch Netzwerksicherheitskontrollen.
- Der Datenverkehr von Citrix Secure Private Access und Chrome Enterprise Premium als legitim erkannt und nicht versehentlich gefiltert oder abgelehnt wird.

HINWEIS:

Für eine Anwendung, die über die Connector Appliance mit dem Routing-Typ „Intern über Connector“ geleitet wird, müssen Kunden die Citrix IP-Zulassungsliste verwenden.

Konfiguration von Richtlinien für die Zugriffsbegrenzung von Prinzipalen

Richtlinien für die Zugriffsbegrenzung von Prinzipalen können Endbenutzer daran hindern, auf das von Citrix verwaltete Google Secure Gateway zuzugreifen.

Wenn Ihre GCP-Organisation standardmäßig eine Richtlinie zur Zugriffsbegrenzung von Prinzipalen hat, die den Zugriff auf mandantenübergreifende Ressourcen blockiert, erstellen Sie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

eine Richtlinie zur Zugriffsbegrenzung von Prinzipalen, die den Zugriff auf das Google Secure Gateway erlaubt. Sie können den Secure Gateway-Bezeichner von der Seite **Browsereinstellungen > Browser** abrufen. Details zur Konfiguration einer geeigneten Richtlinie finden Sie unter Google Cloud IAM – Dokumentation zu Richtlinien für die Zugriffsbegrenzung von Prinzipalen.

Google-Integrationsdetails nach dem Onboarding aktualisieren

Sobald Kunden erfolgreich in Chrome Enterprise Premium integriert wurden, ermöglicht Secure Private Access die Verwaltung ihrer Integrationsdetails nach dem Onboarding. Dies umfasst die Möglichkeit, kritische Bezeichner wie die Kunden-ID zu aktualisieren und zugehörige Benutzergruppen zu ändern.

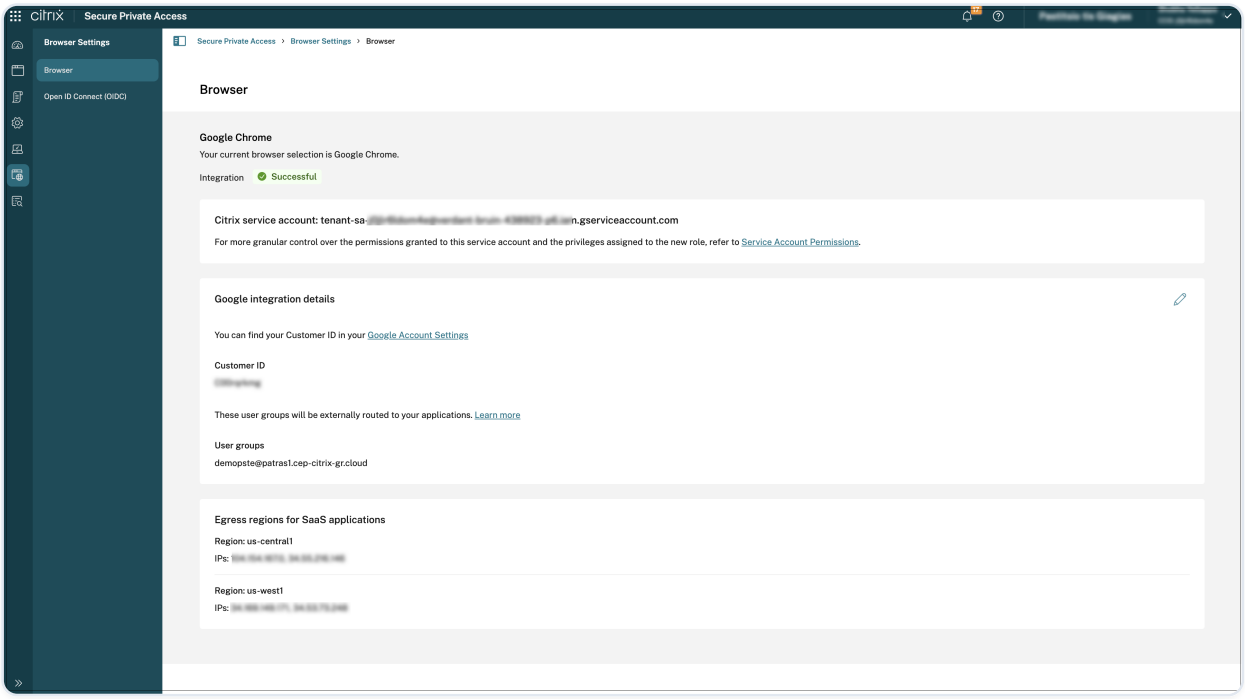
Führen Sie die folgenden Schritte aus, um die Integrationsdetails nach dem Onboarding zu aktualisieren:

1. Gehen Sie in der Secure Private Access-Administratorkonsole zu **Browsereinstellungen > Browser**.

   Die Browser-Seite zeigt die Integrationsdetails von Google Chrome an.

   Das System zeigt auch die ausgehenden IP-Adressen an, die mit dem Secure Gateway verknüpft sind. Jedes Mal, wenn ein Benutzer versucht, auf eine Software-as-a-Service (SaaS)-Anwendung innerhalb dieser Integration zuzugreifen, wird der Datenverkehr über das Google Secure Gateway geleitet, das als Partner-Konnektor fungiert, anstatt sich direkt mit der SaaS-Anwendung zu verbinden. Dieses Gateway prüft und sichert den Datenverkehr, setzt Sicherheitsrichtlinien und Zugriffssteuerungen durch und gewährleistet die Einhaltung der Sicherheitslage des Unternehmens.

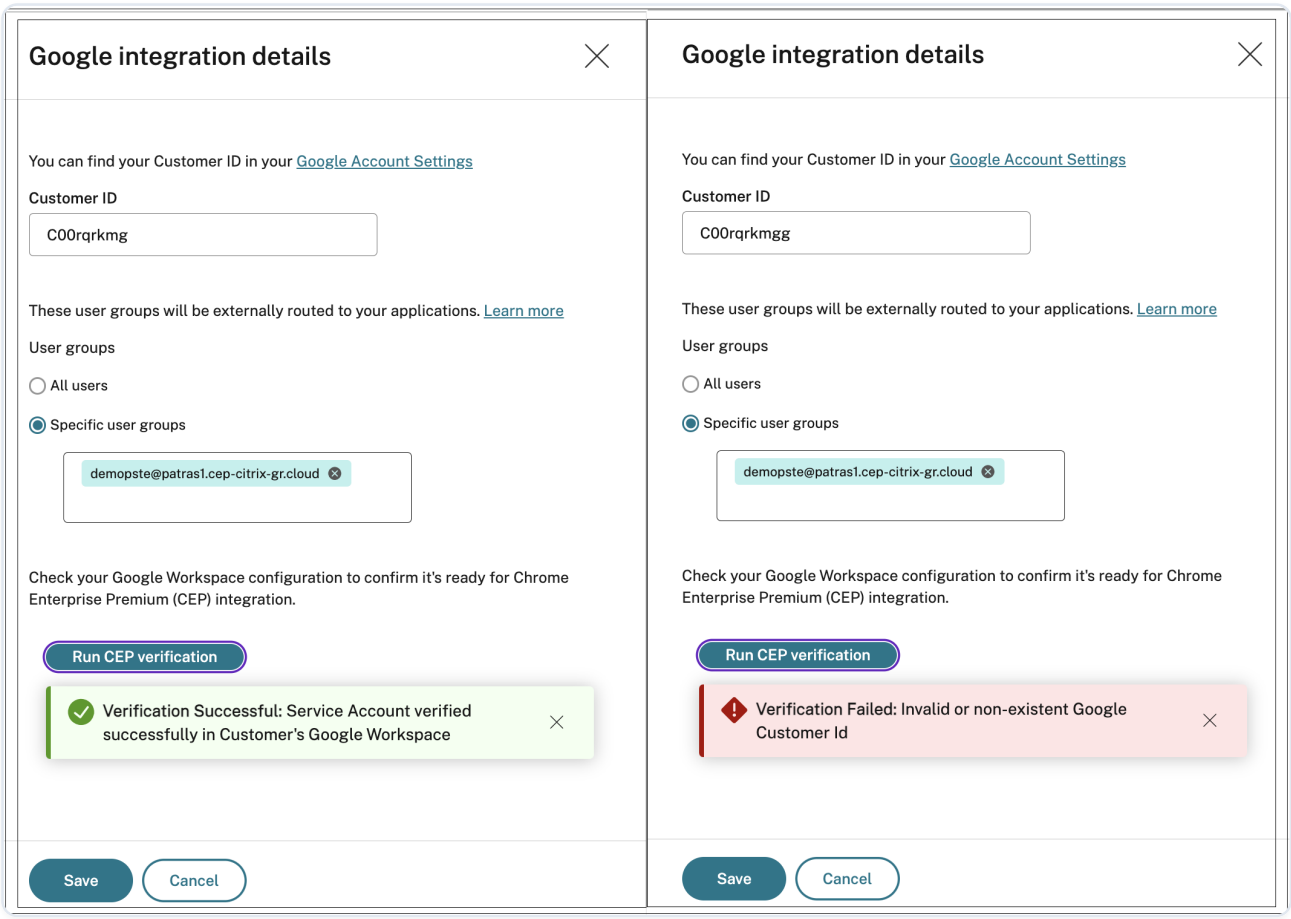
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Klicken Sie auf das Bearbeitungssymbol und aktualisieren Sie die Kunden-ID oder die Benutzergruppen oder beides.
3. Klicken Sie auf **CEP-Verifizierung ausführen**, um zu überprüfen, ob Ihre Google Workspace-Konfiguration für die Chrome Enterprise Premium-Integration bereit ist.

   Wenn es Probleme mit den Integrationsdetails gibt, zeigt die CEP-Verifizierung eine Fehler- oder Warnmeldung mit Details an, die Ihnen bei der Behebung helfen. Weitere Informationen finden Sie unter Bekannte Verifizierungsfehler und Warnungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CEP für Google Directory Organisationseinheiten konfigurieren

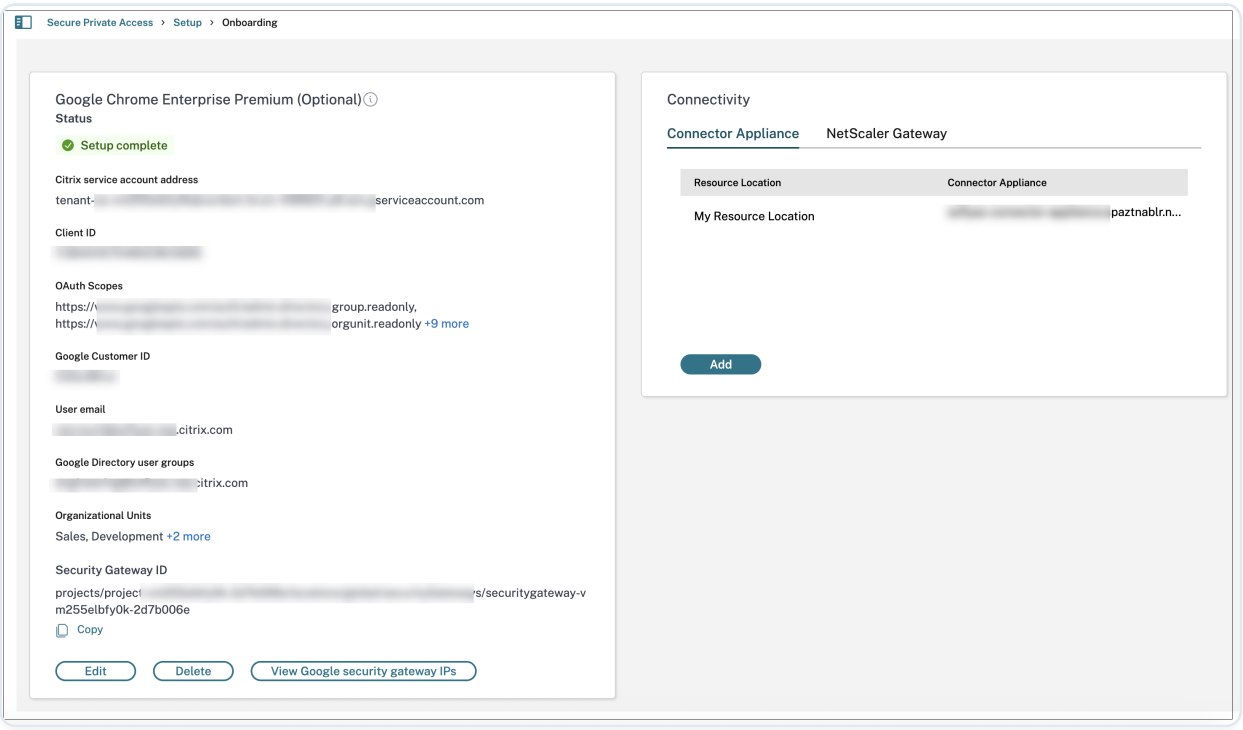
Zusätzlich zu allen Benutzern und Google Directory-Benutzergruppen können Sie eine Chrome Enterprise Premium (CEP)-Konfiguration auf ausgewählte Google Directory-Organisationseinheiten anwenden. Benutzergruppen und Organisationseinheiten schließen sich nicht gegenseitig aus, sodass eine einzelne Konfiguration beide Zielgruppen ansprechen kann. Sie können auch eine Konfiguration speichern, die nur Organisationseinheiten verwendet, ohne dass Benutzergruppen ausgewählt sind. Diese Option ist sowohl für Secure Private Access Cloud- als auch für Hybrid-Bereitstellungen verfügbar.

Eine ausgewählte Organisationseinheit wird vererbt: Die Konfiguration gilt für die Benutzer in dieser Organisationseinheit und für alle ihre untergeordneten Organisationseinheiten, einschließlich derer, die später erstellt werden.

Organisationseinheiten werden im selben Bereich wie die Google Directory-Benutzergruppen ausgewählt. Führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Chrome Enterprise Premium-Einrichtungskarte auf **Bearbeiten**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

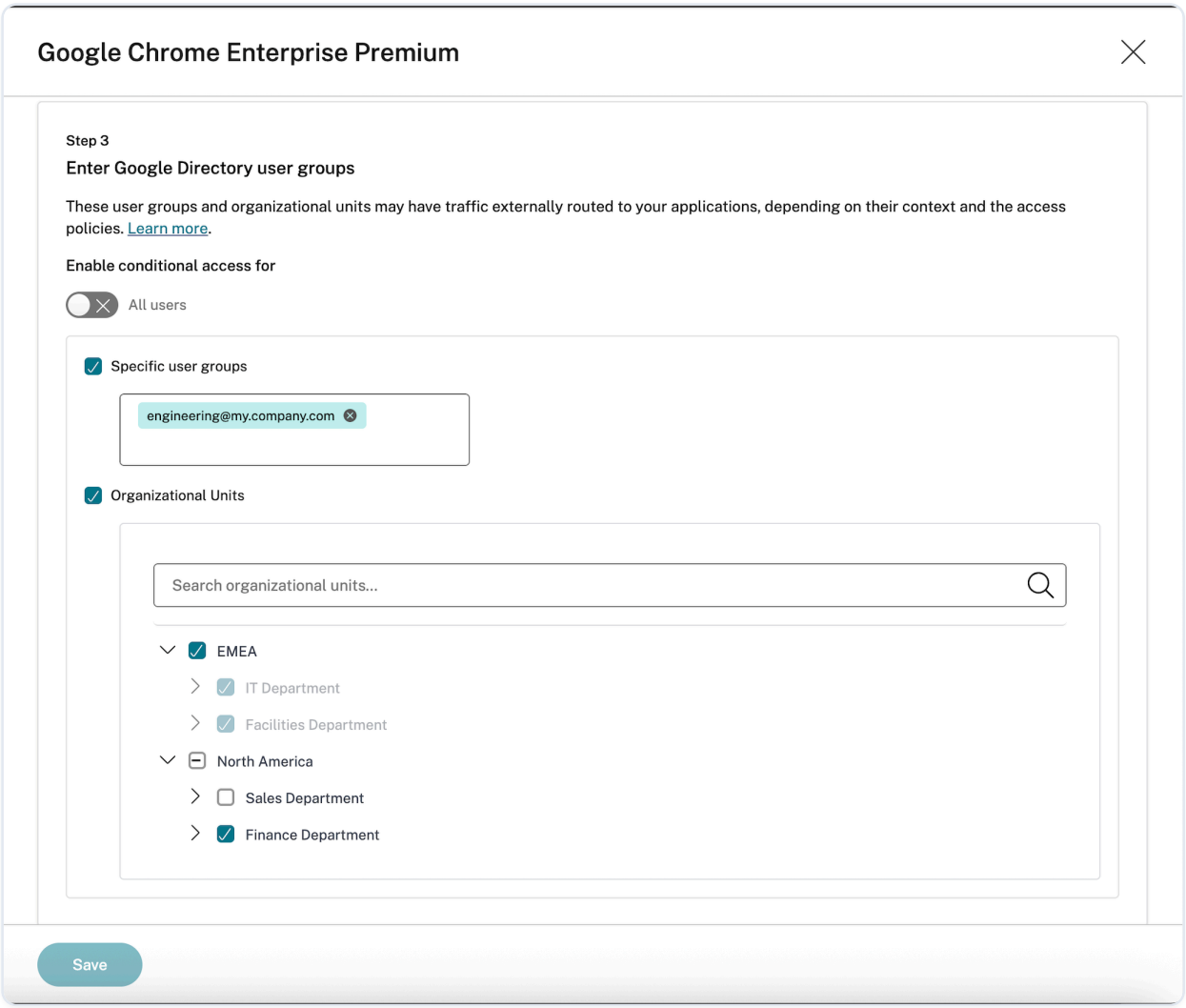


Alternativ gehen Sie in der Secure Private Access-Administratorkonsole zu **Browsereinstellungen > Browser** und klicken Sie auf das Bearbeitungssymbol.

Die Karte listet die Organisationseinheiten auf, die derzeit ausgewählt sind.

2. Klicken Sie auf **Organisationseinheiten**, um Ihre Google Directory-Hierarchie als Baum von Kontrollkästchen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

- Die Stammorganisationseinheit wird in der Struktur nicht angezeigt. Um die CEP-Integration für alle zu aktivieren, wählen Sie Alle Benutzer aus.
- Die Hierarchie wird aus Ihrem Google-Verzeichnis mithilfe des Citrix-Dienstkontos gelesen. Wenn das Dienstkonto nicht über das Recht **Organisationseinheiten > Lesen** verfügt, kann die Hierarchie nicht geladen werden, und anstelle der Struktur wird ein Fehler angezeigt. Weitere Informationen finden Sie unter Google-Administratorrollen und -Berechtigungen.

3. Wählen Sie die einzuschließenden Organisationseinheiten aus.

   Wenn Sie eine Organisationseinheit auswählen, werden auch deren untergeordnete Organisationseinheiten ausgewählt. Die untergeordneten Einheiten werden als ausgewählt angezeigt und sind ausgegraut. Sie können nicht einzeln deaktiviert werden. Um nur eine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Untergruppe einzuschließen, deaktivieren Sie das übergeordnete Element und wählen Sie die gewünschten untergeordneten Organisationseinheiten aus.

4. Klicken Sie auf **CEP-Überprüfung ausführen** und dann auf **Speichern**. Wenn Sie die Auswahl nach einer erfolgreichen Überprüfung ändern, führen Sie die Überprüfung erneut aus, bevor Sie speichern. Informationen zu den Fehlern und Warnungen, die bei der Überprüfung gemeldet werden, finden Sie unter Bekannte Überprüfungsfehler und -warnungen.

   Wenn Sie den Bereich erneut öffnen, wird die Struktur erweitert, um Ihre gespeicherte Auswahl anzuzeigen. Organisationseinheiten, die im Google-Verzeichnis gelöscht wurden, werden aus dem Bereich entfernt.

Bekannte Überprüfungsfehler und -warnungen

Bei der Überprüfung der CEP-Konfiguration kennzeichnet Secure Private Access alle Fehler oder Warnungen, die für die ausgewählte Einrichtung identifiziert wurden, bevor die Konfiguration abgeschlossen werden kann.

Sie müssen alle identifizierten Fehler beheben, bevor Sie mit der Konfiguration fortfahren. Verwenden Sie die folgende Tabelle, um spezifische Fehler zu identifizieren und zu beheben, die während der Überprüfung erkannt wurden:

FEHLERMELDUNG	AKTION
Ungültige Google-Kunden-ID oder dem Dienstkonto fehlen die Berechtigungen für den Zugriff auf Google Workspace.	Überprüfen Sie, ob die Google-Kunden-ID korrekt ist.
\^	Stellen Sie sicher, dass die erforderlichen Berechtigungen dem Dienstkonto zugewiesen sind. Details finden Sie unter Administratorrollen und -berechtigungen.
Dem Dienstkonto fehlen die Berechtigungen für den Zugriff auf Chrome-Erweiterungsrichtlinien.	Stellen Sie sicher, dass die erforderlichen Berechtigungen dem Dienstkonto zugewiesen sind. Details finden Sie unter Administratorrollen und -berechtigungen.
\^Dem Dienstkonto fehlen die Berechtigungen für den Zugriff auf Chrome-Erweiterungsrichtlinien für die Benutzergruppe.	\^

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEHLERMELDUNG	AKTION
\^Dem Dienstkonto fehlen die Berechtigungen für den Zugriff auf die Chrome-Clientzertifikatsrichtlinie.	\^
Null- oder leere Benutzergruppen-ID in Google Workspace gefunden.	Dies kann ein vorübergehendes Problem sein. Wenn es weiterhin besteht, liegt möglicherweise ein Problem mit der Google-Gruppe vor.
\^	Wenn das Problem bei mehreren Google-Gruppen weiterhin besteht, wenden Sie sich an den Citrix Support.
Ungültige oder nicht vorhandene Benutzergruppe	Überprüfen Sie den Namen der Google-Gruppe auf Rechtschreibfehler.
\^	Überprüfen Sie in der Google Admin-Konsole, ob die Gruppe noch existiert.
Dem Dienstkonto fehlen die Berechtigungen, um Chrome-Erweiterungsrichtlinien auf die Organisationseinheit anzuwenden.	Stellen Sie sicher, dass dem Dienstkonto die erforderlichen Berechtigungen zugewiesen sind. Weitere Informationen finden Sie unter Administratorrollen und -berechtigungen.

Alle identifizierten Warnungen müssen beachtet und untersucht werden, verhindern jedoch nicht den Abschluss der Konfiguration. Die folgende Liste beschreibt häufige Warnungen und wie Sie diese beheben können:

WARNMELDUNG	AKTION
Google-Kunden-ID wird bereits verwendet	Ihre Organisation verfügt über mehrere Citrix Secure Private Access-Mandanten, die dieselbe Google-Kunden-ID für die Chrome Enterprise Premium-Integration verwenden. Konfigurieren Sie dies sorgfältig, da sich überschneidende Google-Gruppen (einschließlich der Auswahl von „Alle Benutzer“ für einen oder mehrere Mandanten) vorhandene Chrome Enterprise Premium-Einstellungen in Ihren anderen Citrix-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WARNMELDUNG	AKTION
	Mandanten überschreiben oder teilweise überschreiben können.
Überschneidende Google Directory-Benutzergruppen erkannt	Überprüfen Sie die Chrome Enterprise Premium-Integration in Ihren anderen Citrix-Mandanten für die angegebenen Google-Gruppen.
\^	Entscheiden Sie, welcher Citrix-Mandant die Chrome Enterprise Premium-Einrichtung für jede der relevanten Google-Gruppen haben muss.
\^	Entfernen Sie die entsprechende Einrichtung aus den anderen Citrix-Mandanten.
\^	Wenden Sie die Google-Gruppen-Einrichtung für den ausgewählten Citrix-Mandanten erneut an, falls sie während der Bereinigung entfernt wurde.
Die Option „Alle Benutzer“ kann sich mit anderen Kunden überschneiden, die mit dieser Google-Kunden-ID verknüpft sind.	Das Konfigurieren von Chrome Enterprise Premium für „Alle Benutzer“ (die Stamm-Organisationseinheit von Google) kann andere Secure Private Access-Einrichtungen überschreiben, die dieselbe Google-Kunden-ID verwenden.
\^	Verwenden Sie diese Einstellung nur, wenn die anderen Citrix-Mandanten nicht aktiv von Benutzern verwendet werden.
Die Option „Alle Benutzer“ wird von mindestens einem Kunden verwendet, der mit dieser Google-Kunden-ID verknüpft ist.	Wenn ein anderer Citrix-Mandant Chrome Enterprise Premium für „Alle Benutzer“ (die Stamm-Organisationseinheit von Google) konfiguriert hat, kann dies die für diesen Citrix-Mandanten geplanten Google-Gruppen-Integrationen überschreiben.
\^	Bestätigen Sie, ob der andere Citrix-Mandant die „Alle Benutzer“-Integration benötigt. Falls

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WARNMELDUNG	AKTION
	nicht, ändern Sie diesen Mandanten in eine bestimmte Google-Gruppe.
Überlappende Google Directory-Organisationseinheiten erkannt	Ein anderer Kunde, der mit dieser Google-Kunden-ID verknüpft ist, verwendet bereits die Organisationseinheit oder eine Organisationseinheit in ihrem Pfad.
\^	Die Überschneidung gilt für die Organisationseinheit und alle ihre untergeordneten Organisationseinheiten. Überprüfen Sie die Chrome Enterprise Premium-Integration auf Ihren anderen Citrix-Mandanten für die aufgeführten Organisationseinheiten.
Dem Dienstkonto fehlt die Berechtigung `Services > Chrome Management > Settings > Managed Browsers > Read`	Bestätigen Sie, dass das entsprechende Privileg zugewiesen wurde. Falls ja, überprüfen Sie, ob Sie ein Abonnement für Chrome Enterprise Core oder Chrome Enterprise Premium in Ihrer Google Admin-Konsole haben (unter Abrechnung > Abonnements).

Problem bei der Bereitstellung mit mehreren Benutzergruppen

Beim Konfigurieren der Chrome Enterprise-Integration in Secure Private Access (während des Onboardings oder über die Seite **Browsereinstellungen**) kann die Angabe von mehr als acht Benutzergruppen zu Bereitstellungsfehlern führen. Führen Sie als Problemumgehung Folgendes aus:

- Verwenden Sie eine dedizierte übergeordnete Verzeichnisgruppe, die alle erforderlichen Gruppen umfasst.
- Konfigurieren Sie diese übergeordnete Gruppe während des Onboardings.
- Wenn sich die Gruppenmitgliedschaft im Verzeichnis ändert, wiederholen Sie den Synchronisierungsprozess mit dem Google-Verzeichnis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nächste Schritte

Nachdem Sie Connector Appliance und Chrome Enterprise Premium konfiguriert haben, können Sie die Anwendungen und Richtlinien für Ihre Benutzer konfigurieren.

- Anwendungen konfigurieren.
- Zugriffsrichtlinien konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenregionalisierung

Die Datenregionalisierung in Citrix Secure Private Access ermöglicht es Kunden, zu steuern, wo ihre Daten gespeichert werden, indem sie eine bevorzugte geografische Region auswählen. Kunden können die Region wählen, in der ihre Daten gespeichert werden, mit Optionen wie Global, Europa (EU), APAC (Asien-Pazifik) und Nordamerika (NA). Alle Konfigurationsdaten im Ruhezustand verbleiben innerhalb der ausgewählten Region, wodurch sichergestellt wird, dass sie die festgelegte Geografie nicht verlassen.

Bei jeder Benutzerzugriffsanfrage wird der Anwendungsverkehr innerhalb der ausgewählten Region verarbeitet und durchquert oder verlässt diese geografische Region nicht. Dies gilt unabhängig vom Standort des Benutzers. Selbst wenn Benutzer global verteilt sind, wird der Datenverkehr jedes Benutzers durch die ausgewählte Region geleitet und durchquert keine andere Geografie.

Die Funktion zur Datenregionalisierung bietet die folgenden Vorteile:

- Gewährleistet eine starke Datenresidenzkontrolle, indem alle Konfigurationsdaten innerhalb der ausgewählten Region verbleiben.
- Gewährleistet eine starke Datenresidenzkontrolle, indem Konfigurationsdaten sowie anwendbare Verwaltungs- und unterstützende Dienstdaten innerhalb der ausgewählten Region verbleiben, wobei regionale Daten-PoPs und Verwaltungs-Endpunkte für Kundenbereitstellungen verwendet werden.
- Stellt sicher, dass der Datenverkehr von Benutzerzugriffsanfragen für jede Anwendung innerhalb der ausgewählten Region verbleibt, indem ein standortbasiertes Routing genutzt wird, das den Benutzerdatenverkehr unabhängig vom Standort des Benutzers an bestimmte PoPs leitet.
- Hilft Organisationen, regulatorische Anforderungen und Anforderungen an die Datensouveränität zu erfüllen.
- Reduziert das Risiko, indem verhindert wird, dass Daten festgelegte geografische Gebiete verlassen.
- Unterstützt flexible globale Bereitstellungen mit regionsspezifischen Anforderungen, wodurch Kunden cloud-basierten sicheren Zugriff, der ihren Residenzrichtlinien entspricht, vertrauensvoll einführen können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Ohne Datenregionalisierung könnten Organisationen, die über Regionen hinweg tätig sind, strengen Anforderungen an die Datenresidenz und Compliance gegenüberstehen, während sie keine Kontrolle darüber haben, wo ihre Dienstdaten gespeichert werden. Ohne regionale Datengrenzen könnten Konfigurationsdaten außerhalb der erforderlichen geografischen Gebiete gespeichert werden, was das regulatorische Risiko erhöht und die Einführung von cloud-basierten sicheren Zugriffslösungen einschränkt.

Unterstützte Bereitstellungen

Diese Funktion gilt für alle Citrix Secure Private Access-Bereitstellungen, einschließlich sowohl Service- als auch Hybridmodellen, und ist besonders relevant für Organisationen mit regionalen Anforderungen an Datenresidenz, Compliance und Regulierung.

Konfiguration

Die Auswahl einer Region ist eine einmalige Einstellung während des Onboardings des Secure Private Access-Dienstes oder einer Hybridbereitstellung. Nachdem sie festgelegt wurde, verbleiben alle Daten in der ausgewählten Region, ohne Auswirkungen auf laufende Vorgänge oder Benutzer-Workflows.

1. Melden Sie sich bei Citrix Cloud an und klicken Sie dann auf **Secure Private Access**.
2. Wählen Sie **Setup for cloud** oder **Hybrid** und klicken Sie dann auf **Weiter**.
3. Wählen Sie unter **Bereitstellungsregion auswählen** die Region aus, in der Ihre Daten gespeichert werden sollen. Die verfügbaren Regionen basieren auf der Region Ihres Citrix Cloud-Kontos.
4. Klicken Sie auf **Weiter**.

Einschränkungen

Einige der Einschränkungen der Datenregionalisierung sind:

- Die Datenregionalisierung gilt für kundeneigene Konfigurationsdaten im Ruhezustand und Benutzerzugriffsanfragen für Anwendungsdaten. Andere Datentypen (wie Telemetrie- oder Übertragungsdaten) sind möglicherweise nicht auf die ausgewählte Region beschränkt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Es gibt Abhängigkeiten von anderen Citrix Cloud-Diensten, die global betrieben werden und möglicherweise nicht denselben regionalen Grenzen folgen.
- Dies ist eine einmalige Konfiguration während des Onboardings und kann später nicht geändert werden.
- Die Funktion ist nur für Neukunden verfügbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App-Konfiguration und -Verwaltung

Citrix Secure Private Access bietet eine benutzerfreundliche, zentralisierte Plattform zur Konfiguration und Verwaltung des Zugriffs auf eine Vielzahl von Anwendungen (SaaS/Web und TCP/UDP). Die Secure Private Access-Konsole vereinfacht die Administration, indem sie einen zentralen Kontrollpunkt für verschiedene Konfigurationsaufgaben bietet. Mithilfe des Konfigurationsassistenten können Administratoren auf einfache Weise die adaptive Authentifizierung einrichten, Anwendungen konfigurieren, Zugriffsrichtlinien zur Steuerung von Benutzerberechtigungen definieren und Sicherheitsbeschränkungen zum Schutz sensibler Daten implementieren – alles innerhalb derselben Konsole. Darüber hinaus unterstützt Secure Private Access den agentenlosen Zugriff auf Unternehmens-Web-Apps, ohne dass ein VPN-Client installiert werden muss.

Weitere Informationen finden Sie in den folgenden Themen:

- Unterstützung für Unternehmens-Web-Apps
- Agentenloser Zugriff auf Unternehmens-Web-Apps
- Unterstützung für Software-as-a-Service-Apps
- Unterstützung für Client-Server-Apps
- Unterstützung für Server-zu-Client-Verbindungen
- Citrix Secure Access-Client
- Best Practices für Web- und SaaS-Anwendungskonfigurationen
- App-Zugriff für Endbenutzer – Erläutert

Unternehmens-Web-Apps konfigurieren

Die Bereitstellung von Web-Apps über den Secure Private Access-Dienst ermöglicht die Remote-Bereitstellung unternehmensspezifischer Anwendungen als webbasierter Dienst. Häufig verwendete Web-Apps sind SharePoint, Confluence, OneBug und so weiter.

Sie können den Secure Private Access-Dienst in Citrix® StoreFront Cloud integrieren. Benutzer greifen über einen Webbrowser oder die Citrix Workspace™-App auf ihren Cloud Store zu. Der

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Store bietet eine einheitliche Benutzererfahrung für die konfigurierten SaaS-Apps, konfigurierten virtuellen Apps oder andere Ressourcen.

Systemanforderungen

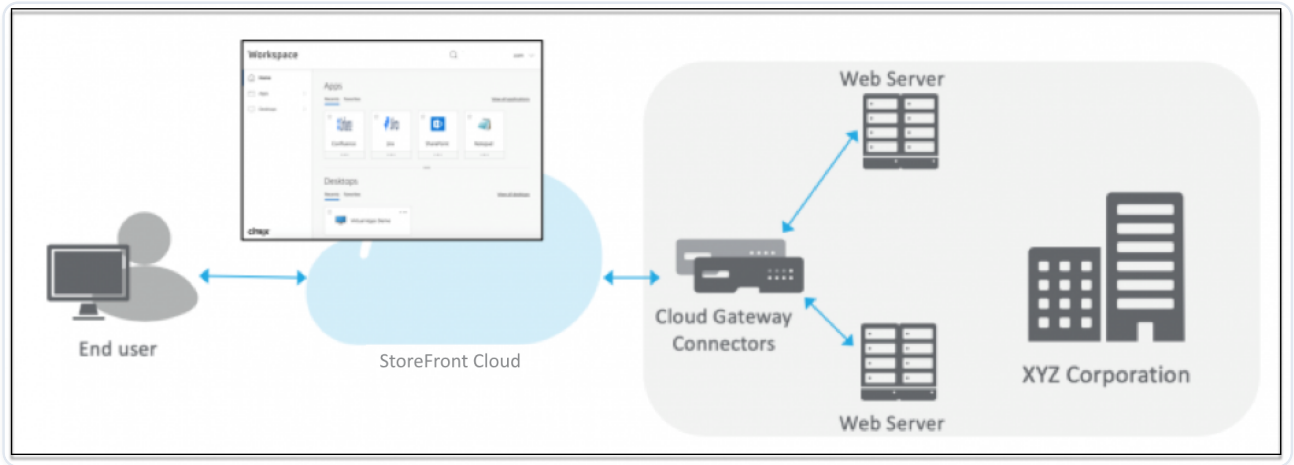
Connector Appliance – Verwenden Sie die Connector Appliance mit dem Citrix Secure Private Access-Dienst, um VPN-losen Zugriff auf die Unternehmens-Web-Apps im Rechenzentrum des Kunden zu unterstützen. Weitere Informationen finden Sie unter Connector Appliance für Secure Private Access.

Funktionsweise

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

Eine TLS-Verbindung zwischen der Connector Appliance und dem Citrix Secure Private Access-Dienst in der Cloud sichert die lokalen Anwendungen, die in den Cloud-Dienst aufgenommen werden. Webanwendungen werden über ihren Store mit einer VPN-losen Verbindung aufgerufen und bereitgestellt.

Die folgende Abbildung zeigt den Zugriff auf Webanwendungen aus ihrem Store über StoreFront Cloud.

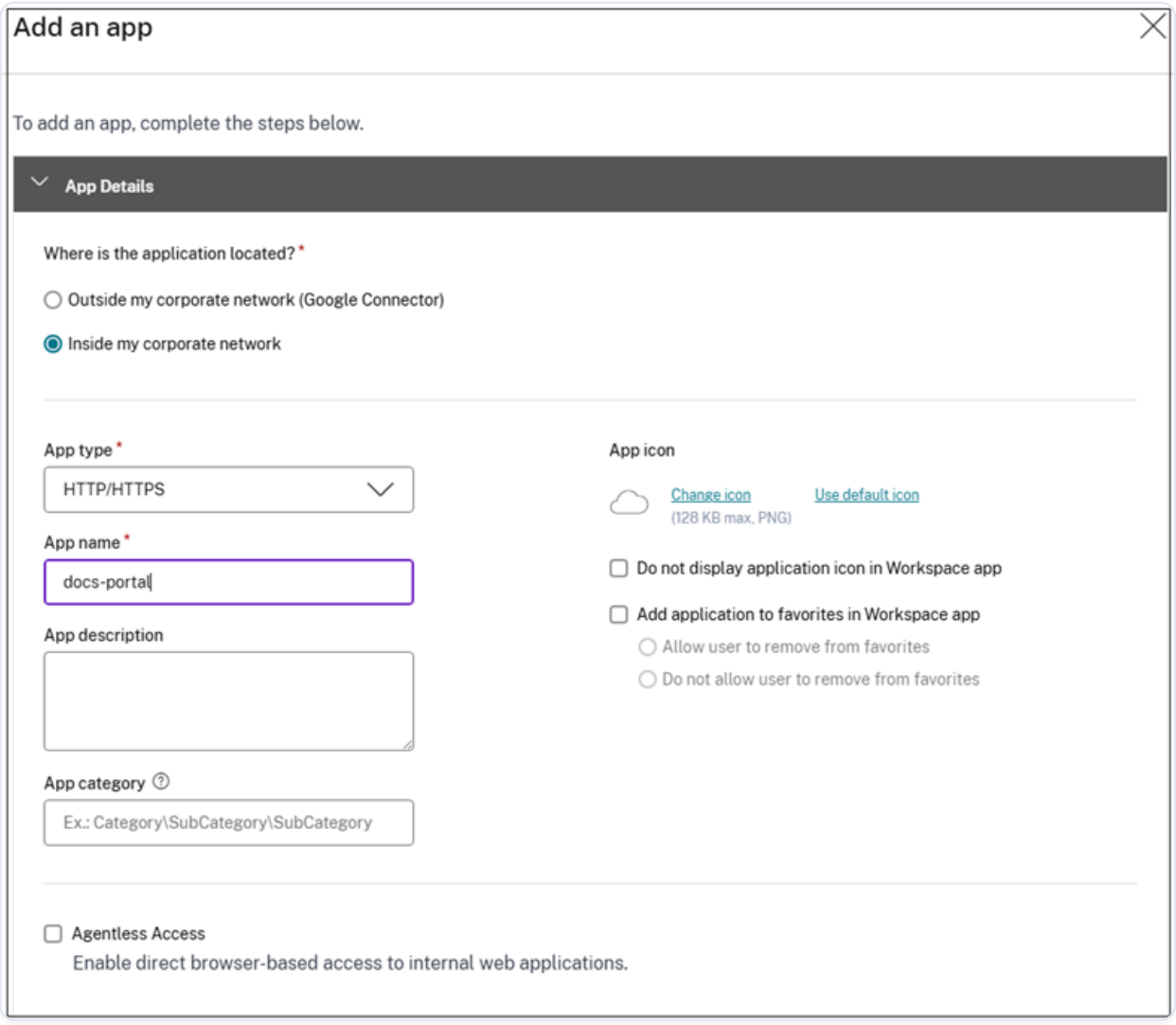


Eine Web-App konfigurieren

1. Melden Sie sich bei Citrix Cloud an und wählen Sie **Secure Private Access** aus.
2. Klicken Sie auf **Applications > App Configuration** und dann auf **Add an app**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie im Abschnitt **Choose a template** auf **Skip**. Vorlagen sind nur für SaaS-Apps verfügbar.
4. Wählen Sie unter **Where is the application location?** die Option **Inside my corporate network** aus.
    - Wählen Sie **Innerhalb meines Unternehmensnetzwerks** für Anwendungen, die innerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden, hinter Firewalls und nur über eine interne Netzwerkverbindung zugänglich sind.
    - Wählen Sie **Außerhalb meines Unternehmensnetzwerks (Google Connector):** Für Anwendungen, die außerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden. Die Datenverkehrsführung erfolgt direkt von den Benutzern zur externen Anwendung über den Google Cloud Connector.
5. Geben Sie die folgenden Details im Abschnitt **App-Details** ein und klicken Sie auf **Weiter.**



- **App-Typ** – Wählen Sie den App-Typ aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Für Chrome Enterprise Premium (CEP) werden nur HTTPS-Unternehmens-Web- und SaaS-Apps unterstützt. HTTP-Unternehmens-Web- und SaaS-Apps werden nicht unterstützt.

- **App-Name** – Name der Anwendung.
- **App-Beschreibung** – Eine kurze Beschreibung der App. Diese Beschreibung wird Ihren Benutzern im Store angezeigt.
- **App-Kategorie** – Fügen Sie die Kategorie und den Unterkategorienamen (falls zutreffend) hinzu, unter dem die von Ihnen veröffentlichte App in der Store-Benutzeroberfläche erscheinen soll. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien aus der Store-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angeben, wird die App in der Store-Benutzeroberfläche unter der spezifischen Kategorie angezeigt.
  - Die Kategorien/Unterkategorien sind vom Administrator konfigurierbar, und Administratoren können für jede App eine neue Kategorie hinzufügen.
  - Das Feld **App-Kategorie** ist für HTTP/HTTPS-Apps anwendbar und für TCP/UDP-Apps ausgeblendet.
  - Die Namen der Kategorien/Unterkategorien müssen durch einen Backslash getrennt werden. Zum Beispiel: **Business And Productivity\Engineering**. Außerdem ist dieses Feld Groß-/Kleinschreibung-sensitiv. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn es eine Diskrepanz zwischen dem Namen in der Store-Benutzeroberfläche und dem im Feld **App-Kategorie** eingegebenen Kategorienamen gibt, wird die Kategorie als neue Kategorie aufgeführt.

    Wenn Sie beispielsweise die Kategorie **Business and Productivity** im Feld **App-Kategorie** fälschlicherweise als **Business And productivity** eingeben, wird zusätzlich zur Kategorie **Business And Productivity** eine neue Kategorie namens **Business and productivity** in der Store-Benutzeroberfläche aufgeführt.
- **App-Symbol** – Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Symbol-Dateigröße 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.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie **Agentless Access**, damit Benutzer direkt über einen Client-Browser auf die App zugreifen können. Weitere Informationen finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.
- **URL** – URL mit Ihrer Kunden-ID. Die URL muss Ihre Kunden-ID (Citrix Cloud™ Kunden-ID) enthalten. Informationen zum Abrufen Ihrer Kunden-ID finden Sie unter 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.

  Wenn Sie beispielsweise eine Salesforce-App hinzufügen, lautet 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 verwandte Domäne wird automatisch basierend auf der von Ihnen angegebenen URL ausgefüllt. Die verwandte Domäne hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domäne hinzufügen.

  HINWEIS:

  Eine Warnmeldung wird angezeigt, wenn doppelte verwandte Domänen hinzugefügt werden oder wenn eine verwandte Domäne auch als URL für eine andere App hinzugefügt wird. Um diese Probleme zu vermeiden, siehe Best Practices für Web- und SaaS-Anwendungskonfigurationen.
- **HAR importieren** – Sie können eine HAR-Datei hochladen, um die Domänen, auf die eine Anwendung zugreift, automatisch zu ermitteln. Überprüfen Sie die ermittelten Domänen und wählen Sie diejenigen aus, die Sie der Konfiguration der verwandten Domänen der Anwendung hinzufügen möchten. Dies vereinfacht das Onboarding von Anwendungen, da die manuelle Identifizierung und Konfiguration verwandter Domänen reduziert wird. Weitere Informationen finden Sie unter Verwandte Domänen mithilfe einer HAR-Datei ermitteln.
- **Konsistente Verbindung aufrechterhalten** – Aktivieren Sie dieses Kontrollkästchen, um eine konsistente Verbindung zur selben Connector Appliance zu ermöglichen. Weitere

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen zu konsistenten Verbindungen finden Sie unter Konsistente Verbindung aufrechterhalten.

HINWEIS:

Wenn die Option **Konsistente Verbindung aufrechterhalten** ausgewählt ist, muss der Routing-Typ für die Anwendung im Abschnitt „App-Konnektivität“ auf **Intern über Connector** eingestellt sein.

- Klicken Sie auf **Anwendung zu Favoriten-Workspace-App hinzufügen**, um diese App als Favoriten-App in der Citrix Workspace-App hinzuzufügen.
  - Klicken Sie auf **Benutzer das Entfernen aus Favoriten erlauben**, damit App-Abonnenten die App aus der Favoritenliste in der Citrix Workspace-App entfernen können. Wenn Sie diese Option auswählen, wird ein gelbes Sternsymbol in der oberen linken Ecke der App in der Citrix Workspace-App angezeigt.
  - Klicken Sie auf **Benutzer darf nicht aus Favoriten entfernen**, um Abonnenten daran zu hindern, die App aus der Favoritenliste in der Citrix Workspace-App zu 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.

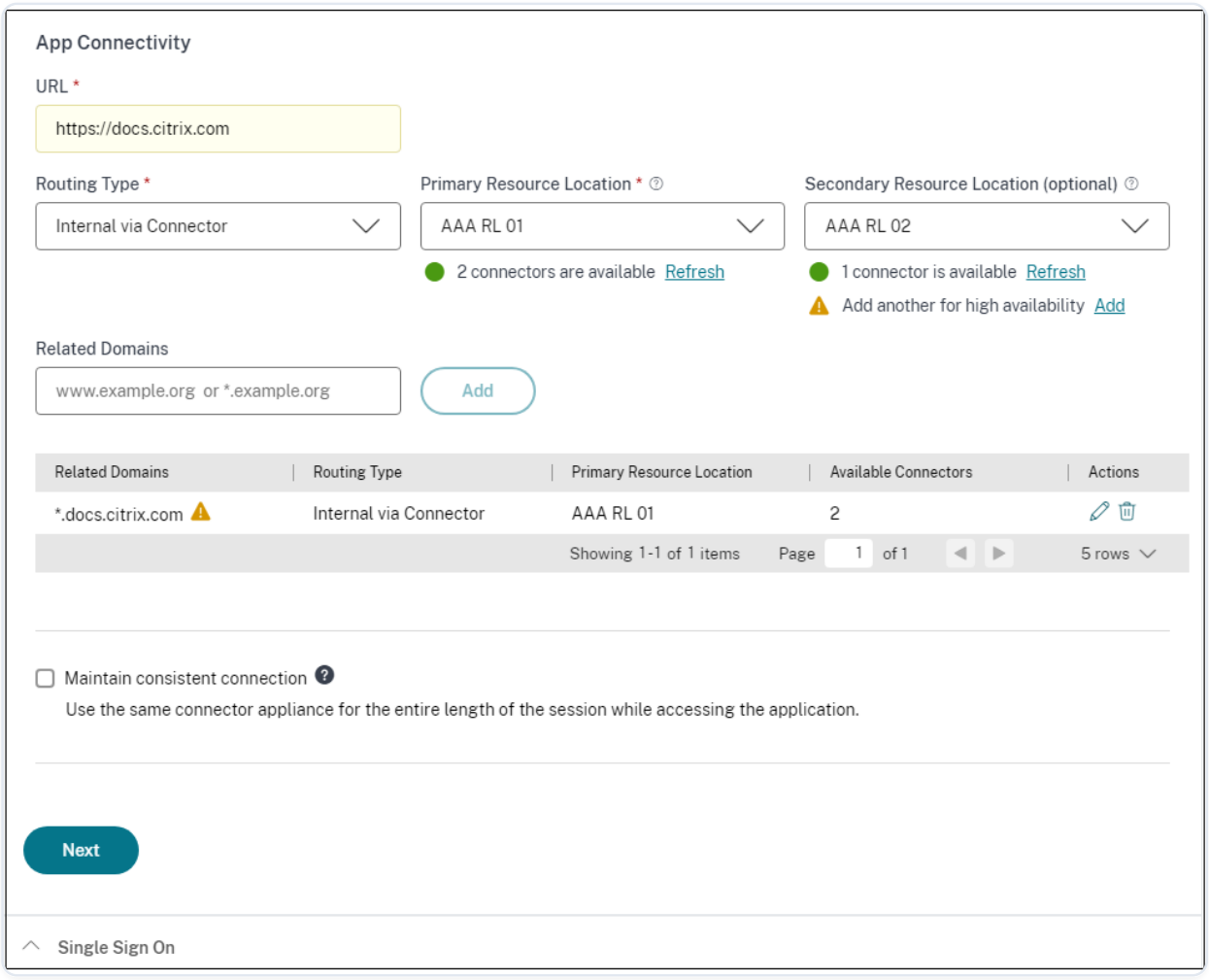
    Wenn Sie die als Favoriten markierten Apps aus der Secure Private Access-Dienstkonsole entfernen, müssen Benutzer die App manuell aus der Favoritenliste in ihrem Store entfernen. Die Apps werden nicht automatisch aus dem Store gelöscht, wenn sie aus der Secure Private Access-Dienstkonsole entfernt werden.

WICHTIG:

- Um den Zero-Trust-basierten Zugriff auf die Apps zu ermöglichen, wird der Zugriff auf Apps standardmäßig verweigert. Der Zugriff auf die Apps wird nur aktiviert, wenn eine Zugriffsrichtlinie mit der Anwendung verknüpft ist.
- Wenn mehrere Apps mit demselben FQDN oder einer Variation des Wildcard-FQDN konfiguriert sind, kann dies zu einer widersprüchlichen Konfiguration führen.
- Diese Probleme können durch Befolgen einiger Best Practices gelöst werden. Weitere Informationen finden Sie unter Best Practices für Web- und SaaS-Anwendungskonfigurationen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die zugehörigen Anwendungsdomänen, wenn die Domänen extern oder intern über die Citrix Connector™ Appliance geroutet werden müssen.



- **Routingtyp** – Wählen Sie eine der folgenden Optionen aus:
  - **Intern – Proxy umgehen** – Der Domänenverkehr wird über die Connector Appliance™ geleitet, wobei der auf der Connector Appliance konfigurierte Webproxy des Kunden umgangen wird.
  - **Intern über Connector** – Die Apps können extern sein, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
  - **Extern** – Der Datenverkehr fließt direkt ins Internet.
- **Primäre und sekundäre Ressourcenstandorte** – Administratoren können die Hochverfügbarkeit von Anwendungen auch bei Störungen sicherstellen, indem sie einen sekundären Ressourcenstandort konfigurieren oder die Option **Erster verfügbarer** verwenden.

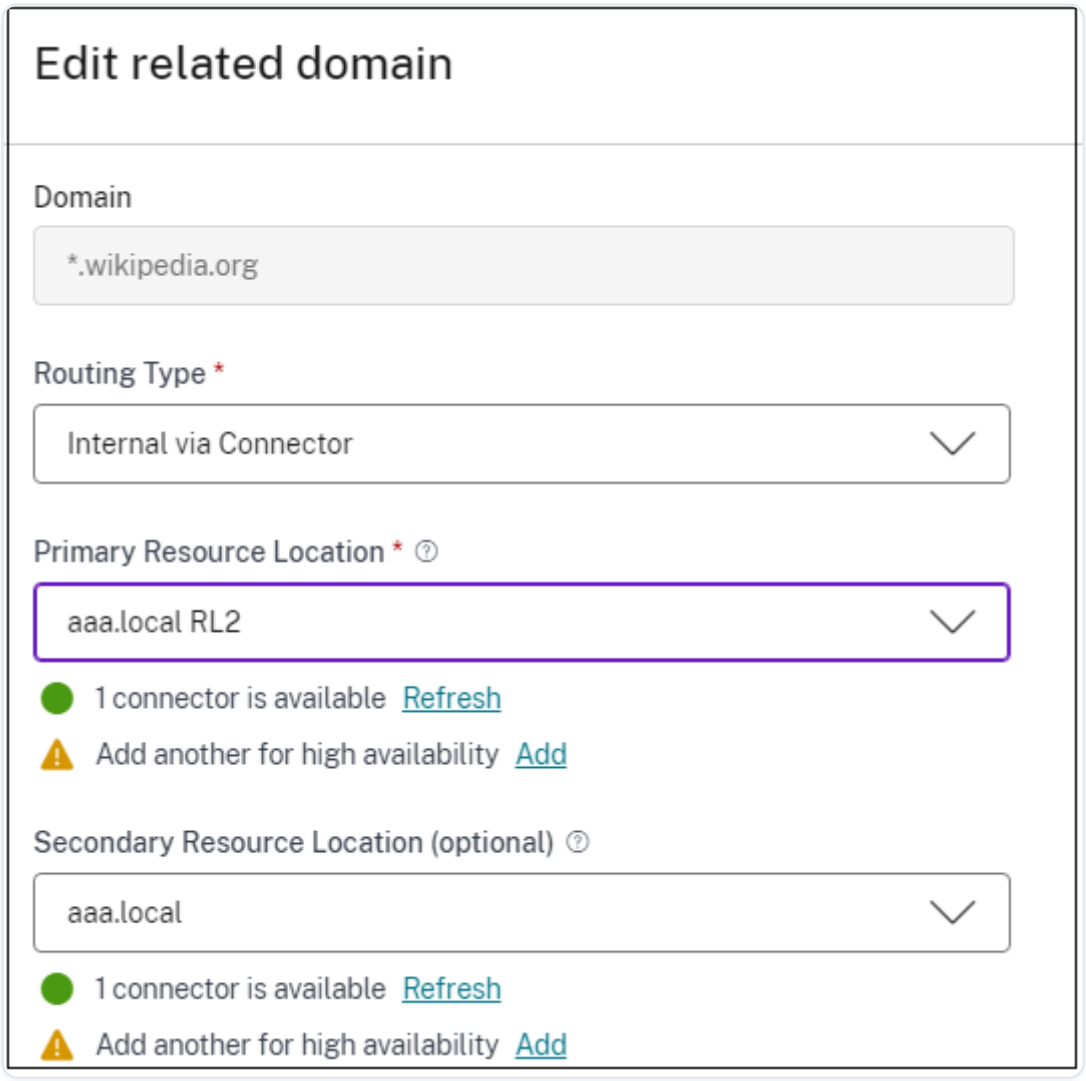
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Primärer Ressourcenstandort:** Wählen Sie den primären Ressourcenstandort aus, an dem die Anwendung gehostet wird. Alternativ können Administratoren die Option **Erster verfügbarer** unter **Primärer Ressourcenstandort** auswählen.
- **Erster verfügbarer:** Die Option **Erster verfügbarer** stellt sicher, dass ein funktionierender Ressourcenstandort verwendet wird. Wenn **Erster verfügbarer** ausgewählt ist, leitet das System den Datenverkehr automatisch an den ersten verfügbaren Standort weiter. Dies gewährleistet einen kontinuierlichen Anwendungszugriff ohne manuelles Eingreifen. Wenn beispielsweise ResourceLocation1 nicht verfügbar ist, ResourceLocation2 aber erreichbar ist, wird ResourceLocation2 standardmäßig ausgewählt, um die Anwendung bereitzustellen.
- **Sekundärer Ressourcenstandort** – Die Option **Sekundärer Ressourcenstandort** wird nur verfügbar, wenn ein primärer Ressourcenstandort explizit angegeben ist. Wenn der primäre Ressourcenstandort aus Gründen wie einem Ausfall der Connector Appliance oder des Rechenzentrums nicht verfügbar ist, wechselt die Anwendung zum angegebenen sekundären Ressourcenstandort. Der sekundäre Ressourcenstandort kann auch als Failover fungieren, selbst wenn die Anwendung in einem anderen Rechenzentrum gehostet wird.

Sie können auch einen primären und sekundären Ressourcenstandort festlegen oder die Option **Erster verfügbarer** für jede der zugehörigen Domänen auswählen.

a. Klicken Sie auf das Bearbeitungssymbol in der Spalte **Aktionen** der Tabelle „Zugehörige Domänen“.
b. Legen Sie den primären und sekundären Ressourcenstandort fest oder wählen Sie die Option **Erster verfügbarer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

- Das Festlegen des Backup-Ressourcenstandorts und die Verwendung der Funktion **Erster verfügbarer** Option befinden sich derzeit in der Vorschau.
- Wenn Sie eine Anwendung löschen, werden ihre Routing-Einträge automatisch entfernt. Weitere Informationen finden Sie unter Automatische Bereinigung von Routing-Einträgen beim Löschen von Anwendungen.

- **Konsistente Verbindung beibehalten** – Aktivieren Sie dieses Kontrollkästchen, um eine konsistente Verbindung zur selben Connector Appliance zu ermöglichen. Details zu konsistenten Verbindungen finden Sie unter Konsistente Verbindungen beibehalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

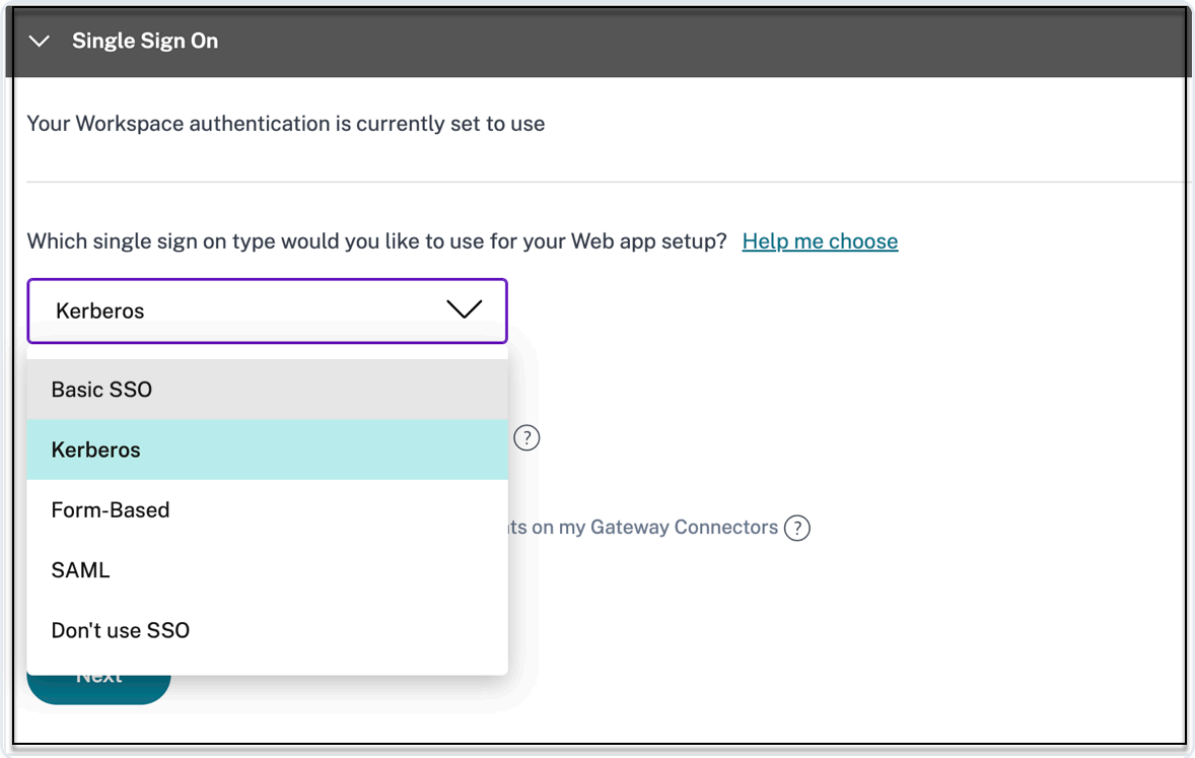
Wenn die Option **Konsistente Verbindung beibehalten** ausgewählt ist, muss der Routing-Typ für die Anwendung im Abschnitt „App-Konnektivität“ auf **Intern über Connector** eingestellt sein.

7. Legen Sie die bevorzugte Anmeldemethode fest.

HINWEIS:

Die Single Sign-On-Option ist für Citrix Secure Access mit Chrome Enterprise (CEP) nicht anwendbar.

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



- **Basic** – Wenn Ihr Back-End-Server Ihnen eine Basic-401-Challenge präsentiert, wählen Sie **Basic SSO**. Sie müssen keine Konfigurationsdetails für den **Basic** SSO-Typ angeben.

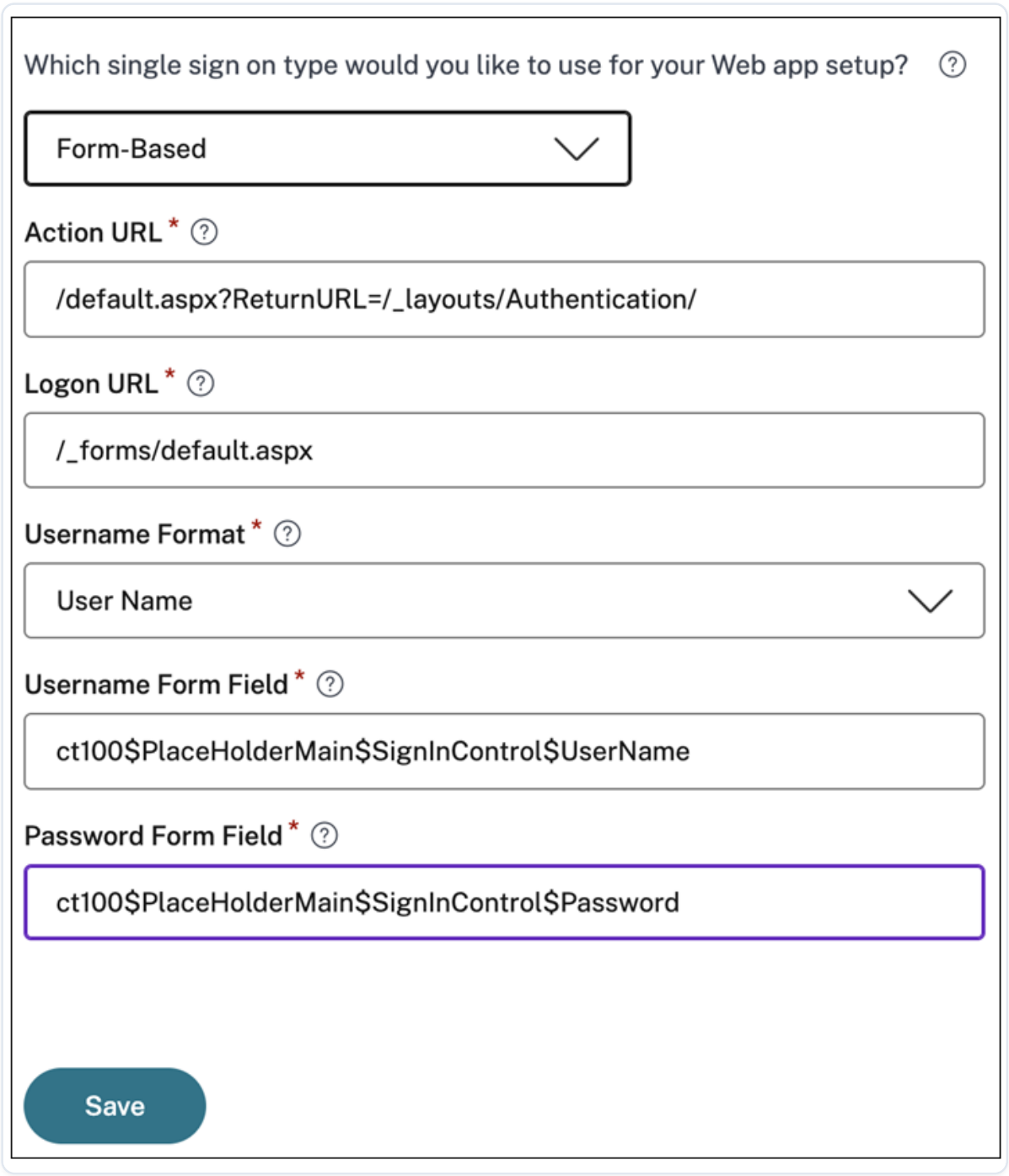
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Kerberos** – Wenn Ihr Back-End-Server Ihnen die Negotiate-401-Challenge präsentiert, wählen Sie **Kerberos**. Sie müssen keine Konfigurationsdetails für den **Kerberos** SSO-Typ angeben.
- **Form-Based** – Wenn Ihr Back-End-Server Ihnen ein HTML-Formular zur Authentifizierung präsentiert, wählen Sie **Form-Based**. Geben Sie die Konfigurationsdetails für den **Form-Based** SSO-Typ ein.
- **SAML** – Wählen Sie **SAML** für SAML-basiertes SSO in Webanwendungen. Geben Sie die Konfigurationsdetails für den **SAML** SSO-Typ ein.
- **Don't use SSO** – Verwenden Sie die Option **Don't use SSO**, wenn Sie einen Benutzer auf dem Back-End-Server nicht authentifizieren müssen. Wenn die Option **Don’t use SSO** ausgewählt ist, wird der Benutzer zu der unter dem Abschnitt **App-Details** konfigurierten URL weitergeleitet.

Formularbasierte Details:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

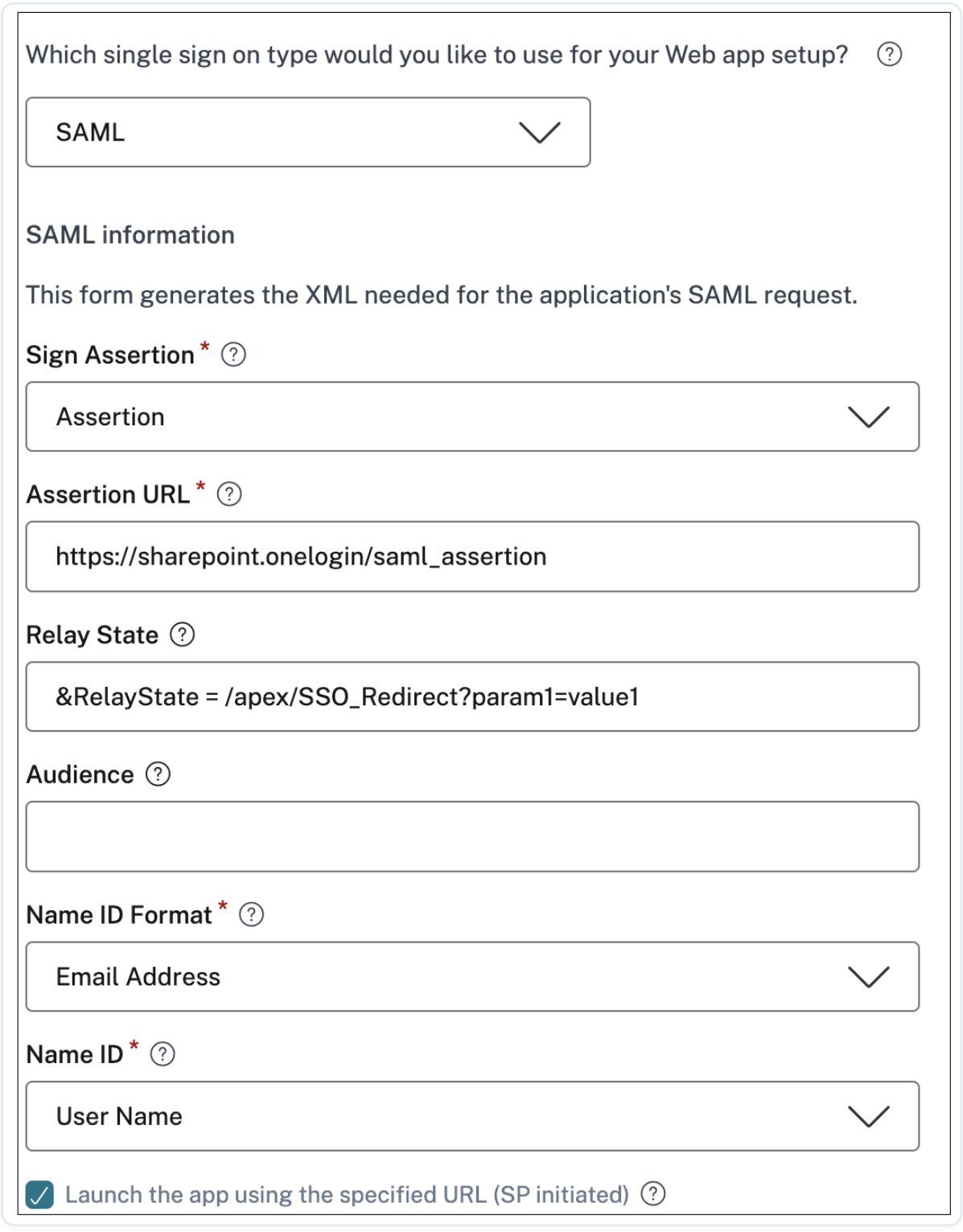


- **Aktions-URL** – Geben Sie die URL ein, an die das ausgefüllte Formular übermittelt wird.
- **Anmeldeformular-URL** – Geben Sie die URL ein, unter der das Anmeldeformular angezeigt wird.
- **Benutzername-Format** – Wählen Sie ein Format für den Benutzernamen aus.
- **Benutzername-Formularfeld** – Geben Sie ein Benutzername-Attribut ein.
- **Passwort-Formularfeld** – Geben Sie ein Passwort-Attribut ein.

SAML:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie die folgenden Details im Anmeldeabschnitt ein und klicken Sie auf **Speichern.**



- **Assertion signieren** – Das Signieren der Assertion oder Antwort gewährleistet die Nachrichtenintegrität, wenn die Antwort oder Assertion an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Antwort, Beide** oder **Keine** auswählen.
- **Assertions-URL** – Die Assertions-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Relay-Status** – Der Relay-Status-Parameter wird verwendet, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und an den Verbundserver der vertrauenden Partei weitergeleitet wurden. Der Relay-Status generiert eine einzige 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.
- **Name-ID-Format** – Wählen Sie das unterstützte Name-ID-Format aus.
- **Name-ID** – Wählen Sie die unterstützte Name-ID aus.

i. Fügen Sie unter **Erweiterte Attribute (optional)** zusätzliche Informationen über den Benutzer hinzu, die zur Zugriffssteuerung an die Anwendung gesendet werden.

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

- Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL bei der Konfiguration von SSO auf dem SaaS-Anwendungsserver verwenden.
- Sie können das Zertifikat auch aus der Liste **Zertifikat** herunterladen und das Zertifikat bei der Konfiguration von SSO auf dem SaaS-Anwendungsserver verwenden.

8. Klicken Sie auf **Speichern** und klicken Sie dann auf **Fertig stellen.**

Nachdem Sie auf **Fertig stellen** geklickt haben, wird die App der 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 Schaltfläche mit den Auslassungspunkten bei einer App und wählen Sie die entsprechenden Aktionen aus.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Um 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 Zugriffsrichtlinien erstellen.

Automatische Bereinigung von Routing-Einträgen beim Löschen von Anwendungen

Wenn Sie eine Anwendung konfigurieren, werden ihre Ziele (FQDNs oder Anwendungsdomänen) zur Routing-Tabelle hinzugefügt, die Secure Private Access für Routing-Entscheidungen verwendet. Wenn Sie eine Anwendung löschen, bereinigt Secure Private Access die Routing-Einträge basierend auf den folgenden Regeln:

- **Nicht referenzierte Einträge werden entfernt** – Wenn ein Routing-Eintrag (FQDN oder Anwendungsdomäne), der der gelöschten Anwendung zugeordnet ist, von keiner anderen Anwendung referenziert wird, entfernt Secure Private Access ihn automatisch aus der Routing-Tabelle.
- **Freigegebene Einträge bleiben erhalten** – Wenn ein Routing-Eintrag von mehr als einer Anwendung verwendet wird, wird der freigegebene Eintrag beim Löschen einer dieser Anwendungen nicht entfernt. Der Eintrag bleibt so lange in der Routing-Tabelle, wie mindestens eine aktive Anwendung darauf verweist.
- **Keine rückwirkende Entfernung** – Routing-Einträge werden nur im Rahmen einer Anwendungs-Löschung ausgewertet und entfernt. Bestehende Einträge werden nicht rückwirkend entfernt, es sei denn, es wird bestätigt, dass sie von keiner Anwendung verwendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die Bereinigung erfolgt automatisch, wenn eine Anwendung von der Seite „Anwendungen“ (über das Ellipsen-Menü (...)) gelöscht wird. Es ist keine Administratoraktion erforderlich.
- Da freigegebene Routing-Einträge erhalten bleiben, unterbricht das Löschen einer Anwendung den Zugriff auf andere Anwendungen, die dasselbe Ziel gemeinsam nutzen, nicht.

SaaS-Apps konfigurieren

Software as a Service (SaaS) ist ein Softwareverteilungsmodell, das Software remote als webbasierten Dienst bereitstellt. Häufig verwendete SaaS-Apps sind Salesforce, Workday, Concur, GoToMeeting und so weiter.

Sie können den Secure Private Access-Dienst in Citrix® StoreFront Cloud integrieren. Benutzer greifen über einen Webbrowser oder die Citrix Workspace™-App auf ihren Cloud Store zu. Der Store bietet eine einheitliche Benutzererfahrung für die konfigurierten SaaS-Apps, konfigurierten virtuellen Apps oder andere Ressourcen. Die Bereitstellung von SaaS-Apps mit dem Secure Private Access-Dienst bietet Ihnen eine einfache, sichere, robuste und skalierbare Lösung zur Verwaltung der Apps.

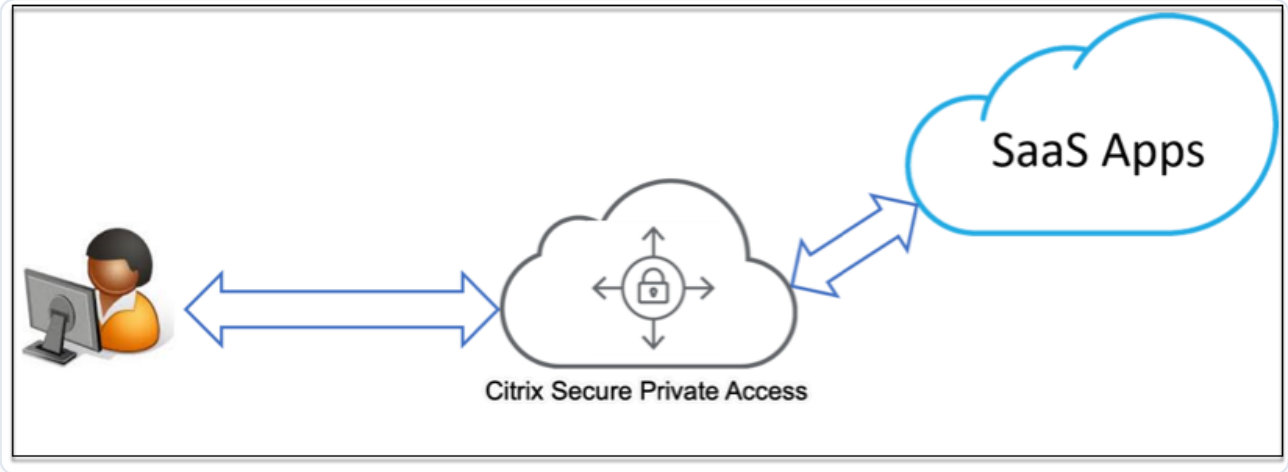
So werden SaaS-Apps mit dem Secure Private Access-Dienst unterstützt

1. Der Kundenadministrator konfiguriert SaaS-Apps über die Benutzeroberfläche des Secure Private Access-Dienstes.
2. Der Administrator stellt den Endbenutzern die Store-URL zur Verfügung.
3. Um die App zu starten, klickt ein Benutzer auf das aufgezählte SaaS-App-Symbol.
4. Die SaaS-App vertraut der vom Secure Private Access-Dienst bereitgestellten SAML-Assertion, und die App wird gestartet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Um Benutzern den Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.
- Konfigurierte SaaS-Apps werden zusammen mit virtuellen Apps und anderen Ressourcen im Store für eine einheitliche Benutzererfahrung aggregiert.



Eine SaaS-App konfigurieren

1. Melden Sie sich bei Citrix Cloud an und wählen Sie **Secure Private Access** aus.
2. Klicken Sie auf **Applications > App Configuration** und dann auf **Add an app**.

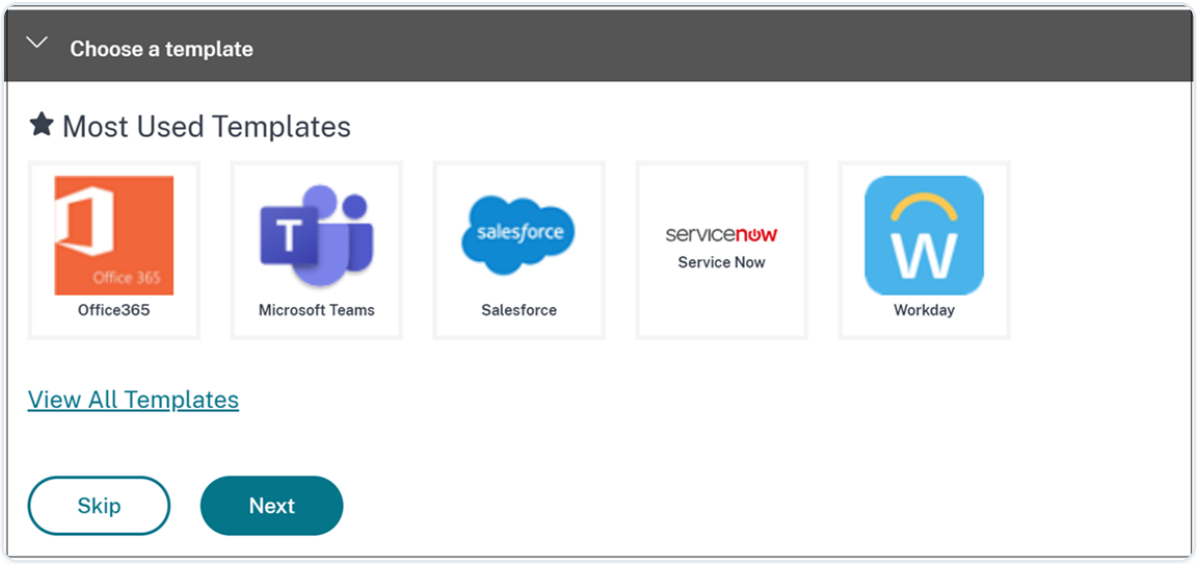
   HINWEIS:

   Sie können eine App manuell oder mithilfe einer Vorlage konfigurieren. Vorlagen füllen die meisten Anwendungseinstellungen voraus, aber Sie müssen dennoch kundenspezifische Details angeben.

   Manuelle Konfiguration: Klicken Sie im Abschnitt **Vorlage auswählen** auf **Überspringen** und konfigurieren Sie dann die Anwendung im Abschnitt **App-Details**. Beginnen Sie mit Schritt 3.
   Vorlagenbasierte Konfiguration: Klicken Sie auf **Vorlage auswählen**, wählen Sie eine Vorlage aus und klicken Sie auf **Weiter**. Überprüfen und aktualisieren Sie die App-Details nach Bedarf.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die App-Konfigurationsseite hebt die fünf am häufigsten verwendeten Vorlagen hervor, um das App-Onboarding zu vereinfachen und zu beschleunigen.
- Wählen Sie **Vorlagen anzeigen**, um Vorlagen für andere unterstützte SaaS-Apps zu durchsuchen.

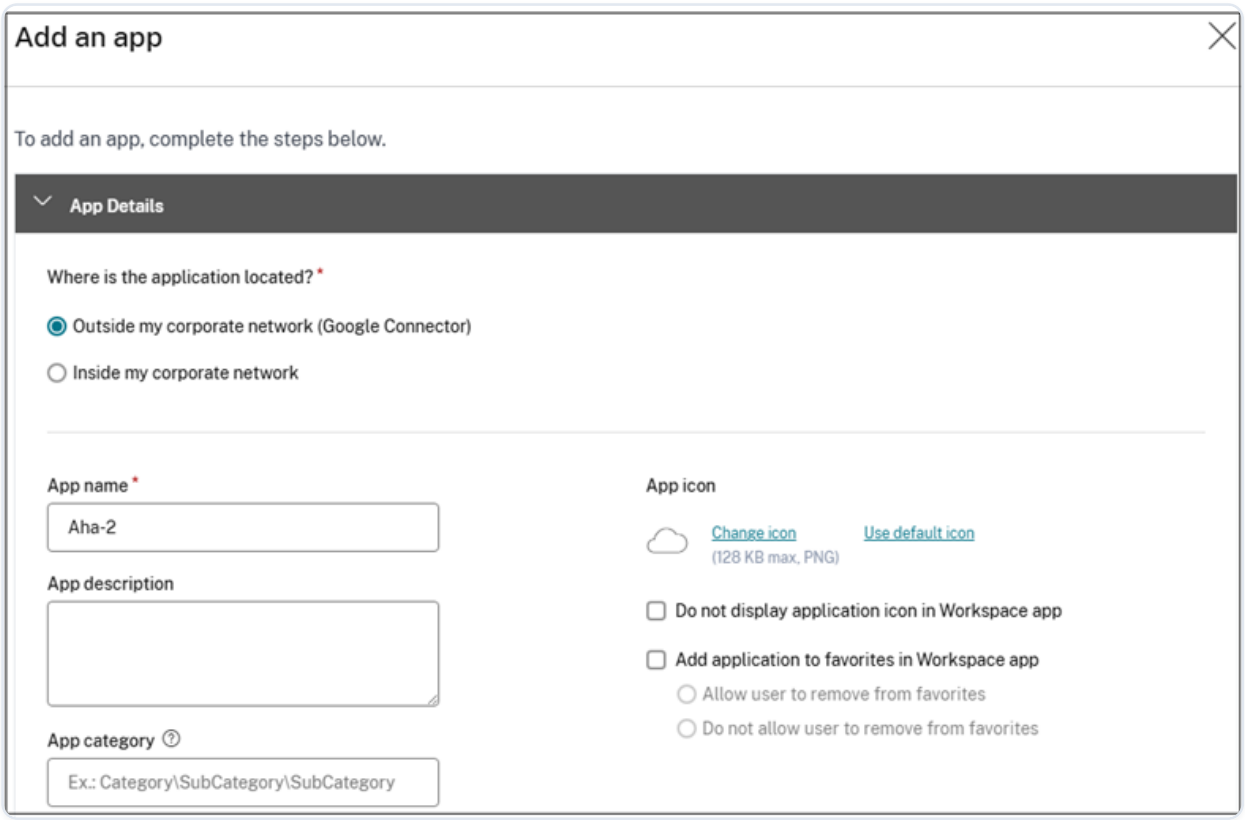


3. Wählen Sie unter **Wo befindet sich der Anwendungsstandort?** den Speicherort der Zielanwendung aus, um den Routingpfad, die Richtlinien und die Zugriffsmechanismen zu bestimmen, die angewendet werden müssen. Wählen Sie für SaaS-Apps **Außerhalb meines Unternehmensnetzwerks (Google Connector)**.

   - **Außerhalb meines Unternehmensnetzwerks (Google Connector):** Für Anwendungen, die außerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden. Die Datenverkehrsweiterleitung erfolgt direkt von Benutzern zur externen Anwendung über Citrix Cloud.
   - **Innerhalb meines Unternehmensnetzwerks**: Für Anwendungen, die innerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden, hinter Firewalls und nur über interne Netzwerkverbindungen zugänglich sind.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **App-Name** – Name der Anwendung.
- **App-Beschreibung** – Eine kurze Beschreibung der App. Diese Beschreibung wird Ihren Benutzern im Store angezeigt.
- **App-Kategorie** – Fügen Sie den Namen der Kategorie und Unterkategorie (falls zutreffend) hinzu, unter der die von Ihnen veröffentlichte App in der Store-Benutzeroberfläche angezeigt werden soll. Sie können für jede App eine neue Kategorie hinzufügen oder vorhandene Kategorien aus der Store-Benutzeroberfläche verwenden. Sobald Sie eine Kategorie für eine Web- oder SaaS-App angeben, wird die App in der Store-Benutzeroberfläche unter der spezifischen Kategorie angezeigt.
    - Die Kategorie/Unterkategorien sind vom Administrator konfigurierbar, und Administratoren können für jede App eine neue Kategorie hinzufügen.
    - Das Feld **App-Kategorie** ist für HTTP/HTTPS-Apps anwendbar und für TCP/UDP-Apps ausgeblendet.
    - Die Namen der Kategorie/Unterkategorien müssen durch einen Backslash getrennt werden. Zum Beispiel: **Business And Productivity\Engineering**. Dieses Feld ist auch Groß-/Kleinschreibung-sensitiv. Administratoren müssen sicherstellen, dass sie die richtige Kategorie definieren. Wenn es eine Diskrepanz zwischen dem Namen in der Store-Benutzeroberfläche und dem im Feld **App-Kategorie** eingegebenen Kategorienamen gibt, wird die Kategorie als neue Kategorie aufgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie beispielsweise die Kategorie **Business and Productivity** im Feld **App-Kategorie** fälschlicherweise als **Business And productivity** eingeben, wird zusätzlich zur Kategorie **Business And Productivity** eine neue Kategorie namens **Business and productivity** in der Store-Benutzeroberfläche aufgeführt.

- **App-Symbol** – Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Symbol-Dateigröße 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 Benutzern nicht anzeigen**.

- **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.

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

  Die Felder für Kundendomänenname und Kunden-ID sind spezifisch für bestimmte Apps.
- **Zugehörige Domänen** – Die zugehörige Domäne wird basierend auf der von Ihnen angegebenen URL automatisch ausgefüllt. 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.

  HINWEIS:

  Eine Warnmeldung wird angezeigt, wenn doppelte zugehörige Domänen hinzugefügt werden oder wenn eine zugehörige Domäne auch als URL für eine andere App hinzugefügt wird. Um diese Probleme zu vermeiden, lesen Sie Best Practices für Web- und SaaS-Anwendungskonfigurationen.

- **HAR importieren** – Sie können eine HAR-Datei hochladen, um die Domänen, auf die eine Anwendung zugreift, automatisch zu ermitteln. Überprüfen Sie die ermittelten Domänen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

und wählen Sie diejenigen aus, die Sie zur Konfiguration der zugehörigen Domänen der Anwendung hinzufügen möchten. Dies vereinfacht das Onboarding von Anwendungen, indem der manuelle Aufwand für die Identifizierung und Konfiguration zugehöriger Domänen reduziert wird. Weitere Informationen finden Sie unter Zugehörige Domänen mithilfe einer HAR-Datei ermitteln.

- **Konsistente Verbindung aufrechterhalten** – Eine konsistente Verbindung zum Connector Appliance wird für SaaS-Apps unterstützt. Aktivieren Sie das Kontrollkästchen **Konsistente Verbindung aufrechterhalten** und wählen Sie **Intern über Connector** als Verbindungstyp im Abschnitt **App-Konnektivität**. Details zu konsistenten Verbindungen finden Sie unter Konsistente Verbindung aufrechterhalten.
- Klicken Sie auf **Anwendung zu Favoriten in der Workspace-App 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 zu erlauben, die App aus der Favoritenliste in der Citrix Workspace-App zu entfernen. Wenn Sie diese Option auswählen, wird ein gelbes Sternsymbol oben links in der App in der Citrix Workspace-App angezeigt.
    - Klicken Sie auf **Benutzer das Entfernen aus Favoriten nicht erlauben**, um Abonnenten daran zu hindern, die App aus der Favoritenliste in der Citrix Workspace-App zu entfernen. Wenn Sie diese Option auswählen, wird ein Sternsymbol mit einem Vorhängeschloss oben links in der App in der Citrix Workspace-App angezeigt.

Wenn Sie die als Favoriten markierten Apps aus der Secure Private Access-Dienstkonsole entfernen, müssen Benutzer die Apps manuell aus der Favoritenliste in ihrem Store entfernen. Die Apps werden nicht automatisch aus dem Store gelöscht, wenn sie aus der Secure Private Access-Dienstkonsole entfernt werden.

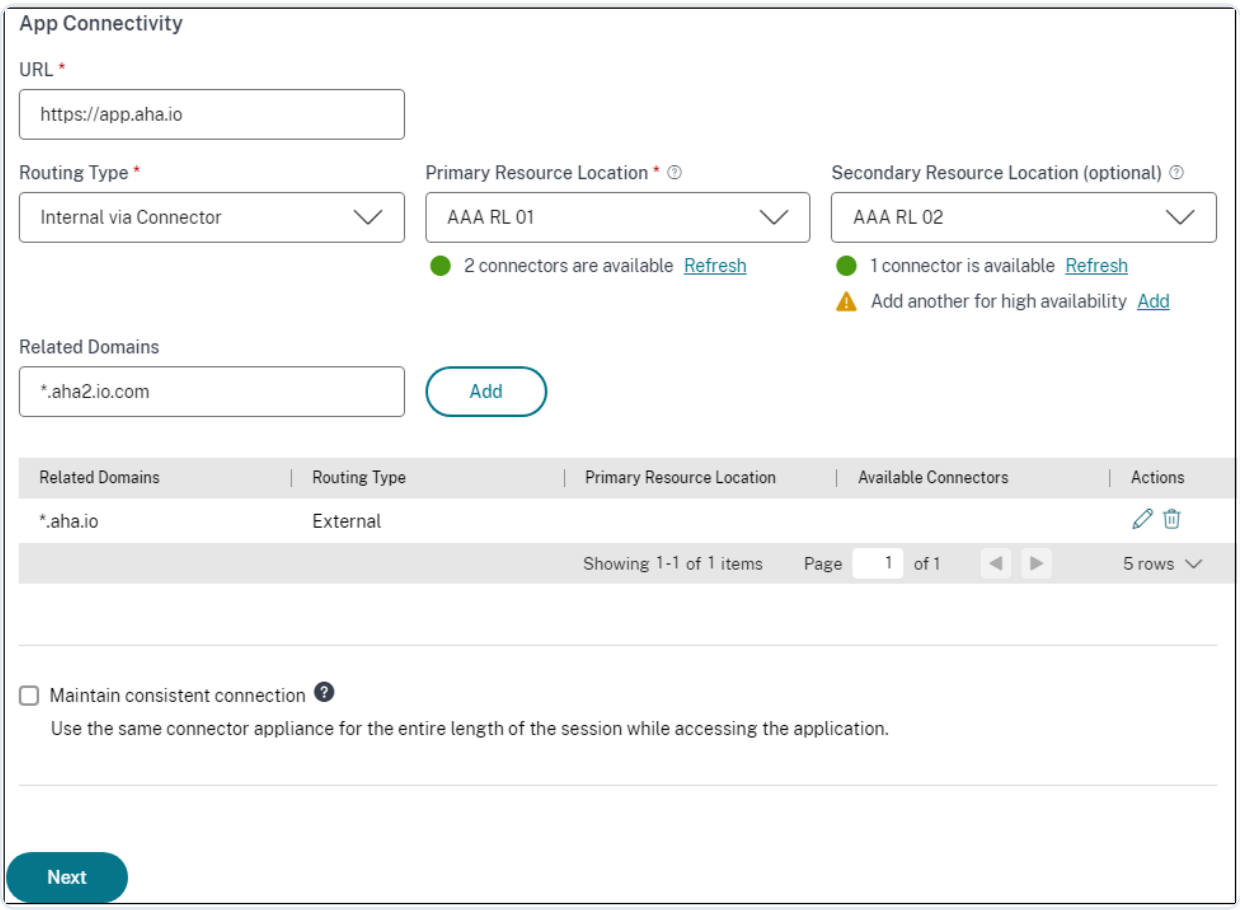
© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Der Zugriff auf eine SaaS-App wird durch ihre Zugriffsrichtlinie geregelt. Einer App wird der Zugriff gewährt, verweigert oder sie wird ungemanagt gelassen, basierend auf der Zugriffsrichtlinienregel, die dem Benutzer entspricht. Wenn keine Regel dem Benutzer entspricht oder keine Zugriffsrichtlinie mit der App verknüpft ist, wird die App nicht blockiert. Sie wird ungemanagt gelassen und der Browser verbindet sich direkt mit ihr. Um eine App für Benutzer zu blockieren, die von keiner Regel abgedeckt sind, fügen Sie eine Regel „Alle Benutzer > Zugriff verweigern“ mit der niedrigsten Priorität hinzu. Weitere Informationen finden Sie unter SaaS-Anwendungen standardmäßig blockieren.
- Wenn mehrere Apps mit demselben FQDN oder einer Variation des Wildcard-FQDN konfiguriert sind, kann dies zu einer widersprüchlichen Konfiguration führen.
- Diese Probleme können durch Befolgen einiger Best Practices gelöst werden. Einzelheiten finden Sie unter Best Practices für Web- und SaaS-Anwendungskonfigurationen.

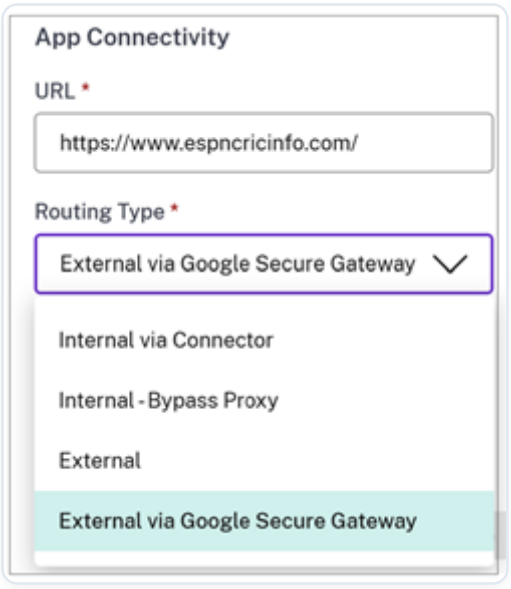
5. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die zugehörigen Anwendungsdomänen, wenn die Domänen extern oder intern über die Citrix Connector™ Appliance geroutet werden müssen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Routing-Typ** – Wählen Sie eine der folgenden Optionen aus:
  - **Intern – Proxy umgehen** – Der Domänenverkehr wird über die Connector Appliance™ geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
  - **Intern über Connector** – Die Apps können extern sein, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
  - **Extern** – Der Datenverkehr fließt direkt ins Internet.
  - **Extern über Google Secure Gateway** – Der Datenverkehr fließt über das Google Secure Gateway ins Internet. Weitere Informationen finden Sie unter Routing über Google Secure Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Primäre und sekundäre Ressourcenstandorte** – Administratoren können die Hochverfügbarkeit von Anwendungen auch bei Störungen sicherstellen, indem sie einen sekundären Ressourcenstandort konfigurieren oder die Option **Erster verfügbarer** verwenden.

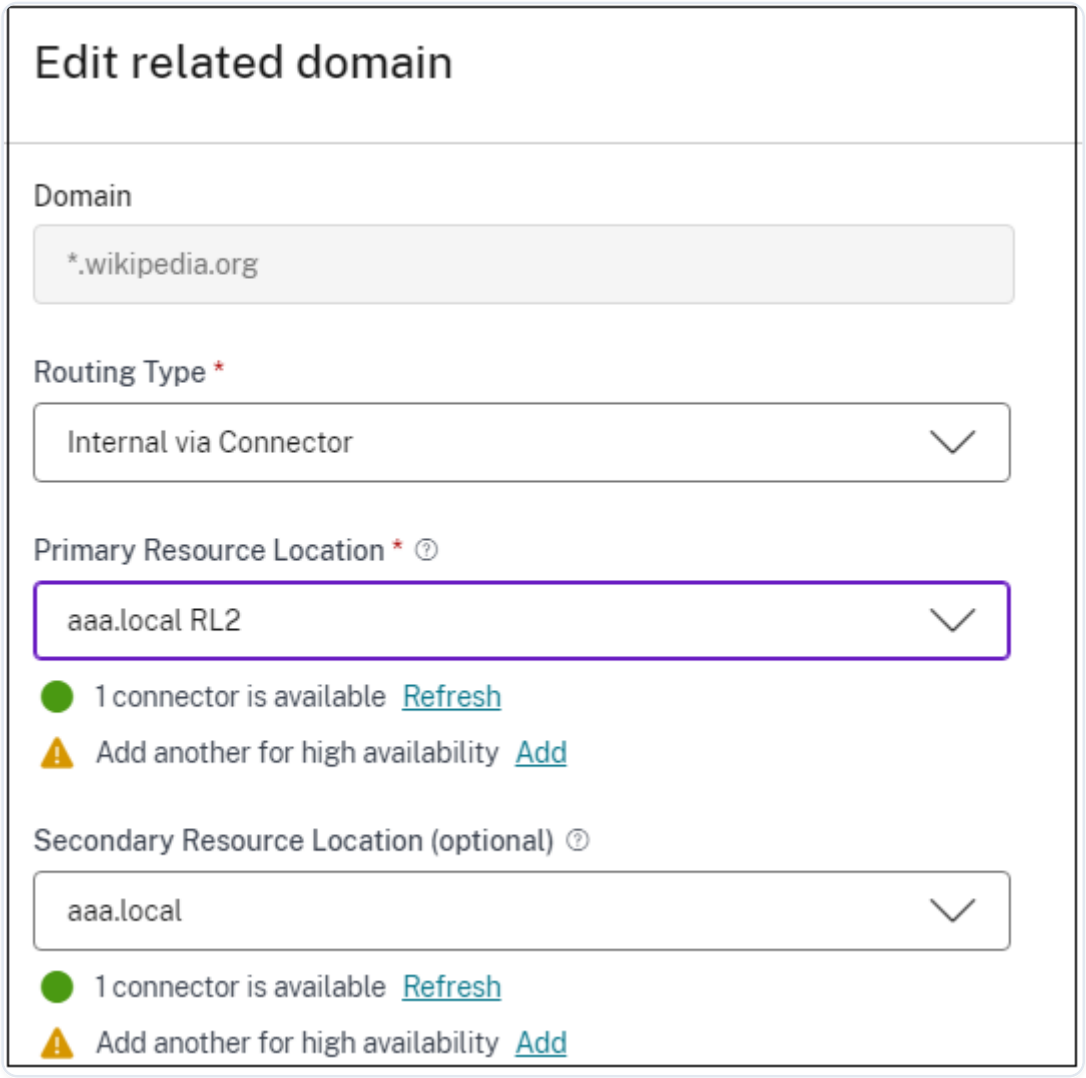
  - **Primärer Ressourcenstandort:** Wählen Sie den primären Ressourcenstandort aus, an dem die Anwendung gehostet wird. Alternativ können Administratoren die Option **Erster verfügbarer** unter **Primärer Ressourcenstandort** auswählen.
  - **Erster verfügbarer:** Die Option **Erster verfügbarer** stellt sicher, dass ein funktionierender Ressourcenstandort verwendet wird. Wenn **Erster verfügbarer** ausgewählt ist, leitet das System den Datenverkehr automatisch an den ersten verfügbaren Standort weiter. Dies gewährleistet einen kontinuierlichen Anwendungszugriff ohne manuelles Eingreifen. Wenn beispielsweise ResourceLocation1 nicht verfügbar ist, ResourceLocation2 aber erreichbar ist, wird ResourceLocation2 standardmäßig ausgewählt, um die Anwendung bereitzustellen.
  - **Sekundärer Ressourcenstandort** – Die Option **Sekundärer Ressourcenstandort** wird nur verfügbar, wenn ein primärer Ressourcenstandort explizit angegeben ist. Wenn der primäre Ressourcenstandort aus Gründen wie einem Ausfall der Connector Appliance oder des Rechenzentrums nicht verfügbar ist, wechselt die Anwendung zum angegebenen sekundären Ressourcenstandort. Der sekundäre Ressourcenstandort kann auch als Failover fungieren, selbst wenn die Anwendung in einem anderen Rechenzentrum gehostet wird.

  Sie können auch einen primären und sekundären Ressourcenstandort festlegen oder die Option **Erster verfügbarer** für jede der zugehörigen Domänen auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Klicken Sie auf das Bearbeitungssymbol in der Spalte **Aktionen** der Tabelle „Zugehörige Domänen“.

b. Legen Sie den primären und sekundären Ressourcenstandort fest oder wählen Sie die Option **Erster verfügbarer**.



HINWEIS:

- Das Festlegen des Backup-Ressourcenstandorts und die Verwendung der Option **Erster verfügbarer** befinden sich derzeit in der Vorschau.
- Wenn Sie eine Anwendung löschen, werden ihre Routing-Einträge automatisch entfernt. Weitere Informationen finden Sie unter Automatische Bereinigung von Routing-Einträgen beim Löschen von Anwendungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Konsistente Verbindung aufrechterhalten** – Aktivieren Sie dieses Kontrollkästchen, um eine konsistente Verbindung zur selben Connector Appliance zu ermöglichen. Details zu konsistenten Verbindungen finden Sie unter Konsistente Verbindungen aufrechterhalten.

  HINWEIS:

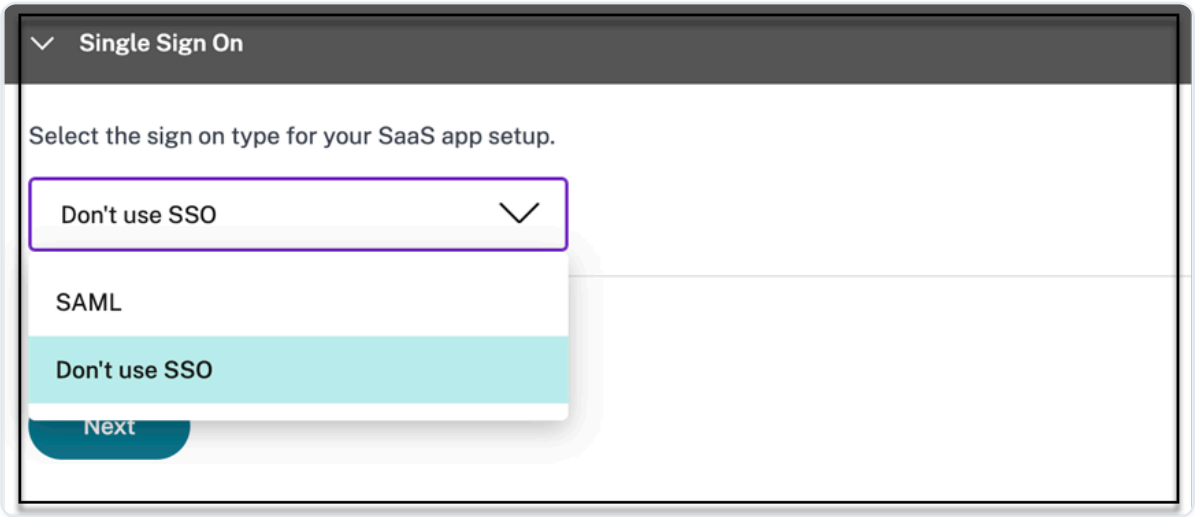
  Wenn die Option **Konsistente Verbindung aufrechterhalten** ausgewählt ist, muss der Routing-Typ für die Anwendung im Abschnitt „App-Konnektivität“ auf **Intern über Connector** festgelegt werden.

6. Legen Sie eine bevorzugte Anmeldemethode fest.

   HINWEIS:

   Die Single Sign-On-Option ist für Citrix Secure Access mit Chrome Enterprise (CEP) nicht anwendbar.

   a. Wählen Sie im Abschnitt **Single Sign-On** den bevorzugten 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 nicht auf dem Backend-Server authentifizieren müssen. Wenn die Option **SSO nicht verwenden** ausgewählt ist, wird der Benutzer zu der unter dem Abschnitt **App-Details** konfigurierten URL umgeleitet.
   - **SAML** – Wählen Sie **SAML** für SAML-basiertes SSO in Webanwendungen. Geben Sie die Konfigurationsdetails für den **SAML**-SSO-Typ ein.

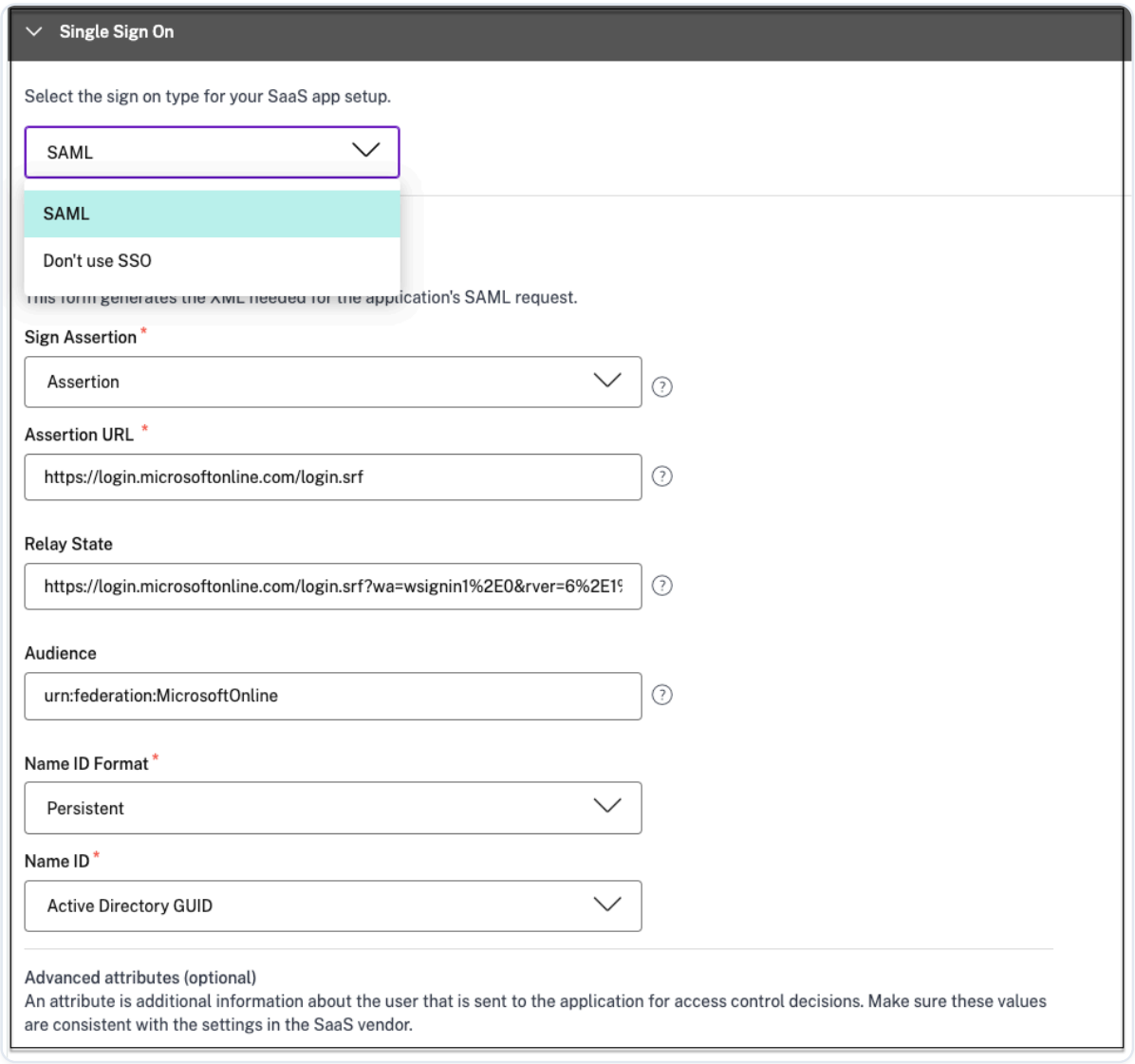
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie die folgenden Details im Abschnitt „Single Sign-On“ ein und klicken Sie auf **Speichern**.

- **Assertion signieren** – Das Signieren der Assertion oder Antwort gewährleistet die Nachrichtenintegrität, wenn die Antwort oder Assertion an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Response, Both** oder **None** auswählen.
- **Assertions-URL** – Die Assertions-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.
- **Relay State** – Der Parameter „Relay State“ wird verwendet, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und zum Föderationsserver der vertrauenden Partei weitergeleitet wurden. Relay State generiert eine einzige 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.
- **Name ID-Format** – Wählen Sie das unterstützte Name ID-Format aus.
- **Name ID** – Wählen Sie die unterstützte Name ID aus.
- Wählen Sie **App über die spezifische URL starten (SP-initiiert)**, um den vom Identitätsanbieter initiierten Fluss zu überschreiben und nur den vom Dienstanbieter initiierten Fluss zu verwenden.

b. Fügen Sie unter **Erweiterte Attribute (optional)** zusätzliche Informationen über den Benutzer hinzu, die zur Zugriffsentscheidung an die Anwendung gesendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

   - Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL bei der Konfiguration von SSO auf dem SaaS-App-Server verwenden.
   - Sie können das Zertifikat auch aus der Liste **Zertifikat** herunterladen und das Zertifikat bei der Konfiguration von SSO auf dem SaaS-App-Server verwenden.

7. Klicken Sie auf **Speichern** und dann auf **Fertig stellen.**

Nachdem Sie auf **Fertig stellen** geklickt haben, wird die App der 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 Schaltfläche mit den Auslassungspunkten bei einer App und wählen Sie die entsprechenden Aktionen aus.

- **Anwendung bearbeiten**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Löschen**

Routing über Google Secure Gateway

Wenn Sie den Routing-Typ einer SaaS-App auf **Extern über Google Secure Gateway** einstellen, wird der Datenverkehr für diese App über Google Secure Gateway ins Internet geleitet, anstatt direkt vom Client.

- Sie können diesen Routing-Typ während der App-Konfiguration festlegen, wo er zur Standardroute für diese App wird.
- Sie können ihn auch als Routing-Ausnahme in einer Zugriffsrichtlinie festlegen, wo er nur für Benutzer in dieser Richtlinie gilt und das Standard-Routing der App überschreibt.
- Dieser Routing-Typ ist nur für SaaS-Apps und nur für Kunden verfügbar, die in Google Chrome Enterprise Premium integriert sind. Er ist nicht für interne Web-Apps verfügbar.
- Im Citrix Secure Access Client verhält sich diese Option genauso wie **Extern**. Legen Sie beim Import den Wert für **Routing-Typ** auf **Extern über Google Secure Gateway** fest.

HINWEIS:

Für SaaS-Apps, auf die über Citrix Enterprise Browser™ zugegriffen wird, wird der **Routing Type** als **External via Google Secure Gateway** anstelle von **External** angezeigt. Dies ist nur ein Unterschied in der Benutzeroberfläche und ändert das Routing-Verhalten nicht. Der Datenverkehr fließt weiterhin direkt ins Internet.

Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung

Wenn Sie eine Anwendung konfigurieren, werden ihre Ziele (FQDNs oder Anwendungsdomänen) der Routing-Tabelle hinzugefügt, die Secure Private Access für Routing-Entscheidungen verwendet. Wenn Sie eine Anwendung löschen, bereinigt Secure Private Access die Routing-Einträge basierend auf den folgenden Regeln:

- **Nicht referenzierte Einträge werden entfernt** – Wenn ein Routing-Eintrag (FQDN oder Anwendungsdomäne), der mit der gelöschten Anwendung verknüpft ist, von keiner anderen Anwendung referenziert wird, entfernt Secure Private Access ihn automatisch aus der Routing-Tabelle.
- **Gemeinsame Einträge werden beibehalten** – Wenn ein Routing-Eintrag von mehr als einer Anwendung verwendet wird, entfernt das Löschen einer dieser Anwendungen den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

gemeinsamen Eintrag nicht. Der Eintrag bleibt so lange in der Routing-Tabelle, wie mindestens eine aktive Anwendung darauf verweist.

- **Keine rückwirkende Entfernung** – Routing-Einträge werden nur im Rahmen einer Anwendungs-Löschung bewertet und entfernt. Bestehende Einträge werden nicht rückwirkend entfernt, es sei denn, es wird bestätigt, dass sie von keiner Anwendung verwendet werden.

HINWEIS:

- Die Bereinigung erfolgt automatisch, wenn eine Anwendung von der Seite „Anwendungen“ (über das Ellipsen-Menü (...)) gelöscht wird. Es ist keine Administratoraktion erforderlich.
- Da gemeinsame Routing-Einträge beibehalten werden, unterbricht das Löschen einer Anwendung den Zugriff auf andere Anwendungen, die dasselbe Ziel teilen, nicht.

SaaS-App-Server-spezifische Konfiguration

Im Folgenden finden Sie Links zu Dokumenten, die Anleitungen zur App-Server-spezifischen Konfiguration mithilfe einer Vorlage enthalten. Citrix unterstützt derzeit die folgenden SaaS-Apps und erweitert die Unterstützung ständig um weitere Apps.

- 15Five – Tool für kontinuierliches Leistungsmanagement zur Mitarbeiterförderung.
- 10000 ft – Projektmanagement-Tool zur Wachstumsplanung.
- 4me – Service-Management-Tool für die Zusammenarbeit zwischen internen, externen und ausgelagerten Teams.
- Abacus - Software für Spesenabrechnungen in Echtzeit.
- Absorb - Lernmanagement-Tool.
- Accompa - Anforderungsmanagement-Tool zur Produktentwicklung.
- Adobe Captivate Prime - Lernmanagementsystem zur Bereitstellung personalisierter Lernerfahrungen auf verschiedenen Geräten.
- Aha - Produkt-Roadmap- und Marketingplanungstool zur Produktentwicklung und Kampagnenstart.
- AlertOps - Kollaboratives Tool zur Reaktion auf Vorfälle zur Verwaltung von IT-Vorfällen.
- Allocadia - Marketing-Performance-Management-Tool zur Verwaltung des Marketingplanungsprozesses einer Organisation.`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ana plan - Planungstool, das Organisationen bei der Entscheidungsfindung unterstützt, indem es Daten, Personen und Pläne verbindet.
- &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 - Versionskontroll- und Quellcodeverwaltungstool für die Softwareentwicklung.
- Automox - Patch-Management-Tool zur Verfolgung, Steuerung und Verwaltung des Patching-Prozesses.
- Azendoo - Kollaborationstool für Teams zum Kommunizieren und Zusammenarbeiten.
- BambooHR - Personalmanagement-Tool zur Verwaltung von Mitarbeiterdaten.
- Bananatag – Tool zum Verfolgen und Planen von E-Mails, Verfolgen von Dateien und Erstellen von E-Mail-Vorlagen
- Base CRM – Vertriebsmanagement-Tool zum Verwalten von E-Mails, Telefonanrufen und Notizen.
- Beekeeper – Tool zur Integration mehrerer Betriebssysteme und Kommunikationskanäle in einem sicheren Hub, der von Desktop- und Mobilgeräten aus zugänglich ist.
- BitaBIZ – Tool zur Abwesenheits- und Urlaubsplanung sowie zur Kommunikation für das Urlaubs- und Abwesenheitsmanagement.
- BlazeMeter – Testsuite.
- Blissbook – Richtlinienmanagement-Tool zum Erstellen von Mitarbeiterhandbüchern.
- BlueJeans – Videokonferenzlösung.
- Bold360 – Live-Chat-Tool für die Kundenbindung.
- Bonusly – Tool zur Mitarbeiteranerkennung und Prämienverwaltung, um Teamleistungen zu würdigen.
- Box – Content-Management- und Dateifreigabe-Tool zum Verwalten, Teilen und Zugreifen auf Ihre Inhalte.
- Branch – Eine mobile Verknüpfungsplattform, die Deep Links und mobile Anwendungen unterstützt.
- Brandfolder – Tool für digitales Asset Management zum Speichern und Teilen digitaler Assets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Breezy HR – Rekrutierungssoftware und Bewerber-Tracking-System.
- `Buddy Punch` – Zeitmanagement-Tool zur Überwachung der Mitarbeiteranwesenheit.
- Bugsnag – Überwachungstool zur Verwaltung der Anwendungsstabilität und zur Meldung von Fehlern und Diagnosedaten.
- Buildkite – Infrastruktur-Tool für die Softwareentwicklung mit kontinuierlicher Integration.
- Bullseye Locations – Filialfinder-Tool, um ein Geschäft oder einen Händler auf einem Gerät zu finden.
- CA Flowdock – Kollaborationstool für Teams zur Kommunikation und Zusammenarbeit.
- CakeHR – Personalmanagement-Tool für Anwesenheits- und Leistungsmanagement.
- Cardboard – Kollaboratives Produktplanungstool zur Verfolgung unorganisierter Informationen.
- Citrix Cedexis – Traffic-Management-Tool für große Websites, um Multi-Vendor-Sourcing von Rechenzentren, Cloud-Anbietern und Content-Delivery-Netzwerken zu nutzen.
- CipherCloud – Plattform, die End-to-End-Datenschutz und erweiterten Bedrohungsschutz sowie umfassende Compliance-Funktionen für Unternehmen bietet, die Cloud-basierte Anwendungen nutzen.
- Celoxis – Projektmanagement-Tool zum Erstellen von Projektplänen, Automatisieren von Aufgaben und zur Zusammenarbeit.
- CircleHD – Trainings-, Lern- und Kollaborationstool zum Teilen von Videos und Folien innerhalb der Organisation.
- Circonus – Datenanalyse- und Überwachungstool zur Bereitstellung von Warnungen, Diagrammen, Dashboards und Machine-Learning-Intelligenz.
- Cisco Umbrella – Cloud-Sicherheitsplattform, die die erste Verteidigungslinie gegen Bedrohungen im Internet bietet.
- ClearSlide – Vertriebs-Engagement-Tool, mit dem Benutzer Inhalte und Vertriebsmaterial für die Kundeninteraktion teilen können.
- Cloudability – Cloud-Kostenmanagement-Plattform zur Verbesserung der Transparenz, Optimierung und Governance in Cloud-Umgebungen.
- CloudAMQP – Nachrichtenwarteschlangen-Tool zum Übertragen von Nachrichten zwischen Prozessen und anderen Systemen.
- CloudCheckr – Kostenmanagement-, Sicherheits-, Berichts- und Analysetool, das Benutzern hilft, ihre AWS- und Azure-Bereitstellungen zu optimieren.
- CloudMonix – Tool zur Überwachung und Automatisierung von Cloud- und lokalen Ressourcen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CloudPassage – Tool für Transparenz und kontinuierliche Überwachung zur Reduzierung von Cyberrisiken und zur Einhaltung von Vorschriften.
- CloudRanger – Tool zur Optimierung Ihrer Backups, Notfallwiederherstellung und Serversteuerung für die AWS Cloud.
- Clubhouse – Projektmanagement-Tool für die Softwareentwicklung.
- Coggle – Webanwendung für Mindmapping zur Erstellung hierarchisch strukturierter Dokumente, wie ein verzweigter Baum.
- Comm100 – Kundenservice-Software und Kommunikationstool für Kundendienstmitarbeiter.
- Confluence – Tool für die Zusammenarbeit an Inhalten, um Teams bei der Zusammenarbeit und dem Wissensaustausch zu unterstützen.
- ConceptShare – Korrektur-Tool, um Inhalte schneller, zügiger und kostengünstiger bereitzustellen.
- Concur – Reise- und Spesenmanagement-Tool zur Verwaltung von Ausgaben unterwegs.
- ConnectWise Control – Business-Management-Tool zur Bereitstellung von Remote-Support und -Zugriff.
- Contactzilla – Kontaktmanagement-Tool für den Zugriff auf aktuelle Kontaktinformationen.
- ContractSafe – Vertragsmanagement-Tool zum Verfolgen, Speichern und Verwalten von Verträgen.
- Contentful – Software für Inhalte zum Erstellen, Verwalten und Verteilen von Inhalten auf jeder Plattform.
- Convo – Teamkommunikations- und Kollaborationstool für interne Gespräche.
- Copper – CRM-Tool.
- Cronitor – Überwachungstool für Cron-Jobs.
- Crowdin – Lösung, die nahtlose und kontinuierliche Lokalisierung für Entwickler bietet.
- Dashlane – Passwortverwaltungstool, das auch digitale Geldbörsen verwaltet.
- Declaree – Reise- und Spesenverwaltungstool für Geschäftsreisen.
- Dell Boomi – Ein Integrationstool zum Verbinden von Cloud- und lokalen Anwendungen und Daten.
- Deskpro – Helpdesk-Tool zur Erleichterung der Ticketverwaltung, Kunden-Selbsthilfe und des Kundenfeedbacks.
- Deputy – Personalmanagement-Tool zur Planung und Verfolgung von Arbeitszeiten, Aufgaben und Kommunikation der Mitarbeiter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DigiCert – Zertifikatsverwaltungs- und Fehlerbehebungstool für SSL-Zertifikate für Websites.
- Dmarcian – E-Mail-Überwachungstool zum Filtern von Spam, Malware und Phishing.
- DocuSign – Ein Online-Signaturtool für verschiedene Dokumente, wie Versicherungs-, Medizin- und Immobiliendokumente.
- DOME9 ARC – Sicherheits- und Compliance-Tool zur Verwaltung öffentlicher Cloud-Umgebungen.
- Dropbox – Cloud-Speicher-Tool für sichere Dateifreigabe und -speicherung.
- Duo – Sicherheitstool zur Bereitstellung eines sicheren Zugriffs auf Ihre Anwendungen.
- Dynatrace – Medizinische Labordienstleistungen.
- Easy Projects – Projektmanagement-Tool.
- EdApp - Lernmanagement-Tool für das Lernen am Arbeitsplatz.
- 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, für Aufgabenlisten und zur Archivierung.
- Expensify - Spesenmanagement-Tool für die Verwaltung von Spesenabrechnungen, die Belegverfolgung und Geschäftsreisen.
- ezeep - Druckinfrastruktur-Management-Tool zum Drucken von jedem Gerät, jedem Standort auf jeden Drucker in der Cloud.
- EZOfficeInventory - Bestandsmanagement-Tool zur Verfolgung all Ihrer Vermögenswerte und Geräte.
- EZRentOut - Gerätevermietungs-Tool zur Verfolgung der Gerätequalität und -verfügbarkeit.
- Fastly - Edge-Cloud-Plattform zum Bereitstellen und Sichern von Anwendungen näher an den Benutzern.
- Favro - Planungs- und Kollaborationstool für den organisatorischen Workflow.
- Federated Directory - Unternehmensübergreifendes Kontaktverzeichnis-Tool zum Durchsuchen der Unternehmensadressbücher verschiedener Unternehmen.
- Feeder
- Feedly - Nachrichtenaggregations-Tool zum Zusammenstellen von Newsfeeds aus verschiedenen Quellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- FileCloud - Softwarelösung, die eine robuste und sichere Plattform für Dateihosting und -freigabe für Organisationen bietet.
- Fivetran – Tool, das Analysten hilft, Daten in ein Cloud-Warehouse zu replizieren.
- Flatter Files – Digitaler Aktenordner für Zeichnungen und Dokumente, um einen sicheren und einfachen Zugriff auf Inhalte zu ermöglichen.
- Float – Ressourcenplanungstool für die Projektplanung und die Verwaltung der Team-Auslastung.
- Flock – Kollaborationstool.
- Formstack – Ein Online-Formularersteller und Datenerfassungstool.
- FOSSA – Automatisierte Tools zur Überprüfung von Open-Source-Lizenzen und zur Schwachstellenverwaltung, die nativ in CI/CD integriert sind.
- Freshdesk – Kundensupport-Tool, um die Bedürfnisse der Kunden zu unterstützen.
- Freshservice – IT-Helpdesk-Tool zur Vereinfachung von IT-Operationen.
- FrontApp – Kollaborationstool zur Verwaltung aller Konversationen an einem Ort.
- Frontify – Plattform zur Erleichterung und Optimierung der täglichen Branding-, Marketing- und Entwicklungsabläufe.
- Fulcrum – Mobile Datenerfassungsplattform, mit der Sie einfach mobile Formulare erstellen und Daten sammeln können.
- Fusebill – Software für Rechnungsverwaltung und wiederkehrende Abrechnungen.
- G-Suite – Eine Reihe intelligenter Apps, um die Mitarbeiter in Ihrem Unternehmen zu verbinden.
- GetGuru – Wissensmanagement-Software.
- GitBook – Tool zum Erstellen und Pflegen Ihrer Dokumentation.
- GitHub - Ein webbasierter Hosting-Dienst für die Versionskontrolle mit Git für Repositorys, die hinter einer Unternehmens-Firewall gehostet werden.
- GitLab - Eine vollständige DevOps-Plattform, die als einzelne Anwendung bereitgestellt wird.
- GlassFrog - Software für die Holacracy-Praxis.
- GoodData - Eine eingebettete BI- und Analyseplattform, die schnelle, zuverlässige und benutzerfreundliche Analysen bietet
- GotoMeeting - Online-Meeting-Software mit HD-Videokonferenzfunktionen.
- HackerRank - Bietet Wettbewerbsprogrammierungs-Herausforderungen für Verbraucher und Unternehmen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HappyFox - Online-Helpdesk-Software und webbasiertes Support-Ticket-System.
- Helpjuice - Wissensmanagementlösung zum Erstellen und Pflegen von Wissensdatenbanken.
- Help Scout - Kundenservice-Software und Wissensdatenbank-Tool für Kundenservice-Profis.
- Hello sign - E-Signatur-Schnittstelle, um das Unterschreiben von überall, jederzeit und auf jedem Gerät zu ermöglichen.
- HelpDocs - Wissensdatenbank-Software, um Ihre Benutzer zu führen, wenn sie nicht weiterkommen.
- Honeybadger - Tool zur Überwachung der Anwendungszustands.
- Harness - Tool für kontinuierliche Bereitstellung und Integration für Java-, .NET-Anwendungen in AWS, GCP, Azure und Bare Metal.
- HelpDocs - Tool zum Erstellen einer maßgeblichen Wissensdatenbank, um Ihre Benutzer zu führen, wenn sie nicht weiterkommen.
- Helpmonks - Eine kollaborative E-Mail-Plattform für die Teamzusammenarbeit.
- Hoshinplan - Tool zur Visualisierung Ihrer strategischen Pläne und zur Verfolgung von Status auf einer einzigen Leinwand.
- Hosted Graphite - Tool zur Überwachung der Leistung Ihrer Website, App, Ihres Servers und Ihrer Container.
- Humanity - Online-Software zur Personalplanung zur Verwaltung von Schichten, Zeitplänen, Gehaltsabrechnungen und Zeiterfassung.
- Igloo - Anbieter von digitalen Arbeitsplatz- und Intranetlösungen zur Bewältigung von IT-Herausforderungen in Ihrem Unternehmen.
- iLobby - Cloud-basierte Lösung für das Besuchermanagement.
- 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-Anwendungen und eine Plattform für die Entwicklung und Bereitstellung benutzerdefinierter Integrationsdienste.
- Intelligent contract - Software für Vertragsmanagement.
- iMeet Central - Projektmanagement-Software für Marketingfachleute, Kreativagenturen und Großunternehmen.
- InteractGo - Tool zur Messung von Echtzeit- und historischen Daten zur Systemleistung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- iQualify One - Lern- und Management-Tool zur Bereitstellung authentischer Lernerfahrungen.
- InsideView - Daten- und Intelligenzlösungen zur Bewältigung von Herausforderungen in Vertrieb, Marketing und anderen Geschäftsbereichen.
- Insightly - Ein cloudbasiertes Customer Relationship Management (CRM) und Projektmanagement-Tool für kleine und mittelständische Unternehmen.
- ITGlue - Eine cloudbasierte IT-Dokumentationsplattform, die MSPs dabei hilft, die Dokumentation zu standardisieren, Wissensdatenbanken zu erstellen, Passwörter zu verwalten und Geräte zu verfolgen.
- Jitbit – Helpdesk-Software und Ticketing-System zur Verwaltung und Nachverfolgung eingehender Supportanfragen per E-Mail und der zugehörigen Tickets.

JupiterOne – Softwareplattform zum Erstellen und Verwalten Ihres gesamten Sicherheitsprozesses.

- Kanbanize – Eine Online-Portfolio-Kanban-Software für Lean Management.
- Klipfolio – Eine Online-Dashboard-Plattform zum Erstellen leistungsstarker Echtzeit-Business-Dashboards für Ihr Team oder Ihre Kunden.
- Jira – Tool zum Planen, Verfolgen und Verwalten Ihrer Probleme und Projekte.
- Kanban Tool – Visuelle Management-Software zur Verbesserung der Teamleistung und Steigerung der Produktivität.
- Keeper Security – Passwort-Manager und Sicherheitssoftware zum Schutz Ihrer Passwörter und privaten Informationen.
- Kentik – Tool zur Anwendung von Big Data für Netzwerk- und Leistungsüberwachung, DDoS-Schutz und Echtzeit-Ad-hoc-Netzwerkflussanalysen.
- Kissflow – Workflow-Tool und Software für das Geschäftsprozess-Workflow-Management zur Automatisierung Ihres Workflow-Prozesses.
- KnowBe4 – Tool zur Bereitstellung von Sicherheitsschulungen und simuliertem Phishing.
- KnowledgeOwl – Wissensdatenbank und Autoren-Tool.
- Kudos – Systeme für Einzelhandel, Aufträge, Projekte und Abwicklungsprozesse.
- LaunchDarkly – Feature-Management-Plattform, die Entwicklungs- und Betriebsteams die Kontrolle über den Feature-Lebenszyklus ermöglicht.
- Lifesize – Videokonferenzlösung.
- Litmos – Lernmanagementsystem für Mitarbeiterschulungen, Kundenschulungen, Compliance-Schulungen und Partnerschulungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- LiquidPlanner – Online-Projektmanagement-Software für Ihr Unternehmen.
- LeanKit – Lean-basierte Unternehmensprozess- und Arbeitsmanagement-Software, die Unternehmen hilft, Arbeit zu visualisieren, Prozesse zu optimieren und schneller zu liefern.
- LiveChat – Live-Chat- und Helpdesk-Software für Unternehmen.
- LogDNA – Tool zum Sammeln, Überwachen, Parsen und Analysieren von Protokollen aus allen Quellen in einem zentralisierten Protokollierungstool.
- Mango – Team-Kollaborationssoftware zur Konsolidierung und Straffung isolierter Anwendungen in einer einzigen Plattform.
- Manuscript – Ein Schreibtool, das Ihnen hilft, Ihre Arbeit zu planen, zu bearbeiten und zu teilen.
- Marketo – Automatisierungssoftware, die Marketingteams hilft, die Kunst und Wissenschaft des digitalen Marketings zu beherrschen.
- Matomo – Eine Webanalyse-Plattform, die die gesamte User Journey aller Website-Besucher bewertet.
- Meisterplan – Software, die Organisationen hilft, Projektportfolios zu erstellen.
- Mingle – Ein agiles Projektmanagement- und Kollaborationstool, das einen kombinierten Arbeitsplatz für das gesamte Team bietet.
- MojoHelpdesk – Helpdesk-Software und Ticketing-System.
- Monday – Teammanagement-Software, um Ihre gesamte Arbeit in einem Tool zu planen, zu verfolgen und zusammenzuarbeiten.
- Mixpanel – System zur Verfolgung von Benutzerinteraktionen mit Web und Mobilgeräten.
- MuleSoft – Integrationssoftware zum Verbinden von SaaS- und Unternehmensanwendungen in der Cloud und On-Premises.
- MyWebTimesheets – Online-Zeiterfassungssystem zur Erfassung der auf verschiedene Projekte/Aufgaben/Aktivitäten verwendeten Zeit.
- New Edge – Sicherer Anwendungsnetzwerkdienst für Hybrid-IT.
- NextTravel – Software-Tool für das Geschäftsreisemanagement.
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nuclino – Kollaborationssoftware zur Zusammenarbeit und zum Austausch von Informationen in Echtzeit.
- Office365 – Der cloudbasierte Abonnementdienst von Microsoft.
- OfficeSpace – Eine cloudbasierte Plattform, die Unternehmen bei der Zuweisung von Arbeitsbereichen unterstützt.
- OneDesk – Projektmanagement- und Helpdesk-Software zur Verbindung mit und Unterstützung Ihrer Kunden.
- OpsGenie – Eine Incident-Management-Plattform für DevOps- und IT-Ops-Teams zur Optimierung von Alarmen und Incident-Resolution-Prozessen.
- Orginio – Ein Online-Tool zur Erstellung von Organigrammen zur Visualisierung der Organisationsstruktur.
- Oomnitza – IT-Asset-Management-Plattformlösung zur Verfolgung und Verwaltung von Assets.
- OpenEye – Mobile App zum Anzeigen von Live- und aufgezeichneten Videos auf dem Apex-Recorder.
- Oracle ERP Cloud – Cloudbasierte Softwareanwendungssuite zur Verwaltung von Unternehmensfunktionen.
- Pacific Timesheet – Webbasiertes Zeiterfassungstool für Gehaltsabrechnung, Projektstunden und Spesen.
- PagerDuty – Digitales Betriebsmanagement-System.
- PandaDoc – Eine mobile App, mit der iPhone-Benutzer direkt auf ihren Mobiltelefonen auf ihre Dokumente, Analysen und Dashboards zugreifen können.
- Panopta – Infrastruktur-Überwachungstool.
- Panorama9 – Cloud-basierte IT-Management-Plattform für die Überwachung von Unternehmensnetzwerken.
- Papyrs – Editor zum Entwerfen eigener Intranetseiten.
- ParkMyCloud – Einzweck-SaaS-Tool zur Verbindung mit AWS, Azure Services oder GCP.
- Peakon – Tool zur Messung und Verbesserung der Mitarbeiterbindung.
- People HR – HR-Softwaresystem für alle wichtigen HR-Funktionen.
- Pingboard – Tool zum Erstellen von Organigrammen für die Teamorganisation und Personalplanung.
- Pigeonhole Live – Interaktive Frage-und-Antwort-Plattform.
- Pipedrive – Vertriebs-CRM- und Pipeline-Management-Software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- PlanMyLeave – Urlaubsverwaltungssystem zur Verwaltung und Nachverfolgung von Abwesenheiten der Mitarbeiter.
- PlayVox – Tool zur Überwachung der Kundendienstqualität.
- Podbean – Podcast-Dienstanbieter.
- Podio – Ein webbasiertes Tool zur Organisation von Teamkommunikation, Geschäftsprozessen, Daten und Inhalten in Projektmanagement-Arbeitsbereichen.
- POPin – Crowd-solving-Plattform und mobile App, die das Team-Engagement zur Problemlösung operationalisiert
- Postman – API-Entwicklungsumgebung.
- Prescreen – Bewerber-Tracking-Tool zum Veröffentlichen von Stellenangeboten online und offline.
- ProductBoard – Produktmanagement-Tool.
- ProdPad – Produktmanagement-Software zur Entwicklung von Produktstrategien.
- Proto.io – Anwendungs-Prototyping-Plattform zur Erstellung vollständig interaktiver, hochauflösender Prototypen.
- Proxyclick – Cloud-basierte Besuchermanagement-Lösung zur Verwaltung von Besuchern, zum Aufbau des Markenimages und zur Gewährleistung der Sicherheit.
- Pulumi – Cloud-native Entwicklungsplattform für Container, Serverless, Infrastruktur und Kubernetes.
- PurelyHR – Urlaubsmanagement-Tool für den Zugriff auf Mitarbeiterurlaubsdaten.
- Promapp – Tool für Geschäftsprozessmanagement (BPM).
- Prescreen – Cloud-basiertes Bewerber-Tracking-System zum Veröffentlichen von Stellenangeboten online und offline.
- QAComplete – Software-Testmanagement-Tool.
- Qualaroo – Feedback-Tool, um Erkenntnisse von Kunden zu gewinnen.
- Quality Built, LLC – Versicherungs-, Finanz- und Bauindustrie zur Bereitstellung zuverlässiger und innovativer Dienstleistungen zur Qualitätssicherung durch Dritte.
- Qubole – Self-Service-Plattform für Big-Data-Analysen, die auf Amazon basiert.
- Questetra BPM Suite – Webbasierte Geschäftsprozessplattform für Routine-Workflows.
- QuestionPro – Online-Umfragesoftware zum Erstellen von Umfragen und Fragebögen.
- Quandora – Frage- und Antwort-basierte Wissensmanagementlösung.
- Quip – Kollaborative Produktivitätssoftware-Suite für Mobilgeräte und das Web.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rackspace – Verwaltete Cloud-Computing-Dienste.
- ReadCube – Tool für Web-, Desktop- und mobiles Referenzmanagement.
- RealtimeBoard – Whiteboard-Kollaborationstool für Organisationen zur Zusammenarbeit über Formate, Tools, Standorte und Zeitzonen hinweg.
- Receptive – Tool zum Sammeln von Feedback von Kunden, Teams und dem Markt an einem Ort.
- Remedyforce – IT-Service-Management- und Helpdesk-System.
- Retrace – Ein Tool für das Anwendungsleistungsmanagement, das Fehlerverfolgung, Datenaggregation und automatische Warnmeldungen bietet.
- Robin – Tools für die Arbeitsplatzerfahrung zur Planung von Konferenzräumen und Schreibtischbuchungen.
- Rollbar – Echtzeit-Fehlerwarnungs- und Debugging-Tools für Entwickler.
- Really Simple Systems – Cloud-basierte CRM-Software für kleine Unternehmen zur Verwaltung ihrer Verkäufe und ihres Marketings.
- Reamaze – Kundensupport-Software zur Unterstützung, Einbindung und Konvertierung von Kunden mit Chat, sozialen Medien, SMS, FAQ und E-Mail auf einer einzigen Plattform.
- Resource Guru – Ressourcenmanagement-Software zur Planung von Personal, Ausrüstung und anderen Ressourcen.
- Retrace – Anwendungsleistungsmanagement zur Integration von Code-Profiling, Fehlerverfolgung, Anwendungs-Logs und Metriken.
- Roadmunk – Produkt-Roadmap-Software und Roadmap-Tool zum Erstellen von Produkt-Roadmaps.
- Runscope – Tool zum Erstellen, Verwalten und Ausführen von funktionalen API-Tests und -Monitoren.
- Salesforce – CRM-Tool zur Verwaltung von Kundenkontaktinformationen, Integration von sozialen Medien und zur Erleichterung der Echtzeit-Kundenkollaboration.
- SalesLoft – Sales-Engagement-Plattform für effizienten und umsatzsteigernden Vertrieb
- Salsify – Plattform für Produkt-Erfahrungsmanagement (PXM).
- Samanage – Tool für IT-Service-Management.
- Samepage – Kollaborationssoftware zur Verwaltung von Online-Projekten.
- Screencast-O-Matic – Tool zum Screencasten und Bearbeiten von Videos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ScreenSteps – Tools zum Erstellen visueller Dokumente, die auf Bildschirmaufnahmen basieren.
- SendSafely – Verschlüsselungsplattform für den sicheren Austausch von Dateien und E-Mails.
- Sentry – Open-Source-Software zur Fehlerverfolgung.
- ServiceDesk Plus – Tool für den IT-Service-Desk.
- ServiceNow – Cloud-Plattform zum Erstellen digitaler Workflows.
- SharePoint – Kollaborative Plattform für Dokumentenmanagement und -speicherung.
- Shufflrr – Präsentationsverwaltungstool zum Erstellen, Aktualisieren, Teilen und Übertragen von Präsentationen.
- Sigma Computing – Ein Analysetool zum Erkunden, Analysieren und Visualisieren 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 von Mitarbeitern.
- Skyprep – Lernmanagementsystem (LMS) zur Schulung von Kunden und Mitarbeitern.
- Slack – Kollaborationstool zur Kommunikation und zum Informationsaustausch.
- Slemma – Datenanalysetool zum Erstellen von Datenberichten aus mehreren Datensätzen.
- Sli.do – Interaktionstool für Meetings, Veranstaltungen und Konferenzen.
- SmartDraw – Diagramm-Tool zum Erstellen von Flussdiagrammen, Organigrammen, Mindmaps, Projektplänen und anderen Geschäftsvisualisierungen.
- SmarterU – Lernmanagementsystem (LMS) zur Schulung von Kunden und Mitarbeitern.
- Smartsheet – Kollaborationstool zum Zuweisen von Aufgaben, Verfolgen von Projektfortschritten, Verwalten von Kalendern und Teilen von Dokumenten.
- SparkPost – E-Mail-Zustelldienst.
- Split – Anwendung zur Rechnungsaufteilung.
- Spoke – Service-Desk-Tool zum Einreichen von Service-Tickets.
- Spotinst – Eine SaaS-Optimierungsplattform, die Unternehmen beim Kauf und der Verwaltung von Cloud-Infrastrukturkapazitäten unterstützt.
- SproutVideo – Plattform zum Hosten von Geschäftsvideos.
- Stackify – Fehlerbehebungstool, das Unterstützung mit einer Suite von Tools, einschließlich Prefix und Retrace, bietet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 zum Senden von Vorfallbenachrichtigungen an Kunden.
- Status Hero – Tool zum Verfolgen von Statusaktualisierungen und Tageszielen Ihres Teams.
- StatusHub – Plattform zum Hosten der Dienststatusseite.
- Statuspage – Tool zur Kommunikation von Status und Vorfällen.
- SugarCRM – CRM-Tool für Salesforce-Automatisierung, Marketingkampagnen, Kundensupport, Zusammenarbeit, Mobile CRM, Social CRM und Berichterstellung.
- Sumo Logic – Datenanalyse-Software, die sich auf Sicherheits-, Betriebs- und BI-Anwendungsfälle konzentriert.
- Supermood – HR-Plattform zur Erfassung von Mitarbeiterfeedback in Echtzeit.
- Syncplicity – Tool zum Teilen und Synchronisieren von Dateien.
- Tableau – Tool zum Erstellen interaktiver Datenvisualisierungen.
- TalentLMS – Lernmanagementsystem (LMS) zur Erleichterung von Online-Seminaren, Kursen und anderen Schulungsprogrammen.
- Tallie – Tool zum Erfassen und Hochladen von Belegen, Generieren von Spesenabrechnungen und Anpassen von Spesendetails.
- Targetprocess – Agile Projektmanagement-Software für Scrum, Kanban, SAFe und so weiter.
- Teamphoria – Software zur Bereitstellung von Echtzeit-Metriken zur Mitarbeiterbindung, 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 zum Erstellen von Verhaltensstudien und Umfragen.
- TestingBot – Tool zur Bereitstellung verschiedener Browserversionen für Live- und automatisierte Tests.
- TestFairy – Mobile Testplattform, die Unternehmen Videoaufzeichnungen, Protokolle und Absturzberichte von mobilen Sitzungen bereitstellt.
- TextExpander – Kommunikationstool zum Einfügen von Textausschnitten aus einem Repository von E-Mails und anderen Inhalten während der Eingabe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TextMagic – Nachrichtendienst zur Verbindung mit Kunden.
- ThousandEyes – Tool zur Überwachung der Netzwerkinfrastruktur, Fehlerbehebung bei der Anwendungsbereitstellung und Abbildung der Internetleistung.
- Thycotic Secret server – Software-Tool zur Kontoverwaltung zum Verwalten von Passwörtern.
- TimeLive – Tool zur Bereitstellung von Zeiterfassungsbögen und zur Zeiterfassung.
- Tinfoil Security – Sicherheitslösungssoftware zur Überprüfung auf Schwachstellen.
- Trisotech – Tool, das Kunden ermöglicht, ihr digitales Unternehmen zu entdecken, zu modellieren und zu analysieren.
- Trumba – Tool zum Veröffentlichen von interaktiven Online-Veranstaltungskalendern.
- TwentyThree - Videomarketing-Plattform zur Integration und Hinzufügung von Videos zum Marketing-Stack.
- Twilio - Eine Entwicklerplattform für Kommunikation.
- Ubersmith - Business-Management-Software für nutzungsbasierte Abrechnung, Angebotserstellung, Auftragsverwaltung, Infrastrukturmanagement und Helpdesk-Ticketing-Lösungen.
- UniFi - Kommunikations- und Kollaborationssoftware mit Sprach-, Web-Kollaborations- und Videokonferenzfunktionen.
- UPTRENDS – Website-Überwachungslösung zur Verfolgung der Website-Verfügbarkeit und -Leistung.
- UserEcho - Community-Forum-Tool, das Unternehmen bei der Verwaltung von Kundenfeedback unterstützt.
- UserVoice - Software für das Produktfeedback-Management, die Unternehmen in die Lage versetzt, datengestützte Produktentscheidungen zu treffen.
- VALIMAIL - E-Mail-Authentifizierungssoftware zur Authentifizierung legitimer E-Mails und zur Blockierung von Phishing-Angriffen.
- Veracode - Quellcode-Analyse- und Code-Scanner schützen Unternehmen vor Cyberbedrohungen und Anwendungs-Backdoors.
- Velpic - Lernmanagementsystem (LMS) zur Optimierung der Mitarbeiterschulung.
- VictorOps - Incident-Management-Software zur Bereitstellung von DevOps-Observability, Zusammenarbeit und Echtzeit-Alarmierung.
- VIDIZMO - Software für Live- und On-Demand-Videostreaming für Unternehmen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Visual Paradigm - Online-Plattform für visuelle Modellierung und Diagrammerstellung zur Teamzusammenarbeit.
- Vtiger - CRM-Tool, das Vertriebs-, Support- und Marketingteams die Organisation und Zusammenarbeit ermöglicht.
- WaveMaker – Software zum Erstellen und Ausführen benutzerdefinierter Apps.
- Weekdone – Tool zur Erstellung von Manager-Dashboards und Teammanagement-Diensten für Unternehmen.
- Wepow – Tool zur Verbindung von Personalvermittlern, Bewerbern und Arbeitgebern über eine mobile Video-Interview-Lösung.
- When I Work – Tool für die Personalplanung 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 Leistung der Organisation.
- Workplace – Kollaborationstool von Facebook, um Mitarbeitern die Kommunikation über eine vertraute Oberfläche zu erleichtern.
- Workstars – Plattform für soziale und Peer-Mitarbeiter-Anerkennungsprogramme.
- Workteam – Tool zur Erfassung von Arbeitszeit und Anwesenheit der Mitarbeiter.
- Wrike – Soziale Projektmanagement- und Kollaborationssoftware.
- XaitPorter – Software zur gemeinsamen Dokumentenerstellung für Angebote, Vorschläge und andere Geschäftsunterlagen.
- Ximble – Tool für die Personalplanung und Zeiterfassung.
- XMatters – Kollaborationsplattform mit einer Alarmierungssoftware, die sich in andere Tools integrieren lässt, um nahtlose Prozesse und effektive Kommunikation zu schaffen.
- Yodeck – Tool zur Fernverwaltung von Bildschirmen über das Web oder Mobilgerät.
- Zendesk – Software zum Anfordern von Kundenservice und zum Protokollieren von Support-Tickets.
- Ziflow – Tool für kreative Produktionsteams.
- Zillable – Kollaborationsplattform mit Kommunikationsfunktionen.
- Zing tree – Ein Toolkit zum Erstellen interaktiver Entscheidungsbäume und zur Fehlerbehebung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ZIVVER – Tool, das sicheren E-Mail- und Dateitransfer von Ihrem vertrauten E-Mail-Programm ermöglicht.
- Zoho – Suite für Geschäftsanwendungen.
- Zoom – Kommunikations- und Kollaborationssoftware mit Sprach-, Web-Kollaborations- und Videokonferenzfunktionen.
- Zuora – Eine abonnementbasierte Software, die es einem Unternehmen ermöglicht, ein Abonnementgeschäft zu starten, zu verwalten und sich in ein solches umzuwandeln.

End-to-End-App-Konfiguration

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

Agentenloser Zugriff auf Unternehmens-Webanwendungen

Auf Unternehmens-Webanwendungen wie SharePoint, JIRA, Confluence und andere, die vom Kunden On-Premises oder in Public Clouds gehostet werden, kann jetzt direkt über einen Client-Browser zugegriffen werden. Endbenutzer müssen den Zugriff auf ihre Unternehmens-Webanwendungen nicht mehr über den Store initiieren. Diese Funktion ermöglicht es Endbenutzern auch, auf Webanwendungen zuzugreifen, indem sie auf Links aus E-Mails, Kollaborationstools oder Browser-Lesezeichen klicken, was den Kunden eine echte Zero-Footprint-Lösung bietet.

Funktionsweise

- Fügen Sie einen neuen DNS-Eintrag hinzu oder ändern Sie einen vorhandenen DNS-Eintrag für die konfigurierten Unternehmens-Webanwendungen.
- Ein IT-Administrator fügt einen neuen öffentlichen DNS-Eintrag hinzu oder ändert einen vorhandenen öffentlichen DNS-Eintrag für den konfigurierten FQDN der Unternehmens-Webanwendung, um den Benutzer zum Citrix Secure Private Access™-Dienst umzuleiten.
- Wenn der Endbenutzer den Zugriff auf die konfigurierte Unternehmens-Webanwendung initiiert, wird der Anwendungsdatenverkehr an den Citrix Secure Private Access-Dienst geleitet, der dann den Zugriff auf die Anwendung als Proxy bereitstellt.
- Sobald die Anfrage beim Citrix Secure Private Access-Dienst eingeht, überprüft dieser die Benutzerauthentifizierung und Anwendungsautorisierung, einschließlich kontextbezogener Zugriffsrichtlinienprüfungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nach erfolgreicher Validierung kommuniziert der Citrix Secure Private Access-Dienst mit den Citrix Cloud Connector™ Appliances, die in der Umgebung des Kunden (entweder On-Premises oder in der Cloud) bereitgestellt werden, um den Zugriff auf die konfigurierte Unternehmens-Webanwendung zu ermöglichen.

Konfigurieren von Citrix Secure Private Access für den agentenlosen Zugriff auf Unternehmens-Webanwendungen

Voraussetzungen:

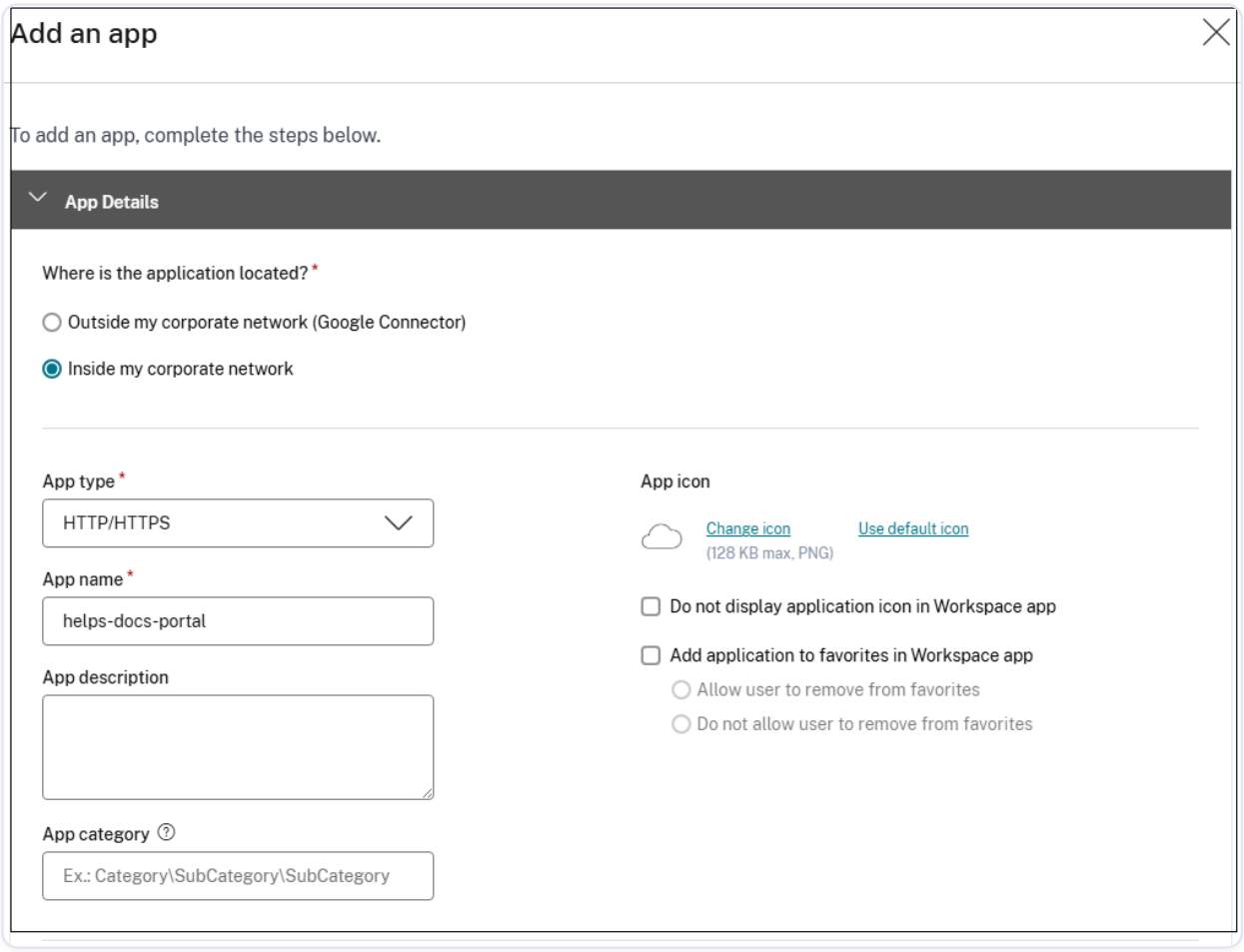
Bevor Sie beginnen, benötigen Sie Folgendes für die zu konfigurierende Anwendung.

- 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 von Citrix® während der App-Konfiguration bereitgestellten kanonischen Namen (CNAME) zu aktualisieren.

Agentenlosen Zugriff auf Unternehmens-Web-Apps konfigurieren:

1. Melden Sie sich bei Citrix Cloud an und wählen Sie **Secure Private Access** aus.
2. Klicken Sie auf **Anwendungen > App-Konfiguration** und dann auf **App hinzufügen**.
3. Klicken Sie im Abschnitt **Vorlage auswählen** auf **Überspringen**. Vorlagen sind nur für SaaS-Apps verfügbar.
4. Wählen Sie unter **Wo befindet sich der Anwendungsstandort?** die Option **Innerhalb meines Unternehmensnetzwerks** aus.
    - Wählen Sie **Innerhalb meines Unternehmensnetzwerks** für Anwendungen, die innerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden, sich hinter Firewalls befinden und nur über eine interne Netzwerkverbindung zugänglich sind.
    - Wählen Sie **Außerhalb meines Unternehmensnetzwerks (Google Connector):** Für Anwendungen, die außerhalb der privaten Netzwerkinfrastruktur Ihres Unternehmens gehostet werden. Die Datenverkehrsweiterleitung erfolgt direkt von den Benutzern zur externen Anwendung über den Google Cloud Connector.
5. Geben Sie die folgenden Details im Abschnitt **App-Details** ein und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **App-Typ** – Wählen Sie den App-Typ (HTTP oder HTTPS) aus.

  HINWEIS:

  Für Chrome Enterprise Premium (CEP) werden nur HTTPS-Unternehmens-Web- und SaaS-Apps unterstützt. HTTP-Unternehmens-Web- und SaaS-Apps werden nicht unterstützt.

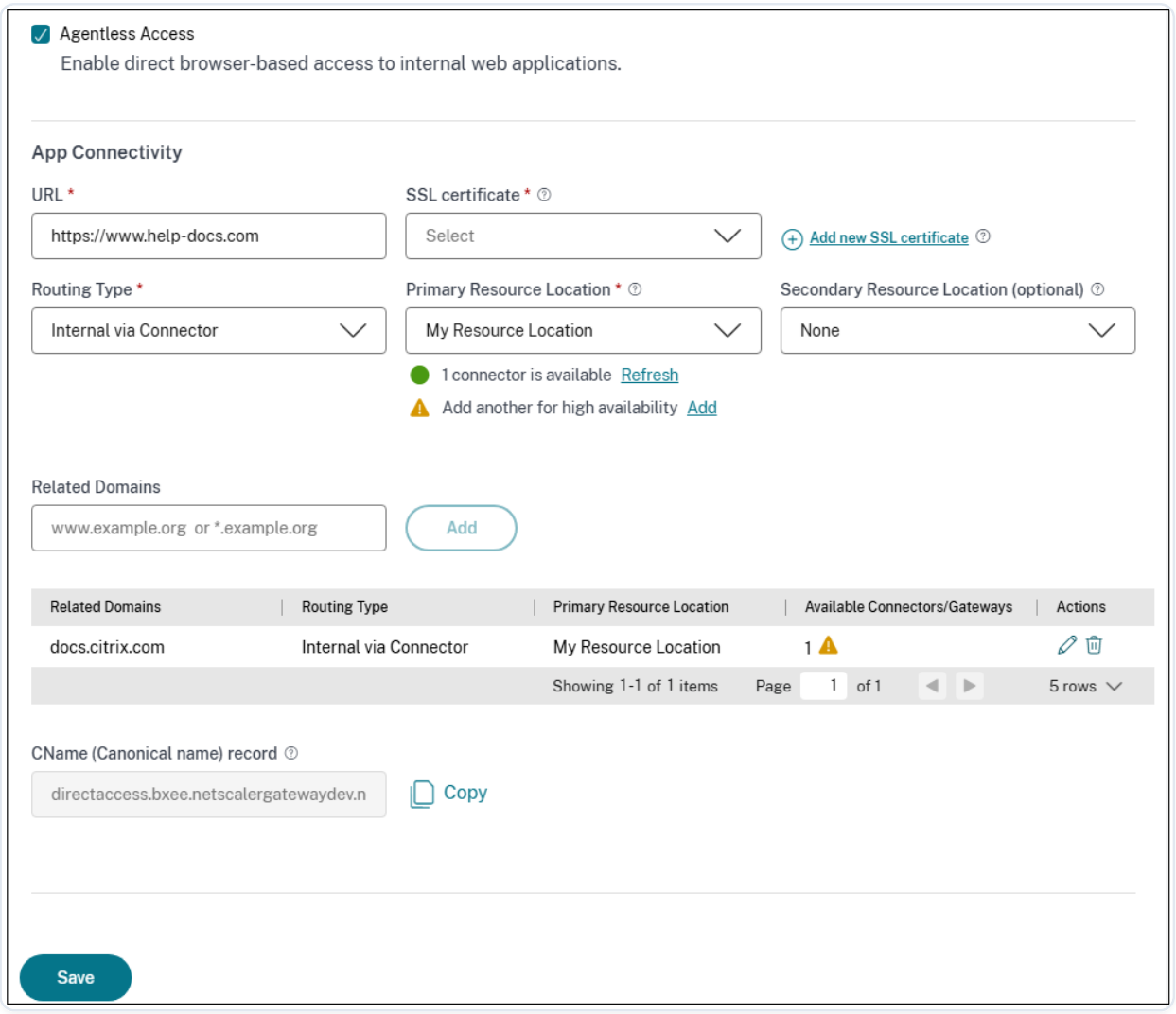
- **App-Name** – Name der Anwendung.
- **App-Beschreibung** – Eine kurze Beschreibung der App. Diese Beschreibung wird Ihren Benutzern im Store angezeigt.
- **App-Symbol** – Klicken Sie auf **Symbol ändern**, um das App-Symbol zu ändern. Die Symbol-Dateigröße muss 128x128 Pixel betragen. Wenn Sie das Symbol nicht ändern, wird das Standardsymbol angezeigt.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Wählen Sie **Agentless Access**, damit Benutzer direkt über einen Client-Browser auf die App zugreifen können. Geben Sie die folgenden Details ein.

   Die Option **Agentless Access** ist nur für Unternehmens-Web-Apps verfügbar.



   - **URL** – URL für die Backend-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.
     - Es wird nur ein öffentliches oder ein vertrauenswürdiges CA-Zertifikat unterstützt.
     - Eine vollständige Zertifikatskette muss hochgeladen werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Administratoren müssen Zertifikate direkt in die Secure Private Access-Konsole hochladen, da Secure Private Access einen eigenen Zertifikatsspeicher verwaltet. Weitere Informationen finden Sie unter Zertifikate in der Secure Private Access-Konsole verwalten.
- Zertifikate, die der NetScaler®-Konsole hinzugefügt wurden, können in Secure Private Access nicht mehr verwendet werden, da die Zertifikate zwischen den beiden Systemen nicht synchronisiert werden.

- **Verwandte Domänen** – Die verwandte Domäne wird automatisch basierend auf der von Ihnen angegebenen URL ausgefüllt. Die verwandte Domäne hilft dem Dienst, die URL als Teil der App zu identifizieren und den Datenverkehr entsprechend weiterzuleiten. Sie können mehr als eine verwandte Domäne hinzufügen. Sie können jeder verwandten Domäne ein SSL-Zertifikat zuweisen, dies ist optional.

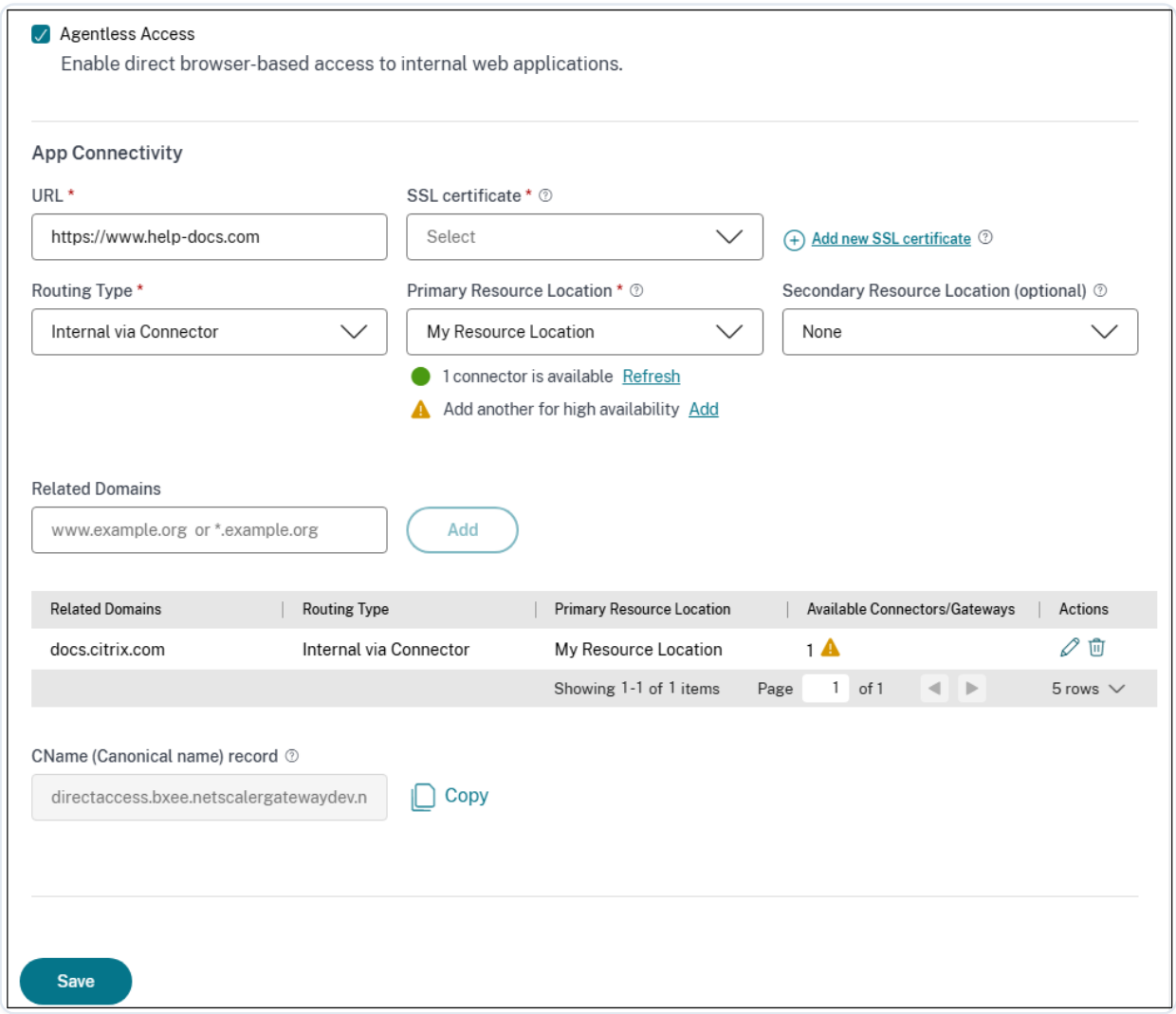
  HINWEIS:

  Eine Warnmeldung wird angezeigt, wenn doppelte verwandte Domänen hinzugefügt werden oder wenn eine verwandte Domäne auch als URL für eine andere App hinzugefügt wird. Um diese Probleme zu vermeiden, lesen Sie Best Practices für Web- und SaaS-Anwendungskonfigurationen.

- **HAR importieren** – Sie können eine HAR-Datei hochladen, um die Domänen, auf die eine Anwendung zugreift, automatisch zu ermitteln. Überprüfen Sie die ermittelten Domänen und wählen Sie diejenigen aus, die Sie der Konfiguration der verwandten Domänen der Anwendung hinzufügen möchten. Dies vereinfacht das Onboarding von Anwendungen, da die manuelle Identifizierung und Konfiguration verwandter Domänen reduziert wird. Weitere Informationen finden Sie unter Verwandte Domänen mithilfe einer HAR-Datei ermitteln.
- **CName-Eintrag** – Automatisch von Secure Private Access generiert. Dies ist der Wert, der im DNS eingegeben werden muss, um den agentenlosen Zugriff auf die Anwendung zu ermöglichen.

7. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die zugehörigen Domänen von Anwendungen, falls die Domänen extern oder intern über die Citrix Connector™ Appliance geroutet werden müssen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Routing-Typ** – Wählen Sie eine der folgenden Optionen aus:
  - **Intern – Proxy umgehen** – Der Domänenverkehr wird über die Connector Appliance™ geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
  - **Intern über Connector** – Die Apps können extern sein, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
  - **Extern** – Der Datenverkehr fließt direkt ins Internet.
- **Primäre und sekundäre Ressourcenstandorte** – Administratoren können die Hochverfügbarkeit von Anwendungen auch bei Unterbrechungen sicherstellen, indem sie einen sekundären Ressourcenstandort konfigurieren oder die Option **Erster verfügbarer** verwenden.
  - **Primärer Ressourcenstandort:** Wählen Sie den primären Ressourcenstandort aus, an dem die Anwendung gehostet wird. Alternativ können Administratoren die Option **Erster verfügbarer** unter **Primärer Ressourcenstandort** auswählen.

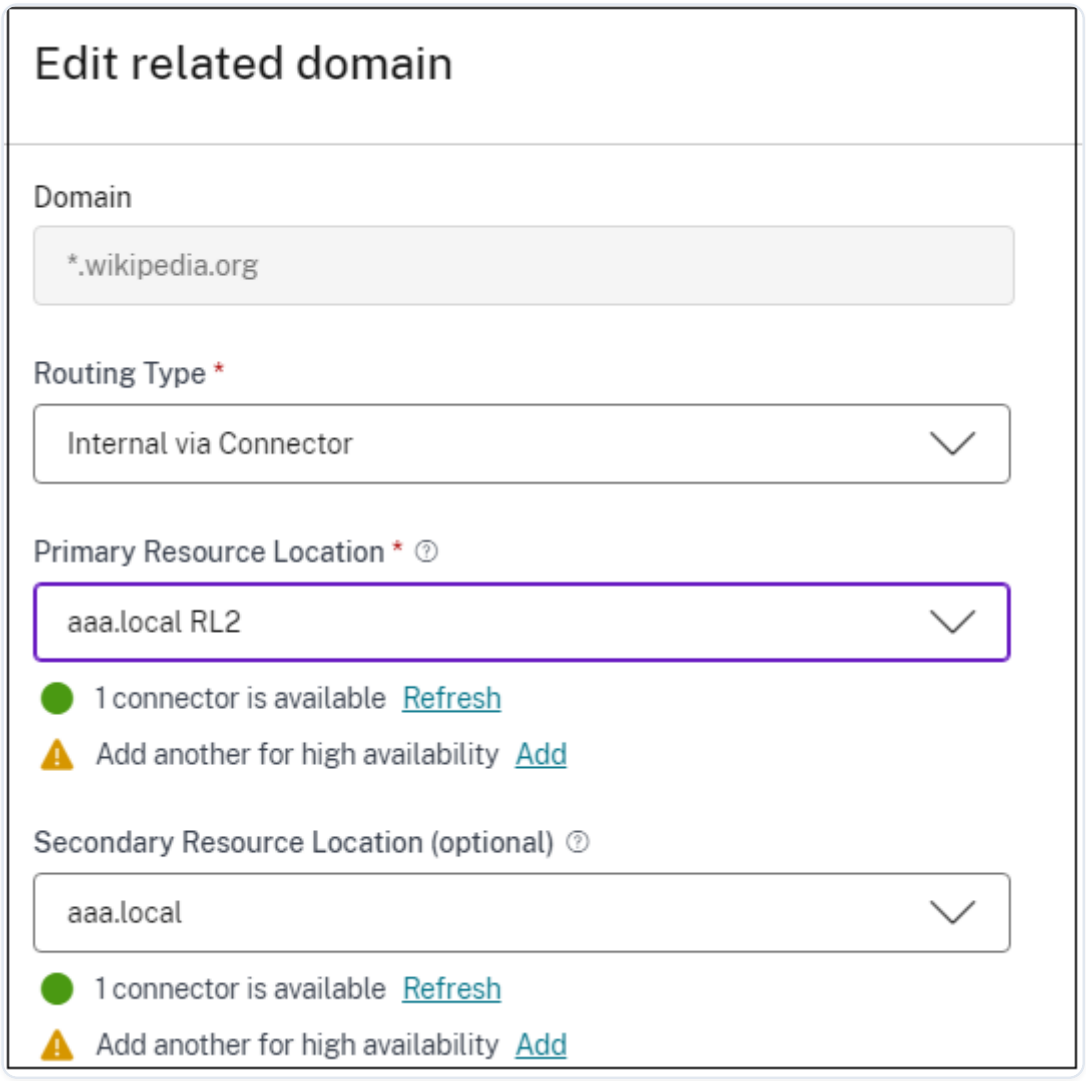
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Erster verfügbarer:** Die Option **Erster verfügbarer** stellt sicher, dass ein funktionierender Ressourcenstandort verwendet wird. Wenn **Erster verfügbarer** ausgewählt ist, leitet das System den Datenverkehr automatisch zum ersten verfügbaren Standort weiter. Dies gewährleistet einen kontinuierlichen Anwendungszugriff ohne manuelles Eingreifen. Wenn beispielsweise ResourceLocation1 nicht verfügbar ist, ResourceLocation2 aber erreichbar ist, wird ResourceLocation2 standardmäßig ausgewählt, um die Anwendung bereitzustellen.
- **Sekundärer Ressourcenstandort** – Die Option **Sekundärer Ressourcenstandort** wird nur verfügbar, wenn ein primärer Ressourcenstandort explizit angegeben ist. Wenn der primäre Ressourcenstandort aus Gründen wie einem Ausfall der Connector Appliance oder des Rechenzentrums nicht verfügbar wird, fällt die Anwendung auf den angegebenen sekundären Ressourcenstandort aus. Der sekundäre Ressourcenstandort kann auch als Failover fungieren, selbst wenn die Anwendung in einem anderen Rechenzentrum gehostet wird.

Sie können auch einen primären und sekundären Ressourcenstandort festlegen oder die Option **Erster verfügbarer** für jede der zugehörigen Domänen auswählen.

a. Klicken Sie auf das Bearbeitungssymbol in der Spalte **Aktionen** der Tabelle „Zugehörige Domänen“.
b. Legen Sie den primären und sekundären Ressourcenstandort fest oder wählen Sie die Option **Erster verfügbarer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

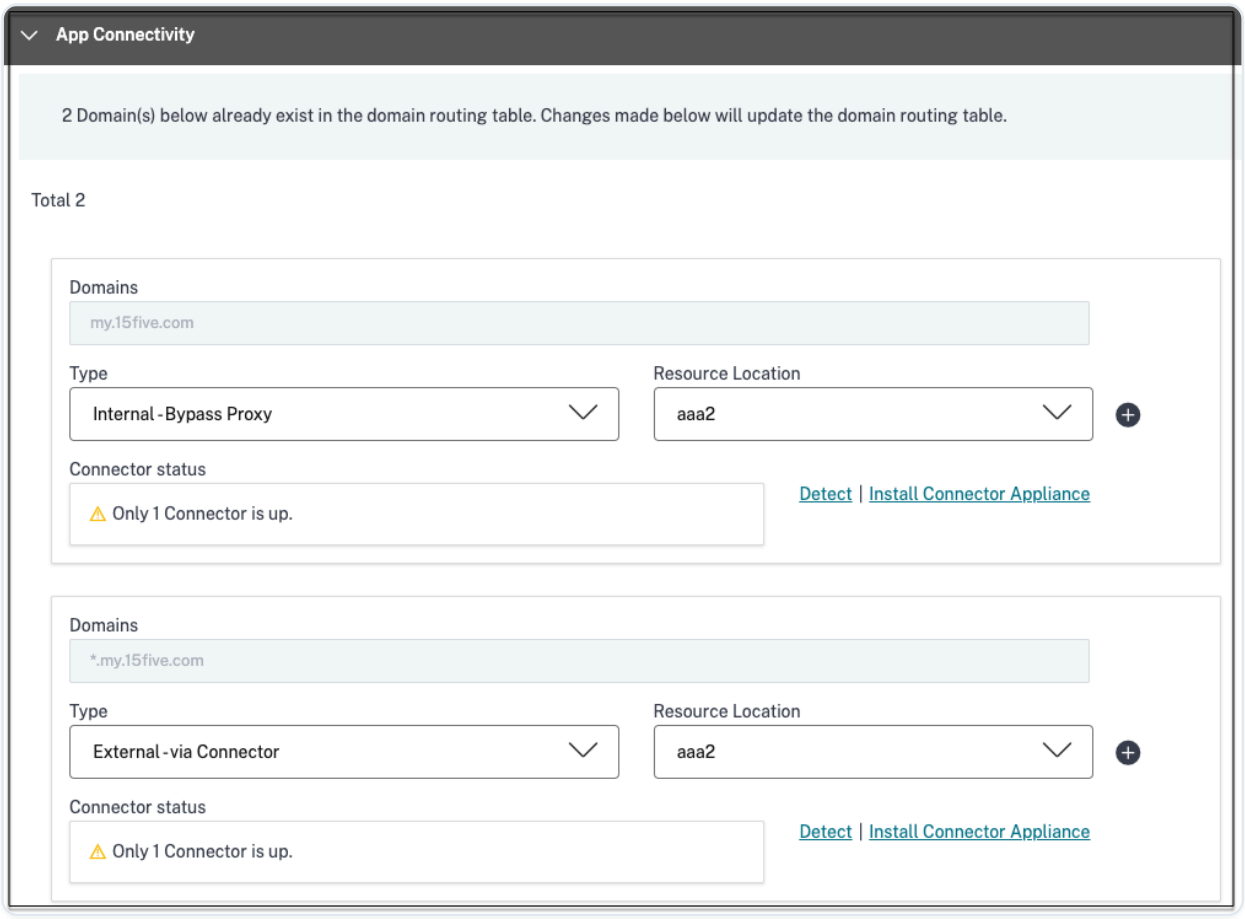


HINWEIS:

- Das Festlegen des Sicherungsressourcenstandorts und die Verwendung der Option **Erster verfügbarer** befinden sich in der Vorschauphase.
- Wenn Sie eine Anwendung löschen, werden ihre Routing-Einträge automatisch entfernt. Weitere Informationen finden Sie unter Automatische Bereinigung von Routing-Einträgen beim Löschen von Anwendungen.

8. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die zugehörigen Domänen von Anwendungen, wenn die Domänen extern oder intern über die Citrix Connector™ Appliance geroutet werden müssen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. **Konsistente Verbindung beibehalten** – Aktivieren Sie dieses Kontrollkästchen, um eine konsistente Verbindung zur selben Connector Appliance zu ermöglichen. Details zu konsistenten Verbindungen finden Sie unter Konsistente Verbindung beibehalten.

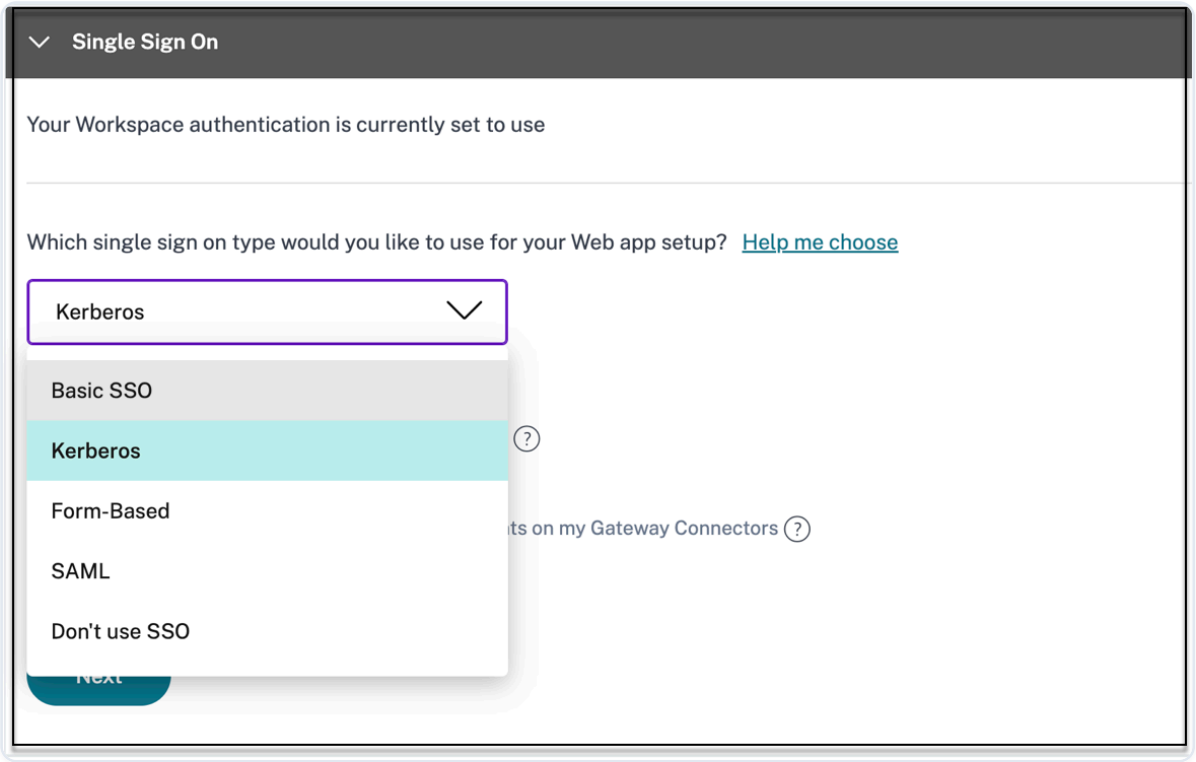
> **HINWEIS:**
>
> Wenn die Option **Konsistente Verbindung beibehalten** ausgewählt ist, muss der Routing-Typ für die Anwendung im Abschnitt App-Konnektivität auf **Intern über Connector** festgelegt werden.

10. Legen Sie die bevorzugte Anmeldemethode fest.

> **HINWEIS:**
>
> Die Single Sign-On-Option ist für Citrix Secure Access mit Chrome Enterprise (CEP) nicht anwendbar.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

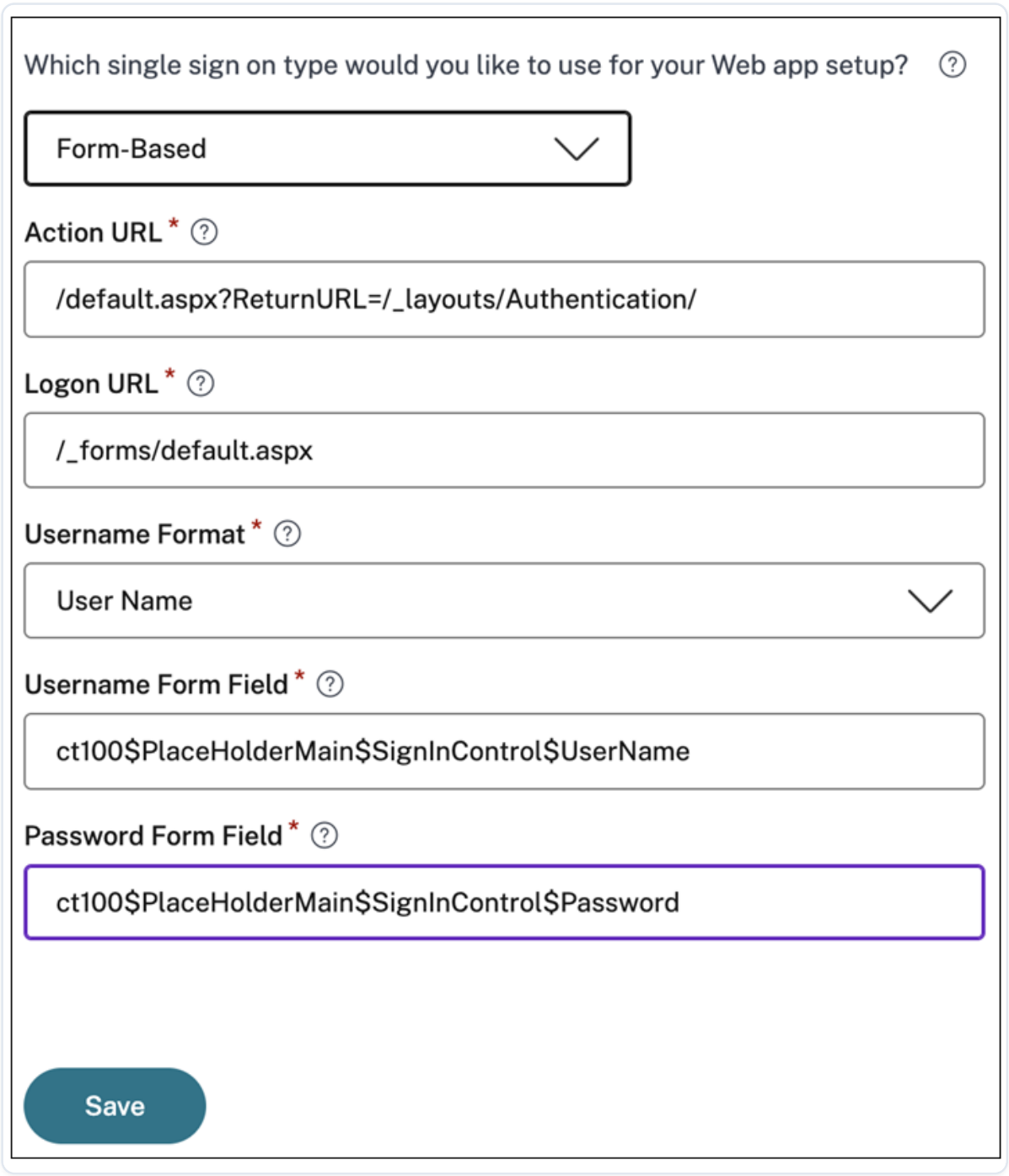


- **Basic** – Wenn Ihr Back-End-Server eine Basic-401-Challenge präsentiert, wählen Sie **Basic SSO**. Sie müssen keine Konfigurationsdetails für den **Basic** SSO-Typ angeben.
- **Kerberos** – Wenn Ihr Back-End-Server die Negotiate-401-Challenge präsentiert, wählen Sie **Kerberos**. Sie müssen keine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

Formularbasierte Details:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

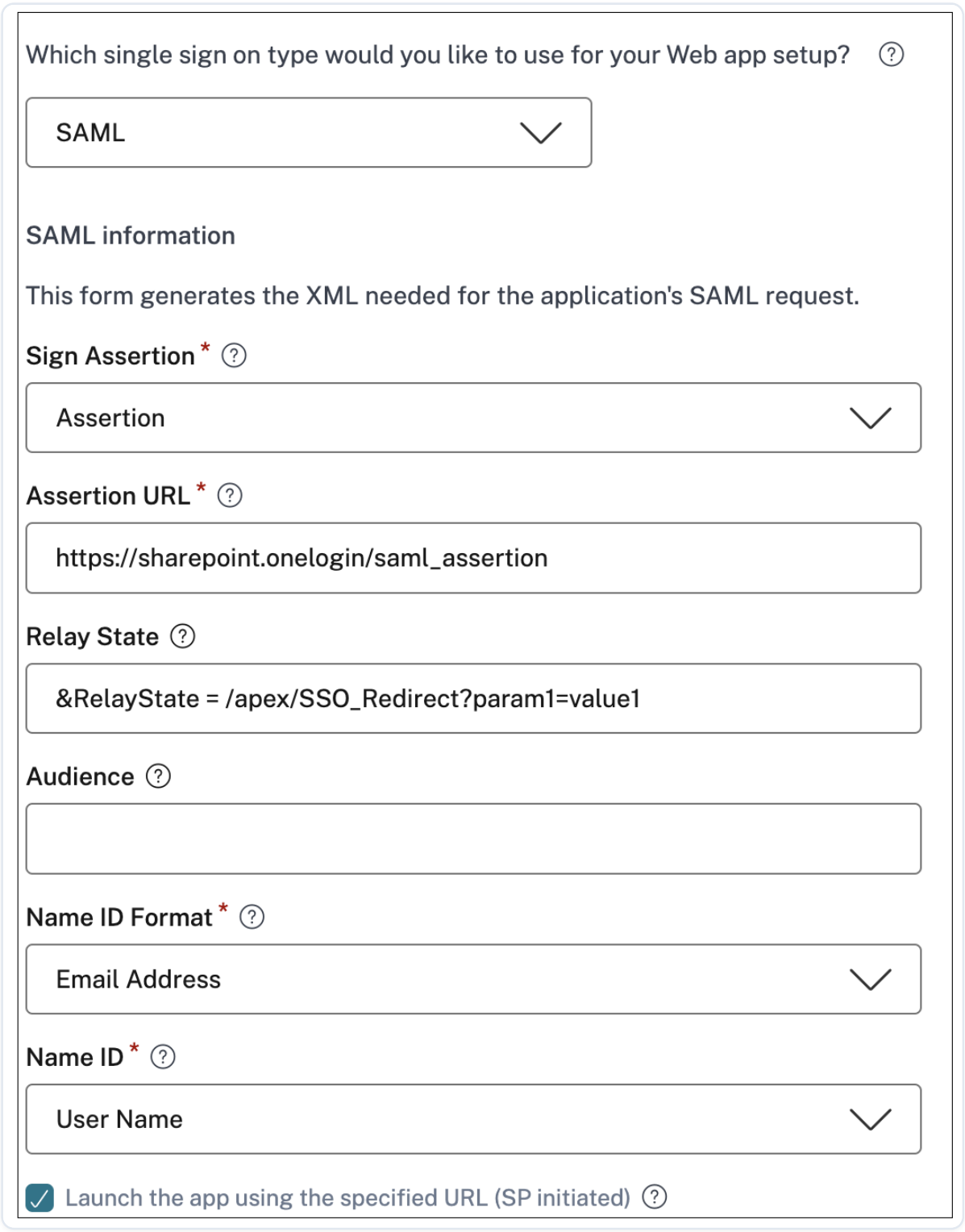


- **Aktions-URL** – Geben Sie die URL ein, an die das ausgefüllte Formular übermittelt wird.
- **Anmeldeformular-URL** – Geben Sie die URL ein, auf der das Anmeldeformular angezeigt wird.
- **Benutzername-Format** – Wählen Sie ein Format für den Benutzernamen aus.
- **Benutzername-Formularfeld** – Geben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

SAML:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie die folgenden Details im Abschnitt „Single Sign-On“ ein und klicken Sie auf Speichern.**



- **Assertion signieren** – Das Signieren der Assertion oder Antwort gewährleistet die Nachrichtenintegrität, wenn die Antwort oder Assertion an die vertrauende Partei (SP) übermittelt wird. Sie können **Assertion, Antwort, Beides** oder **Keine** auswählen.
- **Assertions-URL** – Die Assertions-URL wird vom Anwendungsanbieter bereitgestellt. Die SAML-Assertion wird an diese URL gesendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Relay State** – Der Parameter Relay State wird verwendet, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und an den Federation-Server der vertrauenden Partei weitergeleitet wurden. Relay State generiert eine einzige URL für die Benutzer. Benutzer können auf diese URL klicken, um sich bei der Zielanwendung anzumelden.
- **Zielgruppe** – Die Zielgruppe wird vom Anwendungsanbieter bereitgestellt. Dieser Wert bestätigt, dass die SAML-Assertion für die richtige Anwendung generiert wurde.
- **Name-ID-Format** – Wählen Sie das unterstützte Name-ID-Format aus.
- **Name-ID** – Wählen Sie die unterstützte Name-ID aus.

i. Fügen Sie unter **Erweiterte Attribute (optional)** zusätzliche Informationen über den Benutzer hinzu, die zur Anwendung für Zugriffssteuerungsentscheidungen gesendet werden.

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

- Sie können die SSO-Anmelde-URL unter **Anmelde-URL** kopieren und diese URL bei der Konfiguration von SSO auf dem SaaS-Anwendungsserver verwenden.
- Sie können das Zertifikat auch aus der Liste **Zertifikat** herunterladen und das Zertifikat bei der Konfiguration von SSO auf dem SaaS-Anwendungsserver verwenden.

11. Klicken Sie auf **Speichern** und dann auf **Fertig stellen**. Die App wird der Seite „Anwendungen“ hinzugefügt. Sie können eine App auf der Seite „Anwendungen“ bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu auf die Schaltfläche mit den Auslassungspunkten bei einer App und wählen Sie die entsprechenden Aktionen aus.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

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

Automatische Bereinigung von Routing-Einträgen bei Anwendungs-Löschung

Wenn Sie eine Anwendung konfigurieren, werden ihre Ziele (FQDNs oder Anwendungsdomänen) zur Routing-Tabelle hinzugefügt, die Secure Private Access für Routing-Entscheidungen verwendet. Wenn Sie eine Anwendung löschen, bereinigt Secure Private Access die Routing-Einträge basierend auf den folgenden Regeln:

- **Nicht referenzierte Einträge werden entfernt** – Wenn ein Routing-Eintrag (FQDN oder Anwendungsdomäne), der mit der gelöschten Anwendung verknüpft ist, von keiner anderen Anwendung referenziert wird, entfernt Secure Private Access ihn automatisch aus der Routing-Tabelle.
- **Gemeinsame Einträge bleiben erhalten** – Wenn ein Routing-Eintrag von mehr als einer Anwendung verwendet wird, führt das Löschen einer dieser Anwendungen nicht zur Entfernung des gemeinsamen Eintrags. Der Eintrag bleibt so lange in der Routing-Tabelle, wie mindestens eine aktive Anwendung darauf verweist.
- **Keine rückwirkende Entfernung** – Routing-Einträge werden nur im Rahmen einer Anwendungs-Löschung evaluiert und entfernt. Bestehende Einträge werden nicht rückwirkend entfernt, es sei denn, es wird bestätigt, dass sie von keiner Anwendung verwendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die Bereinigung wird automatisch ausgeführt, wenn eine Anwendung von der Seite „Anwendungen“ (über das Ellipsenmenü (...)) gelöscht wird. Es ist keine Administratoraktion erforderlich.
- Da gemeinsame Routing-Einträge beibehalten werden, unterbricht das Löschen einer Anwendung den Zugriff auf andere Anwendungen, die dasselbe Ziel gemeinsam nutzen, nicht.

Device Posture-Dienst mit agentenlosen Zugriffs-Apps

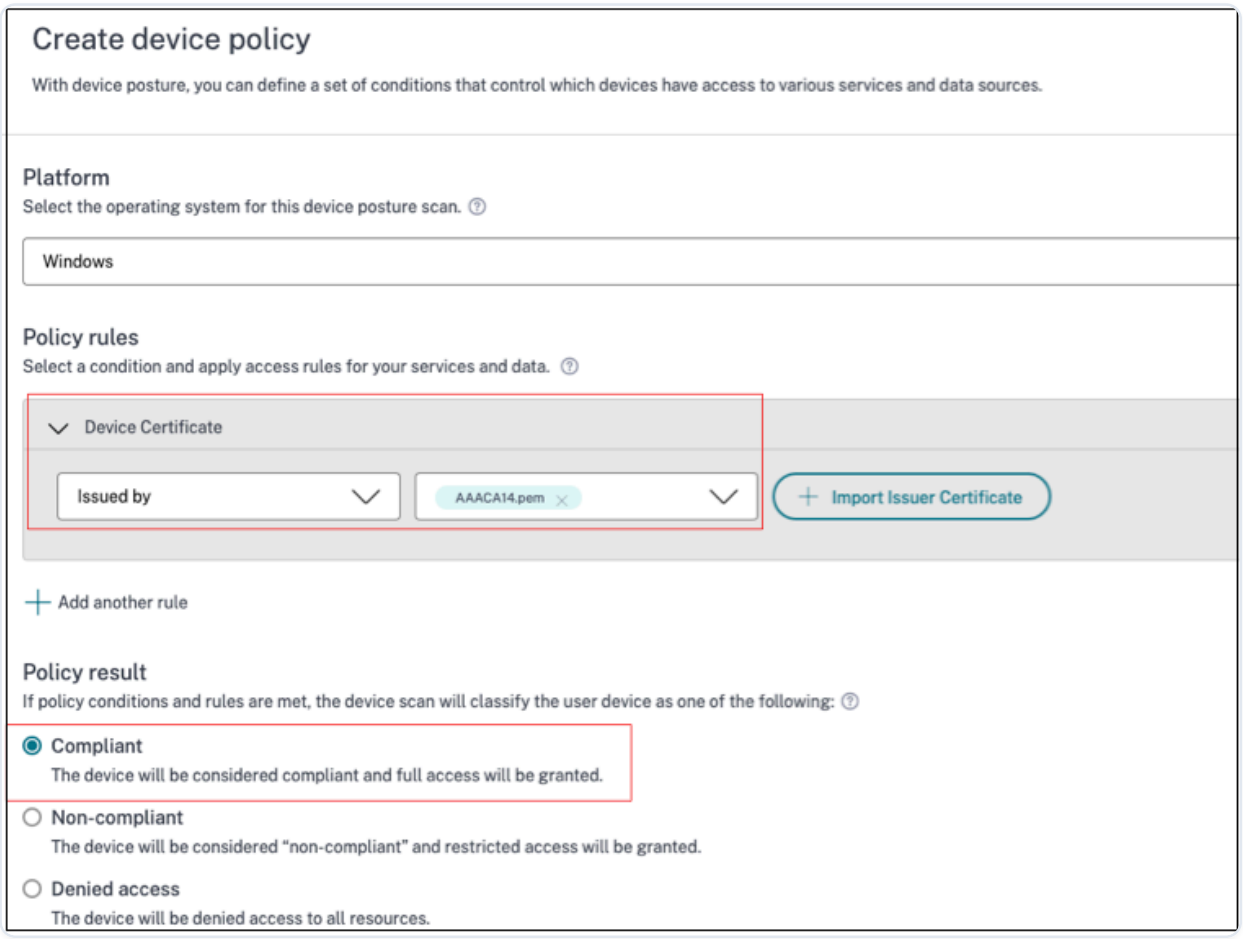
Citrix Secure Private Access mit agentenlosen Zugriffs-Apps kann in Kombination mit dem Device Posture-Dienst sicherstellen, dass nur konforme Geräte über agentenlosen Zugriff auf sensible Anwendungen zugreifen. Administratoren können den Zugriff auf nicht konforme oder nicht verwaltete Geräte basierend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

Schritte zum Aktivieren des agentenlosen Zugriffs nur für konforme Geräte

Um den agentenlosen Zugriff nur für konforme Geräte zu aktivieren, muss der Administrator die folgenden Schritte ausführen:

1. Erstellen Sie in der Verwaltungskonsole des Device Posture-Dienstes eine Device Posture-Richtlinie, um die Scan-Bedingungen für die Gerätehaltung wie Gerätezertifikat, Antivirus und Browser zu überprüfen, und wählen Sie dann **Konform** als Richtlinienergebnisaktion aus. Einzelheiten finden Sie unter (/de-de/device-posture.html#configure-device-posture).

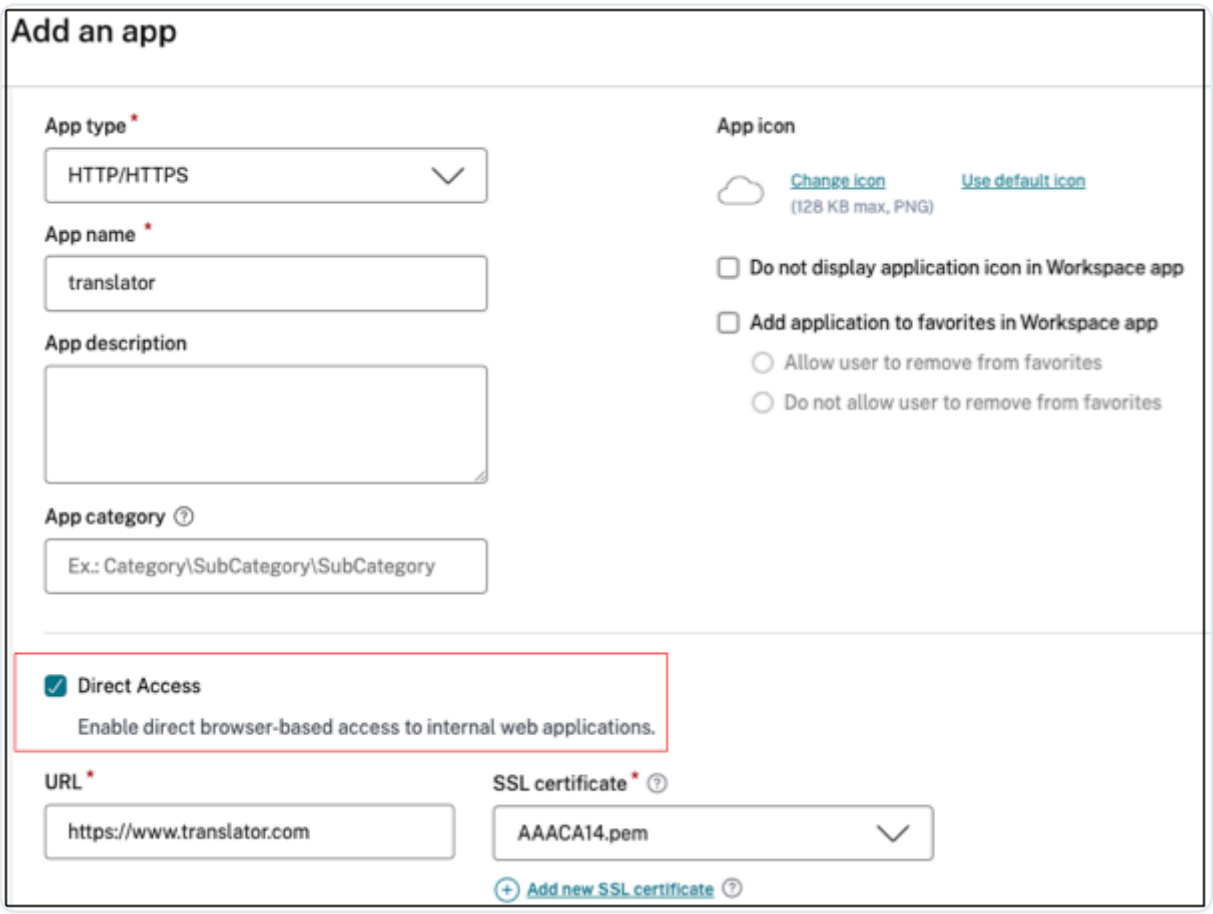
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Führen Sie in der Verwaltungskonsole von Secure Private Access Folgendes aus:

   - Erstellen Sie eine Anwendung, für die Sie den agentenlosen Zugriff aktivieren möchten. Weitere Informationen finden Sie unter Direkter Zugriff auf Unternehmens-Web-Apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

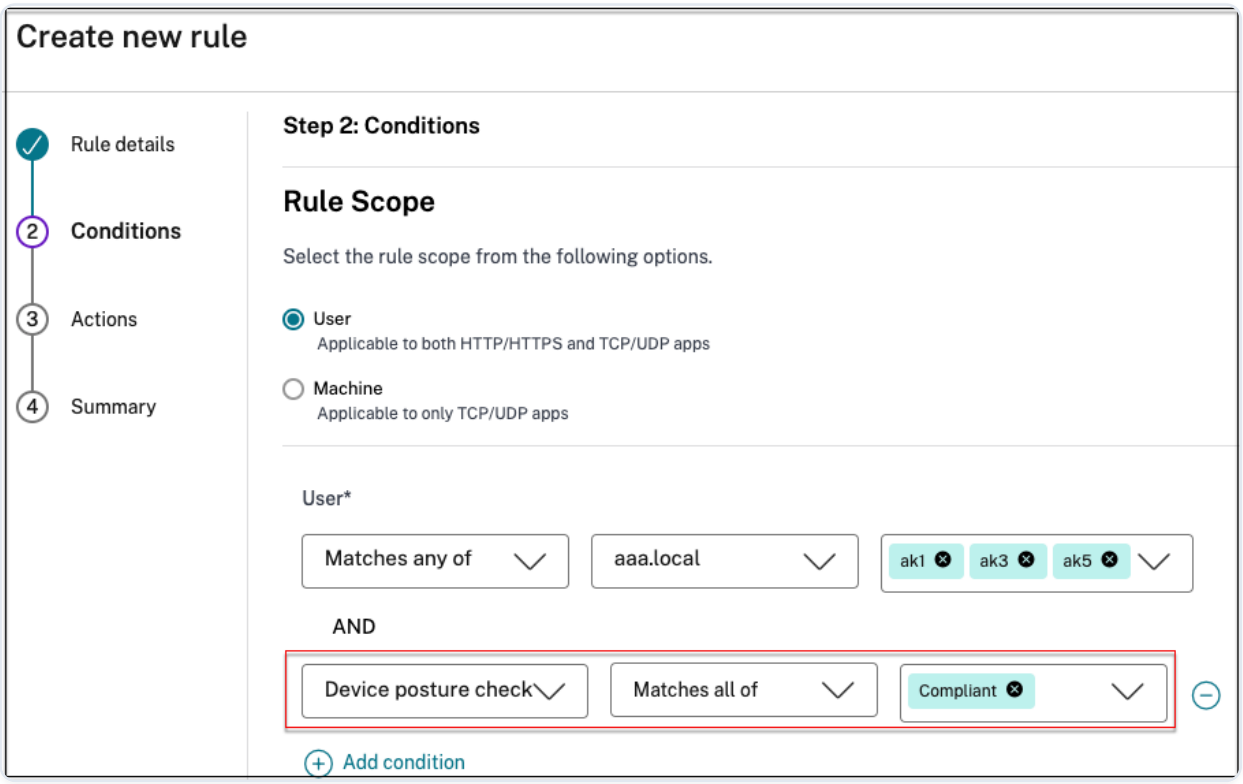


- Konfigurieren Sie Secure Private Access mit Device Posture. Wählen Sie unter **Regelbereich** die Option **Gerätehaltungsprüfung > Entspricht einem beliebigen Wert** und geben Sie das Tag **Compliant** ein. Dieses Tag wird vom Device Posture-Dienst gesendet.

HINWEIS:

Das Tag muss genau wie zuvor erfasst eingegeben werden, mit Großbuchstaben am Anfang (Compliant). Andernfalls funktionieren die Gerätehaltungsrichtlinien nicht wie beabsichtigt. Weitere Informationen finden Sie unter Citrix Secure Private Access-Konfiguration mit Device Posture.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sobald diese Konfiguration durchgeführt wurde, wird das Gerät basierend auf den Ergebnissen des Gerätehaltungs-Scans als konform, nicht konform oder abgelehnter Login getaggt, und der App-Zugriff wird entsprechend aktiviert.

Beispiel:

Angenommen, Sie haben eine Gerätehaltungsrichtlinie erstellt, um das Vorhandensein eines Gerätezertifikats auf einem Endpunktgerät zu überprüfen und dessen Anmeldestatus zu bestimmen. Sobald die Gerätehaltungsrichtlinien festgelegt und die Gerätehaltung aktiviert sind, treten die folgenden Aktionen auf, wenn ein Endbenutzer sich in seinem Store anmeldet.

1. Der Gerätehaltungs-Scan überprüft das Endpunktgerät auf das Vorhandensein eines Gerätezertifikats.
    - Wenn das Gerätezertifikat auf dem Gerät vorhanden ist, wird das Gerät als **compliant** getaggt.
    - Wenn das Gerätezertifikat auf dem Gerät nicht vorhanden ist, wird das Gerät als **non-compliant** getaggt.
2. Diese Informationen werden dann als Tags an den Citrix Secure Private Access-Dienst übermittelt.
3. Die Zugriffsrichtlinie wird basierend auf der Geräteklassifizierung ausgewertet.
    - Wenn das Gerät konform ist, wird der agentenlose Zugriff für die Apps zugelassen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn das Gerät nicht konform ist, wird der agentenlose Zugriff für die Apps deaktiviert.

Endbenutzererfahrung

Die Endbenutzererfahrung basiert auf der Klassifizierung des Geräts als konform oder nicht konform.

- **Konformes Gerät:**

  Der Benutzer kann die App für den agentenlosen Zugriff aus dem Store oder über den Browser mithilfe der App-URL starten.

- **Nicht konformes Gerät:**
  - Die App wird nicht im Store aufgeführt.
  - Der Benutzer kann die App nicht über den Browser mithilfe der App-URL starten.
  - Dem Benutzer wird eine Seite mit blockiertem Zugriff angezeigt.

Unterstützung für TCP/UDP-Anwendungen

Der Secure Private Access-Dienst ermöglicht Ihnen den Zugriff auf TCP/UDP-Anwendungen, die in Ihrer lokalen Umgebung vorhanden sind, entweder über einen nativen Browser oder eine native Clientanwendung über den auf Ihrem Computer ausgeführten Citrix Secure Access-Client. Einzelheiten finden Sie in den folgenden Abschnitten:

- Voraussetzungen
- Secure Private Access für TCP/UDP-Anwendungen konfigurieren
- Administratorkonfiguration – Citrix Secure Access-Client-basierter Zugriff auf HTTP/HTTPS-Anwendungen
- Adaptiver Zugriff auf TCP/UDP- und HTTP(S)-Anwendungen
- Beheben von IP-Adresskonflikten bei Anwendungsdomänen

Voraussetzungen

- Citrix Secure Access-Client – Einzelheiten finden Sie unter Citrix Secure Access-Client.
- Connector Appliance – Citrix empfiehlt die Installation von zwei Connector Appliances in einem Hochverfügbarkeits-Setup an Ihrem Ressourcenstandort. Der Connector kann entweder lokal, im Hypervisor des Rechenzentrums oder in der Public Cloud installiert werden. Weitere Informationen zur Connector Appliance und ihrer Installation finden Sie unter Connector Appliance for Cloud Services. Sie müssen eine Connector Appliance für TCP/UDP-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

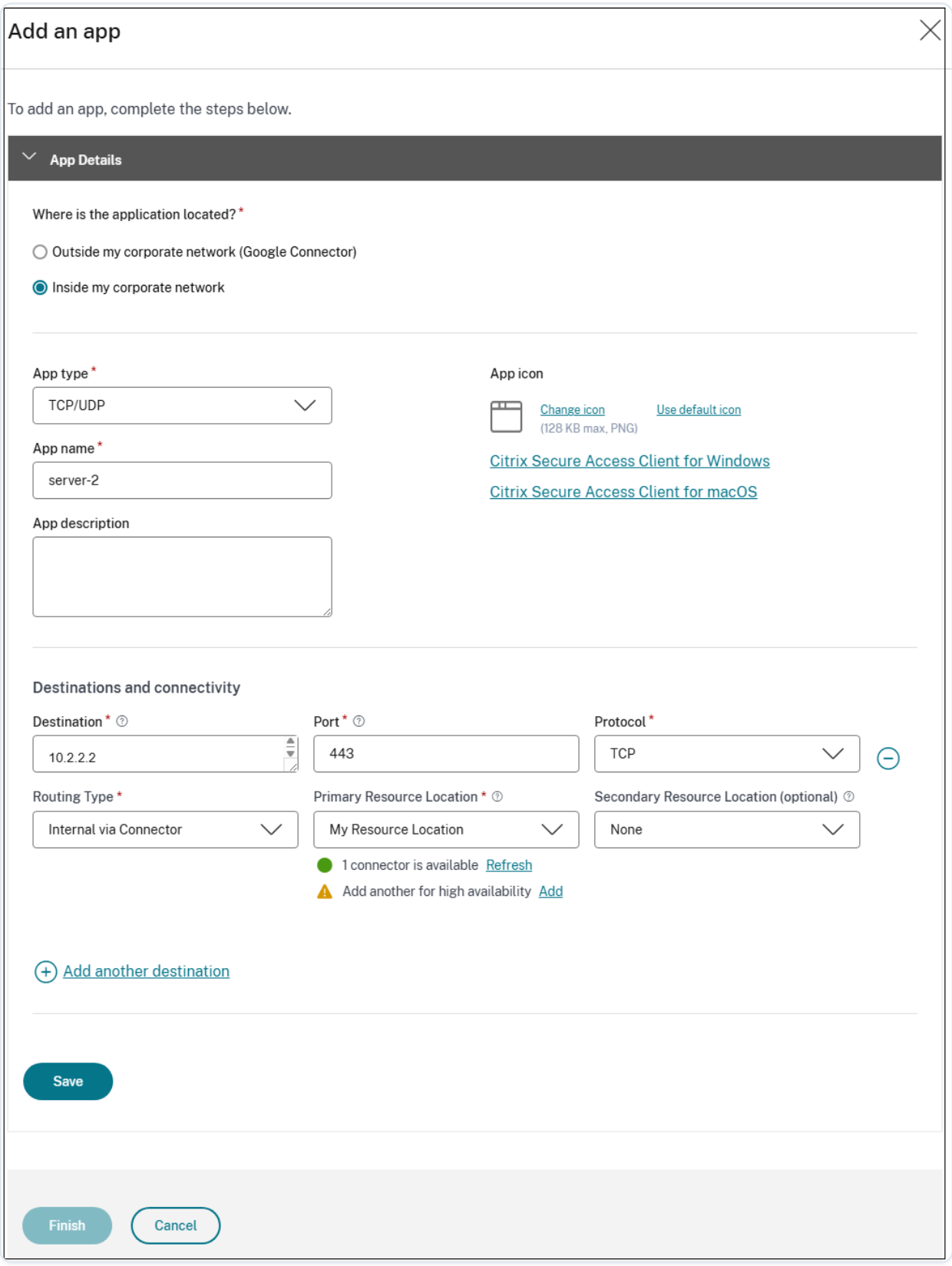
Anwendungen verwenden. Die Connector Appliance muss über eine DNS-Serverkonfiguration für die DNS-Auflösung verfügen.

Secure Private Access für TCP/UDP-Anwendungen konfigurieren

1. Melden Sie sich bei Citrix Cloud an und wählen Sie **Secure Private Access** aus.
2. Klicken Sie auf **Applications > App Configuration** und dann auf **Add an app**.
3. Klicken Sie im Abschnitt **Choose a template** auf **Skip**. Vorlagen sind nur für SaaS-Anwendungen verfügbar.

   Eine App ist eine logische Gruppierung von Zielen. Wir können eine App für mehrere Ziele erstellen – jedes Ziel bedeutet verschiedene Server im Backend. Zum Beispiel kann eine App einen SSH-, einen RDP-, einen Datenbankserver und einen Webserver haben. Sie müssen nicht eine App pro Ziel erstellen, aber eine App kann viele Ziele haben.
4. Wählen Sie im Abschnitt **App-Details** die Option **Innerhalb meines Unternehmensnetzwerks** aus, geben Sie die folgenden Details ein und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **App-Typ** – Wählen Sie TCP/UDP aus.
- **App-Name** – Name der Anwendung.
- **App-Symbol** – Ein App-Symbol wird angezeigt. Dieses Feld ist optional.
- **App-Beschreibung** – Beschreibung der App, die Sie hinzufügen. Dieses Feld ist optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Ziele** – IP-Adressen oder FQDNs der Back-End-Maschinen, die sich am Ressourcenstandort befinden. Ein oder mehrere Ziele können wie folgt angegeben werden.
  - **IP-Adresse v4**
  - **IP-Adressbereich** – Beispiel: 10.68.90.10-10.68.90.99
  - **CIDR** – Beispiel: 10.106.90.0/24
  - **FQDN der Maschinen oder Domänenname** – Einzelne oder Wildcard-Domäne. Beispiel: ex.destination.domain.com, *.domain.com

WICHTIG:

Endbenutzer können auf die Apps über FQDN zugreifen, auch wenn der Administrator die Apps über die IP-Adresse konfiguriert hat. Dies ist möglich, da der Citrix Secure Access™ Client einen FQDN in die tatsächliche IP-Adresse auflösen kann. Die folgende Tabelle enthält Beispiele für verschiedene Ziele und wie auf die Apps mit diesen Zielen zugegriffen werden kann:

ZIELEINGABE	SO GREIFEN SIE AUF DIE APP ZU
10.10.10.1-10.10.10.100	Der Endbenutzer soll auf die App nur über IP-Adressen in diesem Bereich zugreifen.
10.10.10.0/24	Der Endbenutzer soll auf die App nur über IP-Adressen zugreifen, die im IP-CIDR konfiguriert sind.
10.10.10.101	Der Endbenutzer soll auf die App nur über 10.10.10.101 zugreifen.
`*.info.citrix.com`	Der Endbenutzer soll auf Subdomains von `info.citrix.com` und auch auf `info.citrix.com` (die übergeordnete Domäne) zugreifen können. Zum Beispiel: `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Hinweis:** Das Platzhalterzeichen muss immer das erste Zeichen der Domäne sein, und es ist nur ein *. zulässig.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ZIELEINGABE	SO GREIFEN SIE AUF DIE APP ZU
info.citrix.com	Der Endbenutzer soll nur auf `info.citrix.com` und keine Subdomains zugreifen können. Zum Beispiel ist `sub1.info.citrix.com` nicht zugänglich.

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

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

PORTEINGABE	BESCHREIBUNG
*	Standardmäßig ist das Portfeld auf `"*"` (jeder Port) eingestellt. Die Portnummern von 1 bis 65535 werden für das Ziel unterstützt.
1300–2400	Die Portnummern von 1300 bis 2400 werden für das Ziel unterstützt.
38389	Nur die Portnummer 38389 wird für das Ziel unterstützt.
22,345,5678	Die Ports 22, 345, 5678 werden für das Ziel unterstützt.
1300–2400, 42000-43000,22,443	Der Portnummernbereich von 1300 bis 2400, 42000–43000 sowie die Ports 22 und 443 werden für das Ziel unterstützt.

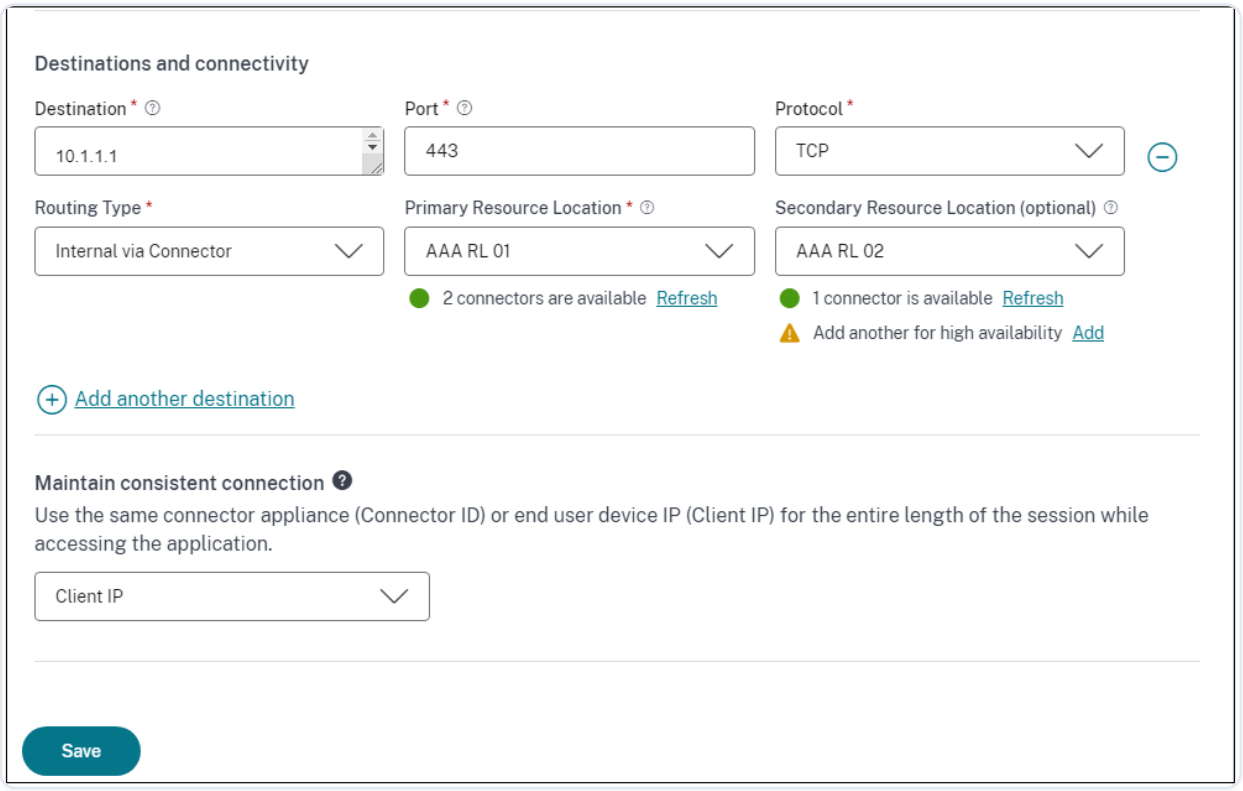
HINWEIS:

Der Wildcard-Port (*) kann nicht zusammen mit Portnummern oder -bereichen existieren.

- **Protokoll** – TCP/UDP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Im Abschnitt **App-Konnektivität** definieren Sie das Routing für die Anwendungen, wenn die Domänen extern oder intern über die Citrix Connector™ Appliance geroutet werden müssen.



- **Routing-Typ** – Wählen Sie eine der folgenden Optionen aus:
  - **Intern über Connector** – Die Anwendungen können extern sein, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
  - **Extern** – Der Datenverkehr fließt direkt ins Internet.
- **Primäre und sekundäre Ressourcenstandorte** – Administratoren können die hohe Verfügbarkeit von Anwendungen auch bei Ausfällen sicherstellen, indem sie einen sekundären Ressourcenstandort konfigurieren oder die Option **First Available** verwenden.
  - **Primärer Ressourcenstandort:** Wählen Sie den primären Ressourcenstandort aus, an dem die Anwendung gehostet wird. Alternativ können Administratoren die Option **First Available** unter **Primärer Ressourcenstandort** auswählen.
  - **First Available:** Die Option **First Available** stellt sicher, dass ein funktionierender Ressourcenstandort verwendet wird. Wenn **First Available** ausgewählt ist, leitet das System den Datenverkehr automatisch an den ersten verfügbaren Standort weiter. Dies gewährleistet einen kontinuierlichen Anwendungszugriff ohne manuelles Eingreifen. Wenn beispielsweise ResourceLocation1 nicht verfügbar, aber ResourceLocation2 erreichbar ist, wird ResourceLocation2 standardmäßig ausgewählt, um die Anwendung bereitzustellen.

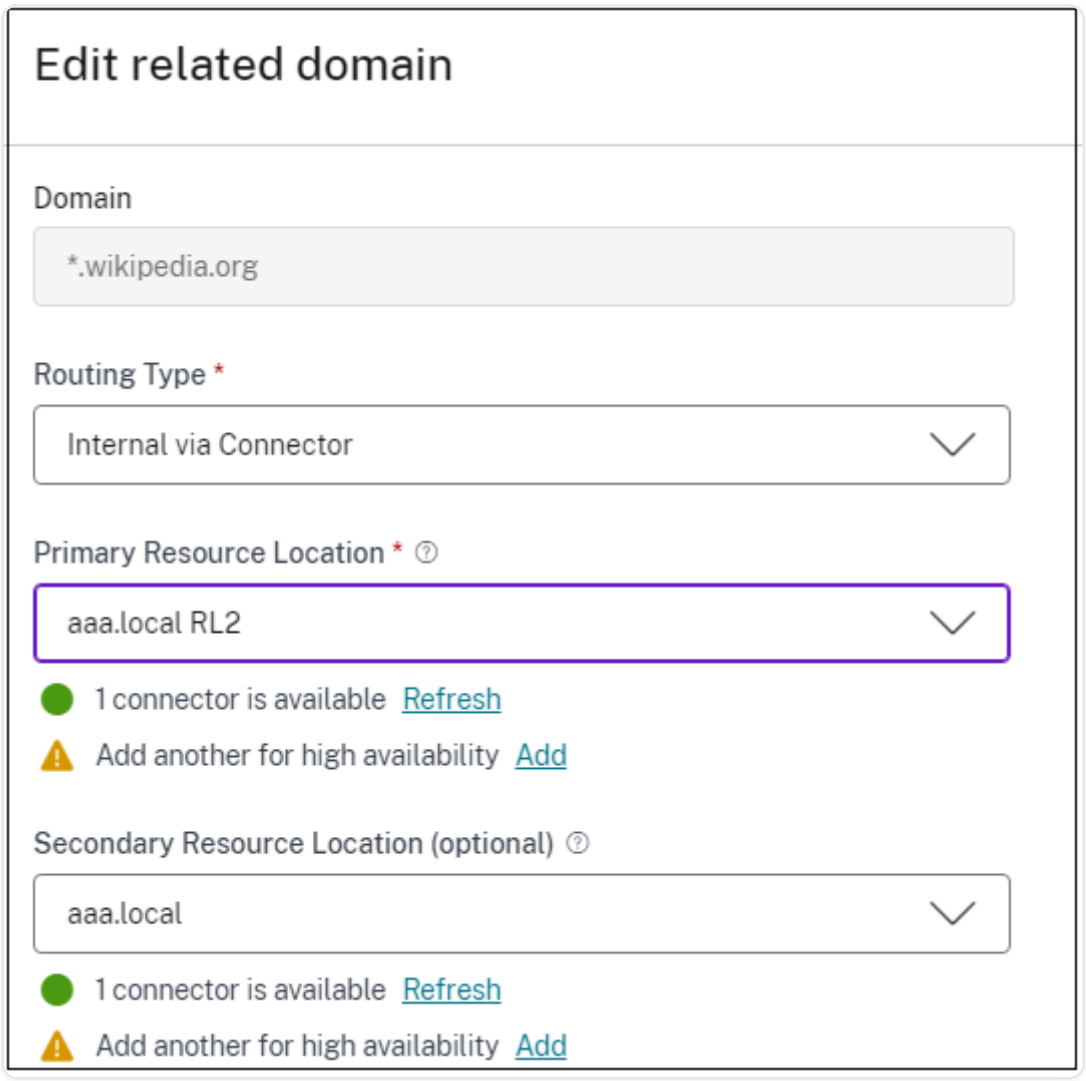
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sekundärer Ressourcenstandort** – Die Option **Sekundärer Ressourcenstandort** wird nur verfügbar, wenn ein primärer Ressourcenstandort explizit angegeben ist. Wenn der primäre Ressourcenstandort aus Gründen wie einem Ausfall der Connector Appliance oder eines Rechenzentrums nicht mehr verfügbar ist, fällt die Anwendung auf den angegebenen sekundären Ressourcenstandort aus. Der sekundäre Ressourcenstandort kann auch als Failover fungieren, selbst wenn die Anwendung in einem anderen Rechenzentrum gehostet wird.

Sie können auch einen primären und sekundären Ressourcenstandort festlegen oder die Option **First Available** für jede der zugehörigen Domänen auswählen.

a. Klicken Sie auf das Bearbeitungssymbol in der Spalte **Aktionen** der Tabelle „Zugehörige Domänen“.

b. Legen Sie den primären und sekundären Ressourcenstandort fest oder wählen Sie die Option **First Available** aus.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Das Festlegen des Backup-Ressourcenstandorts und die Verwendung der Funktion **First Available** befindet sich derzeit in der Vorschauphase.

- **Konsistente Verbindung aufrechterhalten** – Sie können Connector-Persistenz oder Client-IP-Persistenz für die TCP/UDP-Anwendungen aktivieren. Aktivieren Sie das Kontrollkästchen **Konsistente Verbindung aufrechterhalten** und wählen Sie dann eine der folgenden Optionen aus:
  - **Nicht verwenden:** Die Anwendung erfordert keine Persistenz. Die Anwendung kann mit jeder Quell-IP-Adresse arbeiten.
  - **Client-IP:** Die Anwendung verwendet für den Client bei jeder Verbindung dieselbe Quell-IP-Adresse.
  - **Connector-ID:** Die Anwendung verbindet sich bei jeder Sitzung mit derselben Connector Appliance. Wählen Sie eine der folgenden Optionen:

  Details zu konsistenten Verbindungen finden Sie unter Konsistente Verbindung beibehalten.

6. Klicken Sie auf **Speichern** und dann auf **Fertig stellen**.

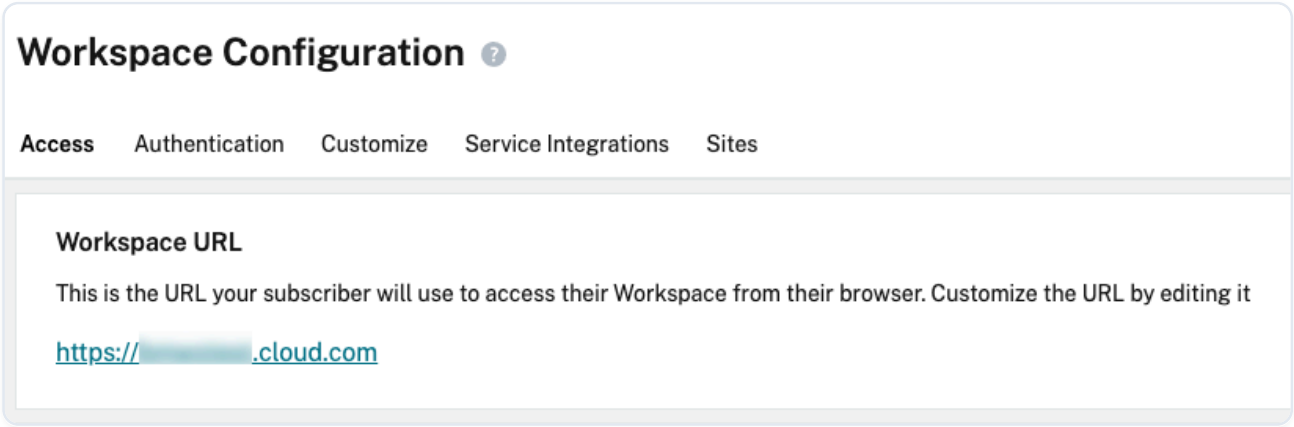
   Die App wird der Seite **Anwendungen** hinzugefügt. Sie können eine App auf der Seite **Anwendungen** bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu auf die Schaltfläche mit den Auslassungspunkten bei einer App und wählen Sie die entsprechenden Aktionen aus.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Um Benutzern Zugriff auf die Apps zu gewähren, müssen Administratoren Zugriffsrichtlinien erstellen. In Zugriffsrichtlinien fügen Administratoren App-Abonnenten hinzu und konfigurieren Sicherheitskontrollen. Details finden Sie unter Zugriffsrichtlinien erstellen.
- Informationen zum Konfigurieren der für die Benutzer erforderlichen Authentifizierungsmethoden finden Sie unter Identität und Authentifizierung einrichten.
- Um die mit den Benutzern zu teilende Store-URL abzurufen, klicken Sie im Citrix Cloud™-Menü auf **StoreFront Cloud** und wählen Sie die Registerkarte **Zugriff** aus.



Administratorkonfiguration – Clientbasierter Zugriff auf HTTP/HTTPS-Apps mit Citrix Secure Access

HINWEIS:

Um auf vorhandene oder neue HTTP/HTTPS-Apps mit dem Citrix Secure Access-Client zuzugreifen, müssen Sie mindestens eine (für Hochverfügbarkeit werden zwei empfohlen) Connector Appliance an Ihrem Ressourcenstandort installieren. Die Connector Appliance kann lokal, im Datacenter-Hypervisor oder in der Public Cloud installiert werden. Details zur Connector Appliance und ihrer Installation finden Sie unter Connector Appliance für Cloud Services.

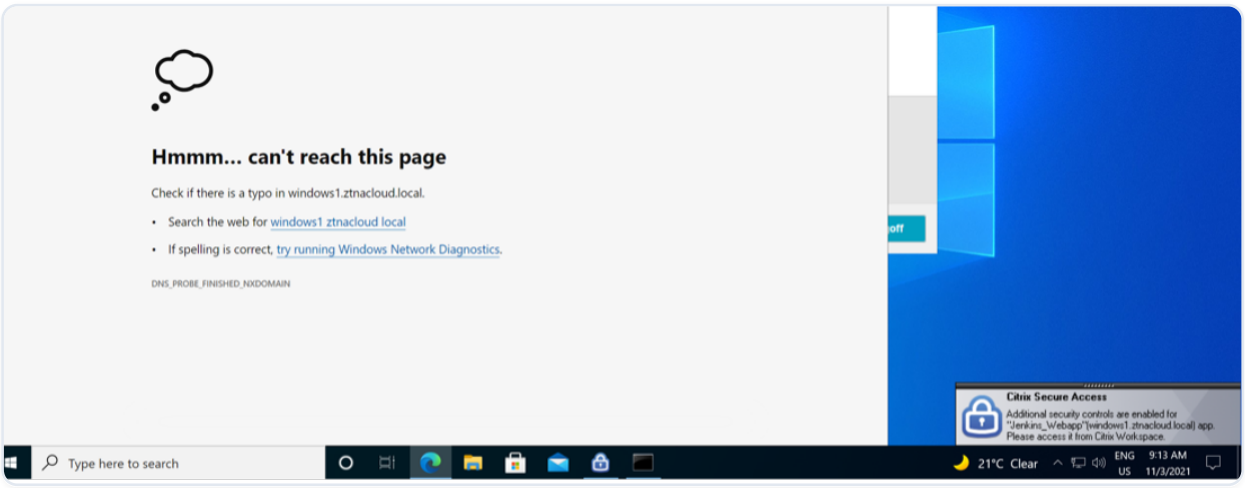
Voraussetzungen

- Zugriff auf Citrix Secure Private Access in Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinweise

- Interne Web-Apps, die mit erweiterten Sicherheitskontrollen erzwungen werden, können nicht über den Citrix Secure Access-Client aufgerufen werden.
- SaaS-Apps können nicht über den Citrix Secure Access-Client aufgerufen werden.
- Wenn Sie versuchen, auf eine HTTP(S)-Anwendung zuzugreifen, für die erweiterte Sicherheitskontrollen aktiviert sind, wird die folgende Pop-up-Meldung angezeigt: **Zusätzliche Sicherheitskontrollen sind für die App „App-Name“ (FQDN) aktiviert. Bitte greifen Sie über Citrix Workspace darauf zu.**



- Wenn Sie eine SSO-Erfahrung aktivieren möchten, greifen Sie über die Citrix Workspace-App oder das Webportal auf die Web-Apps zu.

Die Schritte zum Konfigurieren von HTTP(S)-Apps bleiben dieselben wie die bestehende Funktionalität, die unter Unterstützung für Unternehmens-Web-Apps erläutert wird.

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

Der adaptive Zugriff bietet Administratoren die Möglichkeit, den Zugriff auf geschäftskritische Apps basierend auf mehreren Kontextfaktoren wie Geräte-Posture-Check, Benutzer-Geo-Standort, Benutzerrolle und dem vom Citrix Analytics-Dienst bereitgestellten Risikowert zu steuern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

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

So erstellen Sie eine adaptive Zugriffsrichtlinie

Administratoren können den vom Administrator geführten Workflow-Assistenten verwenden, um Zero Trust Network Access für SaaS-Apps, interne Web-Apps und TCP/UDP-Apps im Secure Private Access-Dienst zu konfigurieren.

HINWEIS:

- Details zum Erstellen einer adaptiven Zugriffsrichtlinie finden Sie unter Zugriffsrichtlinien erstellen.
- Eine End-to-End-Konfiguration von Zero Trust Network Access für SaaS-Apps, interne Web-Apps und TCP/UDP-Apps im Secure Private Access-Dienst finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichtung.

Registrierungen für Anmelde- und Abmeldeskriptkonfiguration

Der Citrix Secure Access-Client greift auf die Anmelde- und Abmeldeskriptkonfiguration aus den folgenden Registrierungen zu, wenn er sich mit dem Citrix Secure Private Access Cloud-Dienst verbindet.

Registrierung: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- Pfad des Anmeldeskripts: SecureAccessLogInScript type REG_SZ
- Pfad des Abmeldeskripts: SecureAccessLogOutScript type REG_SZ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beheben von IP-Adresskonflikten bei Anwendungsdomänen

Ziele, die beim Erstellen einer App hinzugefügt werden, werden einer Hauptroutingtabelle hinzugefügt. Die Routingtabelle ist die maßgebliche Quelle für die Routingentscheidung, um den Verbindungsaufbau und den Datenverkehr zum richtigen Ressourcenstandort zu leiten.

- Die Ziel-IP-Adresse muss über alle Ressourcenstandorte hinweg eindeutig sein.
- Citrix empfiehlt, Überschneidungen von IP-Adressen oder Domänen in der Routingtabelle zu vermeiden. Falls eine Überschneidung auftritt, müssen Sie diese beheben.

Im Folgenden sind die Arten von Konfliktszenarien aufgeführt. **Complete Overlap** ist das einzige Fehlerszenario, das die Administratorkonfiguration einschränkt, bis der Konflikt behoben ist.

KONFLIKTSZENARIEN	VORHANDENER ANWENDUNGSDOMÄNENEINTRAG	NEUER EINTRAG DURCH APP-HINZUFÜGUNG	VERHALTEN
Teilmengenüberschneidung	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	Zulassen; Warnhinweis – Teilmengenüberschneidung der IP-Domäne mit vorhandenen Einträgen
Teilmengenüberschneidung	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	Zulassen; Warnhinweis – Teilmengenüberschneidung der IP-Domäne mit vorhandenen Einträgen
Partielle Überschneidung	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	Zulassen; Warnhinweis – Partielle Überschneidung der IP-Domäne mit vorhandenen Einträgen
Partielle Überschneidung	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	Zulassen; Warnhinweis –

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KONFLIKTSZENARIEN	VORHANDENER ANWENDUNGSDOMÄNENEINTRAG	NEUER EINTRAG DURCH APP-HINZUFÜGUNG	VERHALTEN
			Teilweise Überschneidung der IP-Domäne mit bestehenden Einträgen
Vollständige Überschneidung	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	Fehler; `<Completely overlapping IP domain's value>` IP-Domäne überschneidet sich vollständig mit bestehenden Einträgen. Ändern Sie den bestehenden Routing-IP-Eintrag oder konfigurieren Sie ein anderes Ziel
Vollständige Überschneidung	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	Fehler; `<Completely overlapping IP domain's value>` IP-Domäne überschneidet sich vollständig mit bestehenden Einträgen. Ändern Sie den bestehenden Routing-IP-Eintrag oder konfigurieren Sie ein anderes Ziel
Exakte Übereinstimmung	20.20.20.0/29 RL1	20.20.20.0/29	Zulassen; Domänen existieren bereits in der Domänen-Routing-Tabelle. Änderungen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KONFLIKTSZENARIEN	VORHANDENER ANWENDUNGSDOMÄNENEINTRAG	NEUER EINTRAG DURCH APP-HINZUFÜGUNG	VERHALTEN
			aktualisieren die Domänen-Routing-Tabelle

HINWEIS:

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

  Wenn im Abschnitt **App-Details** keine Fehler vorliegen, kann der Administrator die App-Details speichern. Wenn jedoch im Abschnitt **App-Konnektivität** die Ziele eine Teilmenge und eine teilweise Überschneidung miteinander oder mit vorhandenen Einträgen in der Hauptroutingtabelle aufweisen, wird eine Warnmeldung angezeigt. In diesem Fall kann der Administrator wählen, ob er den Fehler beheben oder mit der Konfiguration fortfahren möchte.
- Citrix empfiehlt, eine saubere **Anwendungsdomänentabelle** zu führen. Es ist einfacher, neue Routing-Einträge zu konfigurieren, wenn die IP-Adressdomänen in geeignete, nicht überlappende Blöcke unterteilt sind.

Wichtige Hinweise

- Der Zugriff auf eine bestehende Web-App, für die erweiterte Sicherheit aktiviert ist, wird über den Secure Access Client verweigert. Es wird eine Fehlermeldung angezeigt, die vorschlägt, sich mit der Citrix Workspace-App anzumelden.
- Richtlinienkonfigurationen für Web-Apps basierend auf dem Benutzerrisikowert, der Geräte-Posture-Prüfung usw. über die Citrix Workspace-App sind beim Zugriff auf die App über den Secure Access Client anwendbar.
- Die an eine Anwendung gebundene Richtlinie gilt für alle Ziele in der Anwendung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Always On vor der Windows-Anmeldung

Die Secure Private Access Always On-Konnektivität stellt sicher, dass ein verwaltetes Gerät vor (nur Maschinentunnel) und nach der Windows-Anmeldung immer mit einem Unternehmensnetzwerk verbunden ist. Die Always On-Funktion stellt einen VPN-Tunnel auf Maschinenebene her, bevor sich ein Benutzer bei einem Windows-System anmeldet. Nachdem sich der Benutzer angemeldet hat, wird der VPN-Tunnel auf Maschinenebene durch einen VPN-Tunnel auf Benutzerebene ersetzt. Der Anwendungszugriff basiert auf Richtlinien, die der Maschine für den Maschinentunnel und dem Benutzer für den Benutzertunnel zugewiesen sind.

Die Secure Private Access Always On vor der Windows-Anmeldung (Maschinentunnel)-Funktion wird auf den folgenden Maschinen unterstützt:

- In die Active Directory-Domäne eingebundene Windows-Maschinen
- Microsoft Entra ID hybrid in die Domäne eingebundene Windows-Maschinen

Die Always On vor der Windows-Anmeldung wird mithilfe der computergerätebasierten Zertifikatsauthentifizierung mit Active Directory authentifiziert.

Das Gerätezertifikat wird von einer Active Directory Enterprise-Zertifizierungsstelle (CA) ausgestellt. Das Gerätezertifikat ist für jede in die Domäne eingebundene Windows-Maschine eindeutig.

Hinweis:

- Die einstufige bis mehrstufige Microsoft Enterprise-Zertifizierungsstelle wird unterstützt.
- Die Secure Private Access Always On nach der Windows-Anmeldung (Benutzertunnel) wird durch eine der folgenden automatischen Anmeldeauthentifizierungsmethoden für Active Directory erreicht:
    - Single Sign-On (SSO) beim Citrix Secure Access™ Client unter Verwendung der Active Directory-Anmeldeinformationen, die während der Windows-Anmeldung bereitgestellt wurden. SSO funktioniert nicht, wenn ein zweiter Faktor konfiguriert ist.
    - Kerberos-basiertes SSO mit Citrix Gateway. Weitere Informationen finden Sie unter Ein lokales Citrix Gateway als Identitätsanbieter mit Citrix Cloud verbinden und adaptive Authentifizierung bereitstellen.
    - Adaptive Authentifizierungskonfiguration. Weitere Informationen finden Sie unter Adaptive Authentifizierung bereitstellen.

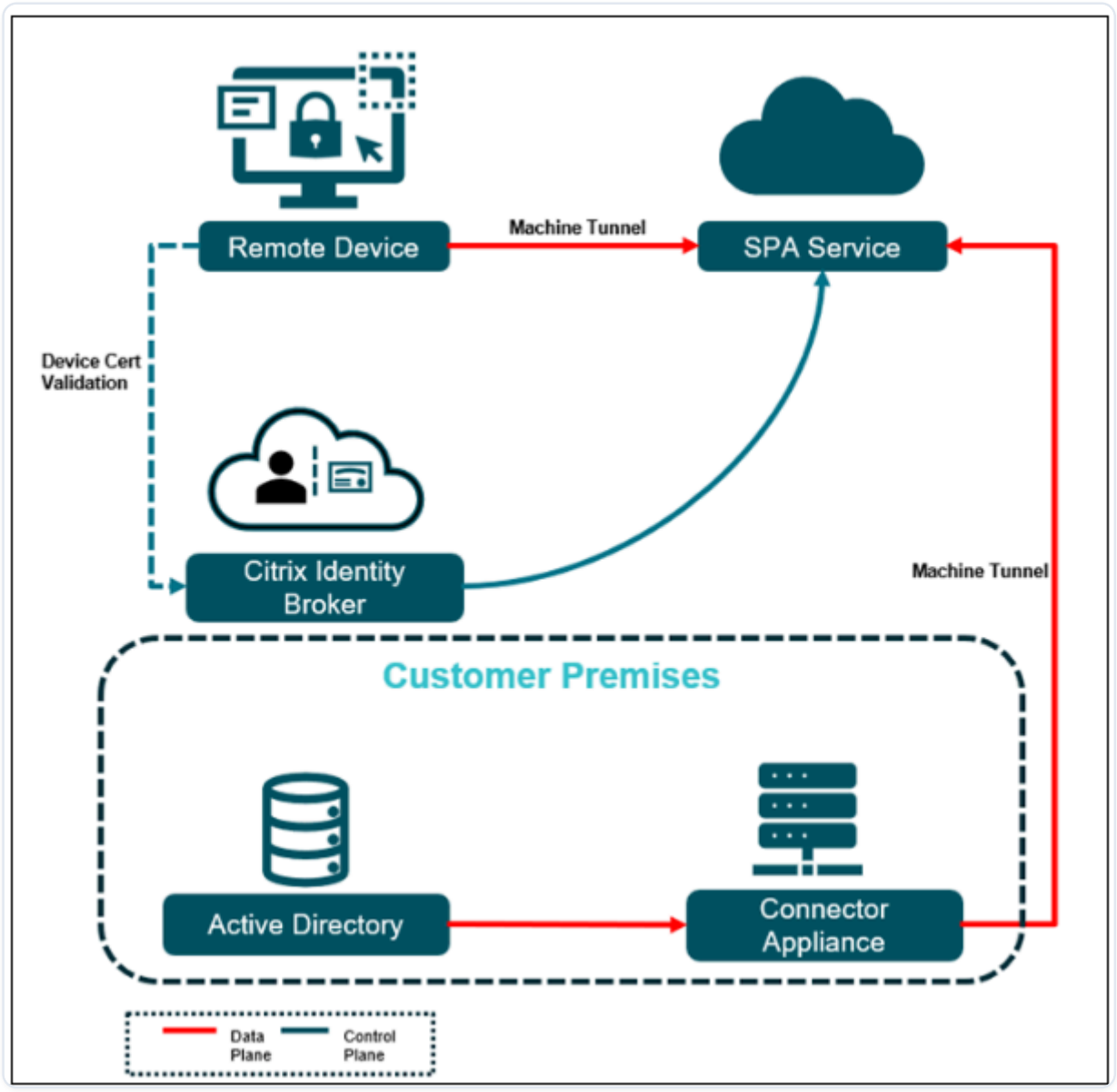
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Secure Private Access Always On nach der Windows-Anmeldung (Benutzertunnel) wird durch die folgende automatische Anmeldeauthentifizierungsmethode für Microsoft Entra ID hybrid eingebundene Maschinen erreicht: SSO mit Primary Refresh Token (PRT) der Microsoft Entra ID-Authentifizierung.

  Endbenutzer immer zur Eingabe ihrer Anmeldeinformationen auffordern deaktivieren.

Wie funktioniert Always On?

Das folgende Diagramm veranschaulicht den Workflow der Always On vor Windows-Anmeldung-Funktion.



- Der Citrix Identity Broker überprüft das Gerätezertifikat, um das Gerät unmittelbar nach dem Start zu authentifizieren. Die folgenden Schritte sind die Überprüfung des Gerätezertifikats:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Der Client präsentiert das Gerätezertifikat basierend auf CA-Zertifikaten, die in die Secure Private Access-Administrationskonsole hochgeladen wurden.
    - Der Citrix Identitätsanbieter führt eine gerätezertifikatbasierte Authentifizierung durch.
    - Der Citrix Identitätsanbieter überprüft die folgenden Details:
        - Signatur des Gerätezertifikats
        - CRL-basierte Überprüfung des Gerätezertifikat-Widerrufs
        - Gerätezertifikat gegen Active Directory-Computerobjekt validieren

- Nach erfolgreicher Überprüfung des Gerätezertifikats wird ein sicherer Maschinentunnel zwischen dem Gerät und den Ressourcen im Unternehmensnetzwerk basierend auf der Zugriffsrichtlinie eingerichtet.
- Nachdem der Zugriff auf Active Directory zugelassen wurde, authentifiziert die Windows-Anmeldung die Benutzeranmeldeinformationen mit Active Directory und unterstützt den Ablauf von Passwörtern sowie die Passwortänderung.
- Nach der Windows-Anmeldung wird der Maschinentunnel automatisch durch den Benutzertunnel mit Autologon ersetzt. Bei einem Fehler des Benutzertunnels/trennen fällt die Verbindung auf den Maschinentunnel zurück.
- Die Autologin-Funktion wird für die Active Directory- und hybride Microsoft Entra ID-Umgebung unterstützt.

Active Directory- und Microsoft Entra ID Hybrid AD-Konfiguration

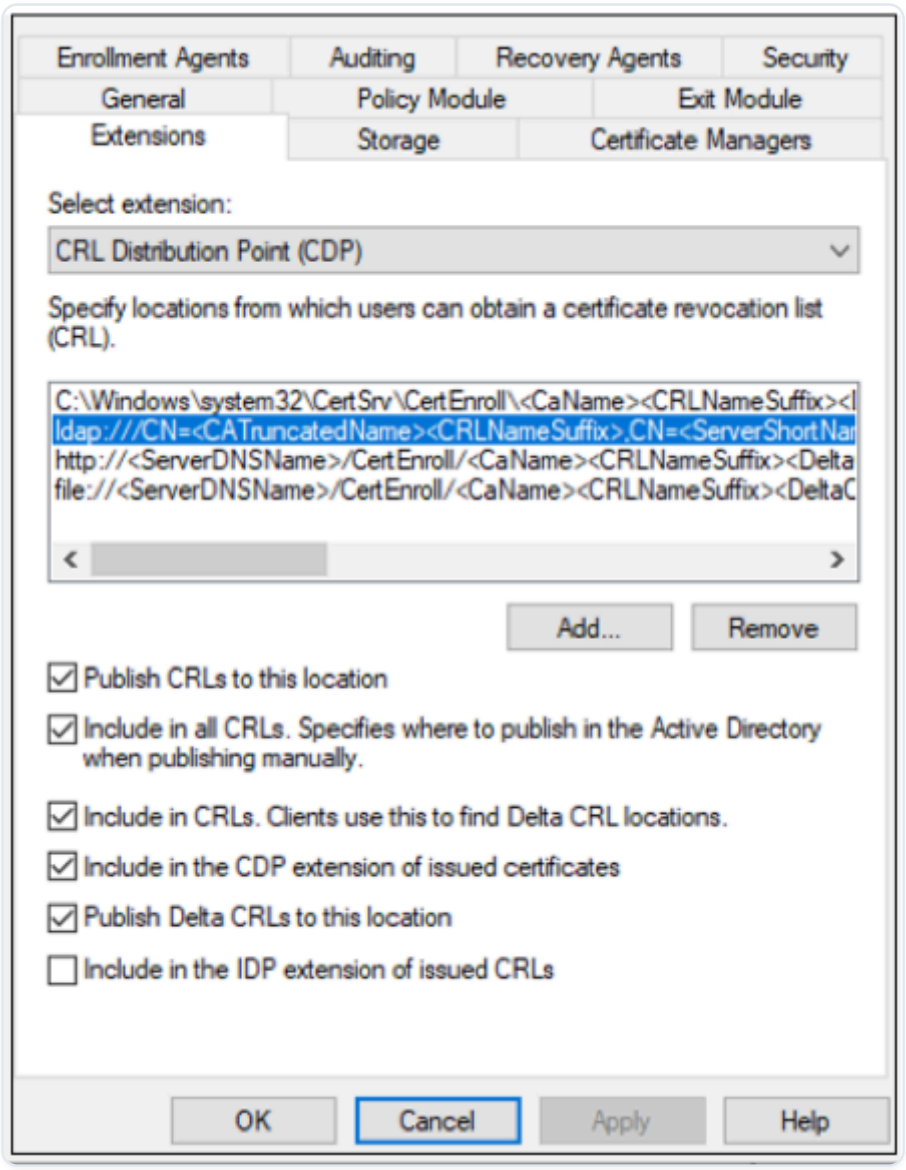
Die Windows-Maschinen müssen als Voraussetzung für Always On in Active Directory oder Microsoft Entra ID Hybrid beigetreten sein. Die Active Directory Enterprise-Zertifizierungsstelle ist erforderlich, um das Gerätezertifikat für die Always On-Maschinenauthentifizierung auszustellen. Der Zertifikatswiderruf wird basierend auf der CDP-Erweiterung mit LDAP-URL-Konfiguration in der Zertifizierungsstelle überprüft.

Konfiguration der Gerätezertifikatregistrierung

Die folgenden Schritte sind bei der Gerätezertifikatregistrierung erforderlich:

1. Die Active Directory Enterprise-Zertifizierungsstelle stellt ein Gerätezertifikat für die Maschinenauthentifizierung aus.
2. Die Zertifizierungsstelle muss die LDAP-URL für die CRL-Verteilungspunkt (CDP)-Erweiterung veröffentlicht haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



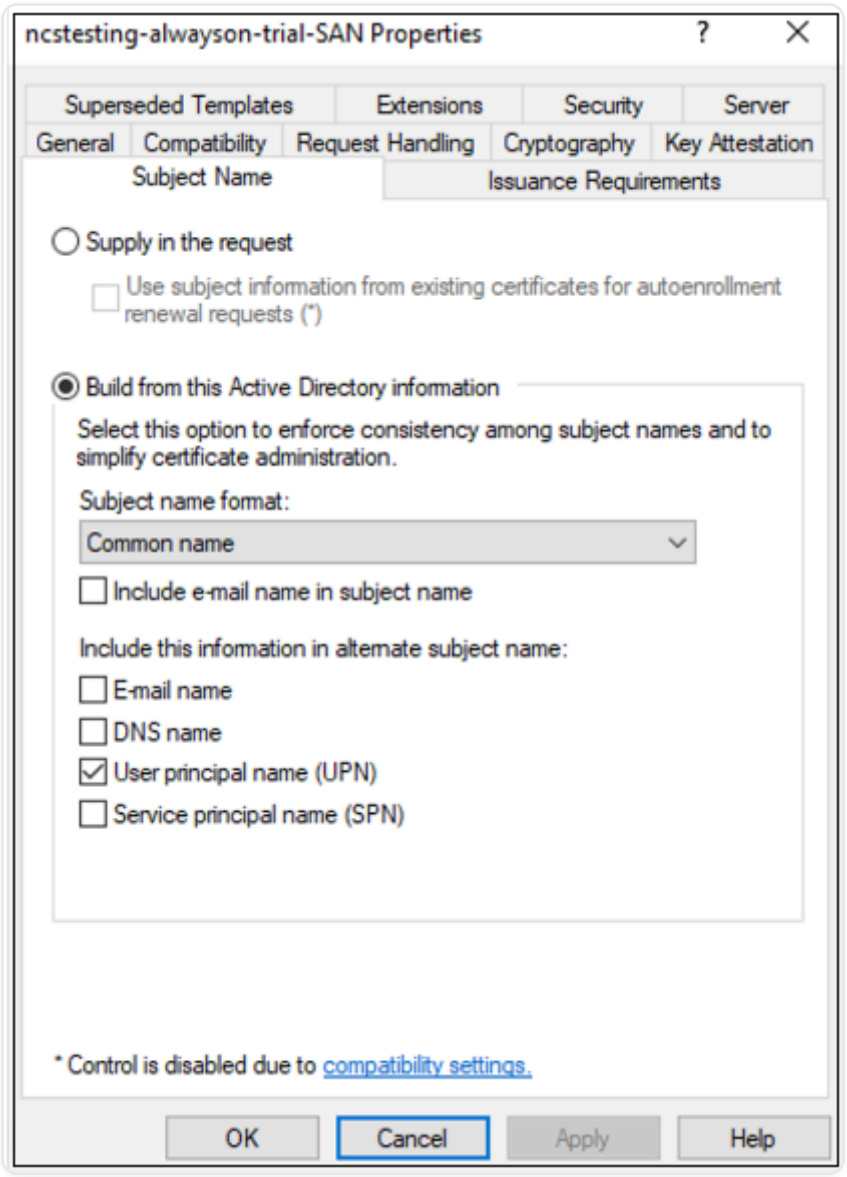
3. Eine Zertifikatvorlage in dieser Zertifizierungsstelle muss erstellt werden, um das Gerätezertifikat mit den folgenden Details zu registrieren.

   a. Öffnen Sie das Zertifikatvorlagen-Snap-In und duplizieren Sie entweder die Vorlage **Computer** oder **Workstation-Authentifizierung** (bevorzugt).

   b. Geben Sie einen neuen Namen für das Zertifikat an.

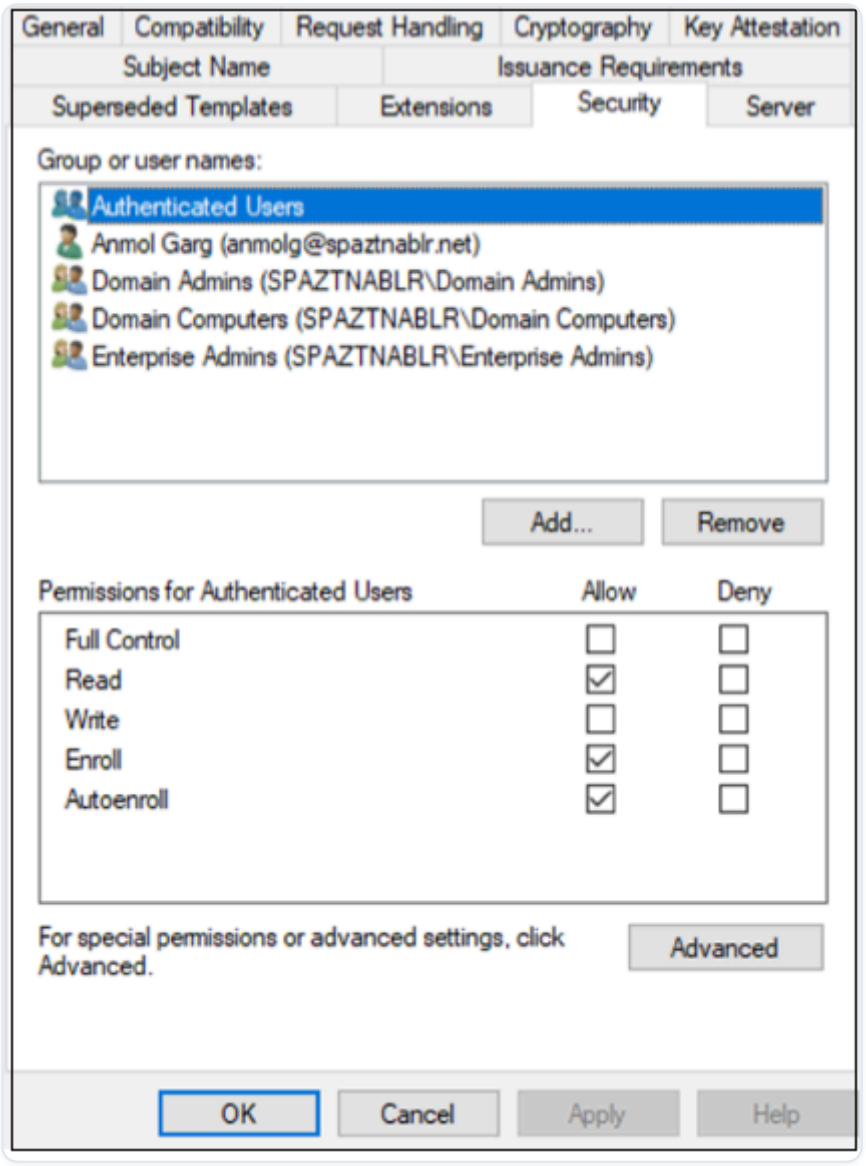
   c. Wechseln Sie zur Registerkarte **Antragstellername**, ändern Sie die Einstellung **Antragstellername-Format** in **Allgemeiner Name**, und aktivieren Sie **Benutzerprinzipalname (UPN)**, der in den alternativen Antragstellernamen aufgenommen werden soll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. Wechseln Sie zur Registerkarte **Sicherheit** und fügen Sie eine Sicherheitsgruppe hinzu (die nur Computerkonten enthält), für die Sie die neue Zertifikatvorlage automatisch registrieren möchten. Wählen Sie die hinzugefügte Gruppe aus und wählen Sie **Zulassen** für **Automatische Registrierung**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

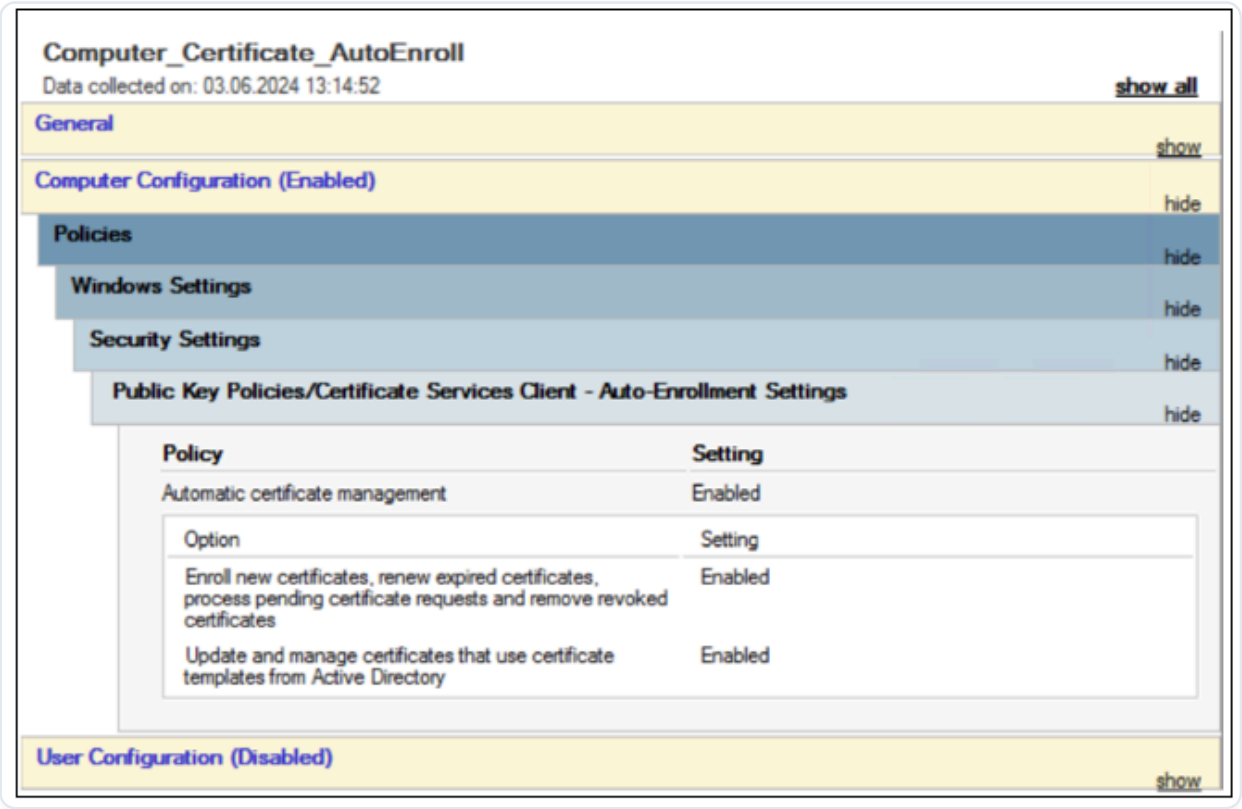


HINWEIS:

Im vorhergehenden Bild dürfen **Authentifizierte Benutzer** (alle Computerobjekte) die neue Zertifikatvorlage registrieren/automatisch registrieren.

e. (Optional) Erstellen Sie ein Gruppenrichtlinienobjekt (GPO), das die automatische Zertifikatsregistrierung ermöglicht, und binden Sie es an eine Organisationseinheit (OU) oder auf Domänenebene.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Secure Private Access-Konfiguration

Die folgenden Abschnitte bieten weitere Informationen zur Konfiguration von Secure Private Access.

Always On vor der Windows-Anmeldung konfigurieren (Maschinentunnel)

1. Navigieren Sie in der Secure Private Access-Administratorkonsole zu **Einstellungen > Zertifikatspeicher**.

   HINWEIS:

   Wir empfehlen, die Option **Maschinenbasierte Authentifizierung** unter **Einstellungen > Zertifikatspeicher** anstelle von **Einstellungen > Maschinenbasierte Authentifizierung** zu verwenden. Die Option **Einstellungen > Maschinenbasierte Authentifizierung** wird in der kommenden Service-Version entfernt.

2. Klicken Sie auf der Seite **Zertifikate** auf die Registerkarte **Maschinenauthentifizierung**.

   Der Umschalter **Maschinenebene-Tunnel vor Benutzeranmeldung erzwingen** ist standardmäßig für die Funktion Always On vor der Windows-Anmeldung aktiviert.

3. CA-Zertifikat hochladen: Klicken Sie auf **Zertifikat hinzufügen**, wählen Sie das Zertifikat aus und klicken Sie auf **Öffnen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Geben Sie unter **Name** einen Namen für das Zertifikat ein.
5. Navigieren Sie unter **Zertifikatsdatei** zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.

    - Zertifikate sowohl für Root-CA als auch für Intermediate-CA werden unterstützt. Die hochzuladenden Zertifikate müssen im PEM-Format vorliegen und die gesamte Kette enthalten. Das Zertifikat muss beginnend mit dem Zwischenzertifikat bis zur Root-CA generiert werden.
    - Wenn das Zertifikat im CER-Format vorliegt, führen Sie den folgenden Befehl in einem Linux- oder Mac-Terminal aus, um das Zertifikat in das PEM-Format zu konvertieren. Nachdem Sie das Zertifikat in das PEM-Format konvertiert haben, laden Sie das Zertifikat in der Secure Private Access-Benutzeroberfläche hoch.

      ```
      openssl x509 -in /Users/t_abhishes2/Downloads/cert12.crt out/Users/t_abhishes2/Downloads/cer_pem12_ao.pem
      ```

6. Klicken Sie auf **Speichern**.

    Das Zertifikat wird der Liste der verfügbaren Zertifikate auf der Registerkarte **Maschinenauthentifizierung** hinzugefügt.
7. Erstellen Sie eine TCP/UDP-Anwendung, um als TCP/UDP-Server auf Active Directory zuzugreifen. Zum Beispiel Active Directory-Domäne, IP-Adresse und Ports. Dies ist für die Windows-Benutzeranmeldung mit AD-Anmeldeinformationen. Details zum Erstellen einer TCP/UDP-App finden Sie unter Admin-Konfiguration – Citrix Secure Access Client-basierter Zugriff auf TCP/UDP-Apps.
8. Erstellen Sie bei Bedarf zusätzliche Anwendungen, auf die vor der Windows-Anmeldung und vor der Migration des Tunnels auf Benutzerebene zugegriffen werden soll.
9. Erstellen Sie eine Zugriffsrichtlinie und gewähren Sie der in die Domäne eingebundenen Maschine oder ihrer AD-Gruppe Zugriff.

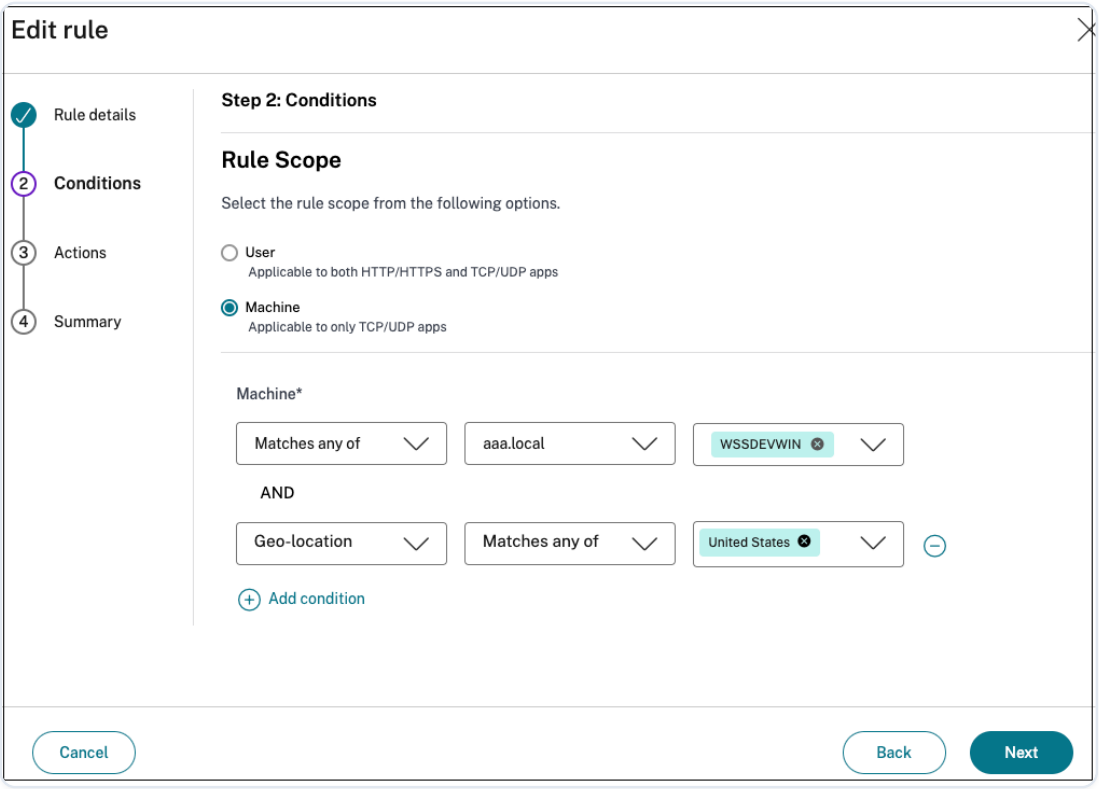
    a. Klicken Sie in der Secure Private Access-Administratorkonsole auf **Zugriffsrichtlinien** und dann auf **Richtlinie erstellen**.
    b. Geben Sie den Richtliniennamen und die Beschreibung der Richtlinie ein.
    c. Wählen Sie unter **Anwendungen** die App oder den Satz von Apps aus, für die diese Richtlinie erzwungen werden soll.
    d. Klicken Sie auf **Regel erstellen**, um Regeln für die Richtlinie zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein und klicken Sie dann auf **Weiter**.
- Wählen Sie unter **Regelbereich** die Option **Maschine** aus.

> **HINWEIS:**
>
> Wenn Sie eine Maschine auswählen, sind die Zugriffsrechte eingeschränkt, da der Tunnel auf Maschinenebene auf einer Ein-Faktor-Authentifizierung basiert.

- Wählen Sie die passende Bedingung und die Domäne aus und suchen Sie nach der Maschine/den Gruppen, auf die die Richtlinie angewendet werden soll. Fügen Sie bei Bedarf weitere Bedingungen hinzu. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
  - **Entspricht einem der folgenden** – Nur die Computer/Gruppen, die einem der im Feld aufgeführten Namen entsprechen und zur ausgewählten Domäne gehören, erhalten Zugriff.
  - **Entspricht keinem** – Alle Computer/Gruppen, außer den im Feld aufgeführten und zur ausgewählten Domäne gehörenden, erhalten Zugriff.



10. Wählen Sie eine der folgenden Aktionen aus, die basierend auf der Bedingungsbewertung angewendet werden soll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

11. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
12. (Optional) Erstellen Sie zusätzliche Regeln für den geografischen Standort und die Netwerkstandort usw. Weitere Informationen finden Sie unter Zugriffsrichtlinie konfigurieren.

    Die Richtlinie wird auf der Seite „Zugriffsrichtlinien“ aufgeführt. Standardmäßig wird der Richtlinie eine Prioritätsreihenfolge zugewiesen. Die Priorität mit einem niedrigeren Wert hat die höchste Präferenz. Die Richtlinie mit der niedrigsten Prioritätsnummer wird zuerst ausgewertet. Wenn die Richtlinie nicht den definierten Bedingungen entspricht, wird die nächste Richtlinie ausgewertet. Wenn die Bedingungen übereinstimmen, werden die anderen Richtlinien übersprungen.

Connector Appliance-Konfiguration

Die Connector Appliance führt die Validierung von Gerätezertifikaten, die Überprüfung des Zertifikatswiderrufs (CRL) und die Überprüfung von Geräteobjekten für die Always-On-Gerätezertifikatsauthentifizierung durch. Die Connector Appliance muss in die Active Directory-Domäne eingebunden sein, damit die Gerätezertifikatsauthentifizierung unterstützt wird.

Clientkonfiguration

- Der Windows-Computer, der Always On-Unterstützung benötigt, muss in Active Directory oder Entra ID Hybrid in die Domäne eingebunden sein.
- Der Windows-Computer muss ein Gerätezertifikat von der Unternehmenszertifizierungsstelle für Secure Private Access Always On registrieren.
- Die Gerätezertifikatattribute müssen die folgenden Details enthalten.
    - Der Ausstellername im Gerätezertifikat muss mit dem allgemeinen Namen des CA-Zertifikats übereinstimmen, das in die Secure Private Access-Administrationskonsole hochgeladen wurde.

      Always On CA-Ausstellername(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-issuer.png)
    - Der Betreff muss den allgemeinen Namen des Computers enthalten.

      Always On Betreffname(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-subject.png)
    - Der Subject Alternate Name (SAN) muss den UPN des Computers enthalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Always On SAN(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-san.png)

- Der CRL-Verteilungspunkt muss die entsprechende LDAP-URL enthalten.

  Always On CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-crl-cdp.png)

- Der Zertifizierungspfad muss der Zertifizierungsstellenkette entsprechen.

  Always On CRL DP(/en-us/citrix-secure-private-access/media/spna-ztna-always-on-cert-path.png)

- Installieren Sie den Citrix Secure Access Client für Always On.
- Die folgenden Registrierungseinträge müssen auf dem Client erstellt werden, um Always On vor der Windows-Anmeldung zu aktivieren.
  - **CloudAlwaysOnURL** in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.

    Registrierungstyp - STRING

    Registrierungswert - `<Customer store FQDN>` (Beispiel: company.cloud.com)
  - **AlwaysOnService** in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.

    Registrierungstyp - DWORD

    Registrierungswert - 0x00000002

Always On nach der Windows-Anmeldung konfigurieren (Maschinen-/Benutzertunnel)

Nach erfolgreicher Windows-Anmeldung wird der Maschinentunnel fortgesetzt, bis die Benutzeranmeldung mit dem Citrix Secure Access Client erfolgreich ist.

- Wenn die automatische Benutzeranmeldung erfolgreich ist, wird der Maschinentunnel zu einem Benutzertunnel migriert.
- Wenn die automatische Benutzeranmeldung fehlschlägt, wird der Maschinentunnel fortgesetzt.
- Wenn der Benutzertunnel getrennt wird, fällt die Verbindung automatisch auf den Maschinentunnel zurück.

Die automatische Benutzeranmeldung nach der Windows-Anmeldung wird für die folgenden Authentifizierungsmethoden in der StoreFront Cloud-Authentifizierungskonfiguration unterstützt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Authentifizierung mit Active Directory (ohne zweiten Faktor) - AD-Anmeldeinformationen SSO
- Authentifizierung mit Citrix Gateway/Adaptive Auth, konfiguriert mit Kerberos SSO
- Authentifizierung mit Azure Active Directory (SSO mit Primary Refresh Token (PRT) der Microsoft Entra ID-Authentifizierung).

HINWEIS:

Deaktivieren Sie Endbenutzer immer zur Eingabe ihrer Anmeldeinformationen auffordern.

Einschränkungen

- Der Computer-UPN-Hostname darf 15 Zeichen nicht überschreiten.
- Der Fall der Windows Auto-Anmeldung (Erstbenutzer (FTU)) wird nur unterstützt, wenn der Computer in die Domäne eingebunden ist und das Gerätezertifikat vorhanden ist.
- Die Always On vor Windows-Anmeldung-Funktion wird nur unter Windows 10 oder höheren Versionen unterstützt.
- Die Always On vor Windows-Anmeldung-Funktion wird für Windows Server-Betriebssysteme nicht unterstützt.
- Die Always On vor Windows-Anmeldung-Funktion wird mit Cloud Connector nicht unterstützt. Auch wenn Sie Connector Appliance nicht als bevorzugten Connector ausgewählt haben, geht der Maschinentunnel-Traffic über die Connector Appliance.

Referenzen

- Erstellen einer TCP/UDP-Anwendung in der Secure Private Access-Konsole(/de-de/citrix-secure-private-access/service/spa-support-for-client-server-apps.html)
- Zuweisen einer Zugriffsrichtlinie zur TCP/UDP-Anwendung(/de-de/citrix-secure-private-access/service/admin-guided-workflow-for-easy-onboarding-and-setup.html#step-3-configure-an-access-policy-with-multiple-rules)
- Verbinden eines lokalen Citrix Gateways als Identitätsanbieter mit Citrix Cloud(/de-de/citrix-cloud/citrix-cloud-management/identity-access-management/connect-ad-gateway.html)
- Adaptive Authentifizierung bereitstellen(/de-de/adaptive-authentication/configure-the-adaptive-authentication-service/provision-adaptive-authentication.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Die folgenden reservierten CIDR-IP-Adressbereiche sind zulässig:

- 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 Elementen 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 Netzwerk-Subnetz 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

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ermöglichen Sie dem Citrix Secure Access™-Client, einen nicht vollständig qualifizierten Domänennamen (Hostnamen) in einen vollständig qualifizierten Domänennamen (FQDN) aufzulösen, indem Sie die DNS-Suffix-Domäne für die Backend-Server hinzufügen.
- Ermöglichen Sie Administratoren, Anwendungen mithilfe von IP-Adressen (IP-CIDR/IP-Bereich) zu konfigurieren, sodass die Endbenutzer die Anwendungen über den entsprechenden FQDN unter der DNS-Suffix-Domäne aufrufen 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. Angenommen, die folgenden Suffixe wurden hinzugefügt:

- `".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 verbleibenden Suffixe übersprungen.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Die DNS-Suffix-Konfiguration kann dem Client nur ermöglichen, einen nicht vollständig qualifizierten Domänennamen aufzulösen, indem das mit der DNS-Suffix-Funktion konfigurierte Domänen-Suffix angehängt wird. Damit ein Endbenutzer auf einen FQDN unter der DNS-Suffix-Domäne zugreifen kann, muss der Administrator eine Anwendung mit einer IP-Adresse, einem FQDN oder einer Wildcard-Domäne konfigurieren. Weitere Informationen finden Sie unter Punkt 4 in Anwendungsbeispiel.
- Wenn zwei verschiedene Anwendungen konfiguriert sind, eine mit FQDN und eine andere mit IP-Adresse, die beide demselben Back-End-Server entsprechen, hat die Richtlinie der Anwendung mit IP-Adresse eine höhere Priorität. Weitere Informationen finden Sie unter Punkt 5 in Anwendungsbeispiel.

Voraussetzungen

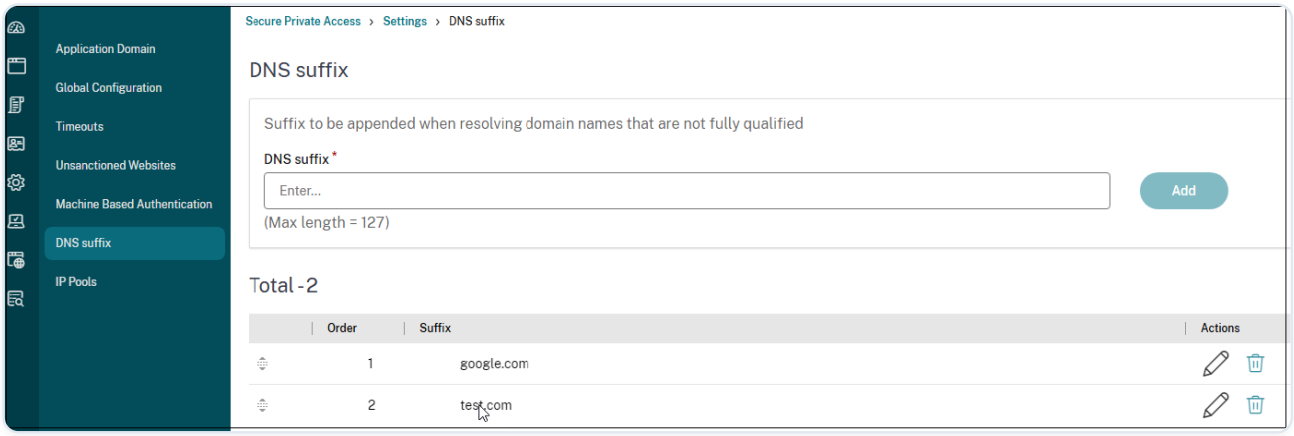
- Kunden müssen zur Secure Private Access Advanced Edition berechtigt sein, um die DNS-Suffix-Funktion nutzen zu können.
- Wenden Sie sich an das Citrix Produktmanagement-Team, um die Feature-Flags für das DNS-Suffix aktivieren zu lassen.

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 beim Auflösen eines nicht vollständig qualifizierten Namens angehängt werden muss.
4. Klicken Sie auf **Hinzufügen**.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Beispielanwendungsfall

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	ENDBENUTZERERFAHRUNG
1	Der Administrator konfiguriert das DNS-Suffix als „citrix.net“ und erstellt eine App mit der IP-Adresse 192.0.2.1 mit einer Zugriffsrichtlinie, die für user1 auf „allow“ gesetzt ist.	Wenn user1 versucht, sich mit „workday“ zu verbinden, wird der FQDN mit „citrix.net“ (workday.citrix.net) versehen und die IP-Adresse wird in 192.0.2.1 aufgelöst. Da 192.0.2.1 für user1 mit einer konfigurierten App zugelassen ist, wird der Zugriff gewährt.
	Hinweis: Der Endbenutzer kann auf die Workday-App mit 192.0.2.1 oder workday.citrix.net oder „workday“ zugreifen.	
	Ohne DNS-Suffix-Konfiguration wird der Zugriff über „workday“ und	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	DNS-SUFFIX UND APP-KONFIGURATION	ENDBENUTZERERFAHRUNG
	„workday.citrix.net“ verweigert.	
2	Der Administrator konfiguriert das DNS-Suffix als „citrix.net“, erstellt eine App mit FQDN (workday.citrix.net) und setzt die Zugriffsrichtlinie für user1 auf „allow“.	Wenn user1 versucht, sich mit „workday“ zu verbinden, wird „citrix.net“ an „workday“ (workday.citrix.net) angehängt. Der Endbenutzer kann auf Workday zugreifen, da eine Anwendung mit „workday.citrix.net“ konfiguriert ist und die Zugriffsrichtlinie für user1 auf „allow“ gesetzt ist.
	Hinweis: Der Endbenutzer kann auf die Workday-App mit workday.citrix.net oder „workday“ zugreifen.	
	Der Zugriff auf 192.0.2.1 wird verweigert, da keine App mit dieser IP-Adresse konfiguriert ist.	
3	Der Administrator konfiguriert das DNS-Suffix als „citrix.net“, erstellt eine App mit der Wildcard-Domäne „*.citrix.net“ und setzt die Zugriffsrichtlinie für user1 auf „allow“.	Wenn user1 versucht, sich mit „workday“ zu verbinden, wird „citrix.net“ an „workday“ (workday.citrix.net) angehängt. Der Endbenutzer kann auf Workday zugreifen, da eine Anwendung mit „*.citrix.net“ konfiguriert ist und die Zugriffsrichtlinie für user1 auf „allow“ gesetzt ist.
	Hinweis: Endbenutzer können auf Workday mit workday.citrix.net oder „workday“ zugreifen.	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	DNS-SUFFIX UND APP-KONFIGURATION	ENDBENUTZERERFAHRUNG
	Der Zugriff auf 192.0.2.1 wird verweigert, da keine App mit dieser IP-Adresse konfiguriert ist.	
4	Der Administrator konfiguriert das DNS-Suffix als „citrix.net“. Für user1 ist keine Anwendung mit FQDN (workday.citrix.net) oder 192.0.2.1 konfiguriert.	Wenn user1 versucht, eine Verbindung zu „workday“ herzustellen, wird „workday“ vom Client mit „citrix.net“ versehen und „workday.citrix.net“ in 192.0.2.1 aufgelöst. user1 kann jedoch keine Verbindung zum privaten Server (workday.citrix.net/ 192.0.2.1) herstellen, da für user1 keine App mit 192.0.2.1 oder workday.citrix.net oder *.citrix.net konfiguriert ist.
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 user1 auf „deny“. Fügt dann eine weitere App mit FQDN (workday.citrix.net) hinzu, die in 192.0.2.1 aufgelöst wird, und setzt die Zugriffsrichtlinie für user1 auf „allow“.	Wenn user1 versucht, eine Verbindung zu „workday“ herzustellen, wird „citrix.net“ an Workday (workday.citrix.net) angehängt und die IP-Adresse 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zugehörige Domänen mithilfe einer HAR-Datei ermitteln

Secure Private Access ermöglicht es Ihnen, eine HTTP-Archivdatei (HAR-Datei) hochzuladen, um die von einer Anwendung aufgerufenen Domänen automatisch zu ermitteln. Sie können die ermittelten Domänen überprüfen und diejenigen auswählen, die Sie der Konfiguration der zugehörigen Domänen der Anwendung hinzufügen möchten. Dies vereinfacht das Onboarding von Anwendungen, da die manuelle Identifizierung und Konfiguration zugehöriger Domänen reduziert wird.

Zuvor mussten Administratoren alle zugehörigen Domänen einer Anwendung im Voraus kennen oder sie reaktiv ermitteln, wenn Benutzer auf blockierte URLs stießen. Da jede URL außer den konfigurierten standardmäßig blockiert wird, führt dieser reaktive Ansatz zu einer schlechten Benutzererfahrung. Secure Private Access hatte keine Möglichkeit, die internen oder eingebetteten URLs innerhalb einer Anwendung zu identifizieren.

Beispiel

Angenommen, Sie konfigurieren eine Anwendung, deren primäre Domäne `example.com` ist. Während der Nutzung der Anwendung greift der Browser auch auf mehrere zusätzliche Domänen zu. Zum Beispiel:

- `api.example.com` – Verarbeitet die Backend-API-Aufrufe der Anwendung.
- `auth.example.com` – Verwaltet die Anmeldung und Authentifizierung.
- `cdn.example.com` – Stellt statische Inhalte wie Bilder, Skripte und Stylesheets bereit.
- `login.microsoftonline.com` – Bietet Authentifizierung durch Drittanbieter-Identitäten.
- `player.vimeo.com` – Lädt eingebettete Videoinhalte.

Anstatt jede dieser Domänen manuell zu identifizieren:

1. Erfassen Sie eine HAR-Datei, während Sie die Anwendung verwenden.
2. Importieren Sie die HAR-Datei in Secure Private Access.
3. Überprüfen Sie die von Secure Private Access ermittelten Domänen. Der Import könnte beispielsweise `api.example.com`, `auth.example.com` und `cdn.example.com` als erforderlich anzeigen, zusammen mit Domänen wie `player.vimeo.com`, die Sie ausschließen können.
4. Wählen Sie die von der Anwendung benötigten Domänen aus.
5. Konfigurieren Sie Routing und Ressourcenstandorte nach Bedarf.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

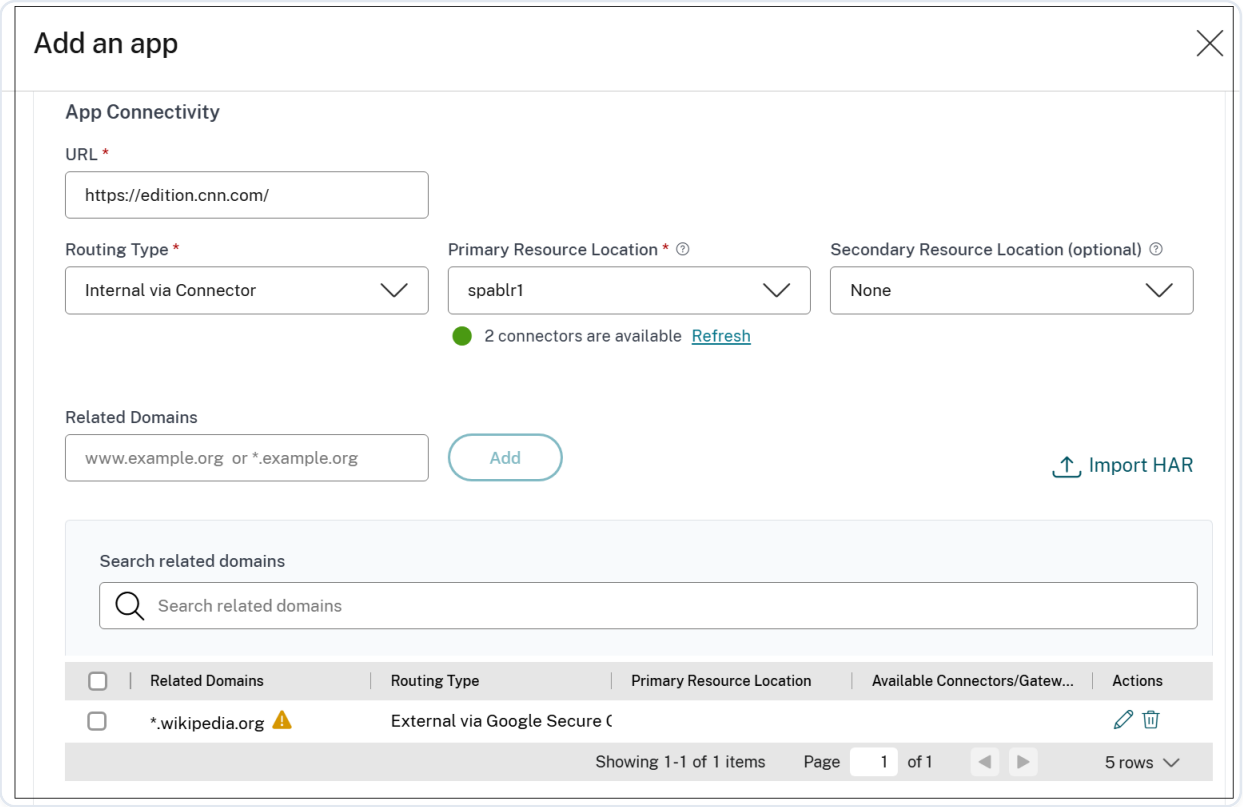
Dies bietet eine schnellere Möglichkeit, die für die Anbindung von Anwendungen erforderlichen Domänen zu identifizieren und zu konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie eine HAR-Datei erfasst haben, während Sie auf die Web- oder SaaS-Anwendung zugreifen. Die HAR-Datei muss die Netzwerkanforderungsinformationen enthalten und darf maximal 50 MB groß sein.

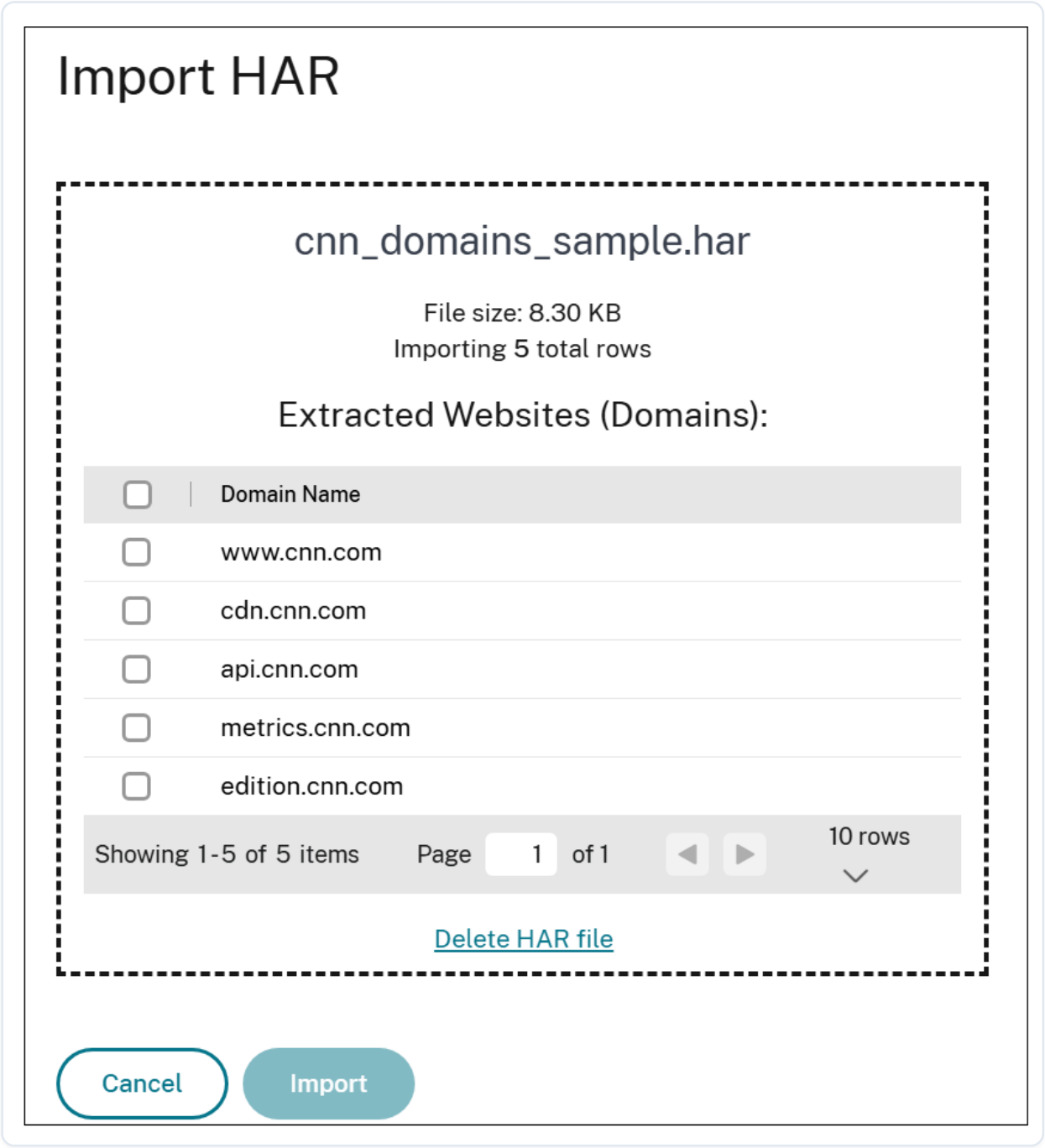
HAR-Datei importieren

1. Öffnen Sie im Secure Private Access-Administratorportal die Web- oder SaaS-Anwendung, die Sie konfigurieren möchten.
2. Gehen Sie zu **App Connectivity** und klicken Sie auf **HAR importieren**.



3. Ziehen Sie die HAR-Datei per Drag & Drop in das Importfenster, oder wählen Sie die Datei von Ihrem Gerät aus.
4. Secure Private Access analysiert die HAR-Datei und zeigt die aus den Netzwerkanforderungen identifizierten Domänen an.

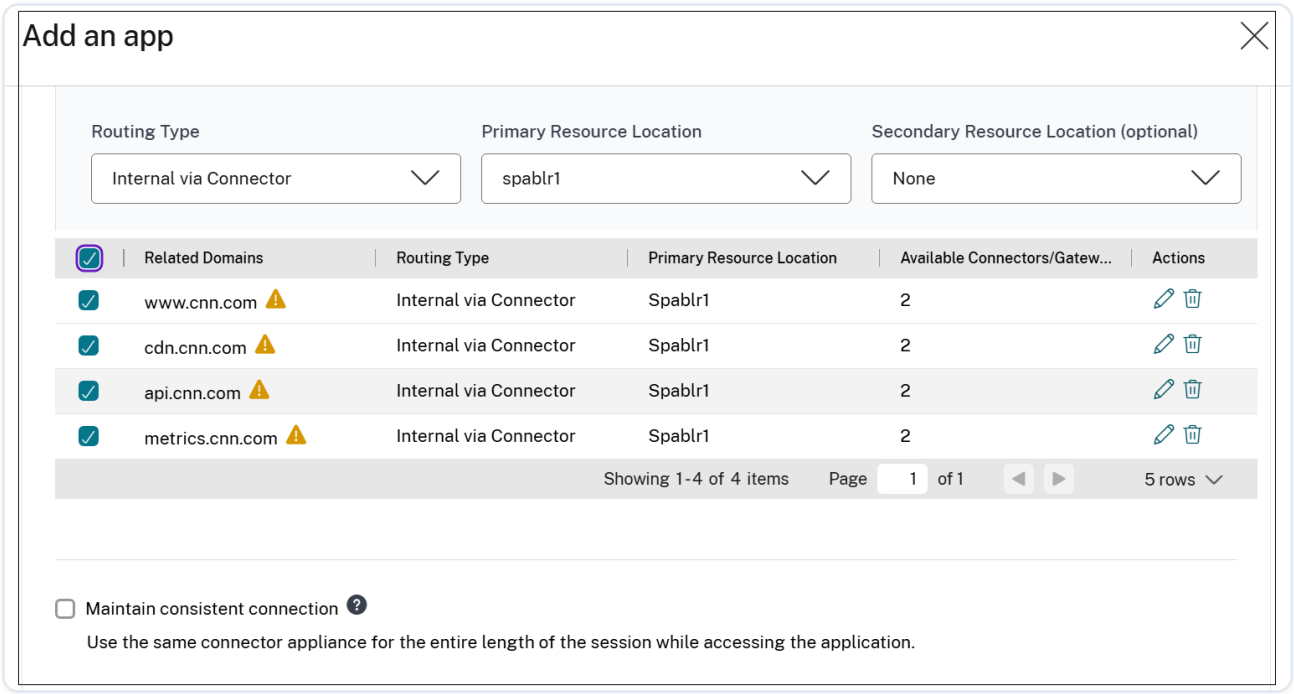
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Überprüfen Sie die erkannten Domänen.
6. Wählen Sie die Domänen aus, die Sie der Anwendung hinzufügen möchten.
7. Wählen Sie **Importieren**.

Die ausgewählten Domänen werden der Konfiguration der **Zugehörigen Domänen** der Anwendung hinzugefügt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Überprüfen Sie die gefundenen Domänen, bevor Sie sie importieren. Eine HAR-Datei kann Domänen enthalten, die für die Konnektivität der Anwendung nicht erforderlich sind.

Zugehörige Domänen verwalten

Nach dem Import der Domänen können Sie diese über die Tabelle **Zugehörige Domänen** verwalten:

- **Domäne suchen** – Verwenden Sie das Suchfeld, um die Tabelle zu filtern und schnell eine bestimmte Domäne zu finden.
- **Domänen auswählen** – Wählen Sie einzelne Domänen aus, oder verwenden Sie das Kontrollkästchen in der Tabellenüberschrift, um mehrere Domänen auszuwählen. Die Auswahl kann verwendet werden, um Aktionen für mehrere Domänen gleichzeitig auszuführen.
- **Domänenkonfiguration bearbeiten** – Aktualisieren Sie die Konfiguration der zugehörigen Domänen, einschließlich des Routingtyps, des primären Ressourcenstandorts und des sekundären Ressourcenstandorts.
- **Domänen in großen Mengen bearbeiten** – Wählen Sie mehrere geeignete Domänen aus und aktualisieren Sie deren Routing- und Ressourcenstandorteinstellungen gleichzeitig. Die Massenbearbeitung ist für anwendbare interne Domänen verfügbar. Externe Domänen unterstützen möglicherweise nicht alle Konfigurationsoptionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Ressourcenstandorte** – Weisen Sie beim Konfigurieren einer zugehörigen Domäne einen primären und, falls zutreffend, einen sekundären Ressourcenstandort zu. Verwenden Sie diese Einstellungen, um zu definieren, wie Secure Private Access den Datenverkehr für die zugehörige Domäne leitet und welche Ressourcenstandorte zur Bereitstellung der Konnektivität verwendet werden.

Validierung und Dateianforderungen

Die HAR-Importfunktion validiert die hochgeladene Datei, bevor sie verarbeitet wird.

- Es können nur gültige HAR-Dateien importiert werden, die Netzwerkanforderungseinträge enthalten.
- Die maximal unterstützte Dateigröße beträgt **50 MB**.
- Domänen werden automatisch aus den URLs in der HAR-Datei extrahiert.
- Doppelte Domänen werden automatisch entfernt.
- Domänen werden normalisiert, bevor sie der Konfiguration für verwandte Domänen hinzugefügt werden.

Portbasiertes Routing mithilfe von Routing-Ausnahmen – Vorschau

Die Funktion für portbasiertes Routing ermöglicht es Administratoren, den Datenverkehr für verschiedene Ports desselben Ziels für TCP/UDP-Anwendungen mithilfe von Routing-Ausnahmen unterschiedlich zu routen. Beim Onboarding von Anwendungen in Secure Private Access können Administratoren festlegen, wie der Anwendungsdatenverkehr über eine der folgenden Optionen geroutet wird:

- **Intern über Connector**: Der Datenverkehr wird sicher über den Connector getunnelt.
- **Intern über NetScaler Gateway**: Der Datenverkehr wird über NetScaler Gateway mithilfe eines hybriden Datenpfads geroutet.
- **Extern**: Der Datenverkehr wird direkt geroutet, ohne ihn durch Secure Private Access zu tunneln.

Um den Datenverkehr für verschiedene Ports desselben Ziels unterschiedlich zu routen, müssen Administratoren Routing-Ausnahmen für Zugriffsrichtlinien verwenden. Jede Ziel- und Portkombination, die eine separate Routing-Entscheidung erfordert, muss als separate Anwendung konfiguriert und an eine separate Richtlinie gebunden werden. Die Benutzeroberfläche erzwingt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

eine Eindeutigkeitsprüfung, sodass unterschiedliche Routen nicht innerhalb verschiedener Anwendungen mit demselben Ziel konfiguriert werden können.

Anwendungsfälle für portbasiertes Routing

Szenario: Ein Administrator hostet zwei Anwendungen auf demselben Server (10.102.124.135).

- SSH-Zugriff auf Port 22
- Webzugriff auf Port 80, 443

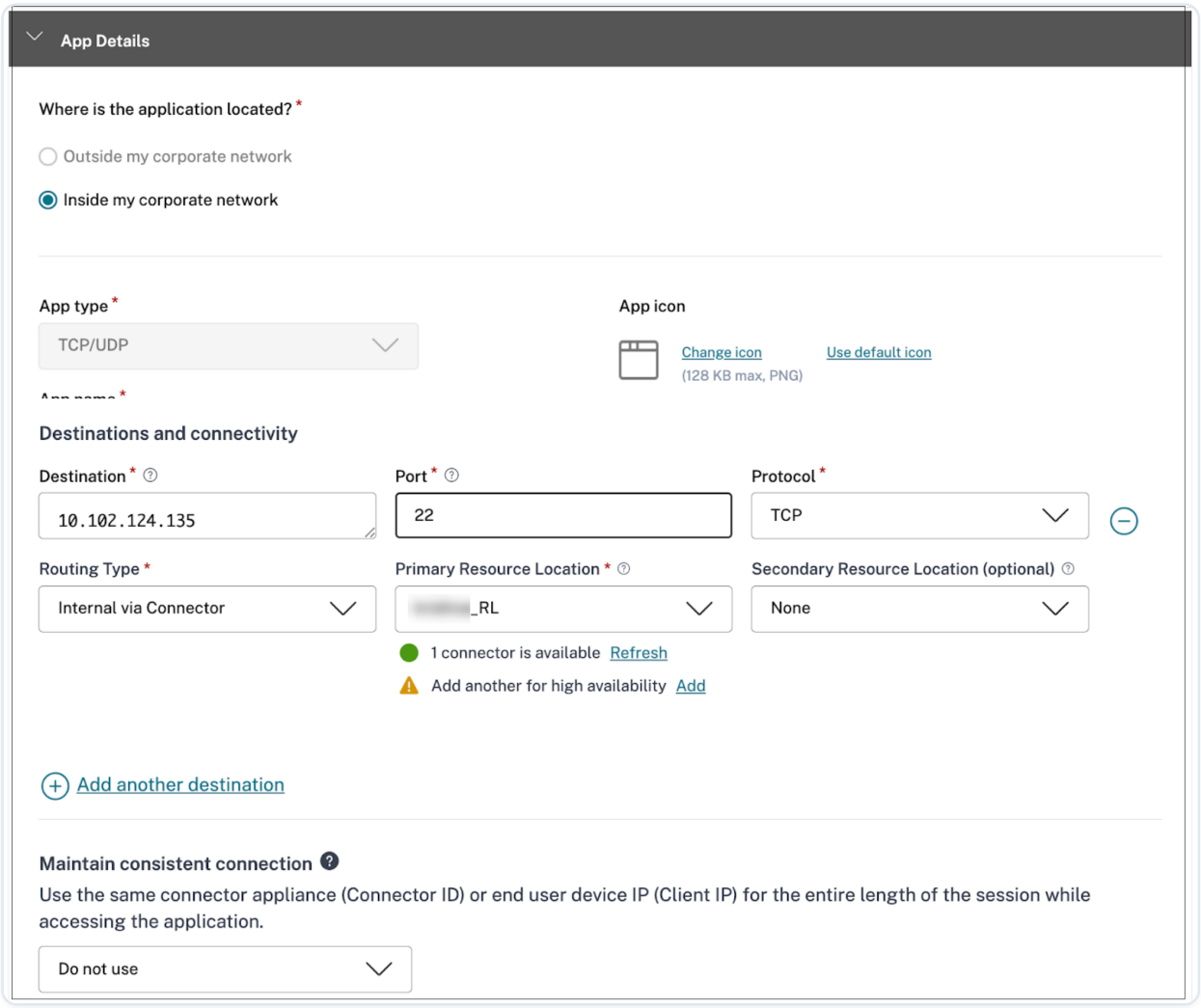
Anforderung:

- Ermöglichen Sie der Benutzergruppe der Entwickler, intern über einen Connector auf SSH zuzugreifen.
- Ermöglichen Sie der Benutzergruppe der Geschäftseinheit, direkt aus dem Unternehmensnetzwerk auf die Webanwendung zuzugreifen.

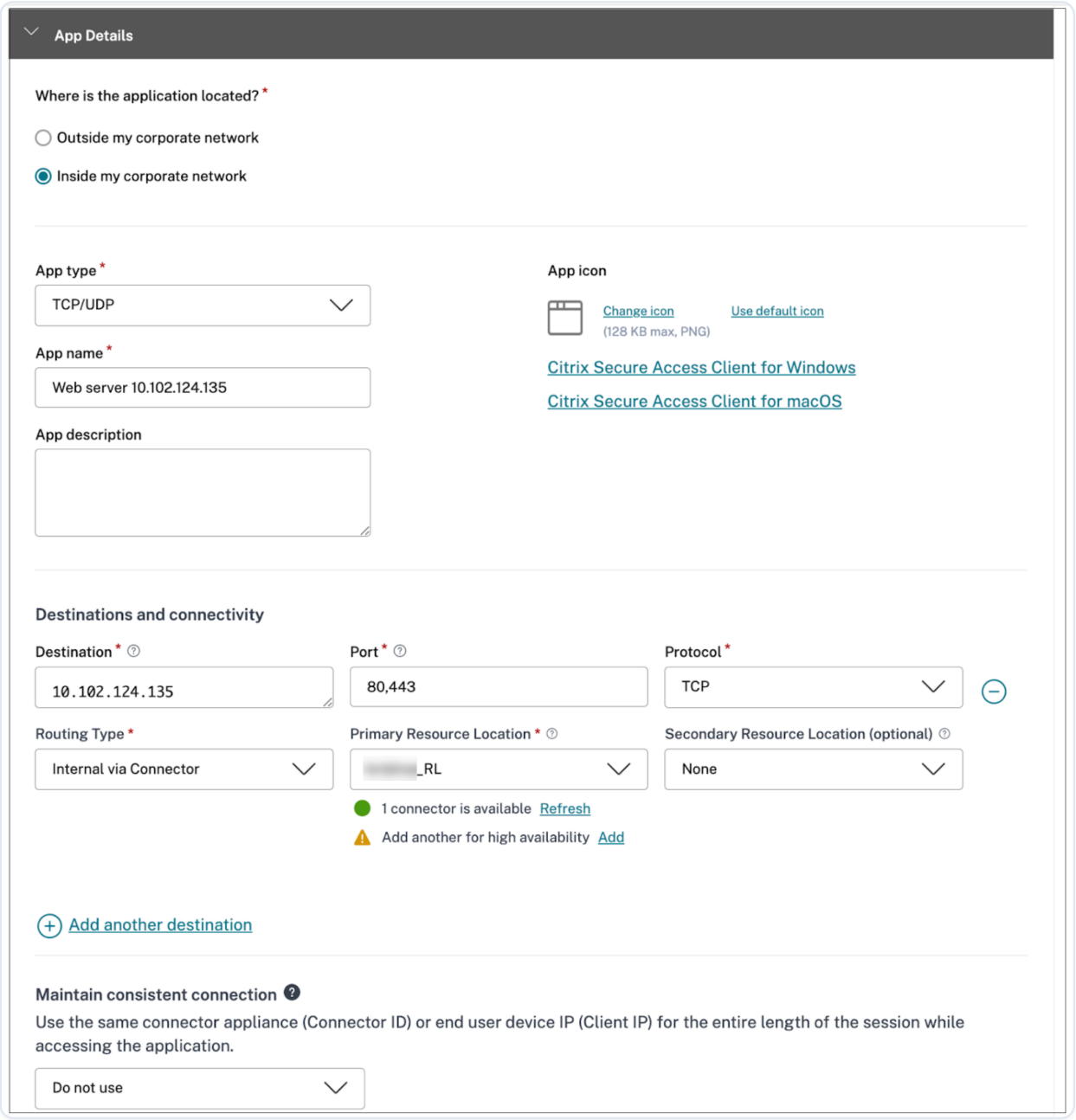
Konfiguration:

1. Erstellen Sie separate Anwendungen für jede Anforderung. Weitere Informationen finden Sie unter Unterstützung für TCP/UDP-Anwendungen.
    - Erstellen Sie eine Anwendung für SSH-Zugriff (Ziel:10.102.124.135, Port 22)
    - Erstellen Sie eine weitere Anwendung für Webzugriff (Ziel :10.102.124.135, Port 80,443)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

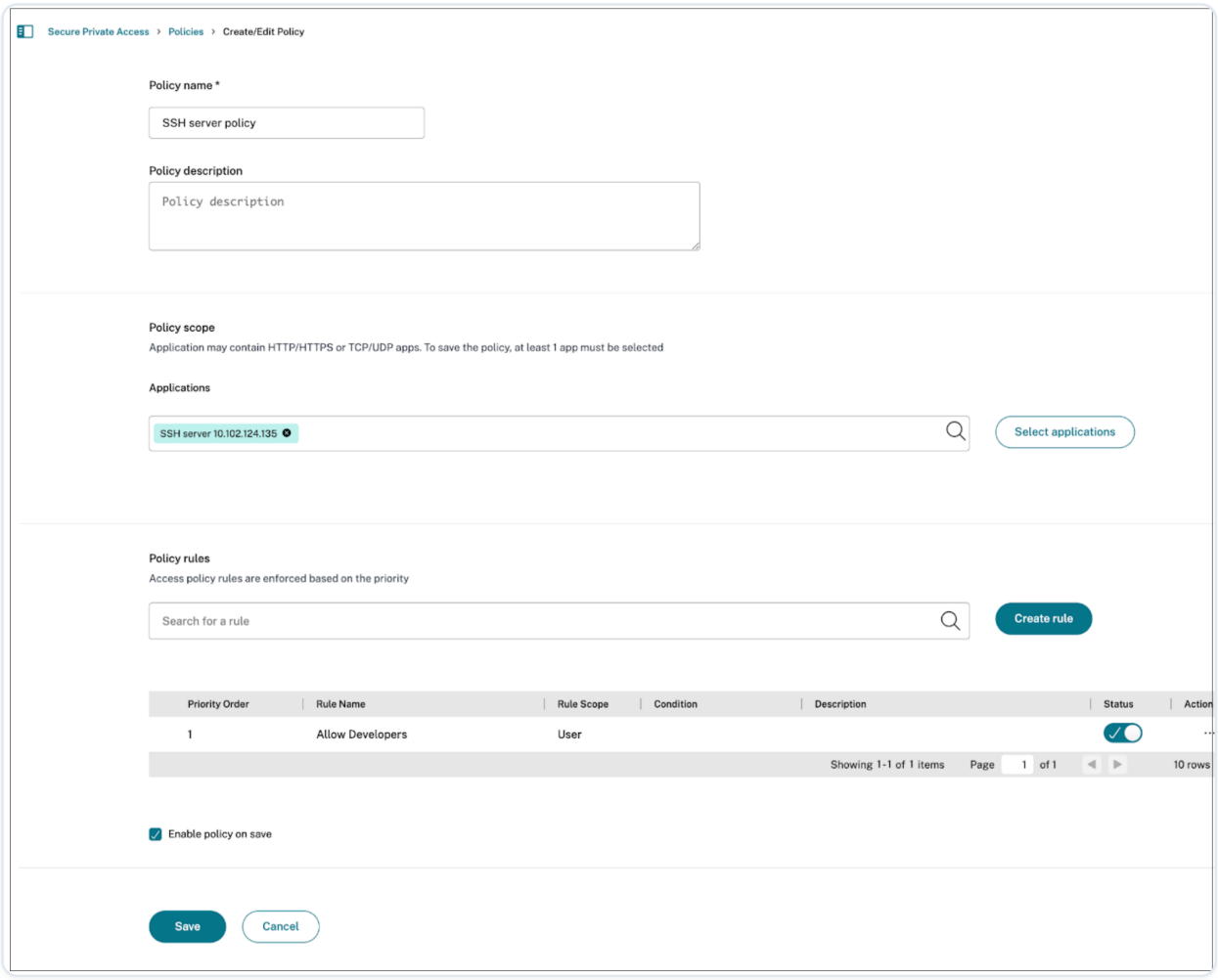


© 1997–2026 Citrix Systems, Inc. All rights reserved.

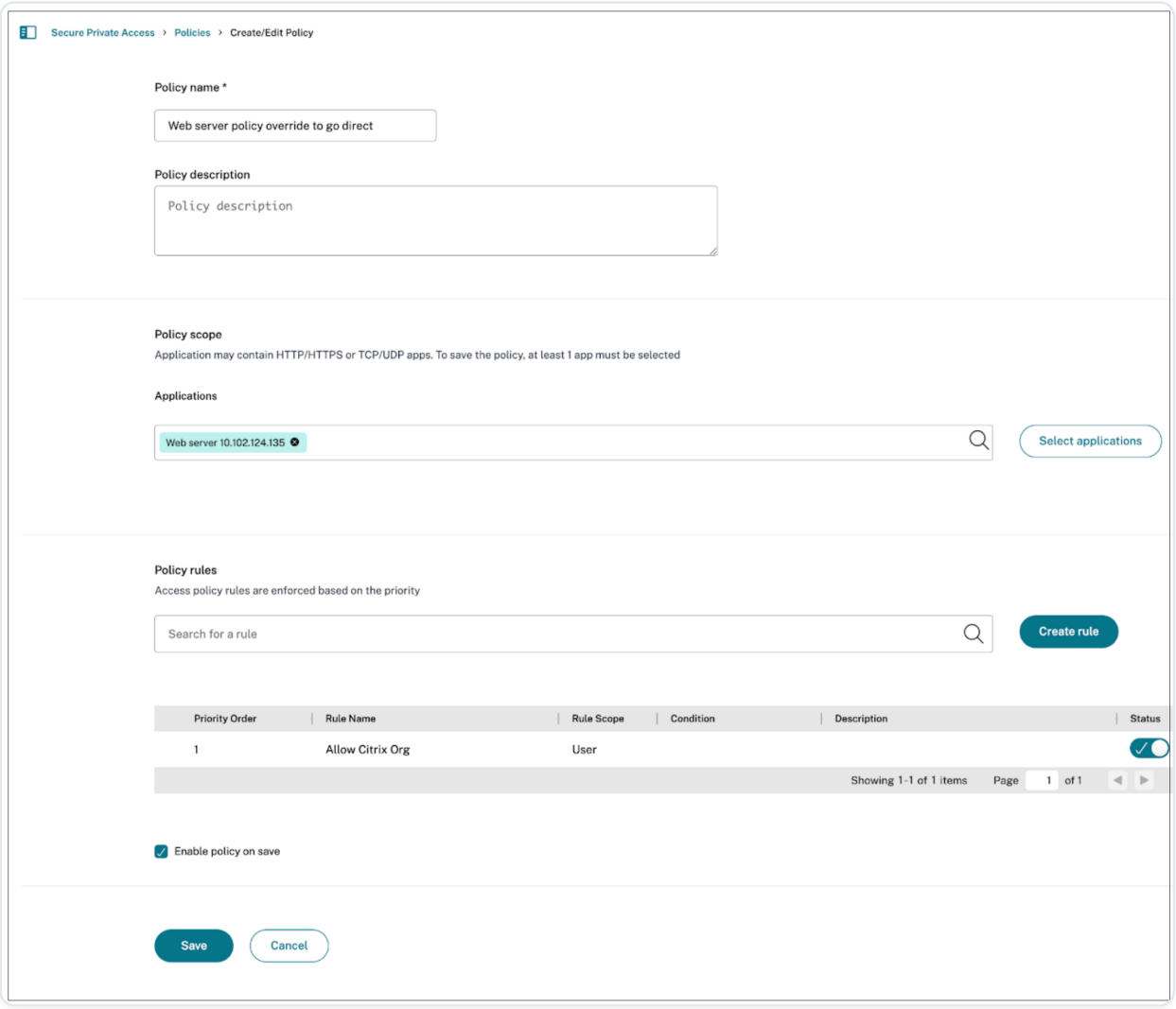


2. Konfigurieren Sie die weiteren Details für jede Anwendung nach Bedarf.
3. Erstellen Sie separate Zugriffsrichtlinien.
   - Definieren Sie individuelle Richtlinien für jede Anwendung.
   - Verwenden Sie Routing-Ausnahmen, um das gewünschte Routing-Verhalten für jede konfigurierte Anwendung festzulegen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

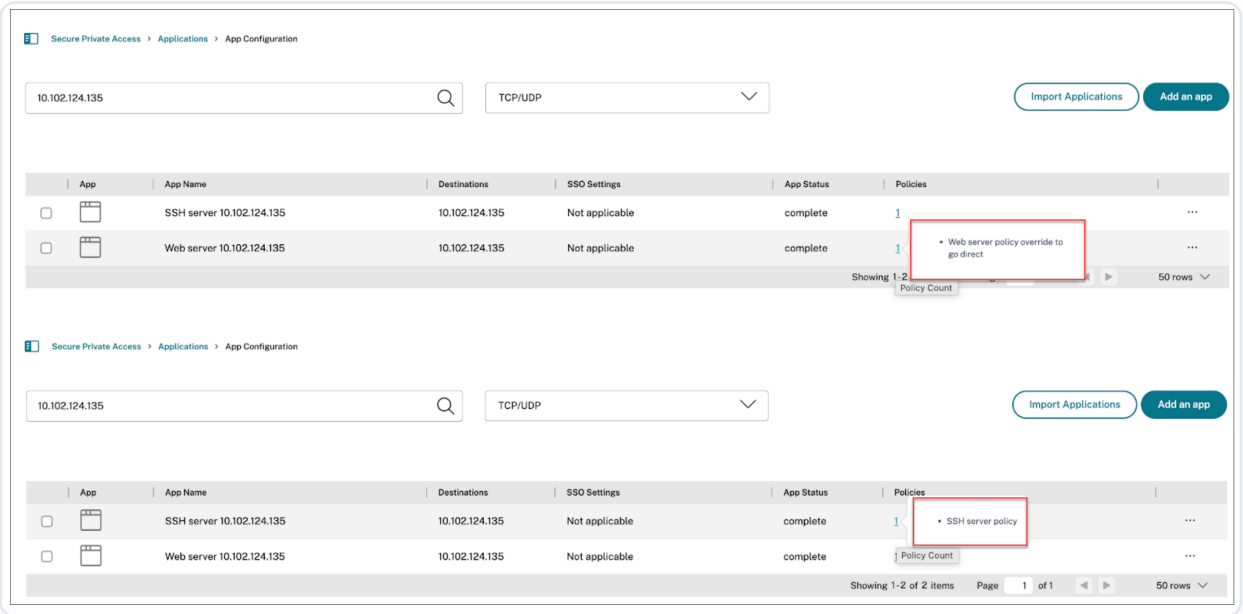


© 1997–2026 Citrix Systems, Inc. All rights reserved.



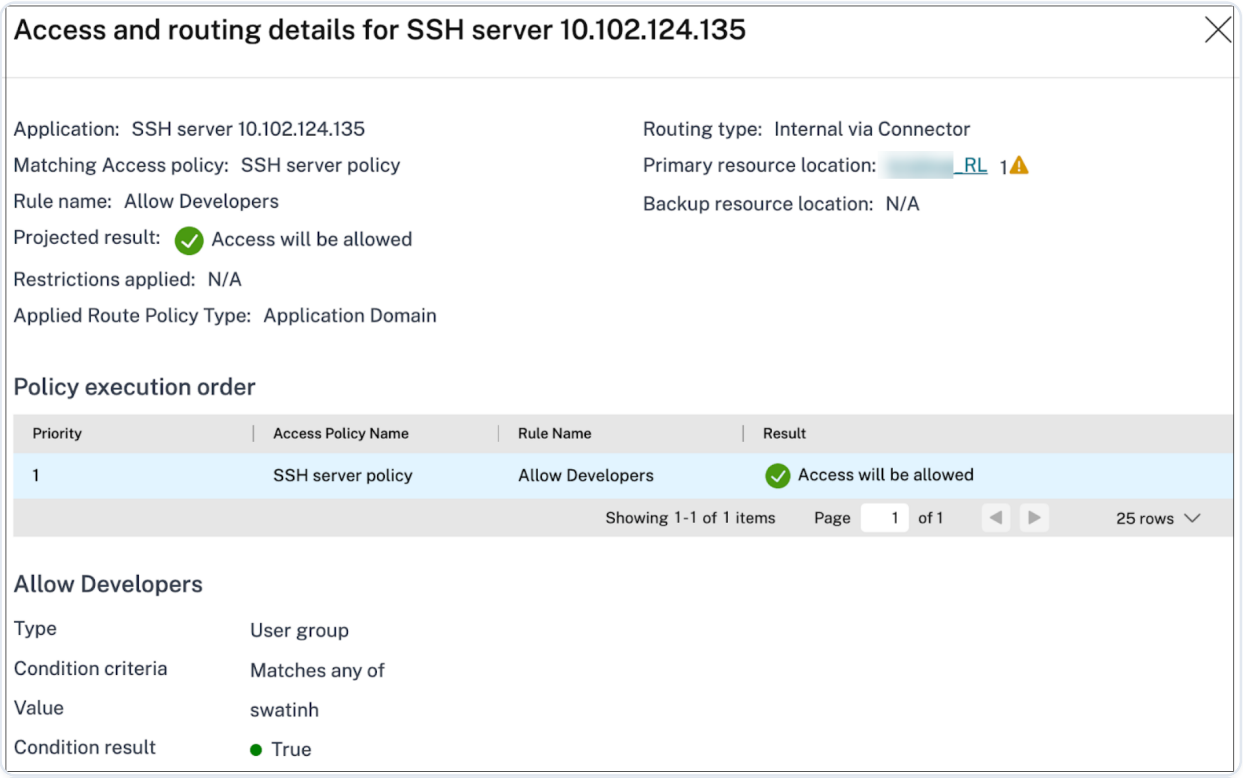
4. Binden Sie Richtlinien an Anwendungen.

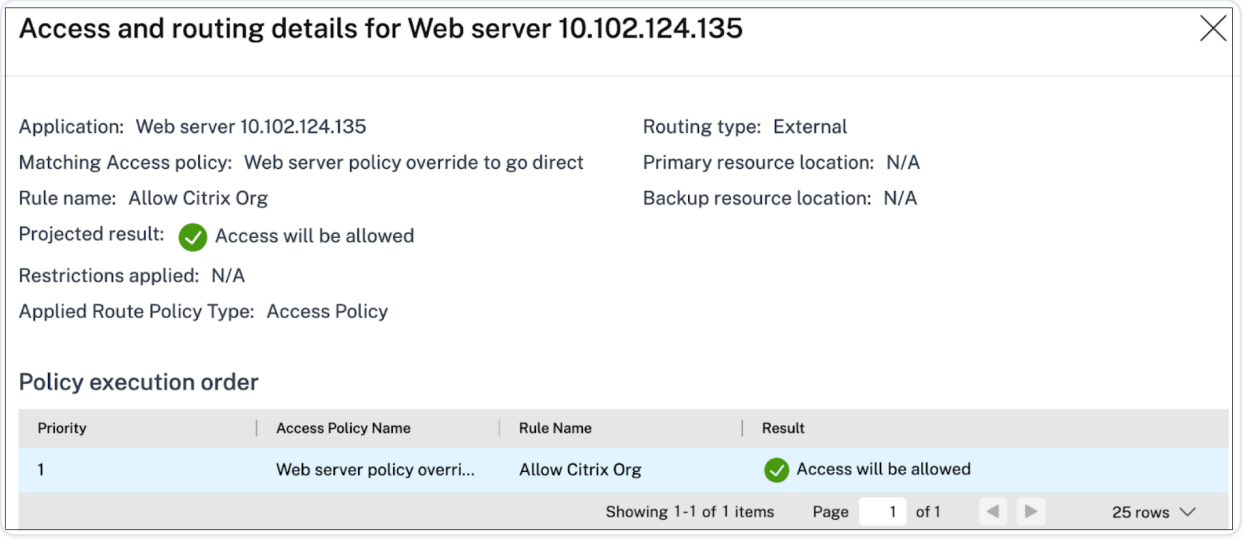
   - Binden Sie die SSH-Zugriffsrichtlinie an die SSH-Anwendung.
   - Binden Sie die Webzugriffsrichtlinie an die Webanwendung.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Verwenden Sie den Richtlinien-Modellierer, um die Anwendungen, Richtlinien und Routing-Bestätigungen zu überprüfen und zu validieren.





EINSCHRÄNKUNGEN DER ROUTING-OPTIONEN:

- Zugriffsrichtlinien werden von oben nach unten ausgewertet, sodass die erste Richtlinie, die mit dem Benutzer, dem Kontext und der Anwendung übereinstimmt, angewendet wird. Für Hostnamen-basierte Anwendungen wird die in der angewendeten Richtlinie definierte Routing-Konfiguration (Routing-Typ und Ressourcenstandort) zur Auflösung des Ziels verwendet.
- Wenn in der Zugriffsrichtlinie keine Routing-Ausnahmen definiert sind, wird die Routing-Konfiguration in der Anwendungskonfiguration verwendet. Route Tunnel und Route Direct

© 1997–2026 Citrix Systems, Inc. All rights reserved.

schließen sich gegenseitig aus. Daher können wir für Hostnamen-basierte Ziele nicht gleichzeitig eine Route über Tunnel (intern) und über Direct (extern) für verschiedene Ports haben.

- Internes Routing (über Connector oder NetScaler Gateway) und direktes Routing (extern) schließen sich gegenseitig aus. Daher können Hostnamen-basierte Ziele nicht sowohl intern als auch extern geroutet werden. Wenn die Anforderung darin besteht, den Datenverkehr für eine Anwendung sowohl intern als auch extern zu routen, wird empfohlen, die Anwendung über ein IP-basiertes Ziel einzubinden.

Beispiel zur Veranschaulichung von Port-basiertem Routing

Die folgende Abbildung zeigt, wie die Richtlinienpriorität und Routing-Ausnahmen das Endbenutzererlebnis beeinflussen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table	Configured applications and policies for a user		Expected behaviour for the user
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: 1. Routing Type:Internal via connector 2. Primary resource location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception : None Higher priority	App name: SSH_app Destination URL: example.com Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	Both example.com:389 and example.com:22 are resolved via Secure Private Access(Resourcelocation1). example.com:389 is launched successfully. example.com:22 fails to launch as it is supposed to go via External. **Note:** It is not recommended to configure the same domain to go via External and Internal. This limitation is only for FQDN.
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy :LDAP_policy for LDAP_app Routing Exception : None Lower priority	App name: SSH_app Destination URL: example.com Port Number:22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy:SSH_policy for SSH_app Routing Exception: External Higher priority	Both example.com:389, example.com:22 are launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception: None Higher priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy : LDAP_policy for LDAP_app Routing Exception: None Lower priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Higher priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.

Zertifikate in der Secure Private Access Konsole verwalten

Der Secure Private Access Zertifikatsspeicher bietet Administratoren einen zentralen Ort zur effizienten Verwaltung von Zertifizierungsstellen- (CA) und Secure Sockets Layer- (SSL) Zertifikaten. Dieser dedizierte Speicher vereinfacht die Zertifikatsverwaltung, indem er

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administratoren ermöglicht, nahtlos neue Zertifikate hinzuzufügen, bestehende zu ändern und nicht mehr benötigte zu entfernen.

Bisher wurden Secure Private Access Zertifikate im Zertifikatsspeicher der NetScaler® Console gespeichert. Mit dem dedizierten Secure Private Access Zertifikatsspeicher werden in der NetScaler Console verwaltete Zertifikate nicht mehr automatisch synchronisiert oder sind für die Verwendung in Secure Private Access zugänglich. Administratoren müssen die erforderlichen Zertifikate direkt in die Secure Private Access Konsole hochladen.

Die in Secure Private Access verwendeten Zertifikate sind auf der Seite „Zertifikate“ in zwei Registerkarten organisiert.

- **Server** – Enthält die Liste der Zertifikate, hauptsächlich SSL-Serverzertifikate, die sich auf die direkten Zugriffsoperationen (agentenloser Zugriff) beziehen.
- **Maschinenauthentifizierung** – Enthält die Liste der Zertifikate, die sich auf die Verwaltung von Maschinentunneln beziehen, die vom Citrix Secure Access™ Client initiiert wurden. Diese Zertifikate werden verwendet, wenn sich ein Administrator beim Citrix Secure Access Client anmeldet.

  Maschinenauthentifizierungszertifikate sind unerlässlich für die Always On-Funktion, die Gerätezertifikate verwendet, die von vertrauenswürdigen Zertifizierungsstellen (CAs) ausgestellt wurden. Diese CA-Zertifikate werden sicher auf der Registerkarte „Maschinenauthentifizierung“ (**Einstellungen > Zertifikatsspeicher**) hochgeladen und verwaltet, um eine nahtlose und robuste Geräteauthentifizierung für die Always On-Funktionalität zu gewährleisten.

Maschinenauthentifizierungszertifikate verwalten

Die folgenden Abschnitte enthalten weitere Informationen zur Verwaltung von Maschinenauthentifizierungszertifikaten.

Zertifikat hinzufügen

Schritte zum Hinzufügen eines Maschinenauthentifizierungszertifikats.

1. Navigieren Sie zu **Einstellungen > Zertifikatsspeicher**.

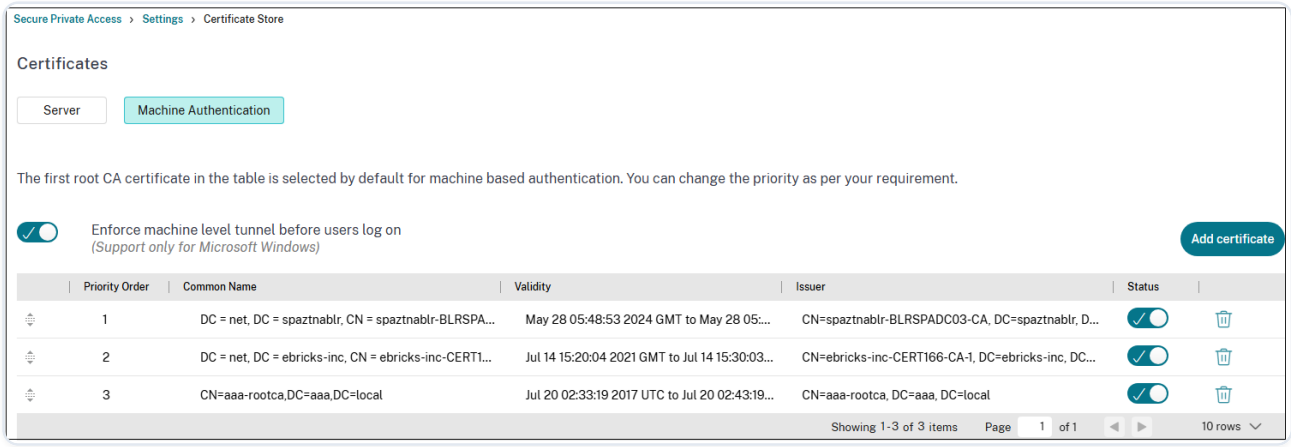
© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wir empfehlen, die Option **Maschinenbasierte Authentifizierung** unter **Einstellungen > Zertifikatsspeicher** anstelle von **Einstellungen > Maschinenbasierte Authentifizierung** zu verwenden. Die Option **Einstellungen > Maschinenbasierte Authentifizierung** wird in der kommenden Serviceversion entfernt.

2. Klicken Sie auf die Registerkarte **Maschinenauthentifizierung** und dann auf **Zertifikat hinzufügen**.
3. Geben Sie unter **Name** einen Namen für das Zertifikat ein.
4. Navigieren Sie unter **Zertifikatsdatei** zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - Zertifikate für Root-CA und Intermediate-CA werden unterstützt.
    - Die hochzuladenden Zertifikate müssen im PEM-Format vorliegen und die gesamte Kette enthalten. Das Zertifikat muss beginnend mit dem Zwischenzertifikat bis zur Root-CA generiert werden.
5. Klicken Sie auf **Speichern**.

Das Zertifikat wird der Liste der verfügbaren Zertifikate auf der Registerkarte **Maschinenauthentifizierung** hinzugefügt.



Ein Zertifikat deaktivieren

Sie können das nicht mehr verwendete Zertifikat deaktivieren, indem Sie den Umschalter in der Spalte **Status** auf AUS stellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein Zertifikat löschen

1. Klicken Sie auf das Löschsymbol, um ein Zertifikat zu löschen.

Priorität für das Zertifikat festlegen

Wenn mehrere Zertifikate für dieselbe Maschine verwendet werden, können Sie die Priorität der Zertifikate mithilfe des Drag-Symbols (Pfeil nach oben/unten) in der Spalte **Prioritätsreihenfolge** ändern.

SSL-Zertifikate verwalten

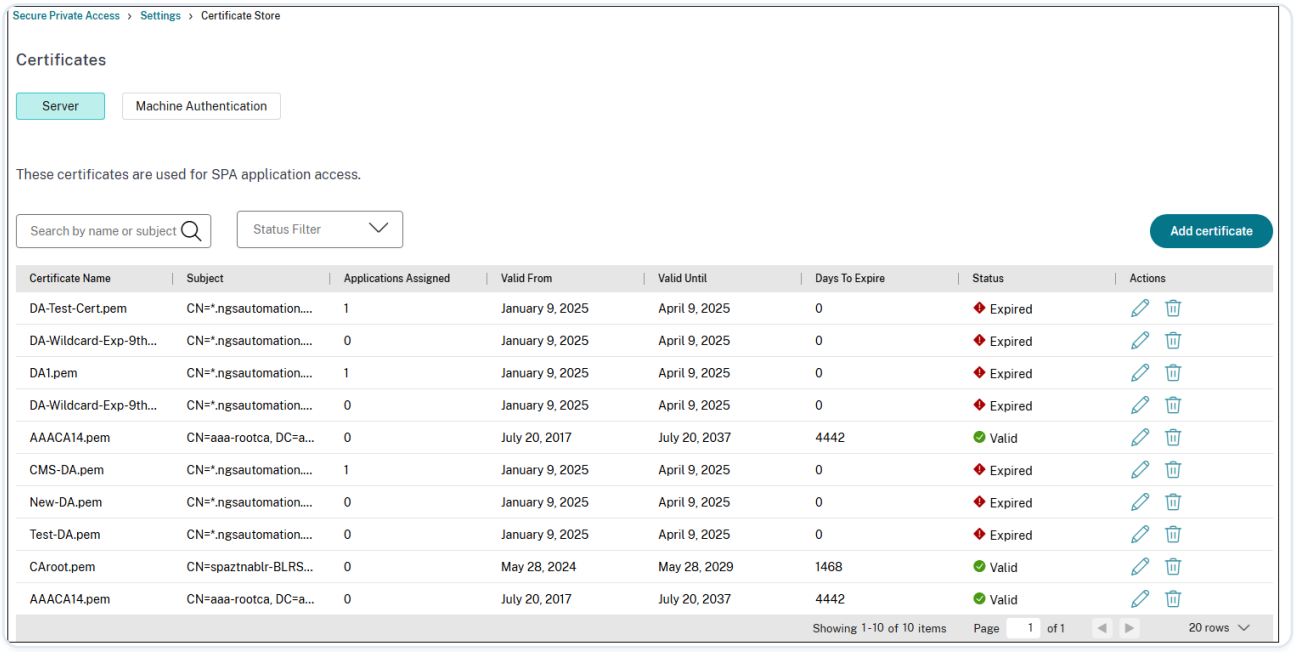
Die folgenden Abschnitte enthalten weitere Informationen zur Verwaltung von SSL-Zertifikaten.

Zertifikat hinzufügen

Schritte zum Hinzufügen eines SSL-Zertifikats.

1. Navigieren Sie zu **Einstellungen > Zertifikatspeicher**.
2. Klicken Sie auf die Registerkarte **Server**.
3. Geben Sie einen Namen für das Zertifikat ein.
4. Navigieren Sie unter **Zertifikatsdatei** zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - Zertifikate für Root-CA und Intermediate-CA werden unterstützt.
    - Die hochzuladenden Zertifikate müssen im PEM-Format vorliegen und die gesamte Kette enthalten. Das Zertifikat muss beginnend mit dem Zwischenzertifikat bis zur Root-CA generiert werden.
5. **Passwort** (Optional) – Anwendbar für PFX-Zertifikate. Wenn Sie einen verschlüsselten RSA-Privatschlüssel haben, geben Sie die RSA-Passphrase ein, die zum Verschlüsseln des privaten Schlüssels verwendet wurde.
6. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



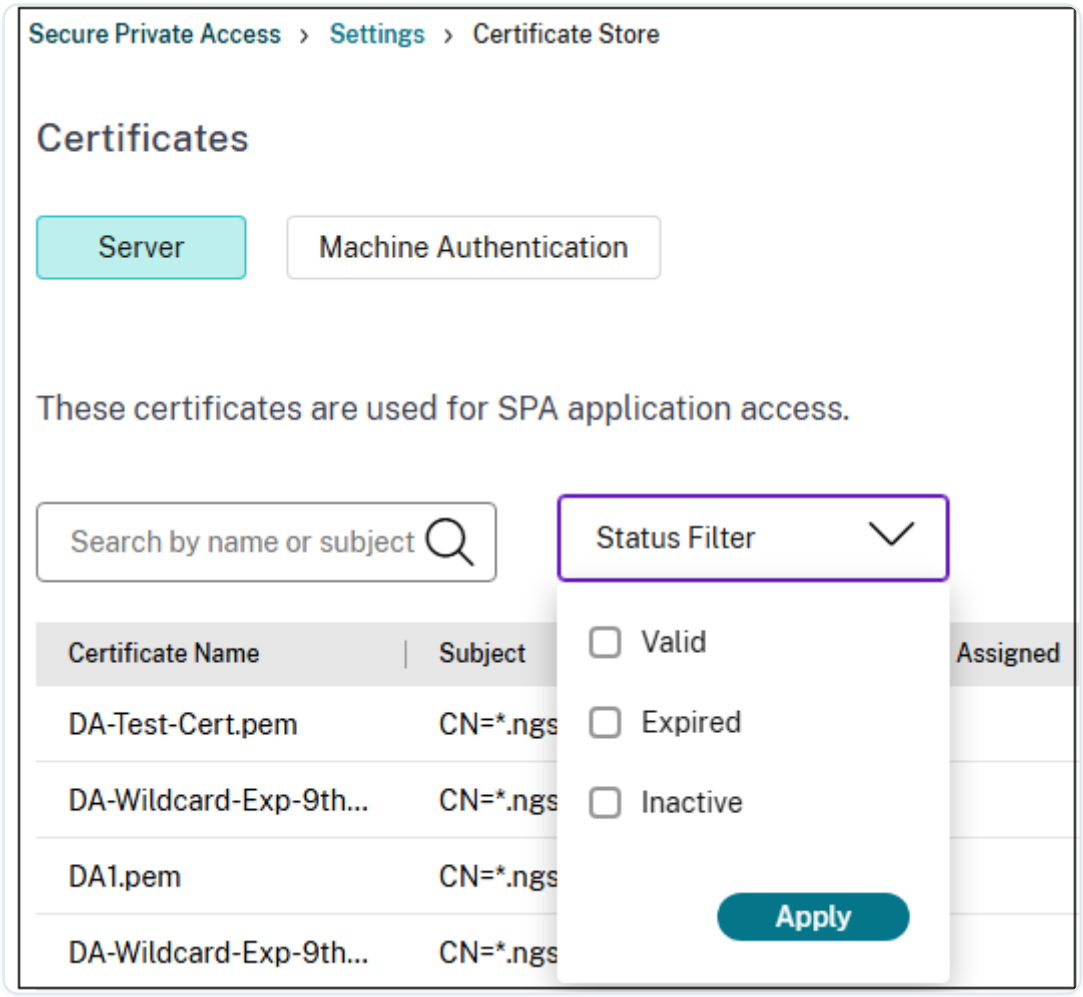
HINWEIS:

- Das Zertifikat wird der Liste der verfügbaren Zertifikate unter der Registerkarte **Server** hinzugefügt.
- Die Spalte **Zugewiesene Anwendungen** zeigt die Anzahl der Anwendungen an, denen ein Zertifikat zugewiesen ist.

Zertifikat suchen

Sie können nach einem SSL-Zertifikat anhand des Zertifikatnamens oder des Betreffs suchen. Sie können auch nach Zertifikaten basierend auf dem Status des Zertifikats suchen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Zertifikat ändern

Schritte zum Ändern eines SSL-Zertifikats.

1. Klicken Sie auf das Bearbeitungssymbol neben dem Zertifikat.
2. Navigieren Sie unter **Zertifikatsdatei** zu Ihrem lokalen Laufwerk und laden Sie die geänderte Zertifikatsdatei hoch.

   Stellen Sie sicher, dass das aktualisierte Zertifikat für dieselbe Domäne oder die Wildcard-Domäne gilt. Andernfalls schlägt der Upload fehl.
3. Klicken Sie auf **Speichern**.

Zertifikat löschen

Klicken Sie auf das Löschsymbol, um ein Zertifikat zu löschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Externe Benachrichtigung

Wenn ein Zertifikat innerhalb des Kontos eines Kunden kurz vor dem Ablaufdatum steht, wird innerhalb des 30-Tage-Fensters vor dem Ablaufdatum automatisch eine E-Mail-Benachrichtigung an die spezifischen Kundenadministratoren gesendet.

Citrix Secure Access™ Client

Mit Citrix Secure Private Access können Sie jetzt auf alle privaten Apps zugreifen, einschließlich TCP/UDP- und HTTPS-Apps, entweder über einen nativen Browser oder eine native Clientanwendung über den Citrix Secure Access Client, der auf Ihrem Computer ausgeführt wird. Sie können jetzt die Abhängigkeit von einer herkömmlichen VPN-Lösung eliminieren, um Remote-Benutzern den Zugriff auf alle privaten Apps zu ermöglichen.

Citrix Secure Access Client für Windows

Details zur Installation des Citrix Secure Access Clients für Windows finden Sie unter Citrix Secure Access Client für Windows installieren.

Weitere Informationen zum Citrix Secure Access Client für Windows finden Sie unter Citrix Secure Access für Windows.

Citrix Secure Access Client für macOS

Details zur Installation des Citrix Secure Access Clients für macOS finden Sie unter Citrix Secure Access Client für macOS installieren.

Weitere Informationen zum Citrix Secure Access Client für macOS finden Sie unter Citrix Secure Access für macOS.

Citrix Secure Access Client für iOS

Details zur Einrichtung des Citrix Secure Access Clients für iOS finden Sie unter Citrix Secure Access für iOS einrichten.

Weitere Informationen zum Citrix Secure Access Client für iOS finden Sie unter Citrix Secure Access für iOS.

Citrix Secure Access Client für Android

Details zur Einrichtung des Citrix Secure Access Clients für Android finden Sie unter Citrix Secure Access für Android einrichten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zum Citrix Secure Access Client für Android finden Sie unter Citrix Secure Access für Android.

Citrix Secure Access Client für Linux

Details zur Installation des Citrix Secure Access Clients für Linux finden Sie unter Installieren des Citrix Secure Access Clients und des Citrix EPA Clients.

Weitere Informationen zum Citrix Secure Access Client für Linux finden Sie unter (/de-de/citrix-secure-access/secure-access-client-linux).

Best Practices für Web- und SaaS-Anwendungskonfigurationen

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

Anwendungszugriff innerhalb von Secure Private Access für veröffentlichte und nicht veröffentlichte Apps

- **Zugriff auf veröffentlichte Webanwendungen und zugehörige Domänen:**
  - Wenn ein Endbenutzer auf einen FQDN zugreift, der mit einer veröffentlichten Web-App verknüpft ist, ist der Zugriff nur zulässig, wenn eine Zugriffsrichtlinie explizit mit der Aktion **Zulassen** oder **Mit Einschränkungen zulassen** für den Benutzer konfiguriert ist.

    HINWEIS:

    Es wird empfohlen, dass nicht mehrere Anwendungen dieselbe Anwendungs-URL-Domäne oder verwandte Domänen für eine exakte Übereinstimmung gemeinsam nutzen. Wenn mehrere Apps dieselbe Anwendungs-URL-Domäne oder verwandte Domänen gemeinsam nutzen, wird der Zugriff basierend auf der exakten FQDN-Übereinstimmung und der Richtlinienpriorisierung gewährt. Weitere Informationen finden Sie unter Abgleich 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. Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Konfiguration und Verwaltung adaptiver Zugriffsrichtlinien.

- **Zugriff auf nicht veröffentlichte interne Webanwendungen und externe Internet-URLs:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 den Zugriff für bestimmte Benutzer zu ermöglichen, stellen Sie sicher, dass Sie eine Zugriffsrichtlinie für Ihre Intranet-Webanwendungen konfiguriert haben.

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

- In solchen Fällen wird der Zugriff auf Intranet-Webanwendungs-URL-Domänen direkt weitergeleitet und somit verweigert (es sei denn, der Benutzer befindet sich bereits im Intranet).
- Für nicht veröffentlichte Internet-URLs basiert der Zugriff auf den Regeln, die für nicht genehmigte Apps konfiguriert sind, falls aktiviert. Standardmäßig ist dieser Zugriff innerhalb von Secure Private Access erlaubt.

Abgleich und Priorisierung von Zugriffsrichtlinien

Secure Private Access führt die folgenden Schritte aus, während eine Anwendung für den Zugriff abgeglichen wird:

1. Gleichen Sie die aufgerufene Domäne mit der Domäne der Anwendungs-URL oder verwandten Domänen für eine exakte Übereinstimmung ab.
2. Wenn eine Secure Private Access-Anwendung mit einer exakten FQDN-Übereinstimmung gefunden wird, wertet Secure Private Access alle für diese Anwendung konfigurierten Richtlinien aus.
    - Richtlinien werden in einer Prioritätsreihenfolge ausgewertet, bis der Benutzerkontext übereinstimmt. Die Aktion (Zulassen/Verweigern) wird gemäß der ersten Richtlinie angewendet, die in der Prioritätsreihenfolge übereinstimmt.
    - Wenn keine Richtlinie übereinstimmt, wird der Zugriff standardmäßig verweigert.
3. Wenn keine exakte FQDN-Übereinstimmung gefunden wird, gleicht Secure Private Access die Domäne basierend auf der längsten Übereinstimmung (z. B. einer Wildcard-Übereinstimmung) ab, um Anwendungen und entsprechende Richtlinien zu finden.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ANWENDUNG	ANWENDUNGS-URL	VERWANDTE DOMÄNE
Intranet	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

RICHTLINIENNAME	PRIORITÄT	BENUTZER UND ZUGEHÖRIGE APPS
PolicyA	Hoch	Eng-User5 (Intranet)
PolicyB	Niedrig	HR-User4 (Wiki)

Wenn `HR-User4` auf `app.intranet.local` zugreift, geschieht Folgendes:

a. Secure Private Access durchsucht alle Richtlinien nach einer exakten Übereinstimmung für die aufgerufene Domäne, in diesem Fall `app.intranet.local`.

b. Secure Private Access findet `PolicyA` und prüft, ob die Bedingungen übereinstimmen.

c. Da die Bedingungen nicht übereinstimmen, stoppt Secure Private Access hier und prüft die Wildcard-Übereinstimmungen nicht weiter, obwohl `PolicyB` übereingestimmt hätte (da `app.intranet.local` mit der zugehörigen Domäne der Wiki-App von `*.intranet.local` übereinstimmt) und Zugriff gewährt hätte.

d. Daher wird `HR-User4` der Zugriff auf die Wiki-App verweigert.

Beispiel 2: Betrachten Sie die folgenden Apps und die Richtlinienkonfiguration, bei der dieselbe Domäne in mehreren Anwendungen verwendet wird:

ANWENDUNG	ANWENDUNGS-URL	ZUGEHÖRIGE DOMÄNE
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

RICHTLINIENNAME	PRIORITÄT	BENUTZER UND ZUGEHÖRIGE APPS
PolicyA	Hoch	Eng-User5 (App1)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RICHTLINIENNAME	PRIORITÄT	BENUTZER UND ZUGEHÖRIGE APPS
PolicyB	Niedrig	HR-Benutzer7 (App2)

Wenn Benutzer `Eng-User5` auf `app.intranet.local` zugreift, stimmen sowohl App1 als auch App2 aufgrund der exakten FQDN-Übereinstimmung überein, und daher erhält der Benutzer `Eng-User5` Zugriff über `PolicyA`.

Wenn App1 jedoch stattdessen `*.intranet.local` als zugehörige Domäne hätte, wäre der Zugriff für `Eng-User5` verweigert worden, da `app.intranet.local` exakt mit `PolicyB` übereingestimmt hätte, für die der Benutzer `Eng-User5` keinen Zugriff hat.

Best Practices für die App-Konfiguration

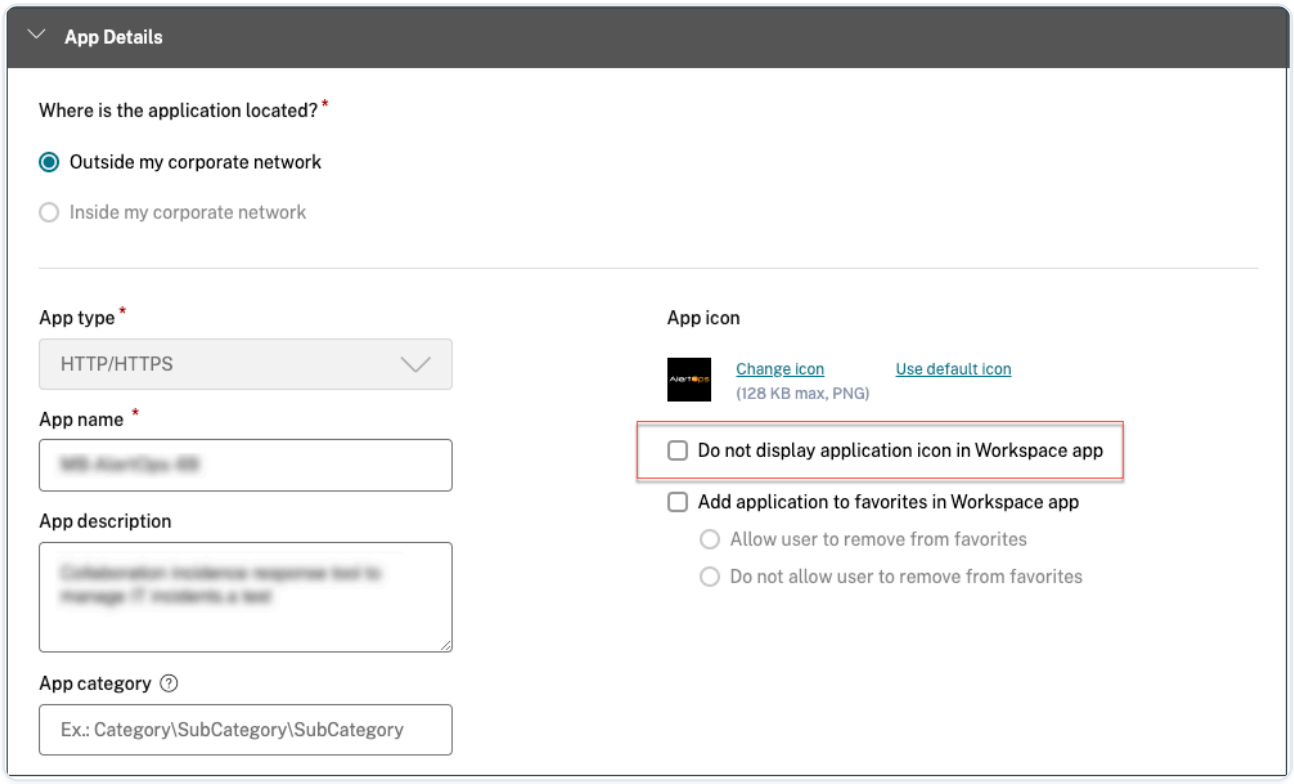
Die folgenden Abschnitte enthalten weitere Informationen zu den Best Practices für die Anwendungskonfiguration.

IdP-Domänen müssen eine eigene Anwendung haben

Anstatt IdP-Domänen als zugehörige Domänen in Ihren Intranet-App-Konfigurationen hinzuzufügen, empfehlen wir Folgendes:

- Erstellen Sie separate Anwendungen für alle IdP-Domänen.
- Erstellen Sie eine Richtlinie, um allen Benutzern, die Zugriff auf die IdP-Authentifizierungsseite benötigen, den Zugriff zu ermöglichen, und legen Sie die Richtlinie mit der höchsten Priorität fest.
- Blenden Sie diese App (indem Sie die Option **Anwendungssymbol Benutzern nicht anzeigen** auswählen) aus der App-Konfiguration aus, damit sie nicht im Store aufgelistet wird. Weitere Informationen finden Sie unter Anwendungsdetails konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Diese App-Konfiguration ermöglicht nur den Zugriff auf die IdP-Authentifizierungsseite. Der weitere Zugriff auf einzelne Anwendungen hängt weiterhin von den jeweiligen App-Konfigurationen und deren 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 `login.microsoftonline.com` sowie andere verwandte Domänen (`*.msauth.net`) konfigurieren müssen, gehen Sie wie folgt vor:

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

2. Wählen Sie beim Konfigurieren der App die Option **Anwendungssymbol Benutzern nicht anzeigen** aus. Weitere Informationen finden Sie unter Anwendungsdetails konfigurieren.
3. Erstellen Sie eine Zugriffsrichtlinie für die gemeinsame Anwendung und aktivieren Sie den Zugriff für alle Benutzer. Weitere Informationen finden Sie unter Zugriffsrichtlinie konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Weisen Sie der Zugriffsrichtlinie die höchste Priorität zu. Weitere Informationen finden Sie unter Prioritätsreihenfolge.
5. Überprüfen Sie die Diagnoseprotokolle, um zu bestätigen, dass der FQDN mit der App übereinstimmt und die Richtlinie wie erwartet durchgesetzt wird.

Dieselben verwandten Domänen dürfen nicht Teil mehrerer Anwendungen sein

Die zugehörige Domäne muss für eine App eindeutig sein. Konfligierende Konfigurationen können zu Problemen beim App-Zugriff führen. Wenn mehrere Apps mit demselben FQDN oder einer Variante des Wildcard-FQDN konfiguriert sind, können folgende Probleme auftreten:

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

Daher empfehlen wir, eine eindeutige zugehörige Domäne innerhalb einer einzelnen App zu konfigurieren.

Beispiele für falsche Konfigurationen:

- **Beispiel: Doppelte zugehörige Domänen in mehreren Anwendungen**

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

APP	ANWENDUNGS-URL-DOMÄNE	ZUGEHÖRIGE DOMÄNE
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

RICHTLINIENNAME	PRIORITÄT	BENUTZER UND ZUGEHÖRIGE APPS
App1 für HR verweigern	Hoch	Benutzergruppe `HR` für `App1`
Allen Benutzern Zugriff auf App1 gewähren	Mittel	Zugriff für die Benutzergruppe „Jeder“ auf App1 aktivieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RICHTLINIENNAME	PRIORITÄT	BENUTZER UND ZUGEHÖRIGE APPS
Allen Benutzern Zugriff auf App2 gewähren	Niedrig	Zugriff für die Benutzergruppe Jeder" auf App2 aktivieren

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

Dieses Szenario ist bei Identitätsanbietern wie Okta üblich, kann aber auch bei anderen eng integrierten Apps mit gemeinsamen verwandten Domänen auftreten. Details zur Richtlinienübereinstimmung und -priorisierung finden Sie unter Abgleich und Priorisierung von Zugriffsrichtlinien.

Empfehlung für die obige Konfiguration:

a. Entfernen Sie example.okta.com als verwandte Domäne aus allen Apps.
b. Erstellen Sie eine neue App nur für Okta (mit der Anwendungs-URL `https://example.okta.com` und einer verwandten Domäne `*.okta.com`).
c. Blenden Sie diese App aus dem Store aus.
d. Weisen Sie der Richtlinie die höchste Priorität zu, um Konflikte zu vermeiden.

Bewährte Methode:

- Die zugehörigen Domänen einer App dürfen sich nicht mit den zugehörigen Domänen einer anderen App überschneiden.
- Wenn dies der Fall ist, muss eine neue veröffentlichte App erstellt werden, um die gemeinsam genutzte zugehörige Domäne abzudecken, und der Zugriff muss dann entsprechend festgelegt werden.
- Administratoren müssen prüfen, ob diese gemeinsam genutzte zugehörige Domäne als tatsächliche App im Store erscheinen soll.
- Wenn die App nicht im Store erscheinen soll, wählen Sie beim Veröffentlichen der App die Option **Anwendungssymbol für Benutzer nicht anzeigen**, um sie aus dem Store auszublenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konflikte beheben, die sich aus denselben zugehörigen Domänen ergeben

In Szenarien, in denen sich die zugehörigen Domänen einer App mit den Domänen einer anderen App überschneiden, haben Administratoren die Flexibilität, diese Anwendungen entweder extern oder intern über die Connector Appliances weiterzuleiten, basierend auf spezifischen Anforderungen. Die Routing-Tabelle in der Secure Private Access-Konsole (**Einstellungen > Anwendungsdomänen**) bietet eine umfassende Liste aller konfigurierten Domänen für alle Anwendungen. Diese Tabelle zeigt wichtige Informationen zu jeder Domäne, einschließlich des Routing-Typs. Administratoren können den Routing-Typ einfach ändern, indem sie auf das Bearbeitungssymbol neben dem entsprechenden Domäneneintrag klicken.

Die Hauptroutingtabelle zeigt die folgenden Informationen für jede Domäne an:

- **FQDN/IP:** FQDN oder die IP-Adresse, für die die Art der Datenverkehrsweiterleitung konfiguriert werden soll.
- **Typ:** App-Typ. **Intern**, **Intern – Proxy umgehen** oder **Extern**, wie beim Hinzufügen der App ausgewählt.
  - **Intern** – Die Apps sind extern, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
  - **Intern – Proxy umgehen** – Der Domänenverkehr wird über den Citrix Cloud Connector™ geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
  - **Extern** – Der Datenverkehr fließt direkt ins Internet.

  WICHTIG:

  Wenn Konflikte vorliegen, wird ein Warnsymbol für die entsprechende Zeile in der Tabelle angezeigt. Um den Konflikt zu beheben, sollten Administratoren auf das dreieckige Symbol klicken, das mit diesem Eintrag verknüpft ist, und den App-Typ ändern.

- **Ressourcenstandort:** Ressourcenstandort für Routing vom Typ Intern. Wenn kein Ressourcenstandort zugewiesen ist, erscheint in der Spalte „Ressourcenstandort“ für die jeweilige App ein dreieckiges Symbol. Wenn Sie den Mauszeiger über das Symbol bewegen, wird die folgende Meldung angezeigt.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Status:** Der Umschalter in der Spalte „Status“ kann verwendet werden, um die Route für einen Routeneintrag zu deaktivieren, ohne die App zu löschen. Wenn der Umschalter AUSGESCHALTET ist, wird der Routeneintrag nicht wirksam. Wenn auch FQDNs mit exakter Übereinstimmung vorhanden sind, können Administratoren die zu aktivierende oder deaktivierende Route auswählen.
- **Kommentare:** Zeigt Kommentare an, falls vorhanden.
- **Aktionen:** Das Bearbeitungssymbol wird verwendet, um einen Ressourcenstandort hinzuzufügen oder den Typ des Routeneintrags zu ändern. Das Löschsymbol wird verwendet, um die Route zu löschen.

HINWEIS:

Eine Mini-Version der Anwendungsdomänentabelle ist verfügbar, um die Routing-Entscheidungen während der App-Konfiguration zu treffen. Die Mini-Routing-Tabelle ist im Abschnitt „App-Konnektivität“ in der Admin-Konsole des Citrix Secure Private Access™-Dienstes verfügbar.

Deep-Link-URLs

Für Deep-Link-URLs muss die URL-Domäne der Intranet-Anwendung als die zugehörige Domäne hinzugefügt werden:

Beispiel:

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

In diesem Fall erstellen Sie separat eine IdP-App mit der URL `https://example.okta.com` und dann die zugehörige Domäne als `*.example.okta.com`.

Endbenutzererfahrung beim App-Zugriff erklärt

Citrix Secure Private Access™-Apps können auf folgende Weisen aufgerufen werden:

- **Über den Citrix Secure Access™-Client:**
  - Zugriff auf Web-/SaaS-Apps: Nach der Anmeldung beim Citrix Secure Access-Client können Endbenutzer Web-/SaaS-Apps über ihren nativen Browser wie Chrome aufrufen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Zugriff auf TCP/UDP-Apps: Nach der Anmeldung beim Citrix Secure Access-Client können Endbenutzer TCP/UDP-Anwendungen über eine Clientanwendung (z. B. Remote Desktop Protocol (RDP)) aufrufen.

- **Agentenloser Zugriff:** Ermöglicht Benutzern den Zugriff auf Unternehmens-Web-Apps, ohne dass ein Client erforderlich ist. Endbenutzer können auf Unternehmens-Webanwendungen zugreifen, ohne einen dedizierten Client auf ihren Geräten installieren zu müssen. Endbenutzer können die App-URLs einfach in ihren nativen Browser eingeben.

Zugriff auf eine Web-App über den Citrix Secure Access-Client

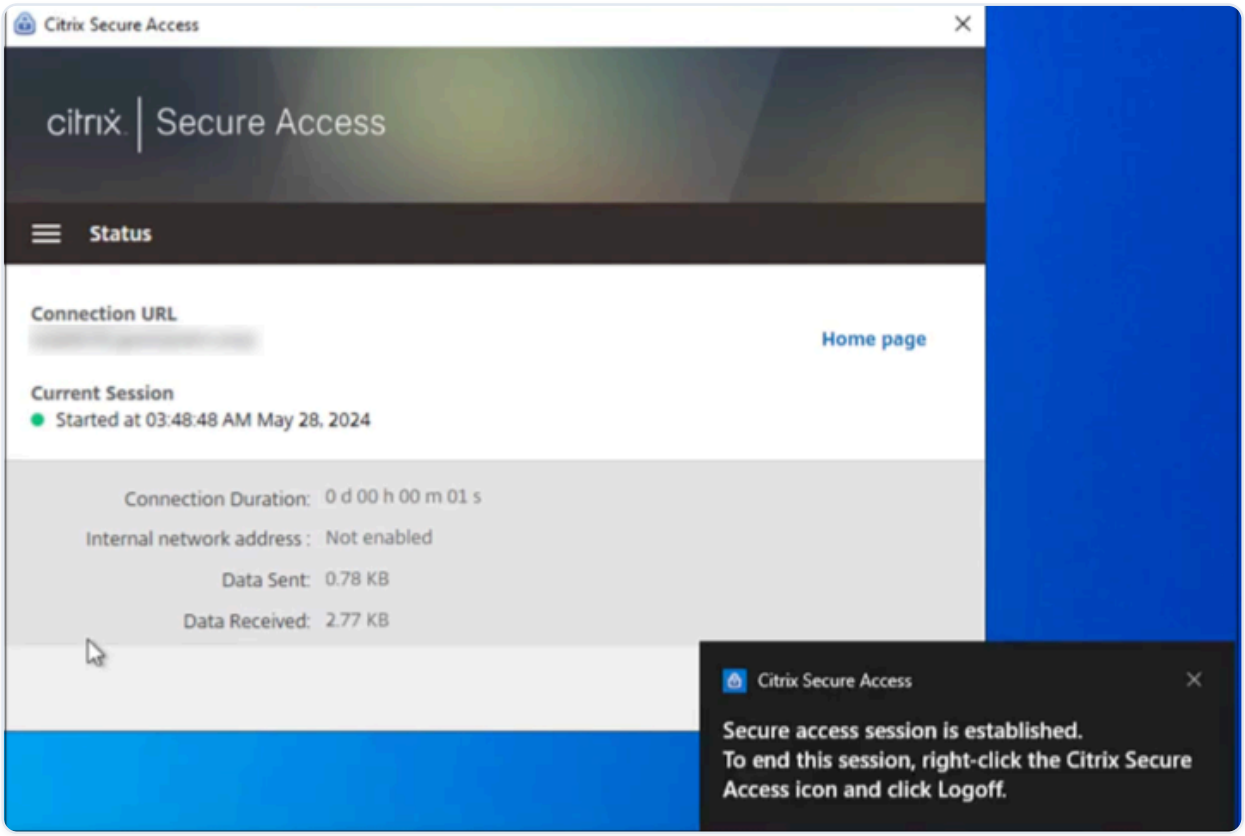
1. Melden Sie sich beim Citrix Secure Access-Client an.
2. Nachdem die sichere Zugriffssitzung hergestellt wurde, öffnen Sie einen nativen Browser (z. B. Chrome).
3. Geben Sie im Browser die URL der Unternehmens-Web-App ein, auf die Sie zugreifen möchten.

Zugriff auf eine TCP/UDP-App über den Citrix Secure Access-Client

Wenn RDP konfiguriert ist, müssen Endbenutzer die folgenden Schritte ausführen, um auf die TCP/UDP-App zuzugreifen.

1. Melden Sie sich beim Citrix Secure Access-Client an.
2. Nachdem die sichere Zugriffssitzung hergestellt wurde, starten Sie eine Remotedesktopverbindung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



RDP-Verbindung2(/en-us/citrix-secure-private-access/media/spaop-rdp-session.png)

a. Drücken Sie die **Windows**-Taste, geben Sie **Remotedesktopverbindung** ein und drücken Sie die **Eingabetaste**.
b. Geben Sie die IP-Adresse oder den Hostnamen des Computers ein, mit dem Sie eine Verbindung herstellen möchten.
c. Klicken Sie auf **Verbinden**. Möglicherweise werden Sie aufgefordert, die Anmeldeinformationen einzugeben.
d. Geben Sie den Benutzernamen und das Kennwort für den Remotecomputer ein und klicken Sie dann auf **OK**.

Eine Remotedesktopverbindung ist nun hergestellt und der Endbenutzer kann mit dem Remotecomputer interagieren.

Weitere Informationen zum Citrix Secure Access Client finden Sie unter Citrix Secure Access Client.

Connector Appliance für Secure Private Access

Die Connector Appliance ist eine Citrix-Komponente, die in Ihrem Hypervisor gehostet wird. Sie dient als Kommunikationskanal zwischen Citrix Cloud™ und Ihren Ressourcenstandorten und ermöglicht Cloud-Management, ohne komplexe Netzwerk- oder Infrastrukturkonfigurationen zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

erfordern. Die Connector Appliance ermöglicht es Ihnen, die Ressourcen zu verwalten und sich auf diese zu konzentrieren, die Ihren Benutzern einen Mehrwert bieten.

Alle Verbindungen werden von der Connector Appliance zur Cloud unter Verwendung des Standard-HTTPS-Ports (443) und des TCP-Protokolls hergestellt. Es werden keine eingehenden Verbindungen akzeptiert. TCP-Port 443 mit den folgenden FQDNs sind ausgehend zulässig:

- *.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 in Ihrem Ressourcenstandort.

   Weitere Informationen zum Einrichten Ihrer Connector Appliances finden Sie unter Connector Appliance für Cloud Services.

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

   a. Fügen Sie Ihre Connector Appliance einer Active Directory-Domäne hinzu.

      Das Beitreten einer Active Directory-Gesamtstruktur ermöglicht die Verwendung von Kerberos Constrained Delegation (KCD) bei der Konfiguration von Secure Private Access, aber es ermöglicht nicht die Verwendung des Connector Appliance für Identitätsanfragen oder Authentifizierung.

      - Verbinden Sie sich in Ihrem Browser mit der Administrationswebseite der Connector Appliance, indem Sie die in der Connector Appliance-Konsole angegebene IP-Adresse verwenden.
      - Klicken Sie im Abschnitt **Active Directory-Domänen** auf **+ Active Directory-Domäne hinzufügen**.

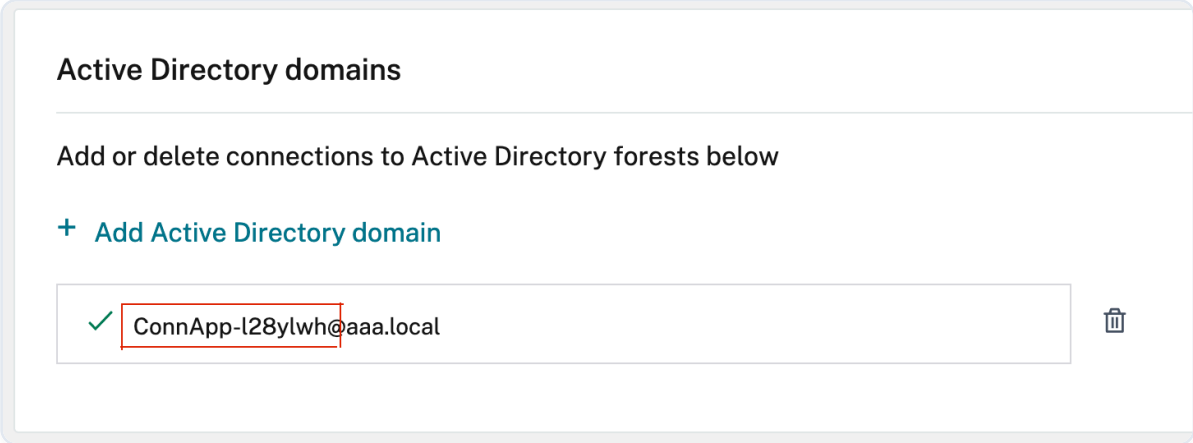
        Wenn Sie keinen Abschnitt **Active Directory-Domänen** auf Ihrer Administrationsseite haben, wenden Sie sich an Citrix®, um die Teilnahme an der Vorschau anzufordern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Geben Sie den Domänennamen in das Feld **Domänenname** ein. Klicken Sie auf **Hinzufügen**.
- Die Connector Appliance überprüft die Domäne. Wenn die Überprüfung erfolgreich ist, wird das Dialogfeld **Active Directory beitreten** geöffnet.
- Geben Sie den Benutzernamen und das Kennwort eines Active Directory-Benutzers ein, der über die Berechtigung zum Beitreten dieser Domäne verfügt.
- Die Connector Appliance schlägt einen Computernamen vor. Sie können den vorgeschlagenen Namen überschreiben und einen eigenen Computernamen mit bis zu 15 Zeichen Länge angeben. Notieren Sie sich den Computerkontonamen.

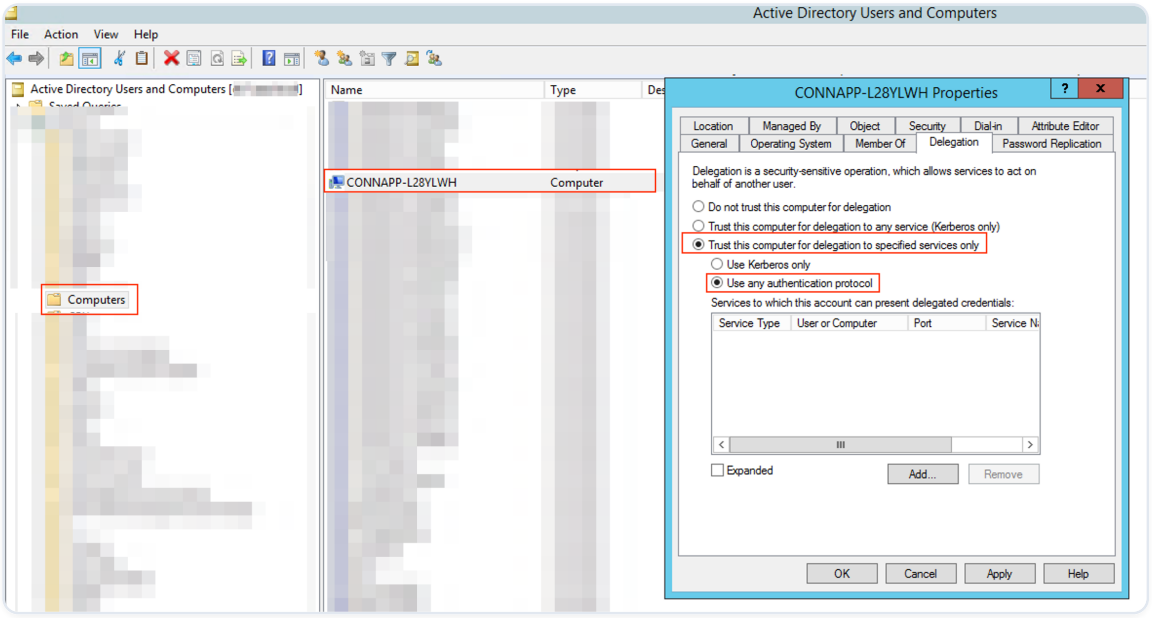
  Dieser Computername wird in der Active Directory-Domäne erstellt, wenn die Connector Appliance ihr beitritt.
- Klicken Sie auf **Beitreten**.

b. Konfigurieren Sie die Kerberos Constrained Delegation für einen Webserver ohne Lastenausgleich.

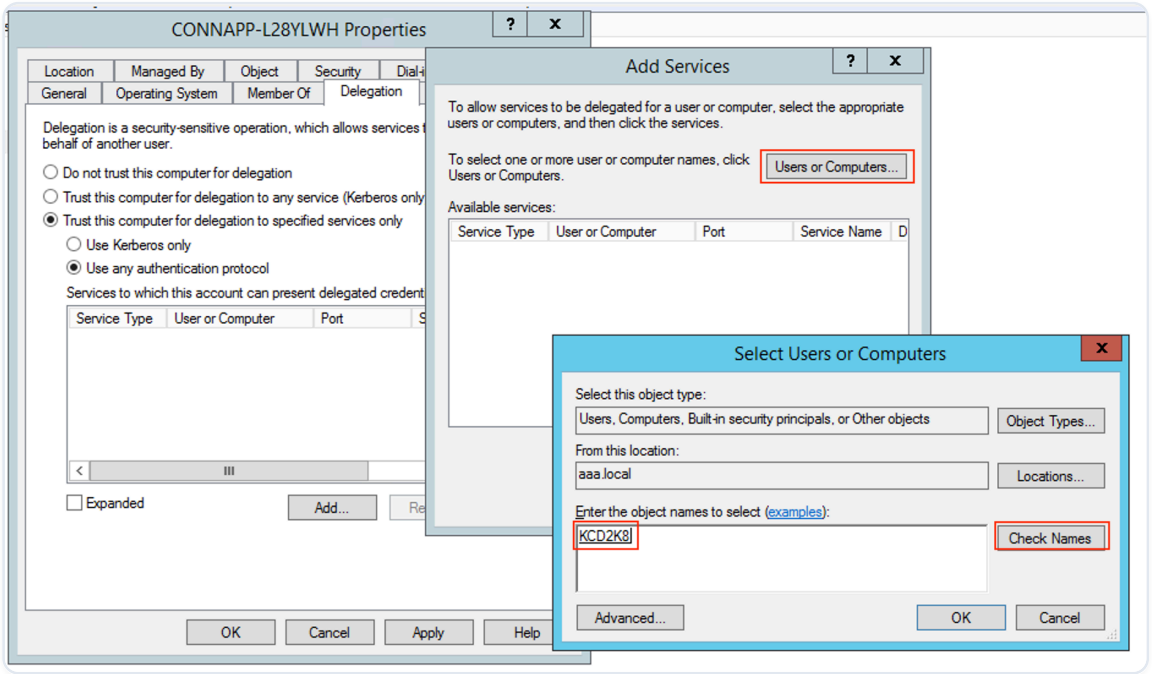


- Identifizieren Sie den Computernamen der Connector Appliance. Sie können diesen Namen entweder von dem Ort erhalten, an dem Sie ihn gehostet haben, oder einfach über die Connector-Benutzeroberfläche.
- Suchen Sie auf Ihrem Active Directory-Controller nach dem Computer der Connector Appliance.
- Gehen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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

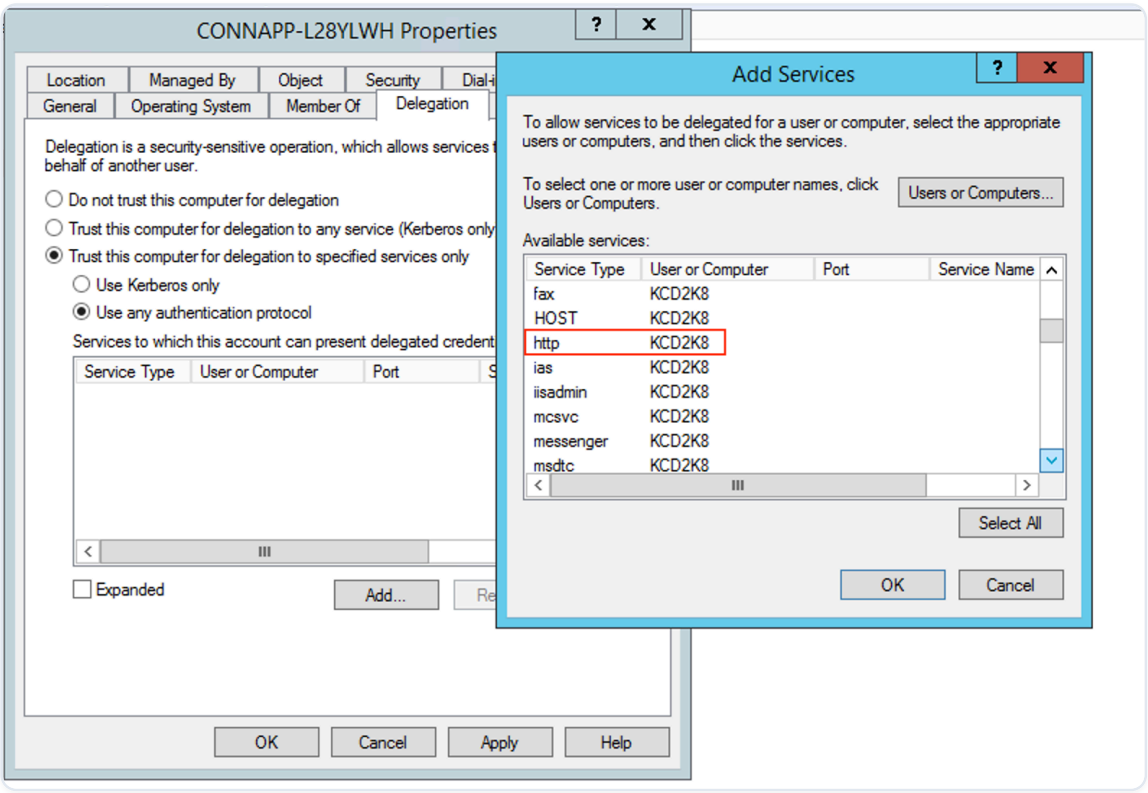


- Klicken Sie auf **Hinzufügen.**
- Klicken Sie auf **Benutzer oder Computer.**
- Geben Sie den Computernamen des Ziel-Webservers ein, und klicken Sie dann auf **Namen überprüfen.** Im vorhergehenden Bild ist **KCD2K8** der Webserver.



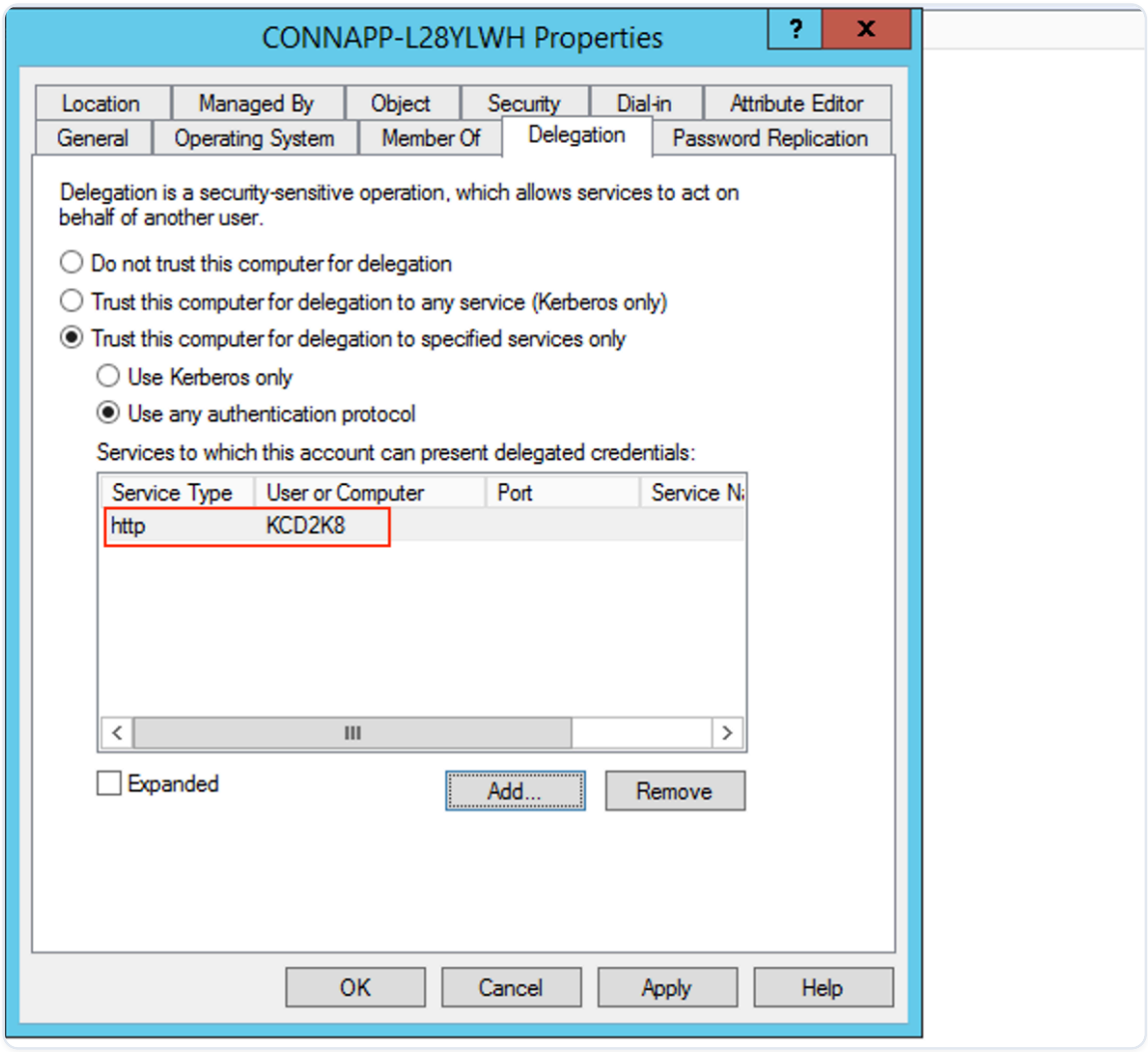
- Klicken Sie auf **OK.**
- Wählen Sie den Diensttyp **http.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

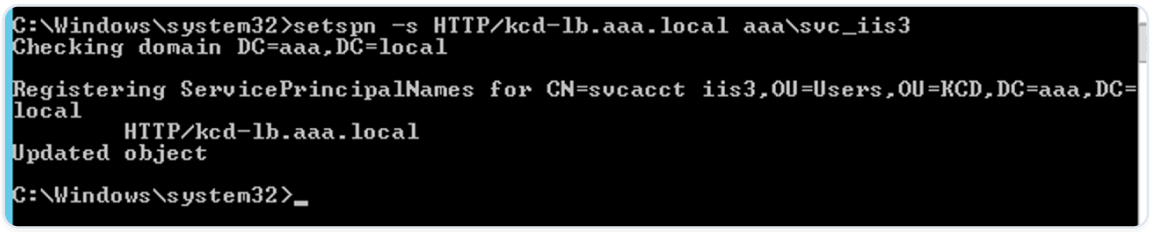
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Damit ist der Vorgang zum Hinzufügen der Delegierung für einen Webserver abgeschlossen.

c. Konfigurieren Sie die Kerberos Constraint Delegation (KCD) für einen Webserver hinter einem Load Balancer.

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

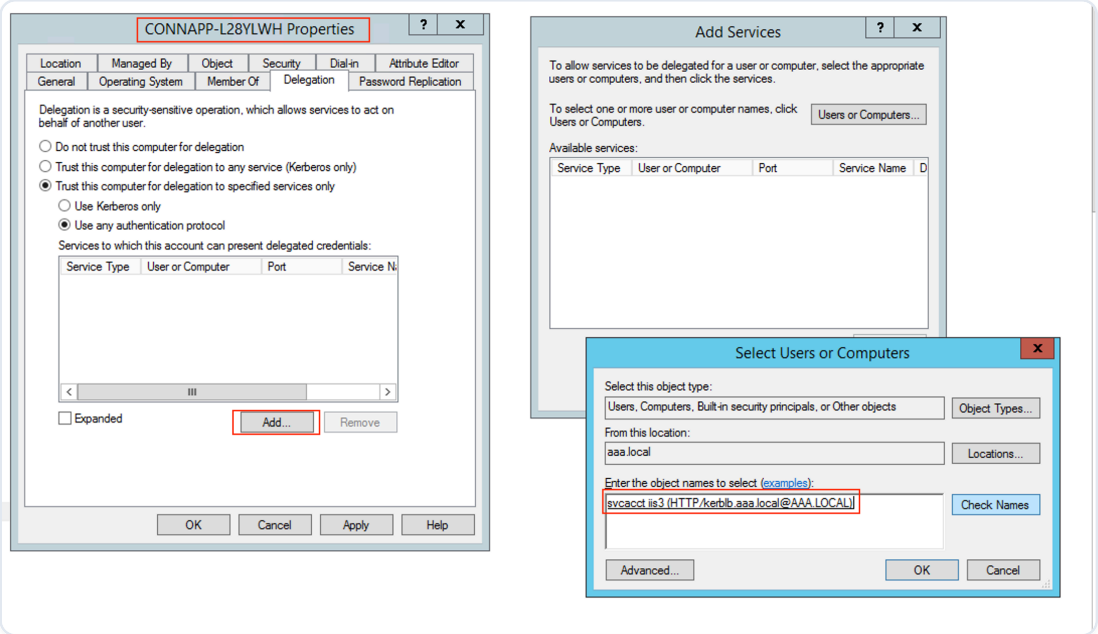


- Bestätigen Sie die SPNs für das Dienstkonto mit dem folgenden Befehl. `setspn -l <service_account>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

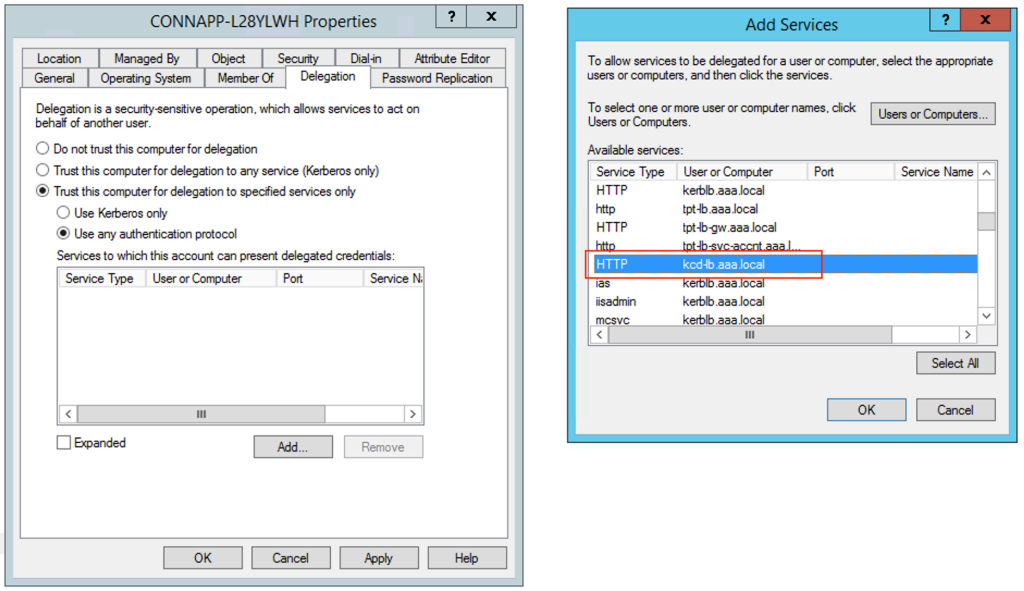


- Erstellen Sie eine Delegierung für das Computerkonto der Connector Appliance.
  - Befolgen Sie die Schritte unter *Kerberos Constraint Delegation für den Webserver ohne Lastenausgleich konfigurieren*, um den CA-Computer zu identifizieren und zur Delegierungs-Benutzeroberfläche zu navigieren.
  - Wählen Sie unter **Benutzer und Computer** das Dienstkonto aus (zum Beispiel aaa\svc_iis3).



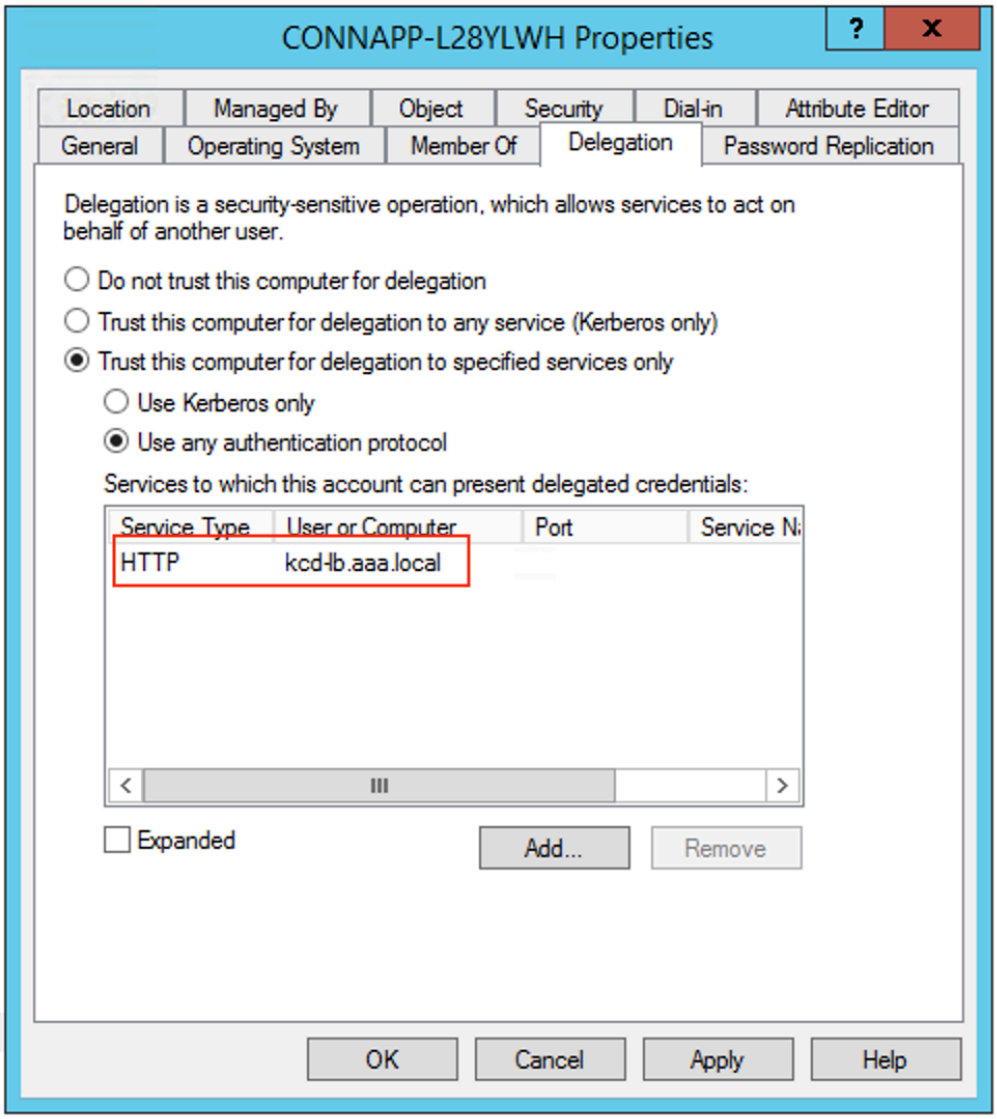
  - Wählen Sie in den Diensten den Eintrag **ServiceType: HTTP** und Benutzer oder Computer: Webserver aus (zum Beispiel `kcd-lb.aaa.local`)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



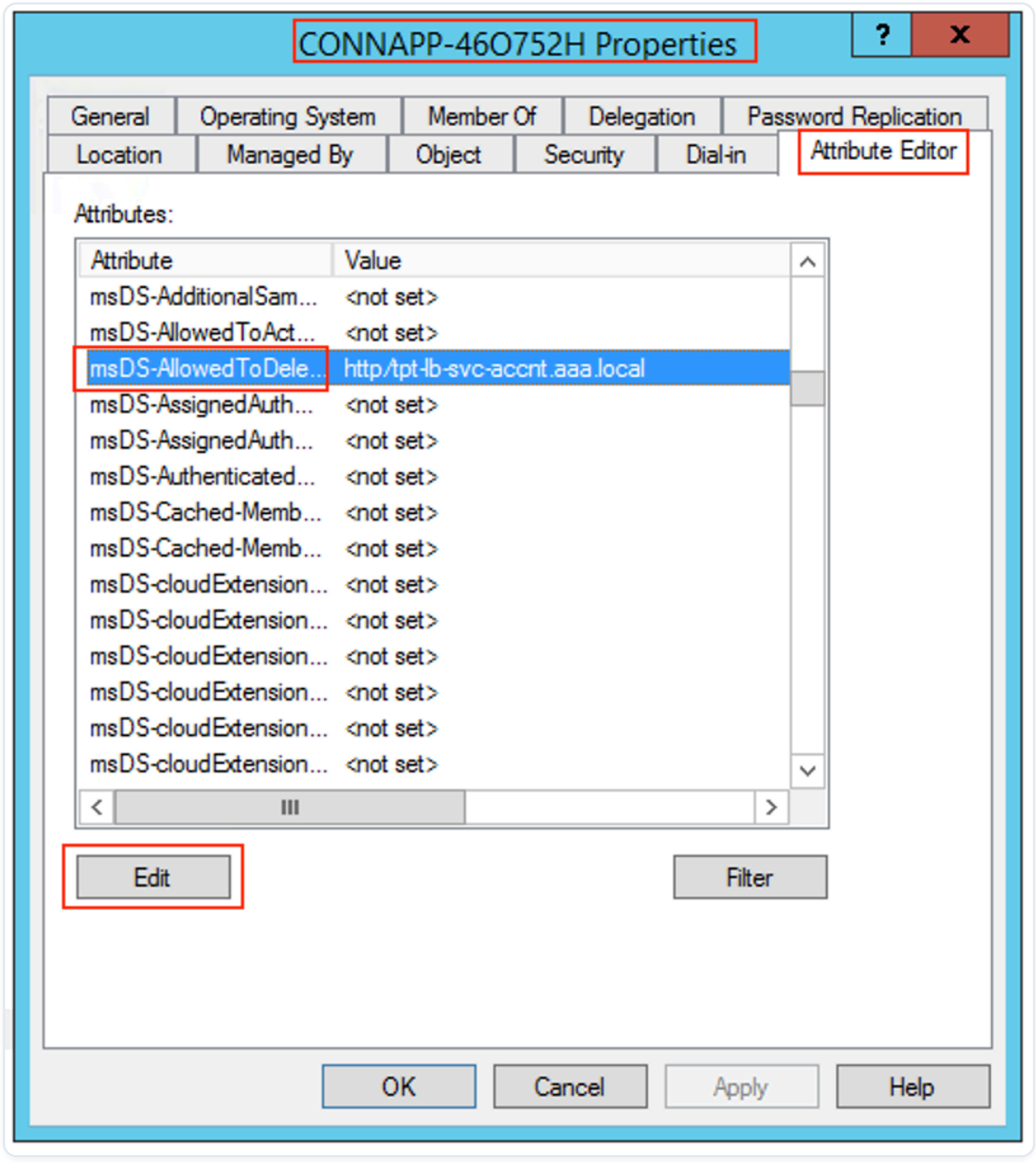
d. Konfigurieren Sie die Kerberos Constrained Delegation (KCD) für ein gruppenverwaltetes Dienstkonto.

   - Fügen Sie dem gruppenverwalteten Dienstkonto einen SPN hinzu, falls noch nicht geschehen. `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 bei der Hinzufügung des Delegierungseintrags für das Computerkonto nicht in der `Users and Computers`-Suche angezeigt werden kann, können Sie die Delegierung für ein Computerkonto nicht mit der üblichen Methode hinzufügen. Daher können Sie diesen SPN als delegierten Eintrag zum CA-Computerkonto hinzufügen, indem Sie den Attribut-Editor verwenden.

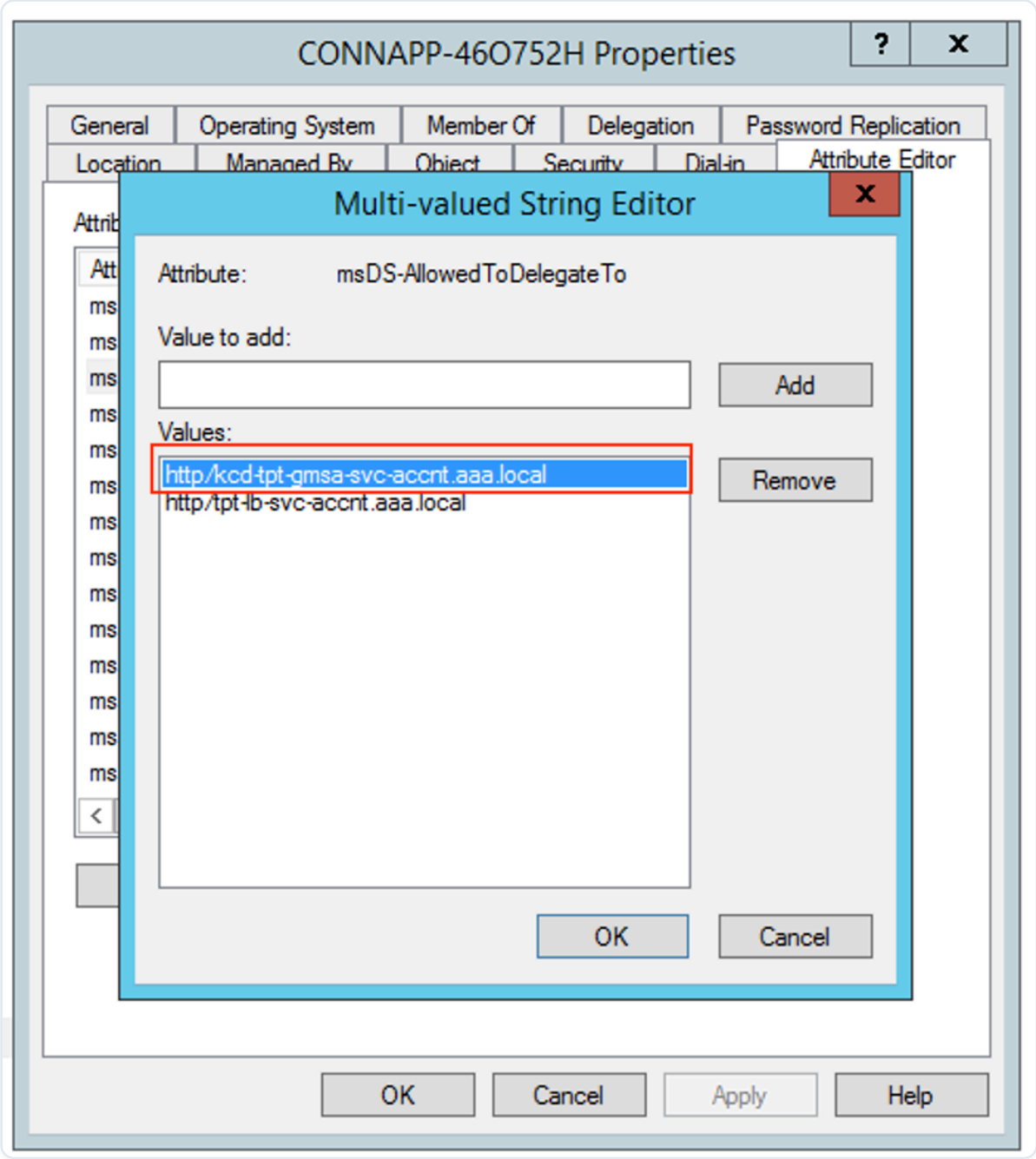
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.



)

© 1997–2026 Citrix Systems, Inc. All rights reserved.



)

e. Von Citrix Gateway Connector™ zu Citrix Connector Appliance migrieren.

- Da SPNs bereits für das Dienstkonto festgelegt sind, während der Gateway-Connector konfiguriert wird, müssen Sie keine weiteren SPNs für das Dienstkonto hinzufügen, wenn keine neue Kerberos-Anwendung konfiguriert ist. Sie können die Liste aller für das Dienstkonto zugewiesenen SPNs mit dem folgenden Befehl anzeigen und sie als delegierte Einträge für das CA-Computerkonto zuweisen.

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

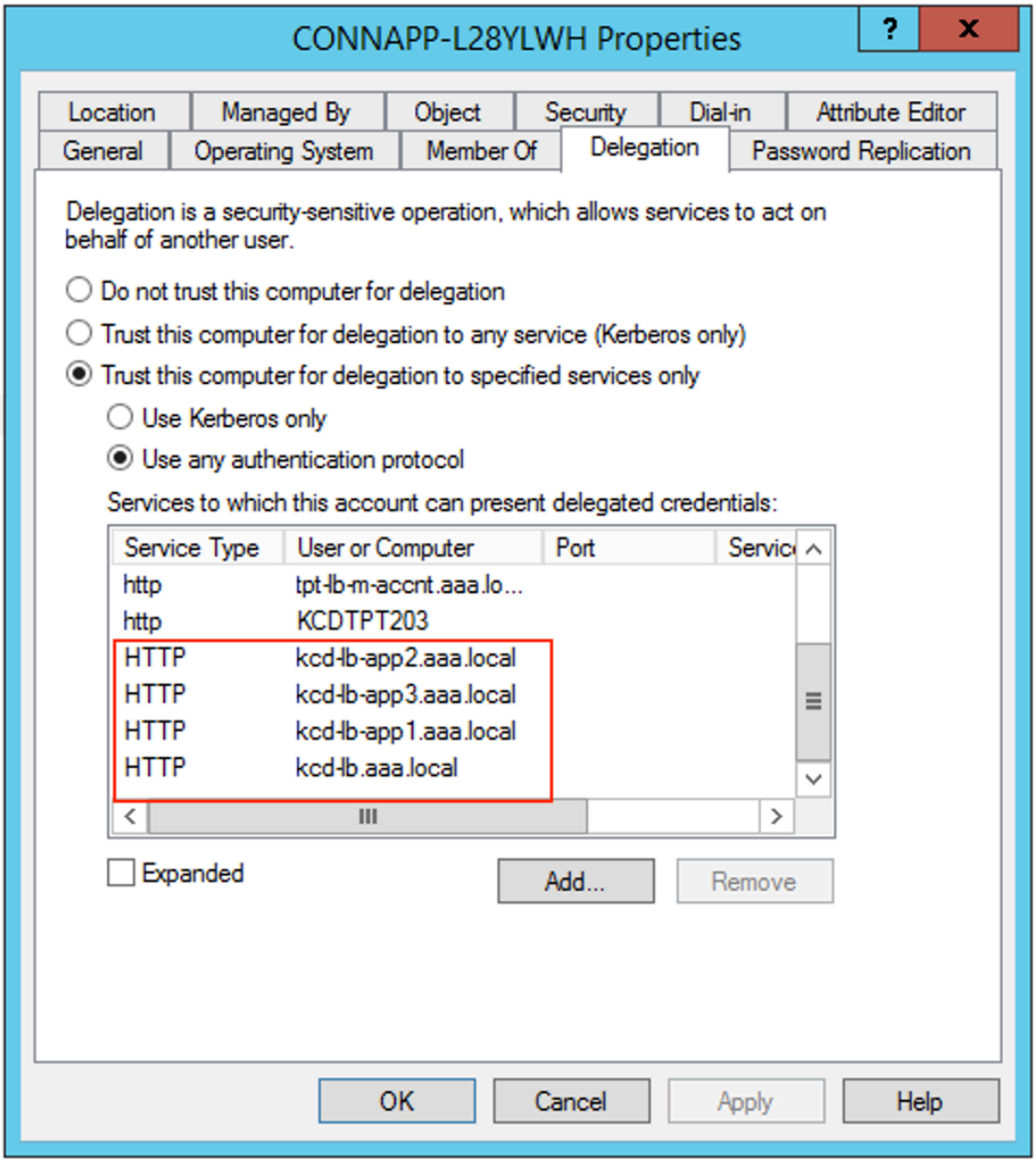
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Hinweis: Diese SPNs wurden dem Dienstkonto als delegierte Einträge hinzugefügt, während der Gateway-Connector konfiguriert wurde. Da Sie von der Dienstkontodelegierung abweichen, können diese Einträge von der Registerkarte **Delegierung** des Dienstkontos entfernt werden.

f. Befolgen Sie die Dokumentation zu Citrix Secure Private Access™, um den Citrix Secure Private Access-Dienst einzurichten. Während der Einrichtung erkennt Citrix Cloud die Präsenz Ihrer Connector Appliances und verwendet sie, um eine Verbindung zu Ihrem Ressourcenstandort herzustellen.

- Erste Schritte mit Citrix Secure Private Access
- Citrix Secure Private Access konfigurieren
- Connector Appliance für Cloud Services
- Anforderungen an die Internetkonnektivität.
- Unterstützung für Enterprise-Webanwendungen

Validieren Ihrer Kerberos-Konfiguration

Wenn Sie Kerberos für Single Sign-On verwenden, können Sie auf der **Verwaltungsseite der Connector Appliance** überprüfen, ob die Konfiguration auf Ihrem Active Directory-Controller korrekt ist. Die Funktion **Kerberos-Validierung** ermöglicht es Ihnen, eine Kerberos-Konfiguration im Realm-Only-Modus oder eine Kerberos Constrained Delegation (KCD)-Konfiguration zu validieren.

1. Gehen Sie zur **Verwaltungsseite der 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 Passwort ein, das Sie bei der Registrierung Ihrer Connector Appliance festgelegt haben.
2. Wählen Sie im Admin-Menü oben rechts die Option **Kerberos-Validierung**.
3. Wählen Sie im Dialogfeld **Kerberos-Validierung** den **Kerberos-Validierungsmodus**.
4. Geben Sie die **Active Directory-Domäne** an oder wählen Sie sie aus.
   - Wenn Sie eine Kerberos-Konfiguration im Realm-Only-Modus validieren, können Sie eine beliebige Active Directory-Domäne angeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn Sie eine Kerberos Constrained Delegation-Konfiguration validieren, müssen Sie aus einer Liste von Domänen in der verbundenen Gesamtstruktur auswählen.

5. Geben Sie den **Dienst-FQDN** an. Der Standarddienstname wird als `http` angenommen. Wenn Sie „computer.example.com“ angeben, wird dies als dasselbe wie `http/computer.example.com` betrachtet.
6. Geben Sie den **Benutzernamen** an.
7. Wenn Sie eine Kerberos-Konfiguration im Realm-Only-Modus validieren, geben Sie das **Passwort** für diesen Benutzernamen an.
8. Klicken Sie auf **Kerberos testen**.

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

Überlegungen zu Skalierung und Größe

Dieser Artikel beschreibt die Richtlinien zur Bestimmung der maximalen Anzahl gleichzeitiger TCP-Verbindungen und gleichzeitiger Web-App-Anfragen für eine einzelne Connector Appliance an einem Ressourcenstandort.

Web- und SaaS-Anwendungen

Die empfohlene Mindestgröße für eine virtuelle Maschine der Connector Appliance beträgt 2 vCPU und 4 GB RAM. Für Hochverfügbarkeit und Ausfallsicherheit wird empfohlen, zwei Connector Appliances bereitzustellen.

Bereitstellungsrichtlinien: Eine Connector Appliance mit 2 vCPU, 4 GB Arbeitsspeicher und einer 10-Gbit/s-NIC kann Folgendes unterstützen:

- Bis zu 500 Web-App-Anfragen pro Sekunde (Secure Browse).
- Datendurchsatzrate von bis zu 1 Gbit/s.

Diese Zahlen wurden bei 90 % CPU-Auslastung und 80 % Speicherauslastung ermittelt.

TCP-Anwendungen

Die empfohlene Mindestgröße für eine virtuelle Maschine der Connector Appliance beträgt 2 vCPU und 4 GB RAM.

Bereitstellungsrichtlinien: Eine Connector Appliance mit 2 vCPU, 4 GB Arbeitsspeicher und einer 10-Gbit/s-NIC kann Folgendes unterstützen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bis zu 50.000 gleichzeitige TCP-Verbindungen.
- Datendurchsatzrate von bis zu 1 Gbit/s.

Diese Zahlen wurden bei 90 % CPU-Auslastung und 80 % Speicherauslastung ermittelt.

Gemischter Datenverkehr (Web, SaaS, TCP)

Bereitstellungsleitfaden: Eine Connector Appliance mit 2 vCPUs und 4 GB Arbeitsspeicher kann Folgendes unterstützen:

- Bis zu 300 Web-App-Anfragen pro Sekunde (Secure Browse).
- Bis zu 10.000 gleichzeitige TCP-Verbindungen.
- Gesamtdatendurchsatzrate von bis zu 1 Gbit/s.

Diese Zahlen wurden bei 90 % CPU-Auslastung und 80 % Speichernutzung ermittelt.

WICHTIG:

Um Ihre Traffic-Anforderungen zu verwalten, die die empfohlenen Grenzwerte für Web-App-Anfragen pro Sekunde (Secure Browse), gleichzeitige TCP-Verbindungen oder den Durchsatz überschreiten, muss die Connector Appliance horizontal skaliert werden, indem weitere Connector Appliances hinzugefügt werden.

Connector-Benachrichtigungen

Der Connector generiert eine Benachrichtigung, sobald die CPU-Auslastung über einen einstündigen Stichprobenzeitraum 80 % überschreitet. Weitere Informationen finden Sie unter Connector-Benachrichtigungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfiguration und Verwaltung adaptiver Zugriffsrichtlinien

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

Die adaptive Zugriffsfunktion des Citrix Secure Private Access™ Dienstes bietet einen umfassenden Zero-Trust-Zugriffsansatz, der sicheren Zugriff auf Anwendungen ermöglicht. Adaptiver Zugriff ermöglicht es Administratoren, einen granularen Zugriff auf die Apps zu 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 (Geo-Standort oder Netwerkstandort)
- Gerätestatus (Gerätestatusprüfung)

Die adaptive Zugriffsfunktion wendet adaptive Richtlinien auf die Anwendungen an, auf die zugegriffen wird. Diese Richtlinien bestimmen die Risiken basierend auf dem Kontext und treffen dynamische Zugriffsentscheidungen, um den Zugriff auf 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, und dem Standort (Land oder Netwerkstandort), von dem aus der Benutzer auf die Anwendung zugreift.

Die adaptiven Zugriffsrichtlinien werden in den folgenden Szenarien ausgewertet:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Während einer Web-, SaaS-, TCP- oder UDP-App-Aufzählung vom Secure Private Access-Dienst – Wenn der Anwendungszugriff für diesen Benutzer verweigert wird, kann der Benutzer diese Anwendung nicht im Store 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.

Zugriffsrichtlinie mit mehreren Regeln erstellen

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-Apps angewendet werden, alles innerhalb einer einzigen Richtlinie.

Zugriffsbeschränkungen müssen über die Google Admin-Konsole und nicht über die Secure Private Access-Oberfläche konfiguriert werden.

Regeln werden in der **Google Admin-Konsole > Regeln** konfiguriert. Diese Regeln sind erweiterte Einstellungen im Zusammenhang mit DLP, wie z. B. das Hinzufügen eines Wasserzeichens, das Blockieren des Downloads von Dateien mit Sozialversicherungsnummern und die URL-Filterung.

Einzelheiten zum Erstellen von Richtlinien und Regeln für Google Chrome in der Google Admin-Konsole finden Sie in den folgenden Themen:

- Chrome Enterprise-Connector-Richtlinien für Chrome Enterprise festlegen
- Datenschutzregeln

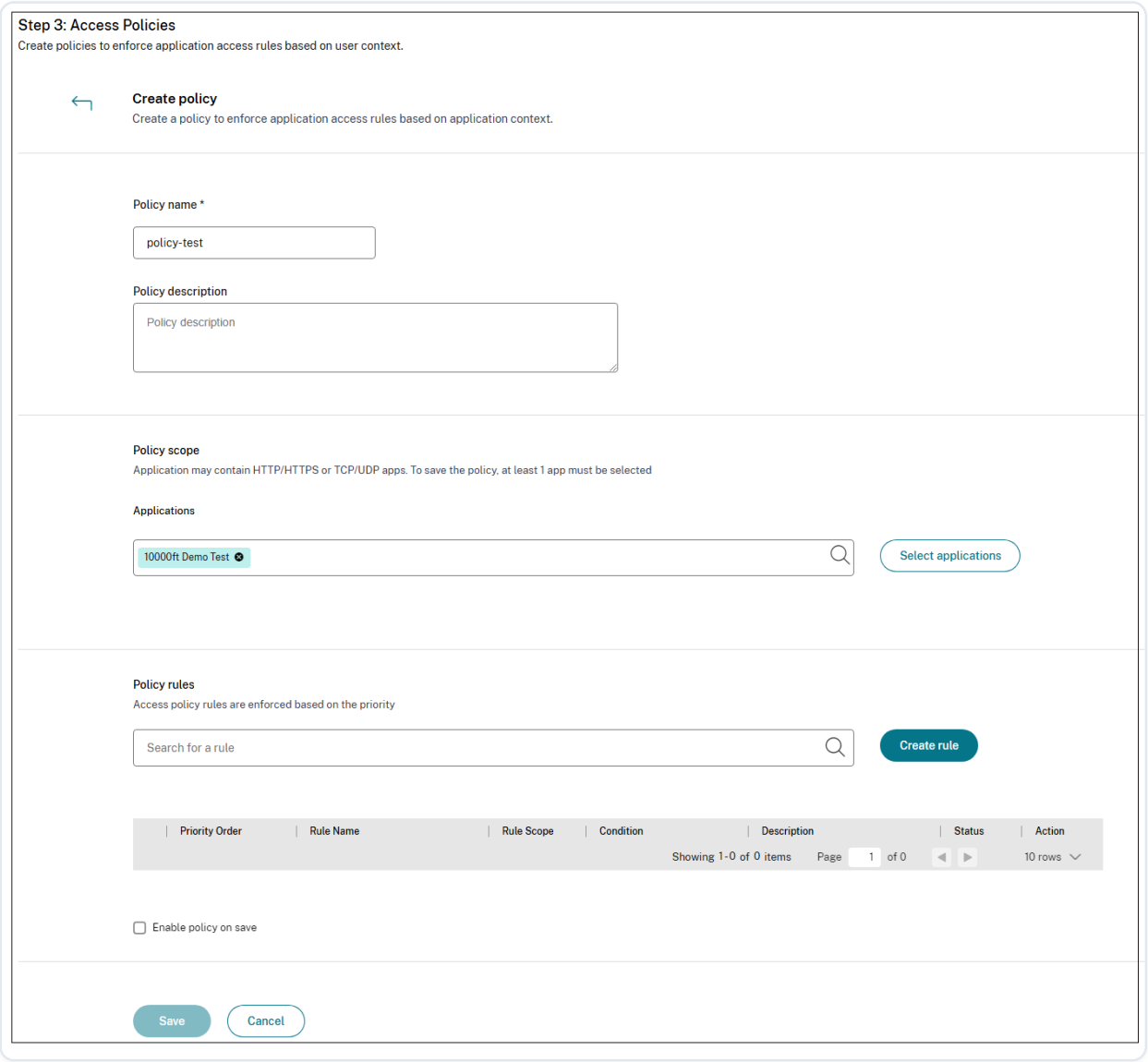
Voraussetzungen

Stellen Sie sicher, dass Sie die Anwendungen für Ihre Benutzer konfiguriert haben. Einzelheiten finden Sie unter Apps für Ihre Benutzer hinzufügen.

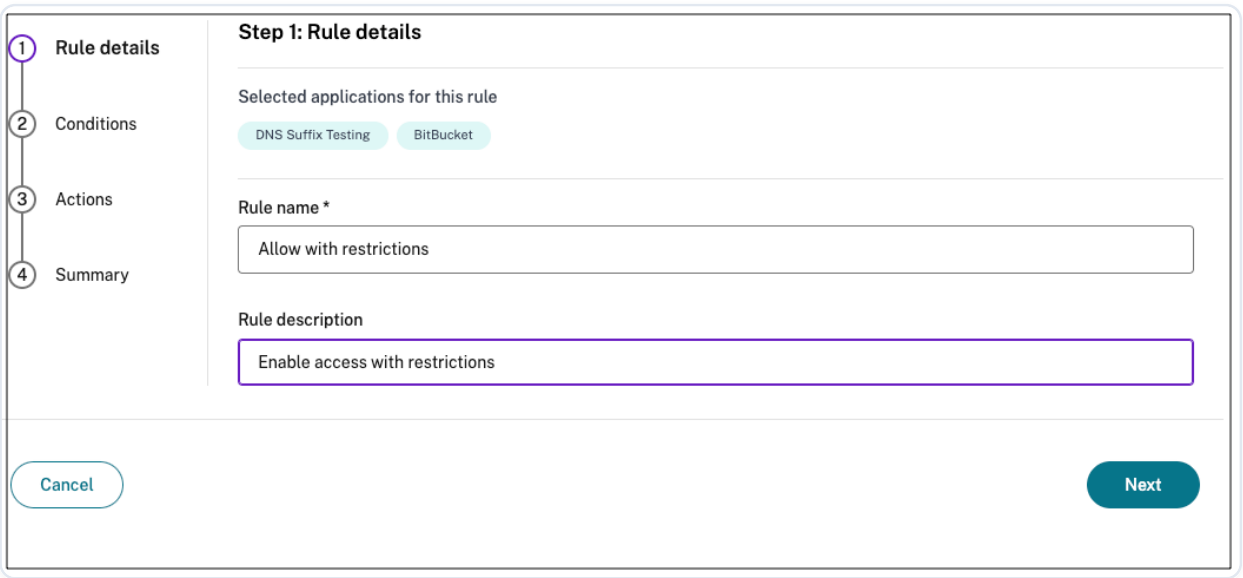
Schritte zum Erstellen einer Zugriffsrichtlinie:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

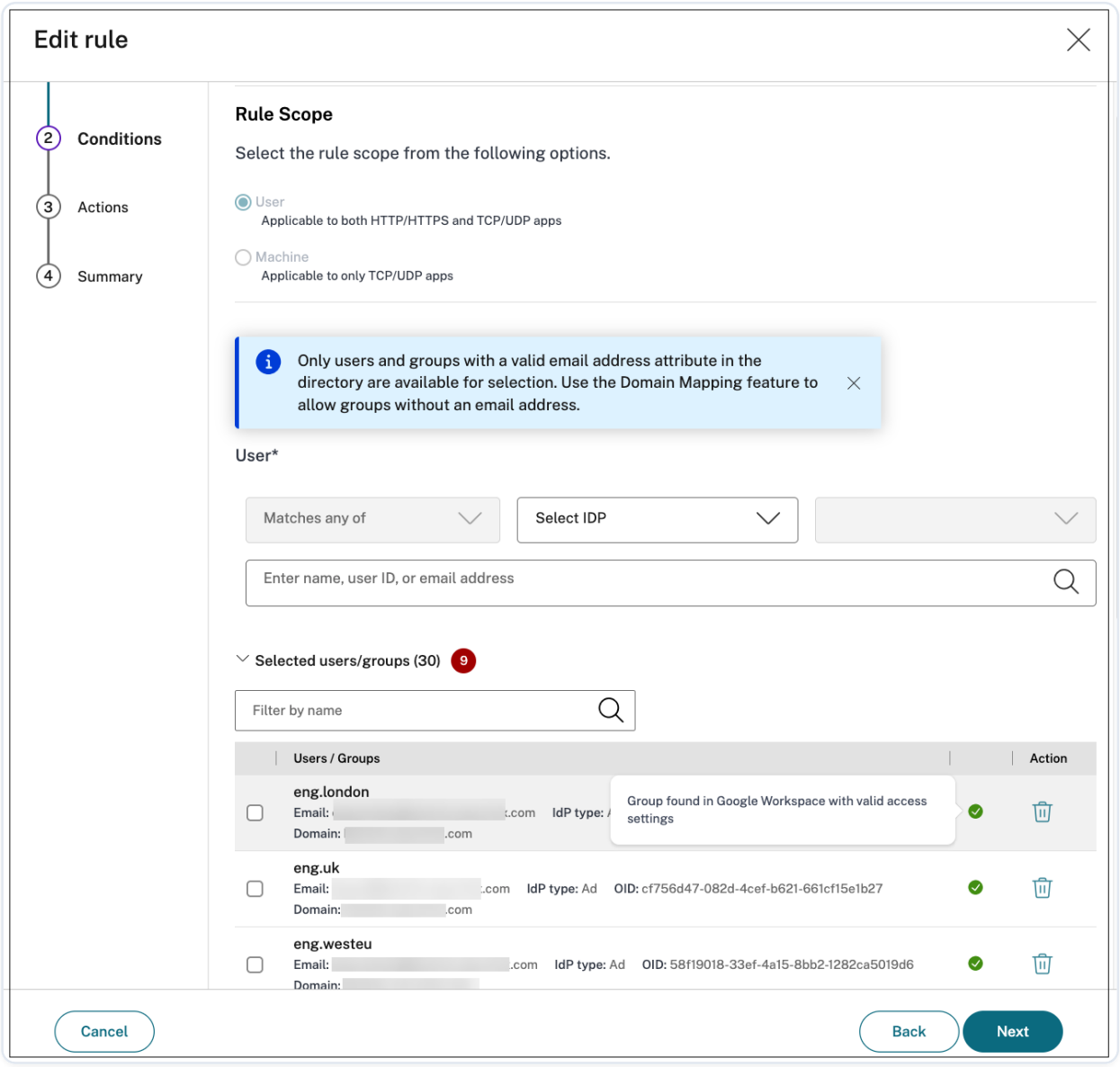


5. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein und klicken Sie dann auf **Weiter**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Wählen Sie die Bedingungen der Benutzer aus. Die Bedingung **Benutzer** ist eine obligatorische Bedingung, die erfüllt sein muss, um Benutzern den Zugriff auf die Apps zu gewähren. Sie können die Bedingung auswählen, gefolgt von der Domäne und dann den Benutzern.



Wählen Sie eine der folgenden Optionen aus:

- **Entspricht einem der folgenden** – Nur die Benutzer oder Gruppen, die einem der im Feld aufgeführten Namen entsprechen und zur ausgewählten Domäne gehören, erhalten Zugriff.
- **Entspricht keinem** – Alle Benutzer oder Gruppen, außer denen, die im Feld aufgeführt sind und zur ausgewählten Domäne gehören, erhalten Zugriff.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Sie können nach Benutzern oder Gruppen anhand des Anzeigenamens, der E-Mail-ID oder des Benutzerprinzipalnamens suchen. Dies hilft Ihnen, den richtigen Benutzer genau zu identifizieren und ihm Zugriff zu gewähren, selbst wenn derselbe Benutzer mehrere Konten hat. Weitere Informationen finden Sie unter Suchen nach Benutzern oder Gruppen.
- Sie müssen auch synchronisierte Benutzer und Gruppen für Secure Private Access-Richtlinien verwenden, damit diese korrekt ausgewertet werden. Andernfalls werden Warnmeldungen angezeigt. Weitere Informationen finden Sie unter Benutzer- und Gruppensynchronisierung überprüfen.

7. Fügen Sie eine Bedingung für den **Zugriffsmodus** hinzu, um den Anwendungszugriff basierend darauf einzuschränken, ob Benutzer über einen browserbasierten Client oder den Citrix Secure Access Client eine Verbindung herstellen. Weitere Informationen finden Sie unter Richtliniendurchsetzung basierend auf dem Zugriffsmodus.

   HINWEIS:

   Sie können den Zugriffsmodus mit der obligatorischen Bedingung **Benutzer** und allen anderen Bedingungen kombinieren.

8. (Optional) Klicken Sie auf +, um mehrere kontextbasierte Bedingungen hinzuzufügen.

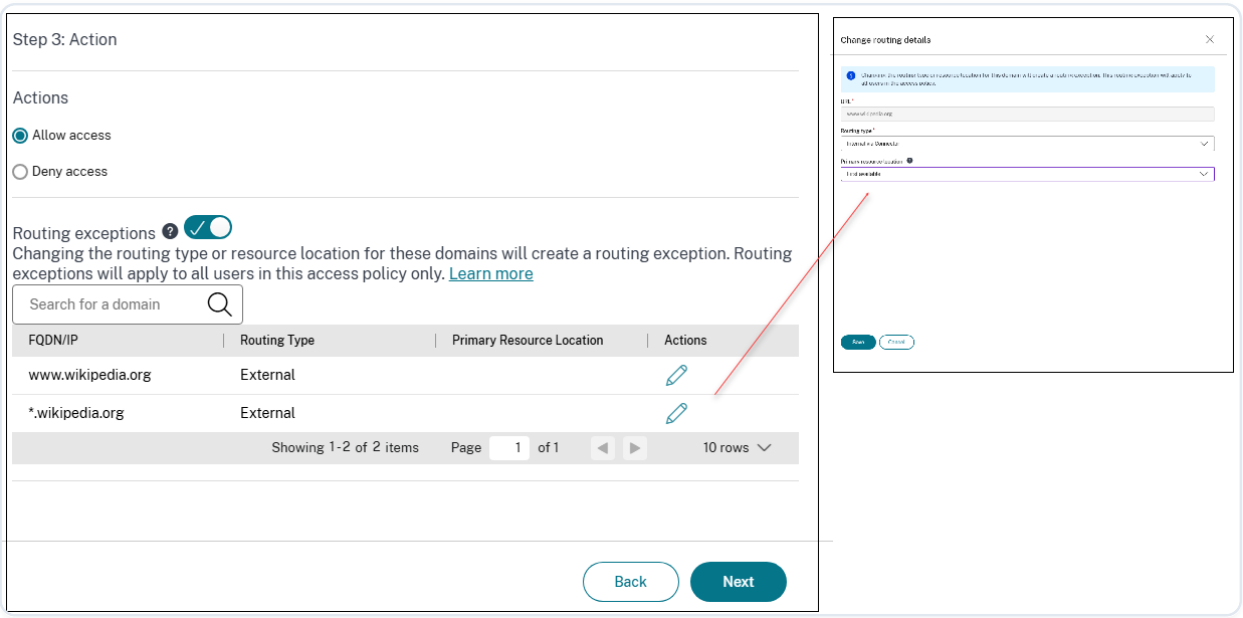
   Wenn Sie kontextbasierte Bedingungen hinzufügen, wird eine UND-Operation auf die Bedingungen angewendet, und die Richtlinie wird nur ausgewertet, wenn die Bedingungen für **Benutzer** und die optionalen kontextbasierten Bedingungen erfüllt sind. Sie können die folgenden kontextbasierten Bedingungen anwenden.

   - **Geografischer Standort** – Wählen Sie die Bedingung und den geografischen Standort aus, von dem aus die Benutzer auf die Apps zugreifen.
     - **Entspricht einem der folgenden:** Nur Benutzer oder Benutzergruppen, die von einem der aufgeführten geografischen Standorte auf die Apps zugreifen, erhalten Zugriff auf die Apps.
     - **Entspricht keinem:** Alle Benutzer oder Benutzergruppen, die nicht aus den aufgeführten geografischen Standorten stammen, erhalten Zugriff.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Netzwerkstandort** – Wählen Sie die Bedingung und das Netzwerk aus, über das die Benutzer auf die Apps zugreifen.
  - **Entspricht einem der folgenden:** Nur Benutzer oder Benutzergruppen, die von einem der aufgeführten Netzwerkstandorte auf die Apps zugreifen, erhalten Zugriff auf die Apps.
  - **Entspricht keinem:** Alle Benutzer oder Benutzergruppen, die nicht von den aufgeführten Netzwerkstandorten stammen, erhalten Zugriff.
- **Geräte-Posture-Prüfung** – Wählen Sie die Bedingungen aus, die das Benutzergerät erfüllen muss, um auf die Apps zugreifen zu können.

9. Klicken Sie auf **Weiter**.
10. Wählen Sie die Aktionen aus, die basierend auf der Bedingungsbewertung angewendet werden sollen.
    - **Zugriff erlauben**
    - **Zugriff verweigern**



11. (Optional) Ändern Sie bei Bedarf den Routing-Typ oder den Ressourcenstandort für eine bestimmte Domäne. Mit der Umschaltfläche **Routing-Ausnahmen** können Sie die Ressourcenstandorte und Routing-Informationen für Domänen der in der Zugriffsrichtlinie hinzugefügten Apps bearbeiten.
    - Ändern Sie unter **Routing-Typ** den Routing-Typ:

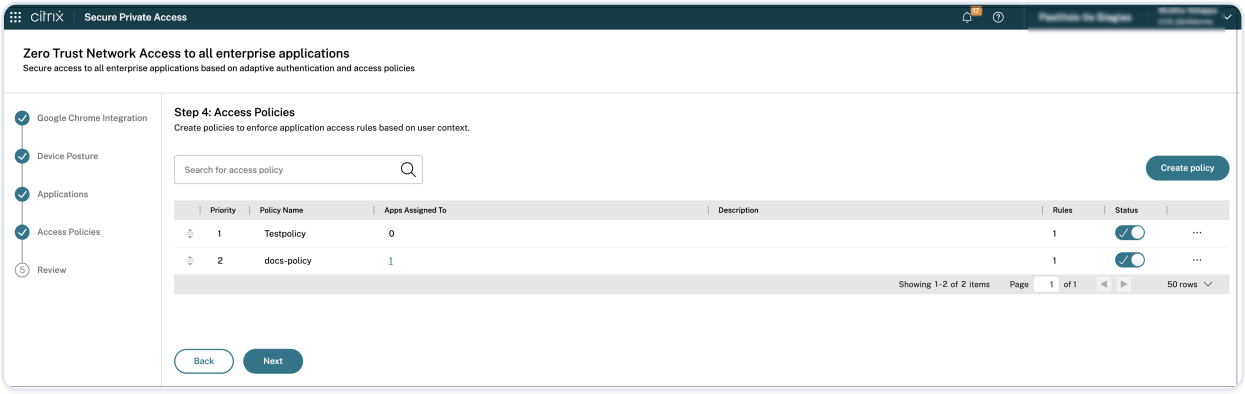
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Intern**: Der Datenverkehr fließt über die Connector Appliance. Bei einer Web-App fließt der Datenverkehr innerhalb des Rechenzentrums. Bei einer SaaS-App wird der Datenverkehr über die Connector Appliance außerhalb des Netzwerks geleitet.
- **Intern – Proxy umgehen**: Der Domänenverkehr wird über Citrix Cloud Connector™ Appliances geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
- **Extern**: Der Datenverkehr fließt direkt ins Internet.

- Unter **Ressourcenstandort** ändern Sie bei Bedarf den Ressourcenstandort. Diese Option gilt nur für intern weitergeleitete Domänen.

Weitere Informationen zum kontextbezogenen Routing finden Sie unter Kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten.

Nachdem Sie die Richtlinien erstellt haben, werden sie auf der Seite **Zugriffsrichtlinien** aufgeführt.



Suchen nach Benutzern oder Gruppen

Die von Ihnen ausgewählten Benutzer und Gruppen werden in einem Raster angezeigt. Jede Zeile im Raster zeigt die folgenden Identitätsdetails an, damit Sie gleichnamige Benutzer oder Gruppen über verschiedene Domänen, Gesamtstrukturen oder Identitätsanbieter (IdPs) hinweg eindeutig unterscheiden können:

- **Name** – Der Anzeigename des Benutzers oder der Gruppe.
- **E-Mail** – Die E-Mail-Adresse, die der Identität zugeordnet ist.
- **IdP-Typ** – Der Identitätsanbieter, z. B. Azure AD, Active Directory, Okta oder Google.
- **OID** – Die Objekt-ID oder Sicherheitskennung der Identität.
- **Domäne** – Die Domäne, zu der der Benutzer oder die Gruppe gehört.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können das Raster nach Namen filtern, einzelne Zeilen entfernen oder mehrere Einträge auswählen und diese gemeinsam mit **Ausgewählte entfernen** löschen.

Benutzer- und Gruppensynchronisierung überprüfen

Beim Auswählen von Benutzern oder Gruppen können Administratoren überprüfen, ob Einträge aus dem ausgewählten Benutzerverzeichnis mit Google Directory synchronisiert und dort korrekt konfiguriert sind. Secure Private Access-Richtlinien werden nur dann korrekt ausgewertet, wenn die Benutzer und Gruppen synchronisiert sind. Andernfalls können die folgenden Warnungen angezeigt werden:

- **Fehlende Mandantenkontoberechtigungen.**

  Problemumgehung:

  Weisen Sie in der Google Admin-Konsole die Berechtigungen **Benutzer > Lesen** und **Gruppen > Lesen** dem Mandanten-Dienstkonto zu. SPA benötigt diese Berechtigungen, um zu überprüfen, ob ein Benutzer oder eine Gruppe existiert.
- **Benutzer oder Gruppe nicht synchronisiert.**

  Problemumgehung:

  Der gesuchte oder ausgewählte Benutzer oder die Gruppe ist nicht mit Google Directory synchronisiert. Synchronisieren Sie die Verzeichnisentität mit Google Directory, bevor Sie sie in einer SPA-Richtlinie verwenden.
- **Unzureichende Gruppenzugriffseinstellungen.**

  Problemumgehung:

  Öffnen Sie in der Google Admin-Konsole die Zugriffseinstellungen für die ausgewählte Gruppe und stellen Sie sicher, dass unter **Wer kann Mitglieder anzeigen** mindestens die Option **Gruppenmitglieder** ausgewählt ist.

HINWEIS:

Diese Funktion ist erst verfügbar, nachdem die Google Chrome-Integration erfolgreich abgeschlossen wurde.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wichtige 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 einem niedrigeren Wert hat die höchste Präferenz. Die Regel mit der niedrigsten Prioritätsnummer wird zuerst ausgewertet. Wenn die Regel (n) nicht den definierten Bedingungen entspricht, wird die nächste Regel (n+1) ausgewertet und so weiter.

Beispiel für die Auswertung von Regeln mit Prioritätsreihenfolge:

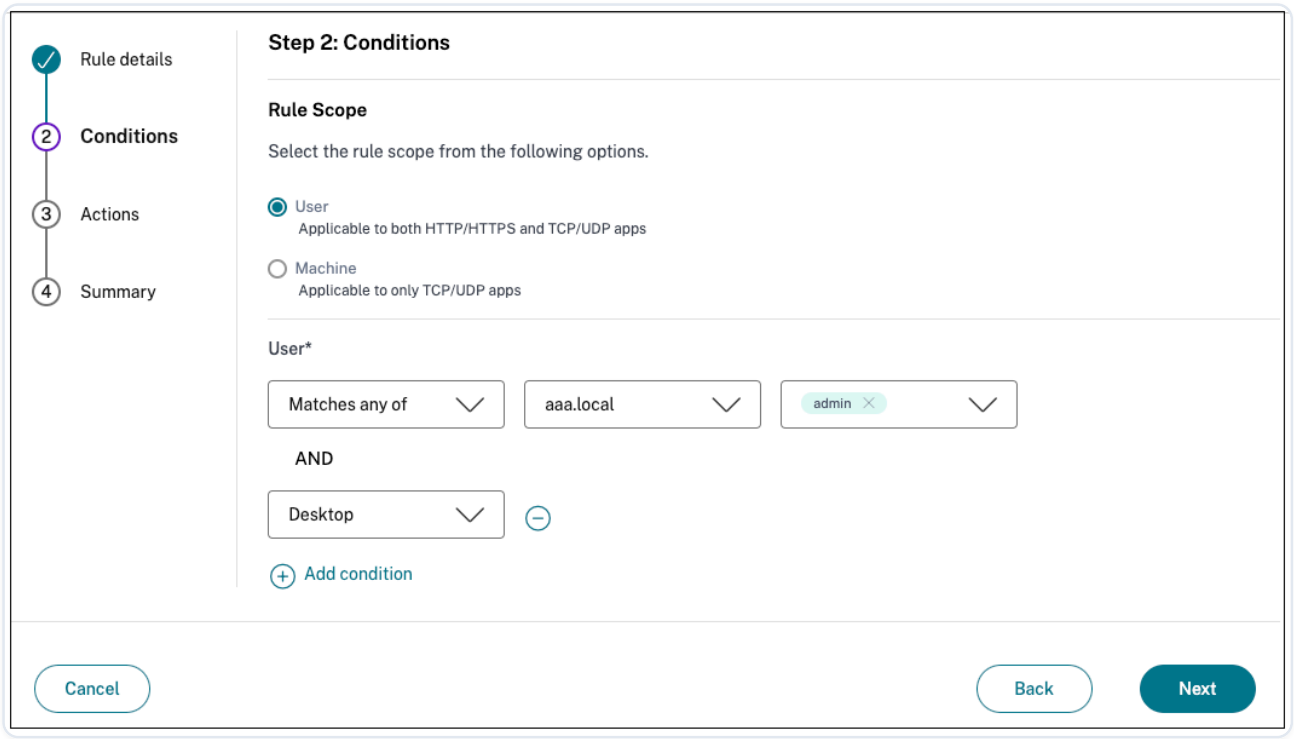
Angenommen, Sie haben zwei Regeln erstellt: Regel 1 und Regel 2. Regel 1 ist Benutzer A zugewiesen und Regel 2 ist Benutzer B zugewiesen, dann werden beide Regeln ausgewertet. Angenommen, beide Regeln, Regel 1 und Regel 2, sind Benutzer A zugewiesen. In diesem Fall hat Regel 1 die höhere Priorität. Wenn 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.

Adaptiver Zugriff basierend auf Geräten

Informationen zum Konfigurieren einer adaptiven Zugriffsrichtlinie basierend auf der Plattform (Mobilgerät oder Desktop-Computer), von der aus der Benutzer auf die Anwendung zugreift, finden Sie unter Konfiguration und Verwaltung adaptiver Zugriffsrichtlinien.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Adaptiver Zugriff basierend auf dem Standort

Ein Administrator kann die adaptive Zugriffsrichtlinie basierend auf dem Standort konfigurieren, von dem aus der Benutzer auf die Anwendung zugreift. Der Standort kann das Land sein, von dem aus der Benutzer auf die Anwendung zugreift, oder der Netwerkstandort des Benutzers. Der Netwerkstandort wird mithilfe eines IP-Adressbereichs oder von Subnetzadressen definiert.

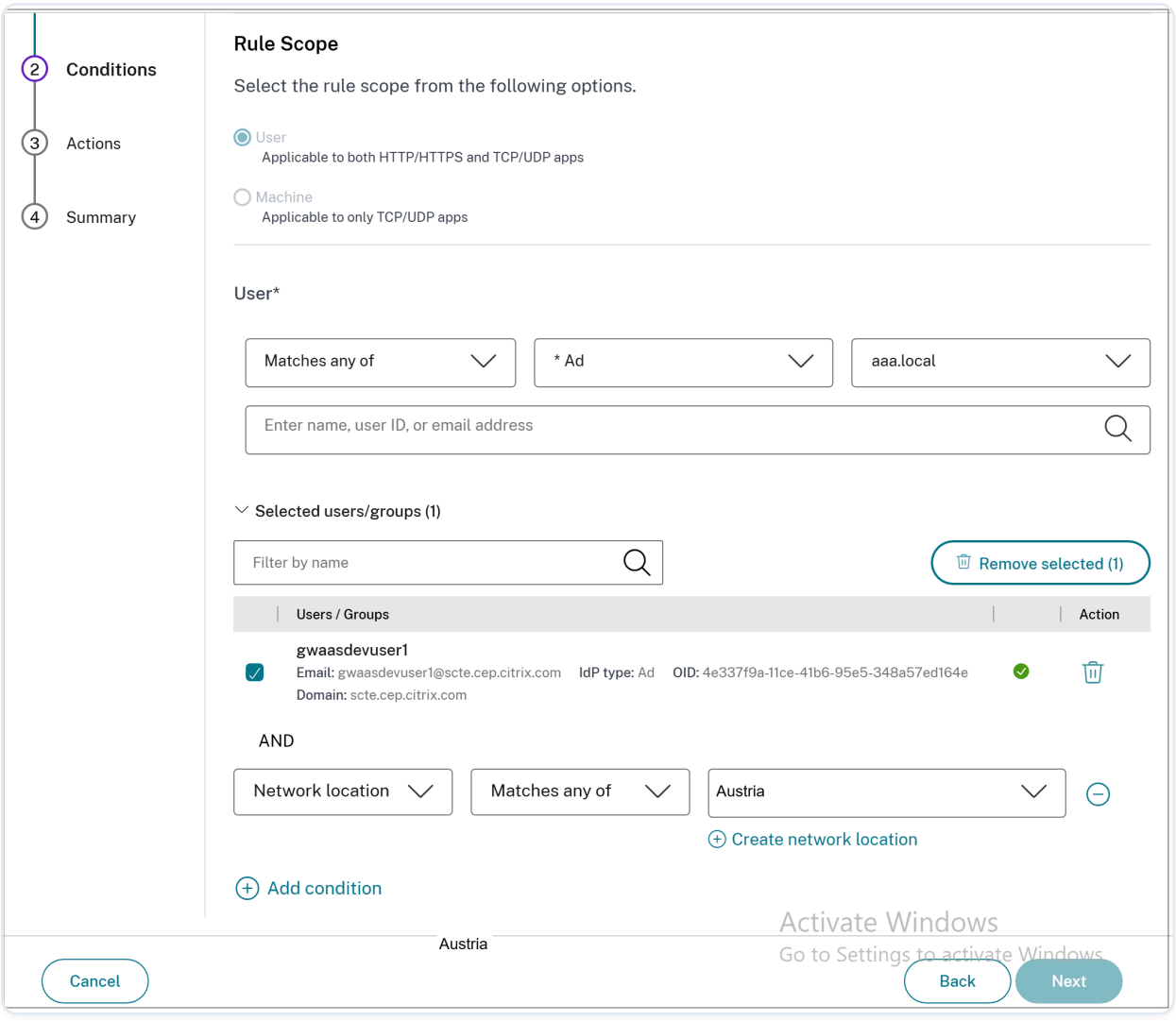
Um eine adaptive Zugriffsrichtlinie basierend auf dem Standort zu konfigurieren, verwenden Sie das Verfahren Erstellen einer adaptiven Zugriffsrichtlinie mit mehreren Regeln mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen.**
- Wählen Sie **Geo-Standort** oder **Netwerkstandort** aus.
- Wenn Sie mehrere Geo-Standorte 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.
    - **Entspricht keinem** – Die geografischen Standorte oder Netzwerkstandorte stimmen nicht mit den in der Datenbank konfigurierten geografischen Standorten oder Netzwerkstandorten überein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinweis:

- Wenn Sie **Geo-Standort** auswählen, wird die Quell-IP-Adresse des Benutzers mit der IP-Adresse der Länderdatenbank abgeglichen. 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 ausgewertet.
- Für **Netwerkstandort** können Sie einen vorhandenen Netwerkstandort auswählen oder einen Netwerkstandort erstellen. Um einen neuen Netwerkstandort zu erstellen, klicken Sie auf **Netwerkstandort erstellen**.
- Stellen Sie sicher, dass Sie den adaptiven Zugriff unter **Citrix Cloud > StoreFront Cloud > Access > Adaptive Access** aktiviert haben. Andernfalls können Sie die Standort-Tags nicht hinzufügen. Weitere Informationen finden Sie unter Adaptiven Zugriff aktivieren.
- Sie können auch einen Netwerkstandort über die Citrix Cloud-Konsole erstellen. Weitere Informationen finden Sie unter Citrix Cloud Netwerkstandort Konfiguration.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Schließen Sie die Richtlinienkonfiguration ab.

Adaptiver Zugriff basierend auf dem Gerätestatus

Sie können den Secure Private Access-Dienst so konfigurieren, dass er die Zugriffssteuerung mithilfe von Gerätestatus-Tags erzwingt. Nachdem einem Gerät nach der Gerätestatusprüfung die Anmeldung gestattet wurde, kann das Gerät als konform oder nicht konform klassifiziert werden. Diese Informationen stehen dem Citrix DaaS™-Dienst und dem Citrix Secure Private Access-Dienst als Tags zur Verfügung und werden verwendet, um kontextbezogenen Zugriff basierend auf dem Gerätestatus bereitzustellen.

Ausführliche Informationen zum Gerätestatusdienst finden Sie unter Gerätestatus.

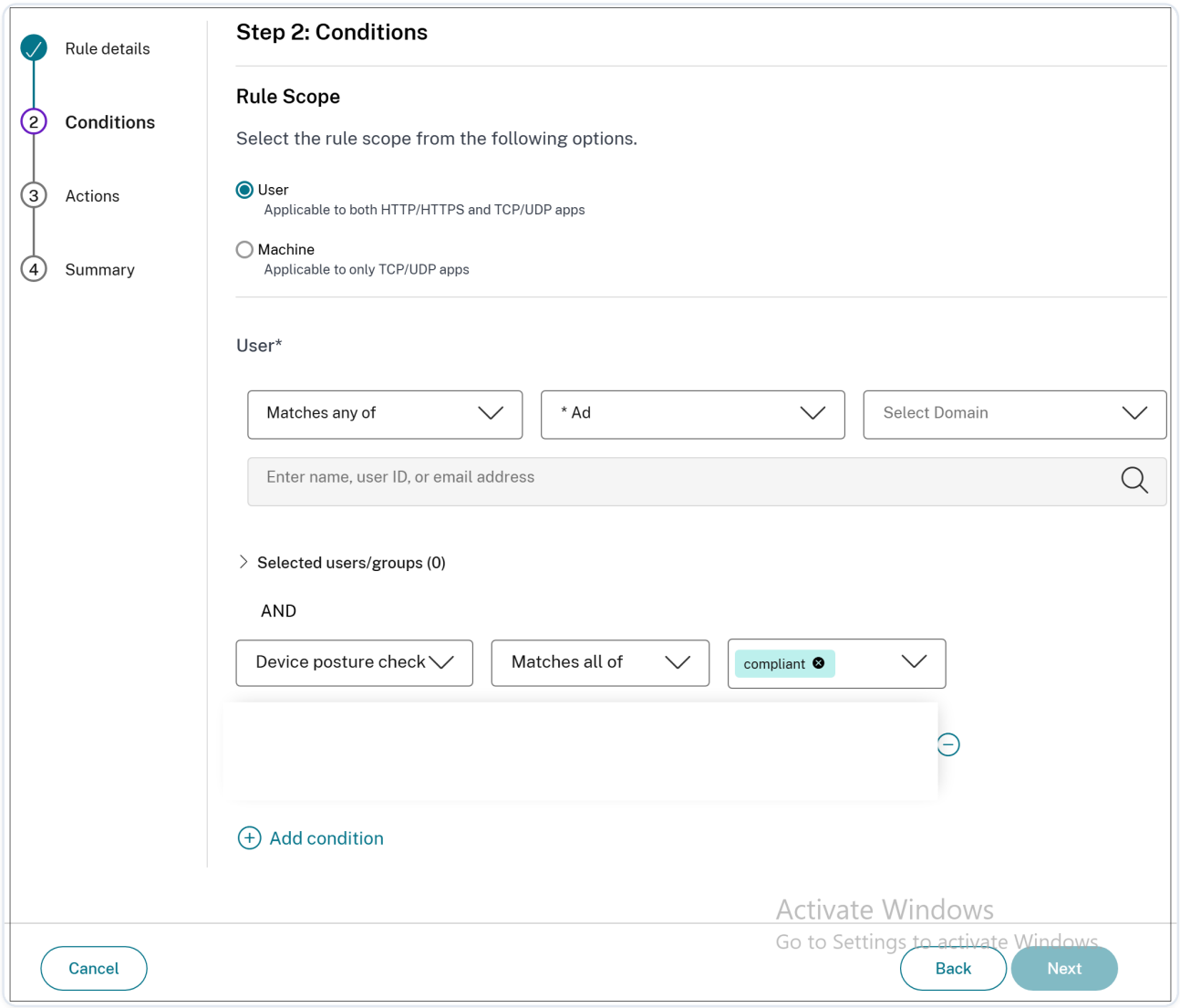
Um eine adaptive Zugriffsrichtlinie basierend auf dem Gerätestatus zu konfigurieren, verwenden Sie das Verfahren Erstellen einer adaptiven Zugriffsrichtlinie mit mehreren Regeln mit den folgenden Änderungen.

- Klicken Sie auf der Seite **Schritt 2: Bedingungen** auf **Bedingung hinzufügen**.
- Wählen Sie **Gerätestatusprüfung** und den logischen Ausdruck aus dem Dropdown-Menü aus.
- Geben Sie einen der folgenden Werte in benutzerdefinierten Tags ein:
  - **Konform** – Für konforme Geräte
  - **Nicht konform** – Für nicht konforme Geräte

HINWEIS:

Die Syntax für die Gerätekategorisierungs-Tags muss auf die gleiche Weise eingegeben werden, wie zuvor erfasst, d.h. mit Großbuchstaben am Anfang (Compliant und Non-Compliant). Andernfalls funktionieren die Gerätestatusrichtlinien nicht wie beabsichtigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sitzungsrichtlinien

Administratoren können Sitzungsrichtlinien konfigurieren, um interne Unternehmensbenutzer direkt zu Backend-Anwendungen zu leiten, ohne den Datenverkehr über Secure Private Access zu tunneln. Sitzungsrichtlinien bieten dynamisches Routing basierend auf Faktoren wie Netwerkstandort und Gerätehaltung.

HINWEIS:

- Sitzungsrichtlinieneinstellungen werden auf Sitzungsebene auf alle Anwendungen angewendet, anstatt an bestimmte Anwendungen gebunden zu sein.
- Sitzungsrichtlinien können allen Benutzern oder einer Untergruppe von Benutzern zugewiesen werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Routing-Priorität

Sitzungsrichtlinien arbeiten zusammen mit Zugriffsrichtlinien, wobei Zugriffsrichtlinien bei einem Konflikt Vorrang haben. In solchen Szenarien überschreiben Routing-Ausnahmen der Zugriffsrichtlinie die Sitzungsrichtlinien. Wenn weder eine Zugriffsrichtlinie noch eine Sitzungsrichtlinie konfiguriert ist, gelten die globalen Routing-Einstellungen (**Settings > Application Domain**).

Unterstützte Citrix Secure Access™ Clients

Die folgenden Versionen des Citrix Secure Access Clients unterstützen das direkte Routing von Benutzern zu Backend-Anwendungen.

- macOS – 24.11.1 und höher
- Windows – 24.11.1.17 und höher. Außerdem muss die VPN-Client-Registrierung **EnableContextualAccess** aktiviert sein. Weitere Informationen finden Sie unter NetScaler Gateway Windows VPN-Client-Registrierungsschlüssel.

Beispiel-Anwendungsfall

Szenario:

In einem Unternehmen, wenn Benutzer mit dem Unternehmensnetzwerk „corporate_network1“ verbunden sind, muss der Datenverkehr von Anwendungen direkt zu den Backend-Anwendungen fließen, da diese Anwendungen im Unternehmensnetzwerk direkt erreichbar sind. Befinden sich die Benutzer außerhalb des Unternehmensnetzwerks, muss der Anwendungsdatenverkehr getunnelt werden.

Lösung:

1. Fügen Sie app1, app2 hinzu, wobei das Routing auf **Intern über Connector** eingestellt ist.
2. Fügen Sie eine Zugriffsrichtlinie für die Apps (app1, app2) hinzu, um den Zugriff zu gewähren.
3. Fügen Sie eine Sitzungsrichtlinie hinzu, um Bedingungen zu konfigurieren, die die Benutzergruppe und Netzwerkstandorte festlegen, die bei der Zugriffsgewährung berücksichtigt werden müssen.
4. Wählen Sie die Bedingung **Benutzer** aus und setzen Sie sie auf **Alle Benutzer**.
5. Fügen Sie eine Bedingung **Netwerkstandort** hinzu. Setzen Sie sie auf **Entspricht einem von** und geben Sie den Netwerkstandort „corporate_network1“ an. Dadurch wird sichergestellt, dass der Datenverkehr von „corporate_network1“ direkt zu den Backend-Anwendungen fließt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

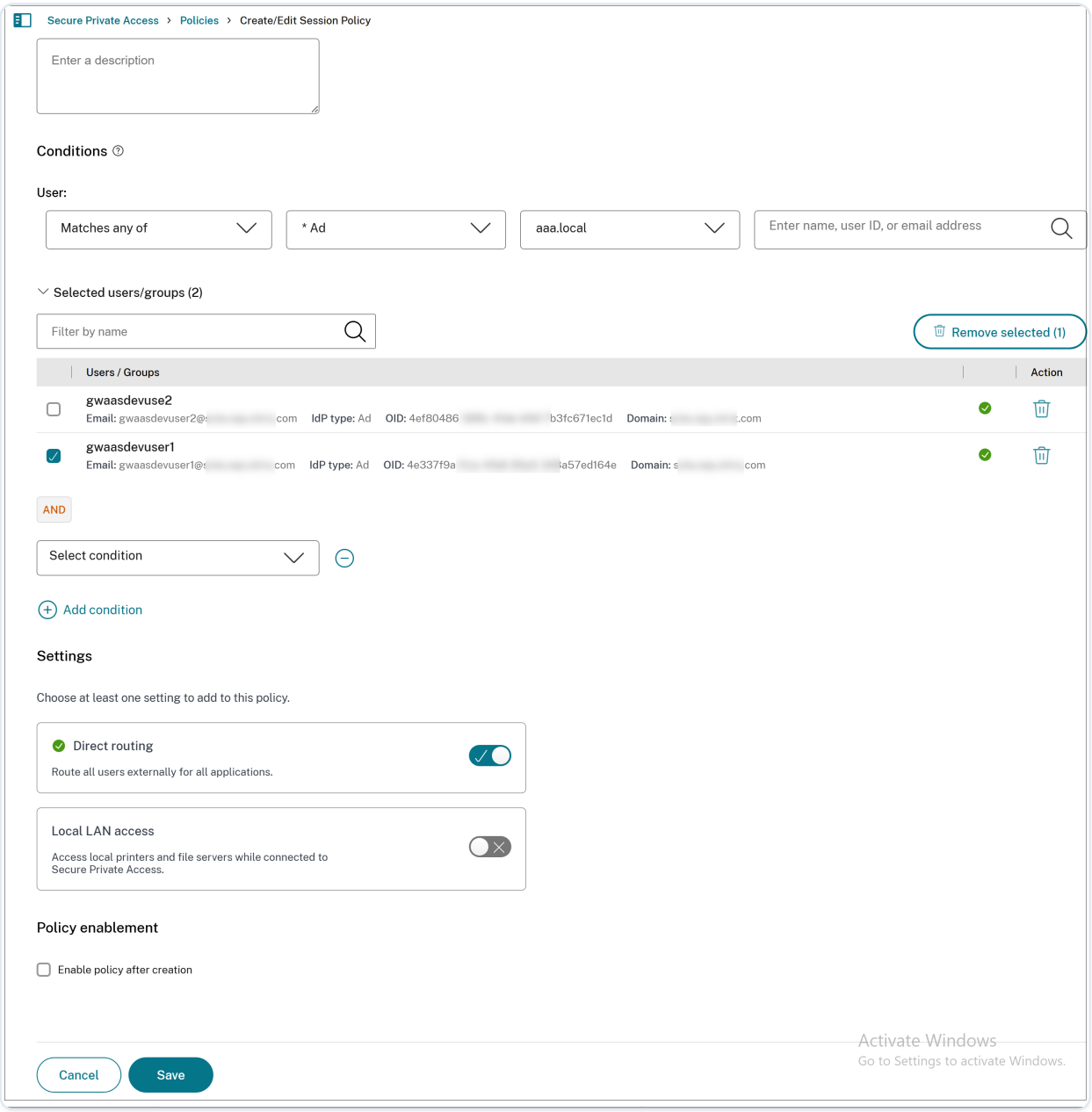
Sie können für dieses Szenario auch Routing-Ausnahmen aktivieren. Wenn beispielsweise app1 auch im Unternehmensnetzwerk immer getunnelt werden muss, können Routing-Ausnahmen für Domänen von app1 in der Zugriffsrichtlinie konfiguriert werden. In diesem Fall hat die Routing-Ausnahme Vorrang vor der Sitzungsrichtlinie.

Direktes Routing innerhalb des Unternehmensnetzwerks mithilfe von Sitzungsrichtlinien konfigurieren

Sie müssen eine Sitzungsrichtlinie erstellen, damit Benutzer direkt auf die Backend-Anwendungen zugreifen können, indem sie das Secure Private Access-Tunneling umgehen. Dazu wählen Sie zunächst die Benutzer aus, für die diese Richtlinie gelten soll. Zweitens wählen Sie unter „Netwerkstandort“ den Namen Ihres Unternehmensnetzwerks aus. Dies ist ein wichtiger Schritt, um sicherzustellen, dass Direct Routing nur aktiviert wird, wenn sich der Benutzer innerhalb des Unternehmensnetzwerks befindet.

1. Navigieren Sie zu **Richtlinien > Sitzungsrichtlinien** und klicken Sie auf **Sitzungsrichtlinie erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Geben Sie einen Namen für die Richtlinie und eine Beschreibung der Richtlinie ein.
3. Wählen Sie die Benutzer und die Bedingungen aus, für die Sie diese Einstellungen anwenden möchten.
4. Sie können die Bedingung so auswählen, dass sie für alle Benutzer gilt, oder eine Untergruppe von Benutzern angeben.

HINWEIS:

Sie können nach Benutzern oder Gruppen anhand des Anzeigenamens, der E-Mail-ID oder des Benutzerprinzipalnamens suchen. Dies hilft Ihnen, den richtigen Benutzer genau zu identifizieren und ihm Zugriff zu gewähren, selbst wenn derselbe Benutzer mehrere Konten hat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die von Ihnen ausgewählten Benutzer und Gruppen werden in einem Raster angezeigt. Jede Zeile im Raster zeigt die folgenden Identitätsdetails an, damit Sie identisch benannte Benutzer oder Gruppen über verschiedene Domänen, Gesamtstrukturen oder Identitätsanbieter (IdPs) hinweg eindeutig unterscheiden können:

- **Name** – Der Anzeigename des Benutzers oder der Gruppe.
- **E-Mail** – Die E-Mail-Adresse, die der Identität zugeordnet ist.
- **IDP-Typ** – Der Identitätsanbieter, z. B. Azure AD, Active Directory, Okta oder Google.
- **OID** – Die Objekt-ID oder Sicherheitskennung der Identität.
- **Domäne** – Die Domäne, zu der der Benutzer oder die Gruppe gehört. Sie können das Raster nach Namen filtern, einzelne Zeilen entfernen oder mehrere Einträge auswählen und diese gemeinsam mit „Ausgewählte entfernen“ löschen.

5. Fügen Sie eine Bedingung für den **Zugriffsmodus** hinzu, um die Sitzungseinstellungen auf den beabsichtigten Clienttyp zu beschränken. Sitzungsrichtlinien, die während des Secure Private Access-Routings ausgewertet werden, werden als CSA-Zugriffsmodus behandelt. Weitere Informationen zu Zugriffsmodi finden Sie unter Richtlinienerzwingung basierend auf dem Zugriffsmodus.
6. (Optional) Klicken Sie auf +, um mehrere kontextbasierte Bedingungen hinzuzufügen.
7. Definieren Sie die Bedingung **Netwerkstandort**, um dynamisches Routing für die gesamte Sitzung zu aktivieren. Dies bestätigt, dass das direkte Routing nur aktiviert ist, wenn sich Benutzer innerhalb des Unternehmensnetzwerks befinden.

   Wenn Sie kontextbasierte Bedingungen hinzufügen, wird eine UND-Operation auf die Bedingungen angewendet, wobei die Richtlinie nur ausgewertet wird, wenn sowohl die Benutzer als auch die optionalen kontextbasierten Bedingungen erfüllt sind. Details zu den Bedingungen finden Sie unter Zugriffsrichtlinie konfigurieren.
8. Wählen Sie **Direktes Routing**, um alle Benutzer extern zu den Back-End-Anwendungen zu leiten.
9. Wählen Sie **Lokaler LAN-Zugriff**, um nahtlosen Zugriff auf lokale LAN-Ressourcen zu ermöglichen. Weitere Informationen finden Sie unter Nahtloser Zugriff auf lokale LAN-Ressourcen (Drucker, Dateiserver).
10. Wählen Sie **Richtlinie nach Erstellung aktivieren**. Wenn Sie diese Option nicht auswählen, wird die Richtlinie nur erstellt und nicht auf die Anwendungen angewendet. Alternativ können Sie die Richtlinie auch auf der Seite „Sitzungsrichtlinien“ über den Umschalter in der Spalte „Status“ aktivieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Klicken Sie auf **Speichern**.

HINWEIS:

Netwerkstandort-Änderungen lösen Sitzungsrichtlinienaktualisierungen aus, und dies kann sich wie folgt auf die Endclients auswirken:

- **Citrix Secure Access agent:** Richtlinienaktualisierungen können Routing-Konfigurationen ändern und somit den Anwendungszugriff beeinträchtigen.
- **Citrix Enterprise Browser™:** Richtlinienaktualisierungen erfolgen alle 30 Minuten. Benutzer müssen den Browser neu starten oder auf die Aktualisierung warten, um auf Anwendungen zugreifen zu können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migration von Citrix Enterprise Browser zu Chrome Enterprise Premium

Der Übergang von Citrix Enterprise Browser (CEB) zu Citrix Enterprise Premium (CEP) stellt einen bedeutenden Fortschritt in der Entwicklung von Citrix Secure Private Access dar, um allen Anwendungen einen sicheren, adaptiven und hochleistungsfähigen Zero Trust Network Access (ZTNA) zu bieten. Dieses Thema enthält detaillierte Informationen für IT-Administratoren und Citrix-Experten, um eine erfolgreiche schrittweise Migration zu planen und durchzuführen, die minimale Unterbrechungen und eine optimale Benutzererfahrung gewährleistet.

Dieser gestufte Migrationsansatz ermöglicht es Unternehmen, die Geschäftskontinuität während der Übergangszeit aufrechtzuerhalten, indem beide Browserlösungen parallel betrieben werden. Mit der gestuften Migration können Kunden die Kompatibilität bestehender Anwendungen und Workflows mit Chrome Enterprise Premium validieren.

Die folgenden wichtigen Schritte sind bei der Migration von CEB zu CEP erforderlich:

- Chrome Enterprise Premium konfigurieren
- Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen
- Secure Private Access Konfigurationsparser für die CEP-Kompatibilitätsanalyse
- Konfigurationsänderungen vor der vollständigen Migration zu CEP
- CEP im Unternehmen einführen (vollständige Migration)

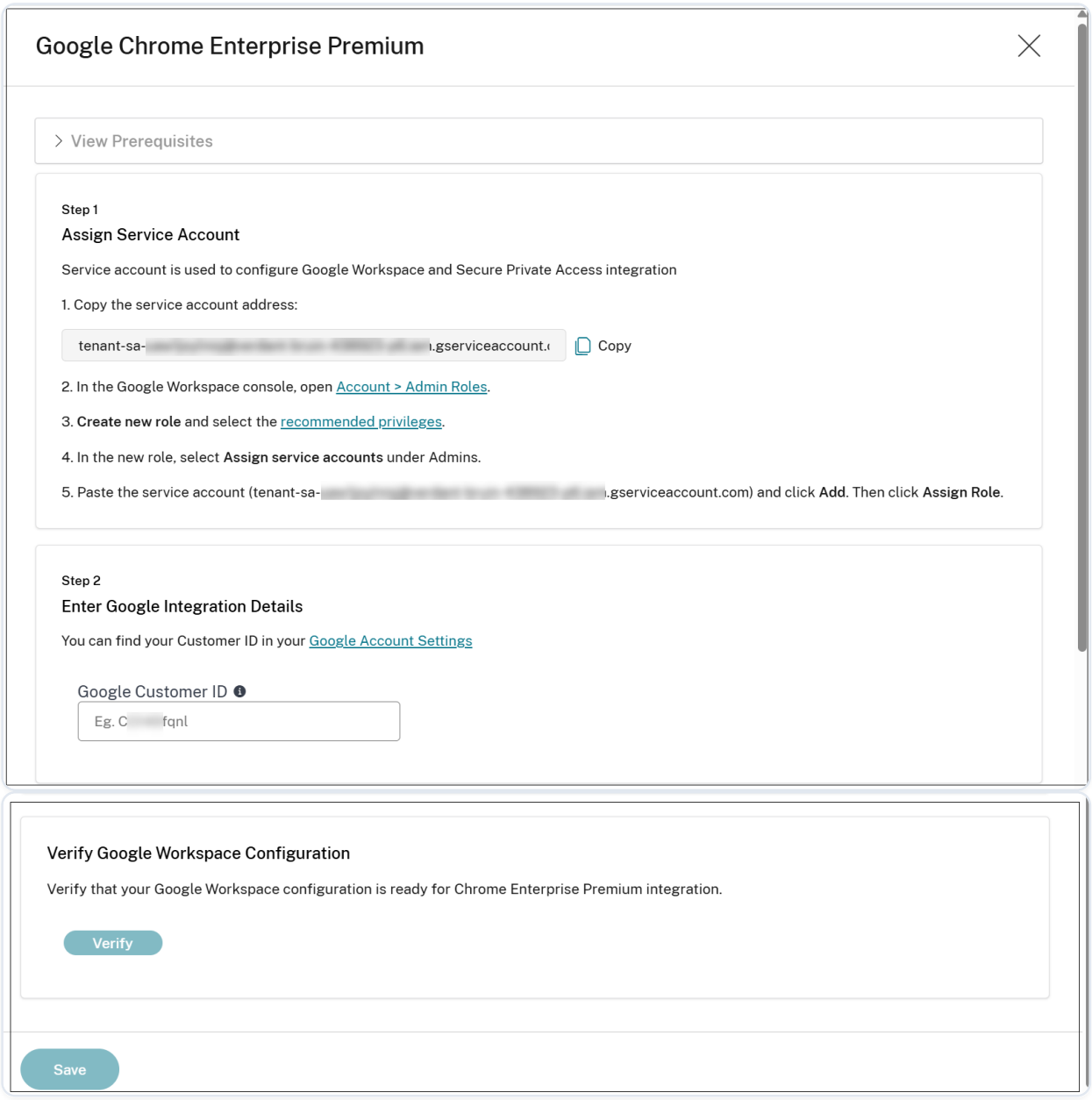
Chrome Enterprise Premium konfigurieren

Für bestehende Secure Private Access-Kunden erleichtert der Migrationsassistent in der Secure Private Access-Konsole die CEP-Bereitstellung, die Erweiterungsinstallation für Benutzer und einen Pfad für die schrittweise Anwendungs- und Benutzermigration.

1. Navigieren Sie in der Secure Private Access-Administrationskonsole zu **Chrome Enterprise Premium > Konfiguration**.

   Sie können die Details der Google-Integration anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Klicken Sie auf **Set up Google CEP**.
3. Weisen Sie die Details des Citrix-Dienstkontos in der Google WorkSecure Private Access-Konsole zu. Weitere Informationen finden Sie unter Setup Google Chrome integration.
4. Klicken Sie auf **Save** und schließen Sie.

Die Bereitstellung von Chrome Enterprise Premium beginnt.

Richtlinienanreicherung für Benutzergruppen ohne E-Mail

Sobald die Bereitstellung von Chrome Enterprise Premium erfolgreich abgeschlossen ist, wird automatisch ein Richtlinienaktualisierungsprozess für die Zugriffsrichtlinien und Sitzungsrichtlinien ausgelöst.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieser Aktualisierungsprozess führt Folgendes aus:

- Überprüfen Sie die vorhandenen Richtlinien (Zugriff und Sitzung).
- Suchen Sie nach Benutzern und Benutzergruppen ohne E-Mails in ihren Regeln.
- Fragen Sie den CC Directory-Dienst ab, um deren E-Mails abzurufen, und fügen Sie sie den Richtlinien hinzu.

Weitere Informationen finden Sie unter Domain mapping for user groups without email addresses.

Secure Private Access Konfigurations-Parser für die CEP-Kompatibilitätsanalyse

Die folgenden wichtigen Richtlinienelemente werden in CEP nicht direkt unterstützt:

- Anwendungen
  - Einmaliges Anmelden
- Zugriffsrichtlinien
  - Zugriff mit Einschränkungen zulassen
  - Gemischte Zulassen-/Verweigern-Aktionen (HTTP/HTTPS vs. TCP/UDP)
  - Gespeicherte URL-Bedingungen
  - Desktop-/Mobil-Bedingungen
- Sitzungsrichtlinien
  - Gespeicherte URL-Bedingungen
  - Desktop-/Mobil-Bedingungen
- Sicherheitsgruppen
- Webfilterung

Diese Inkompatibilitäten müssen behoben werden, bevor Anwendungen von CEB zu CEP migriert werden.

Der Prozess zur Identifizierung von Inkompatibilitäten wird durch den Secure Private Access Konfigurations-Parser `<parse_citrix_spa_configuration.py>` erleichtert. Dieses Tool analysiert die Citrix Secure Private Access Konfigurationsexporte, um Kompatibilitätsprobleme wie die folgenden während der Migration zu CEP zu identifizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anwendungen, die mit CEP inkompatibel sind
- Zugriffsrichtlinien, die mit CEP inkompatibel sind
- Konfigurierte Sicherheitsgruppen
- Webfilterkonfiguration

HINWEIS:

Sicherheitsgruppen und Webfilterung werden in der Citrix Secure Private Access-Integration mit CEP nicht unterstützt.

Nach der Analyse liefert das Tool unterschiedliche Empfehlungen, je nachdem, ob die CEP-Einführung in der gesamten Organisation (Migration aller Anwendungen) abgeschlossen wurde.

So verwenden Sie das Tool

1. Laden Sie das Skript herunter von: Python-Skript zum Parsen der Secure Private Access-Konfiguration.
2. Navigieren Sie in der Secure Private Access-Administratorkonsole zu **Einstellungen > Globale Konfiguration > Bericht erstellen** und exportieren Sie die vorhandene Secure Private Access-Konfiguration in ein JSON-Format.
3. Laden Sie das Python-Skript herunter und führen Sie es aus, wobei der exportierte Bericht als Eingabe dient. Sie müssen Python 3 installiert haben, um dieses Skript auszuführen.

   ```
   # python3 parse_citrix_spa_configuration.py <path_to_spa_report>
   ```

   Das Skript kann entweder vor oder nach der vollständigen Migration verwendet werden und liefert unterschiedliche Empfehlungsaktionen.

HINWEIS:

Das Skript liefert keine Empfehlungen für inkompatible Sitzungsrichtlinien.

Beispielbericht:

```
% python3 parse_citrix_spa_configuration.py
CitrixSpaConfigurationDump.json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Has the CEP rollout to the entire organization been completed?

Enter yes/no (default: no): no

CEP INCOMPATIBLE APPLICATIONS (7 out of 185):

1. Application_1 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

2. Application_2 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

....

--------------------------------------------------

Mitigation guidance:

--------------------------------------------------
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Has SSO configuration other than 'Don't use SSO':

  • Navigate to the application's SSO settings

  • Change the SSO setting to 'Don't use SSO'

==================================================

CEP INCOMPATIBLE POLICIES (15 out of 136):

1. Access_policy_1 ⚠

   Reasons: Contains user(s)/group(s) without email

2. Access_policy_2 ⚠

   Reasons: Mixed actions (HTTP/HTTPS vs TCP/UDP), Contains user(s)/
group(s) without email

...

--------------------------------------------------
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mitigation guidance:

Platform filter (Desktop/Mobile):

- Remove the unsupported Desktop/Mobile condition

Workspace URL:

- Remove the unsupported Workspace URL rule

Access with restrictions:

- Configure access controls without using restrictions

Mixed actions (HTTP/HTTPS vs TCP/UDP):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  • Ensure both actions have the same value



  • If that's not possible, create separate policies for HTTP/HTTPS and
TCP/UDP applications




Policy contains user(s)/group(s) without email



  • Add email to the user(s)/group(s) without email and update the policy
```

Konfigurationsänderungen vor der vollständigen Migration zu CEP

Die folgenden Konfigurationsänderungen müssen vom Secure Private Access-Administrator manuell angewendet werden, bevor die vollständige Migration zu CEP eingeleitet wird. Diese Updates gewährleisten Kompatibilität und Bereitschaft für alle Anwendungen und Richtlinien.

Änderungen an der Single Sign-On-Konfiguration

Um die Kompatibilität mit CEP sicherzustellen, ist es unerlässlich, die Single Sign-On (SSO)-Konfiguration für alle bestehenden Anwendungen zu aktualisieren. Die Administratoren von Secure Private Access müssen die folgenden Schritte ausführen:

1. Navigieren Sie zur Seite Anwendungs-Konfiguration (**Secure Private Access > App Configuration**).
2. Bearbeiten Sie die Anwendungen, um die Single Sign-On-Konfiguration zu ändern.

   Im Abschnitt Single Sign-On wählen Sie unter **Welchen Single Sign-On-Typ möchten Sie für Ihr Web-App-Setup verwenden?** die Option **SSO nicht verwenden** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Dieses Update ist obligatorisch, da der SSO-Schritt in CEP entfernt wird. Indem Sie die Anwendung auf **SSO nicht verwenden** einstellen, stellen Sie die fortgesetzte Funktionalität und die Übereinstimmung mit dem neuen Migrationsfluss sicher.
- Wenn die Single Sign-On-Konfiguration nicht wie angewiesen geändert wird, wird die Anwendung nach der Migration zu CEP unzugänglich.

Updates für Zugriffsrichtlinien und Sitzungsrichtlinien

Um sicherzustellen, dass die Zugriffsrichtlinien mit den CEP-Standards kompatibel sind, sind spezifische Updates in den Zugriffs- und Sitzungsrichtlinien erforderlich. Die Administratoren von Secure Private Access müssen die folgenden Schritte ausführen:

1. Navigieren Sie zu **Secure Private Access > Policies > Access Policies**.
2. Klicken Sie bei der entsprechenden Richtlinie auf **Bearbeiten** und ändern Sie die Aktionseinstellungen.
    a. Innerhalb der Richtlinie navigieren Sie zum Abschnitt **Richtlinienregeln**, klicken Sie auf das Auslassungspunkte-Symbol in der Zeile der Richtlinienregel und klicken Sie auf **Bearbeiten**.
    b. Navigieren Sie zur Seite **Aktionen** und ändern Sie die **Aktionseinstellungen**.

Standardisierung von Aktionen über Anwendungen hinweg

Beim Konfigurieren von Aktionen für sowohl HTTP/HTTPS- als auch TCP/UDP-Anwendungen stellen Sie Folgendes sicher:

- Dieselbe Aktion, entweder **Zugriff erlauben** oder **Zugriff verweigern**, ist in beiden Abschnitten ausgewählt.
- Wenn die Option **Zugriff mit Einschränkungen erlauben** derzeit für HTTP/HTTPS-Anwendungen aktiviert ist, muss sie entfernt werden, da diese Einstellung in CEP nicht unterstützt wird.
- Ersetzen Sie **Zugriff mit Einschränkungen erlauben** durch entweder **Zugriff erlauben** oder **Zugriff verweigern**, basierend auf dem gewünschten Richtlinienverhalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsanforderung für Richtlinienaktualisierungen

Zugriffsrichtlinien ohne zugewiesene Anwendungen können nicht aktualisiert werden. Um diese Richtlinien zu ändern, weisen Sie der Richtlinie zuerst eine Anwendung zu.

WICHTIG:

Wenn diese Aktualisierungen nicht durchgeführt werden, werden Anwendungen, die Zugriffsrichtlinien mit gemischten Aktionen zugeordnet sind, unzugänglich, oder die Einstellung für Verweigerungsaktionen könnte ignoriert werden.

Aktualisierung der Webfilterrichtlinie (optional)

Um die Übereinstimmung mit den neuen CEP-Migrationsstandards zu gewährleisten, ist es erforderlich, die Webfiltereinstellungen in Secure Private Access zu aktualisieren. Führen Sie die folgenden Schritte aus, um die Webfilterkonfiguration zu aktualisieren:

1. Navigieren Sie zu **Secure Private Access > Einstellungen > Nicht genehmigte Websites**.
2. Löschen Sie alle Websites und Remote Browser Isolation (RBI)-Einträge, die derzeit in diesem Abschnitt aufgeführt sind.
3. Nach dem Entfernen dieser Einträge deaktivieren Sie den Schalter **Webfilterung ist aktiviert**, der sich oben auf der Seite befindet.

Diese Konfigurationen sind nach der Migration zu CEP nicht mehr relevant.

WICHTIG:

Wenn diese Schritte nicht abgeschlossen werden, hat dies keine Auswirkungen auf den Systembetrieb nach der vollständigen Migration. Die Seite **Nicht genehmigte Websites** ist jedoch nicht sichtbar.

Weitere Richtlinienanpassungen (optional)

Nicht verwendete Bedingungen überprüfen und löschen:

Im Rahmen des Migrations- und Richtlinienoptimierungsprozesses wird empfohlen, Zugriffs- und Sitzungsrichtlinien auf Bedingungen zu überprüfen, die möglicherweise nicht mehr anwendbar sind. Beispiele für solche Bedingungen sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Workspace-URL
- Desktop- und Mobiloptionen

Diese Bedingungen können gelöscht werden, wenn sie für Ihre aktuelle Umgebung oder Ihre Geschäftsanforderungen nicht relevant sind.

HINWEIS:

Wenn diese Richtlinienanpassungen nicht vorgenommen werden, hat dies keine Auswirkungen auf den Systembetrieb.

Bereinigung von Sicherheitsgruppen (optional)

Überprüfen Sie die Konfiguration der Sicherheitsgruppen in Secure Private Access.

Navigieren Sie zu **Secure Private Access > Anwendungen > Sicherheitsgruppen**, um vorhandene Einträge zu überprüfen.

Nach der Migration ist die Konfiguration der Sicherheitsgruppen nicht mehr verfügbar. Daher können alle derzeit unter dieser Registerkarte aufgeführten Einträge gelöscht werden, da sie für die Umgebung nach der Migration nicht mehr relevant sind.

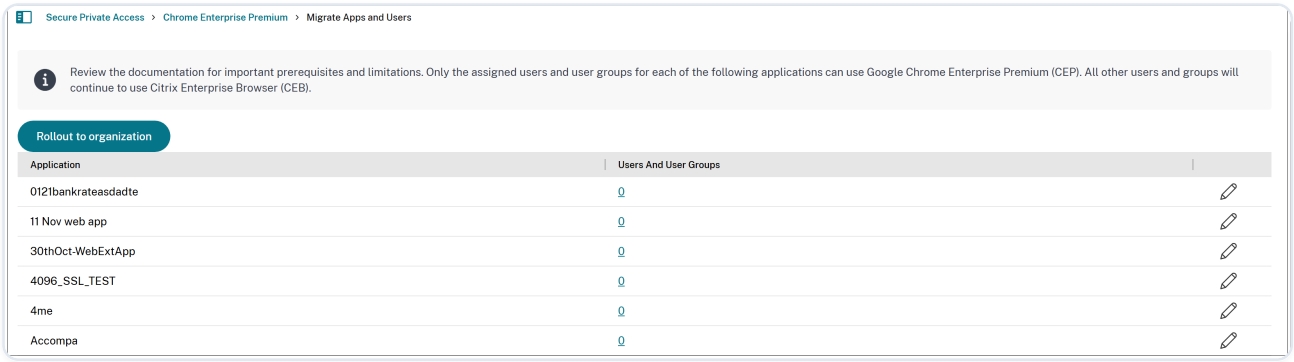
HINWEIS:

Es gibt keine Systemauswirkungen, wenn diese Konfiguration nicht aktualisiert wird. Das Entfernen dieser Einträge ist optional und hilft, eine optimierte Umgebung aufrechtzuerhalten, ist aber für den weiteren Betrieb nicht erforderlich.

CEP für die Organisation einführen (vollständige Migration)

Klicken Sie nach Abschluss der oben genannten Schritte auf **Für Organisation einführen** auf der Seite **Apps und Benutzer migrieren**. Dies ist die letzte Phase des Migrationsprozesses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



WICHTIG:

Sobald die Einführung abgeschlossen ist, wird CEP zum Standard-Enterprise-Browser. Eine Rückkehr zu CEB ist nicht möglich, und inkompatible Einstellungen werden in der Secure Private Access-Administratorkonsole ausgeblendet.

Zusammenfassung des Migrationsprozesses

Führen Sie die folgenden Schritte aus, um Anwendungen von CEB zu CEP zu migrieren:

1. Stellen Sie Chrome Enterprise Premium bereit.
2. Migrieren Sie eine Anwendung für eine bestimmte Benutzergruppe.
    a. Erweitern Sie die Gruppe mit E-Mail (falls nicht vorhanden).
    b. Beheben Sie alle Inkompatibilitäten.
    c. Migrieren Sie die Anwendung zu CEP.
    d. Überprüfen Sie, ob die Anwendung über CEP zugänglich ist (direkt, CWA und WSUI).
3. Erweitern Sie die Benutzer und Benutzergruppen mit E-Mails.
4. Migrieren Sie weitere Anwendungen sowie Benutzer und Benutzergruppen.
5. CEP im Unternehmen ausrollen (vollständige Migration).
6. Verbleibende Inkompatibilitäten beheben.
    a. Führen Sie das Skript erneut aus und geben Sie in der Eingabeaufforderung an, dass die CEP-Einführung abgeschlossen wurde.
    b. Die Inkompatibilitäten beheben.
    c. Überprüfen Sie, ob die Anwendungen über CEP zugänglich sind (direkt, CWA und WSUI).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Herausforderungen beim E-Mail-Anreicherungsprozess

Die E-Mail-Anreicherungsaufgabe kann komplex sein, da sie oft die Zusammenarbeit mehrerer Teams erfordert, um E-Mails verschiedenen Gruppen über mehrere Domänen hinweg zuzuweisen. Die Funktion zur Domänenzuordnung erleichtert diesen Prozess. Weitere Informationen finden Sie unter Domänenzuordnung für Benutzergruppen ohne E-Mail-Adressen.

Bewährte Methoden

1. Beginnen Sie mit einer Pilotmigration für eine kleine Benutzergruppe, bevor Sie eine vollständige Einführung vornehmen.
2. Nutzen Sie die offiziellen Migrationstools und die Dokumentation von Citrix.
3. Führen Sie eine klare Dokumentation aller Änderungen und Konfigurationen.
4. Erstellen Sie einen Rollback-Plan für den Fall kritischer Probleme.

Fazit

Die Migration von CEB zu CEP modernisiert Ihre Citrix-Umgebung mit erweiterten Funktionen. Sorgfältige Planung, gründliche Tests und proaktives Benutzerengagement gewährleisten einen reibungslosen Übergang zu CEP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erweiterte Secure Private Access-Funktionen

Im Folgenden sind einige der erweiterten Funktionen aufgeführt, die von Secure Private Access unterstützt werden:

- **Zugriffsmodus-basierte Richtlinienerzwingung:** Die Zugriffsmodus-basierte Richtlinienerzwingung ermöglicht Administratoren, einzuschränken, wie ein Benutzer eine Verbindung zu einer Anwendung herstellt. Die Verbindung kann über einen Browser-basierten Client oder den Citrix Secure Access Client erfolgen. Weitere Informationen finden Sie unter Zugriffsmodus-basierte Richtlinienerzwingung.
- **Unterstützung für lokalen LAN-Zugriff:** Secure Private Access unterstützt den nahtlosen Zugriff auf lokale LAN-Ressourcen, während eine sichere Verbindung zu Unternehmensressourcen aufrechterhalten wird. Weitere Informationen finden Sie unter [Nahtloser Zugriff auf lokale LAN-Ressourcen (Drucker, Dateiserver)(/de-de/citrix-secure-private-access/service/spa-local-lan-access.html).
- **DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten:** Administratoren können DNS-Abfragen für bestimmte Anwendungen direkt an deren dedizierte Ressourcenstandorte weiterleiten. Dies ermöglicht eine genauere DNS-Auflösung, intelligentes Traffic-Management und eine bessere Benutzererfahrung. Weitere Informationen finden Sie unter DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten.
- **Hybrider Datenpfad für den Secure Private Access-Dienst:** Der hybride Datenpfad für den Secure Private Access-Dienst nutzt sowohl lokale als auch Cloud-Infrastrukturen, um sicheren Zugriff auf Anwendungen zu ermöglichen. Organisationen können den hybriden Datenpfad verwenden, um den gesamten Datenverkehr über ein lokales NetScaler Gateway zu leiten. Dies stellt sicher, dass sensible Daten innerhalb des Unternehmensnetzwerks verbleiben. Obwohl der Datenverkehr über das lokale NetScaler Gateway geleitet wird, kann Citrix Cloud weiterhin zur Überwachung und Verwaltung der Anwendungen und Benutzer verwendet werden. Weitere Informationen finden Sie unter Hybrider Datenpfad für den Secure Private Access-Dienst.
- **Anwendungen, Domänen oder IP-Adressen in Ihrem Netzwerk ermitteln:** Hilft einem Administrator, Einblick in die externen und internen Anwendungen (HTTP/HTTPS- und TCP/UDP-Apps) zu erhalten, auf die in einer Organisation zugegriffen wird. Diese Funktion ermittelt und listet alle Domänen/IP-Adressen auf, ob veröffentlicht oder nicht. So können

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administratoren sehen, auf welche Domänen/IP-Adressen von wem zugegriffen wird, und entscheiden, ob sie diese als Anwendungen veröffentlichen möchten, um diesen Benutzern Zugriff zu gewähren. Weitere Informationen finden Sie unter Anwendungen, Domänen oder IP-Adressen in Ihrem Netzwerk ermitteln.

- **Kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten:** Ermöglicht Administratoren, den internen Routing-Typ pro URL oder Ressourcenstandort basierend auf dem Benutzerkontext zu bearbeiten. Weitere Informationen finden Sie unter Kontextbasiertes App-Routing und Auswahl von Ressourcenstandorten.
- **Richtlinienmodellierungstool:** Bietet Administratoren volle Transparenz über die erwarteten App-Zugriffsergebnisse (zugelassen/zugelassen mit Einschränkung/verweigert) basierend auf ihren bestehenden Konfigurationen. Administratoren können die Zugriffsergebnisse für jeden Benutzer basierend auf Bedingungen wie Gerätetyp, Gerätestatus, geografischem Standort, Netwerkstandort und Workspace-URL überprüfen. Weitere Informationen finden Sie unter Richtlinienmodellierungstool.
- **Anwendungsimport-Tool:** Die Secure Private Access-Administratorkonsole enthält ein Dateiimport-Tool, mit dem Administratoren mehrere Anwendungen mithilfe einer CSV-Datei oder der nsconfig-Datei in das System importieren können. Dieses Tool ist besonders nützlich für Organisationen, die von einem herkömmlichen VPN zu einer fortschrittlicheren Lösung wie Secure Private Access wechseln. Organisationen können dieses Tool beispielsweise verwenden, um Anwendungen, die über ein VPN bereitgestellt wurden, zu Secure Private Access zu migrieren und zu einer ZTNA-basierten Architektur zu wechseln. Der Massen-Upload von Apps ermöglicht es den Organisationen, die Notwendigkeit einer manuellen Konfiguration zu eliminieren. Weitere Informationen finden Sie unter Anwendungsimport-Tool.
- **Aktive Sitzungen beenden und Benutzer/Maschinen blockieren:** – Ermöglicht Administratoren, alle aktiven Sitzungen sofort zu beenden und die Benutzer/Maschinen zur Sperrliste hinzuzufügen. Das Hinzufügen eines Benutzers/einer Maschine zur Sperrliste beendet alle aktiven Secure Private Access-Anwendungssitzungen und blockiert zukünftigen Anwendungszugriff. Weitere Informationen finden Sie unter Aktive Sitzungen beenden und Benutzer/Maschinen zur Sperrliste hinzufügen.
- **Timeouts für Benutzersitzungen:** Ermöglicht Administratoren, einen Timeout-Zeitraum für Web-Apps und den Citrix Secure Access Client zu konfigurieren, um Benutzersitzungen zu beenden, wenn für den angegebenen Zeitraum keine Netzwerkaktivität stattfindet. Weitere Informationen finden Sie unter Timeouts für Benutzersitzungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hybrider Datenpfad für den Secure Private Access Dienst

Der hybride Datenpfad für den Secure Private Access Dienst nutzt sowohl lokale als auch Cloud-Infrastrukturen, um sicheren Zugriff auf Anwendungen bereitzustellen. Organisationen können den hybriden Datenpfad nutzen, um den gesamten Datenverkehr über ein lokales NetScaler Gateway zu leiten. Dies stellt sicher, dass sensible Daten innerhalb des Unternehmensnetzwerks verbleiben. Obwohl der Datenverkehr über das lokale NetScaler Gateway geleitet wird, kann Citrix Cloud™ weiterhin zur Überwachung und Verwaltung der Anwendungen und Benutzer verwendet werden.

Wichtige Vorteile der Nutzung des hybriden Datenpfads

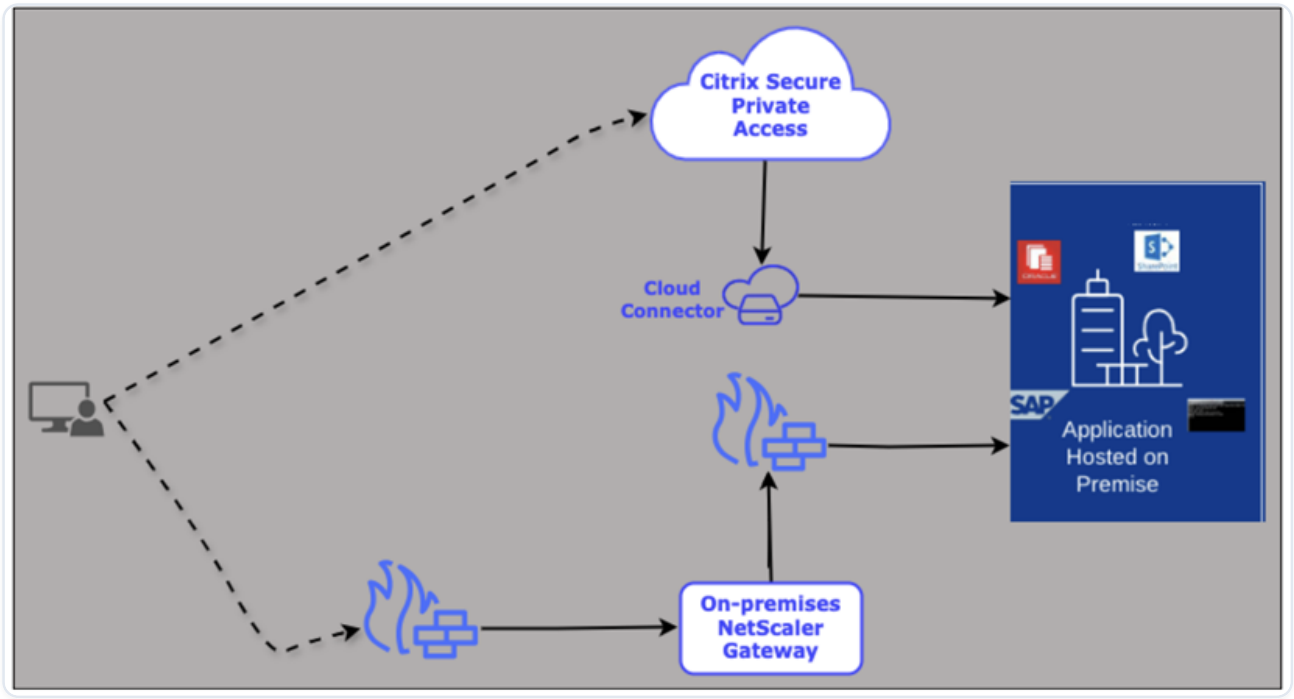
Im Folgenden sind einige der wichtigsten Vorteile der Nutzung des hybriden Datenpfads aufgeführt:

- Erweiterte Reichweite mit lokalem Gateway:
  - Verwenden Sie ein lokales NetScaler® Gateway, um Zugriff auf lokale Anwendungen in Bereichen bereitzustellen, in denen ein Cloud-PoP weit entfernt ist.
  - Sorgen Sie für konsistente Leistung, indem Sie das Routing von Datenverkehr über weit entfernte Cloud-PoPs vermeiden.
- Granulare Sicherheit und Kontrolle:
  - Implementieren Sie selektives Routing, um sensible Anwendungen über sichere, lokale Pfade zu leiten und weniger kritische Anwendungen über die Cloud zu leiten.
  - Ermöglichen Sie benutzerdefiniertes Routing für Anwendungen, um Datensicherheits- und Compliance-Anforderungen basierend auf der Sensibilität der Anwendungsdaten zu erfüllen
- Direkte Konnektivität für eine verbesserte Benutzererfahrung:
  - Stellen Sie direkte Verbindungen zwischen Remote-Benutzern und erforderlichen Anwendungen her, wobei der Cloud-PoP umgangen wird.

Funktionsweise des hybriden Datenpfads

Die folgende Abbildung zeigt den Workflow des hybriden Datenpfads.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Die folgende Liste erläutert den Workflow, der im hybriden Datenpfad involviert ist:

1. Ein Benutzer meldet sich beim Citrix Secure Access™ Client an.
2. Nach erfolgreicher Authentifizierung wird eine Sitzung hergestellt.
3. Der Endbenutzer versucht, eine Anwendung zu starten.
4. Die mit der Anwendung verbundenen Zugriffsrichtlinien werden ausgewertet, und die App wird gestartet.
    - Wenn die Anwendung so konfiguriert ist, dass sie über den Secure Private Access-Dienst geleitet wird, wird die Anfrage an den Cloud Connector gesendet und dann die spezifische App gestartet.
    - Wenn die Anwendung so konfiguriert ist, dass sie über das lokale NetScaler Gateway geleitet wird, wird die Anfrage an das lokale NetScaler Gateway gesendet und die spezifische Anwendung gestartet.

Unterstützte Clients

Der hybride Datenpfad wird von den folgenden Citrix Secure Access Clients unterstützt:

- Windows – 25.1.1.17 und höher
- macOS – 25.02.1 und höher

Unterstützte NetScaler Gateway Builds

Der hybride Datenpfad wird ab NetScaler Gateway Version 14.1 Build 47.46 unterstützt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konnektivitätsanforderungen

Die folgenden Abschnitte enthalten weitere Informationen zu den Konnektivitätsanforderungen.

Zulassungsliste von URLs für ausgehende Verbindungen

Die folgenden URLs müssen für ausgehende Verbindungen von NetScaler Gateway zugelassen werden:

- `https://trust.citrixnetworkapi.net`: Für die Gateway-Registrierung bei Citrix Cloud.
- `https://trust.citrixworkspacesapi.net`: Für die Gateway-Registrierung bei Citrix Cloud.
- `https://policy.netscalergateway.net`: Zur Autorisierung von App-Startanfragen über das Gateway.
- `https://cacerts.digicert.com`: Für die Zertifikatsvalidierung der Policy Service Engine.

Hybriden Datenpfad für Secure Private Access-Anwendungen einrichten

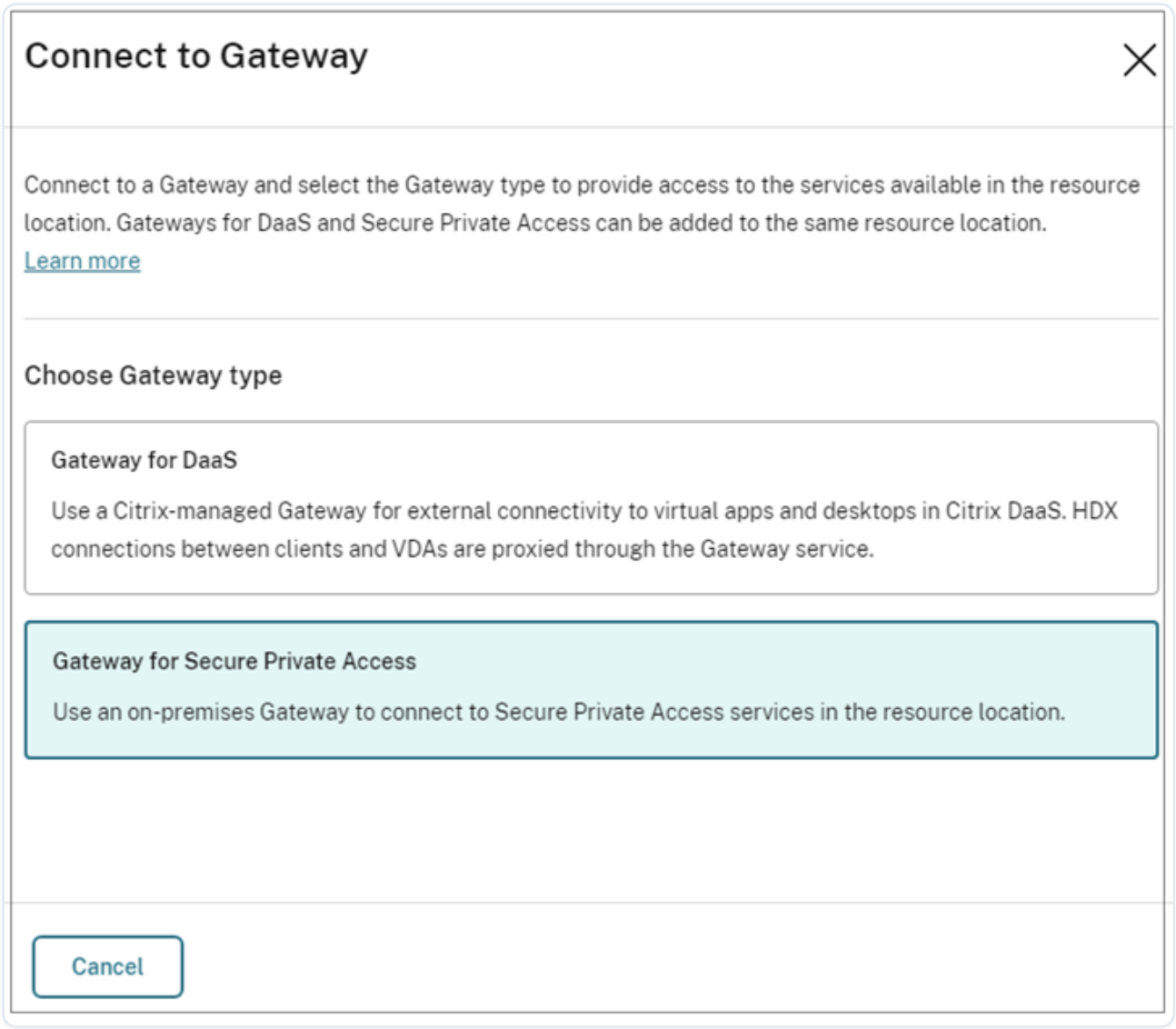
Die folgenden übergeordneten Schritte sind beim Einrichten des hybriden Datenpfads erforderlich:

1. Mit einem Gateway verbinden, um eine Verbindung herzustellen
2. NetScaler Gateway bei Citrix Cloud registrieren
3. Routing des Datenverkehrs über das lokale NetScaler Gateway aktivieren

Mit einem Gateway verbinden, um eine Verbindung herzustellen

Um eine Verbindung mit den Secure Private Access-Ressourcen an einem bestimmten Ressourcenstandort herzustellen, müssen Sie sich zuerst mit einem Gateway verbinden. Citrix Cloud ermöglicht Ihnen, eine Verbindung mit DaaS- und Secure Private Access-Ressourcen an einem bestimmten Ressourcenstandort herzustellen. Der von Ihnen ausgewählte Gateway-Typ bestimmt die Dienste, auf die Sie zugreifen können. Für verbesserte Flexibilität und zur Optimierung der Ressourcennutzung können Sie sowohl ein DaaS-Gateway als auch ein Secure Private Access-Gateway innerhalb desselben Ressourcenstandorts hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Gateway für DaaS:** Das von Citrix verwaltete Gateway dient als externer Zugriffspunkt für virtuelle Anwendungen und Desktops, die in der Citrix DaaS™-Umgebung gehostet werden. Dieses Gateway fungiert als sicherer Proxy, der die HDX-Verbindungen zwischen den Clients (Benutzergeräten) und den virtuellen Desktop-Agenten (VDAs) in Citrix Cloud vermittelt und verwaltet.

  Sie können wählen, wie Sie den Zugriff auf virtuelle Apps und Desktops basierend auf verschiedenen Geschäftsanforderungen zulassen möchten.

- **Gateway für Secure Private Access:** Das Gateway für Secure Private Access stellt sicher, dass Organisationen die Kontrolle über sensible Daten behalten, indem der gesamte Datenverkehr über ein lokales NetScaler Gateway geleitet wird, wodurch gewährleistet ist, dass er innerhalb des Netzwerkperimeters des Unternehmens verbleibt.

  Während das lokale NetScaler Gateway den Datenverkehr verarbeitet, kann Citrix Cloud für zentralisierte Verwaltungs- und Überwachungsfunktionen genutzt werden, wodurch Administratoren Anwendungen und Benutzer nahtlos überwachen und verwalten können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Führen Sie die folgenden Schritte aus, um eine Verbindung zu einem Gateway herzustellen:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie **Ressourcenstandorte > Übersicht** und klicken Sie dann auf **Gateway**.
3. Wählen Sie unter **Gateway-Typ auswählen** die Option **Gateway für Secure Private Access**.
4. Registrieren Sie Ihr Gateway bei Citrix Cloud. Weitere Informationen finden Sie unter Registrieren Ihres NetScaler Gateways bei Citrix Cloud.

Registrieren Ihres NetScaler Gateways bei Citrix Cloud

Sie müssen zuerst das Gateway für Secure Private Access auswählen und dann das lokale NetScaler Gateway bei Citrix Cloud registrieren. Diese Registrierung stellt eine sichere Verbindung zwischen Ihrem lokalen NetScaler Gateway und der Citrix Cloud-Umgebung für den Secure Private Access-Dienst her.

Voraussetzungen:

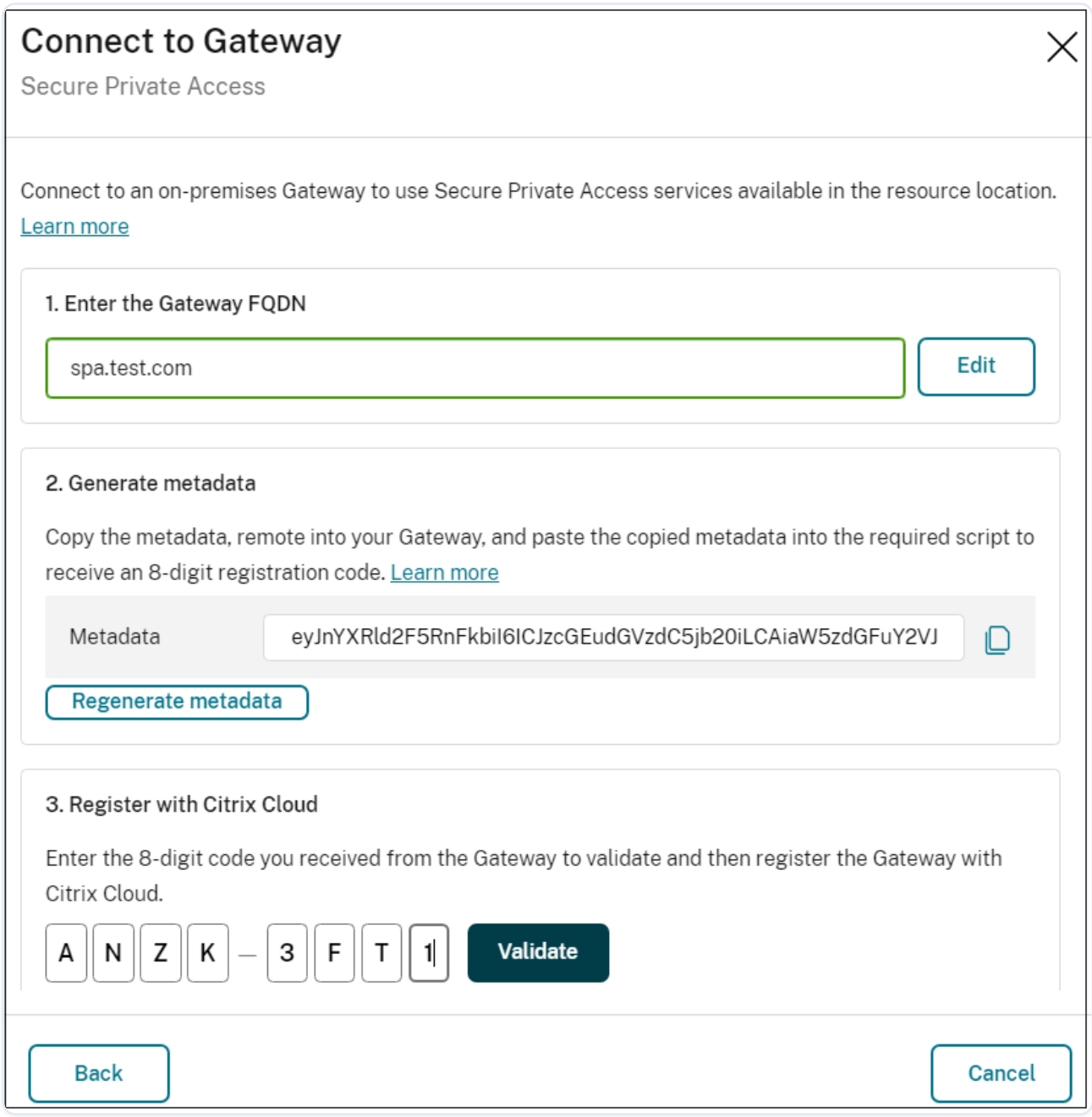
Stellen Sie sicher, dass die folgenden Konfigurationen für die erfolgreiche Ausführung des Registrierungsskripts abgeschlossen sind:

- Eine Subnetz-IP (SNIP) muss auf NetScaler konfiguriert sein.
- Ein DNS-Nameserver muss konfiguriert sein, falls noch nicht vorhanden.
- Eine für den neuen virtuellen VPN-Server vorgesehene IP-Adresse ist erforderlich.
- Der SSL-Zertifikatsschlüsselname für die Bindung an den neuen VPN-Virtual-Server muss angegeben werden. Dieser SSL-Zertifikatsschlüsselname muss NetScaler vor der Skriptausführung hinzugefügt werden.

Führen Sie die folgenden Schritte aus, um Ihr Gateway bei Citrix Cloud zu registrieren:

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie **Ressourcenstandorte > Übersicht** und klicken Sie dann auf **Gateway**.
3. Wählen Sie unter **Gateway-Typ auswählen** die Option **Gateway für Secure Private Access**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Geben Sie den FQDN des Gateways ein, das bei Citrix Cloud registriert werden soll.
2. Klicken Sie auf **Metadaten generieren**. Sie können die Metadaten auch durch Klicken auf **Metadaten neu generieren** neu generieren.
   - Kopieren Sie die Metadaten in die Zwischenablage.
   - Stellen Sie eine Secure Shell (SSH)-Verbindung zum NetScaler Gateway in der lokalen Umgebung her. Diese Verbindung ermöglicht es Ihnen, die Befehle und Skripte remote auf dem NetScaler-Gerät auszuführen.
   - Nach erfolgreicher Verbindung mit dem NetScaler Gateway führen Sie den folgenden Befehl aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
python3 /var/spa/scripts/spa_registration.py <copied metadata>
```

- Ersetzen Sie `<copied metadata>` durch die tatsächlichen Metadaten, die Sie zuvor kopiert haben.

  Das Skript generiert einen 8-stelligen Registrierungscode. Dieser Code ist entscheidend für den Registrierungsprozess.

3. Geben Sie den 8-stelligen Code im Abschnitt **Bei Citrix Cloud registrieren** ein.
4. Klicken Sie auf **Validieren**.

   Eine Warnmeldung wird angezeigt, wenn der Code ungültig ist. Wenn die Validierung erfolgreich ist, wird die Schaltfläche **Registrieren** angezeigt.
5. Klicken Sie auf **Registrieren**.
6. Kehren Sie zum Skriptausführungsfenster zurück. Das System muss zum nächsten Schritt übergehen und Sie zur Eingabe der folgenden Details zur Vervollständigung der Konfiguration auffordern.

   - Eine für den virtuellen VPN-Server vorgesehene IP-Adresse.
   - Der SSL-Zertifikatschlüsselname, der dem virtuellen VPN-Server zugeordnet werden soll.

Sie können nun das Routing von Anwendungen über den lokalen NetScaler konfigurieren.

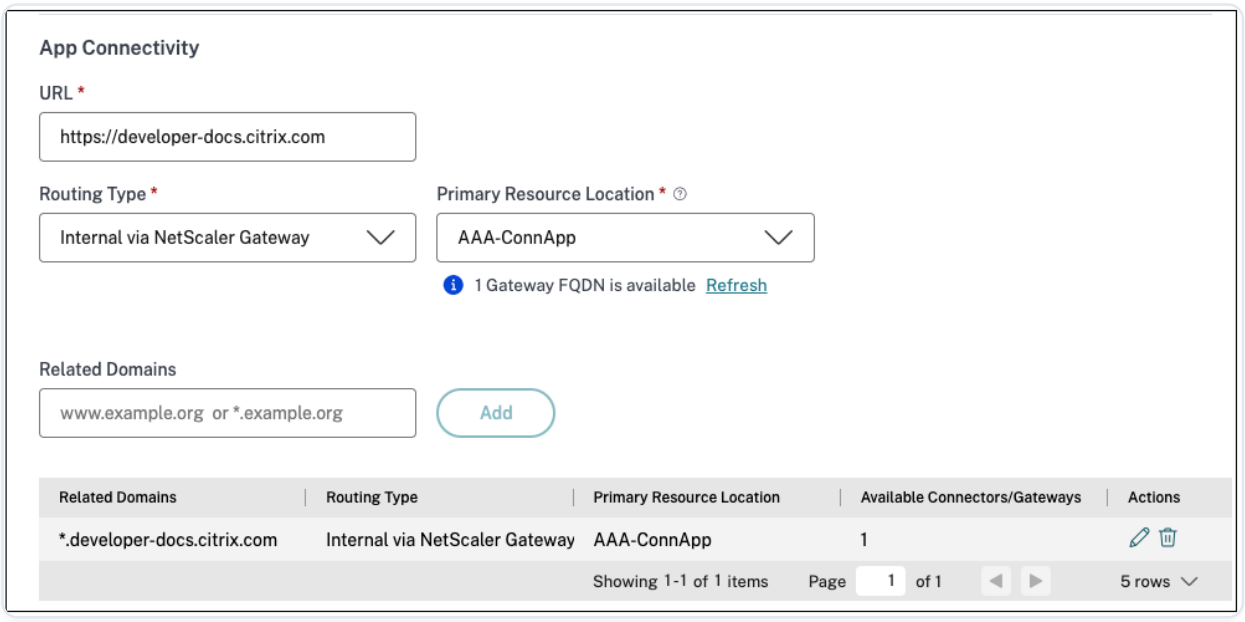
Aktivieren des Routings des Datenverkehrs über das lokale NetScaler Gateway

Führen Sie die folgenden Schritte aus, um das Routing des Datenverkehrs über das lokale NetScaler Gateway zu aktivieren.

1. Konfigurieren Sie die App. Details finden Sie in den folgenden Themen:

   - Unterstützung für Enterprise-Web-Apps
   - Agentenloser Zugriff auf Enterprise-Web-Apps
   - Unterstützung für Software-as-a-Service-Apps
   - Unterstützung für Client-Server-Apps
2. Im Abschnitt **App-Konnektivität** definieren Sie die Routing-Einstellungen für die Anwendungsdomänen und geben an, ob der Datenverkehr extern oder intern über die Citrix Connector™ Appliance oder über das lokale NetScaler Gateway geleitet werden soll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Wählen Sie unter **Routing-Typ** die Option **Intern über NetScaler Gateway**. Dadurch wird sichergestellt, dass der Datenverkehr über das lokale NetScaler Gateway geleitet wird. Sie können den Routing-Typ für die zugehörigen Domänen auch auf **Intern über NetScaler Gateway** aktualisieren.

    - Klicken Sie auf das Bearbeitungssymbol in der Spalte **Aktionen** der Tabelle **Zugehörige Domänen**.
    - Wählen Sie unter **Routing-Typ** die Option **Intern über NetScaler Gateway**.
    - Klicken Sie auf **Speichern**.

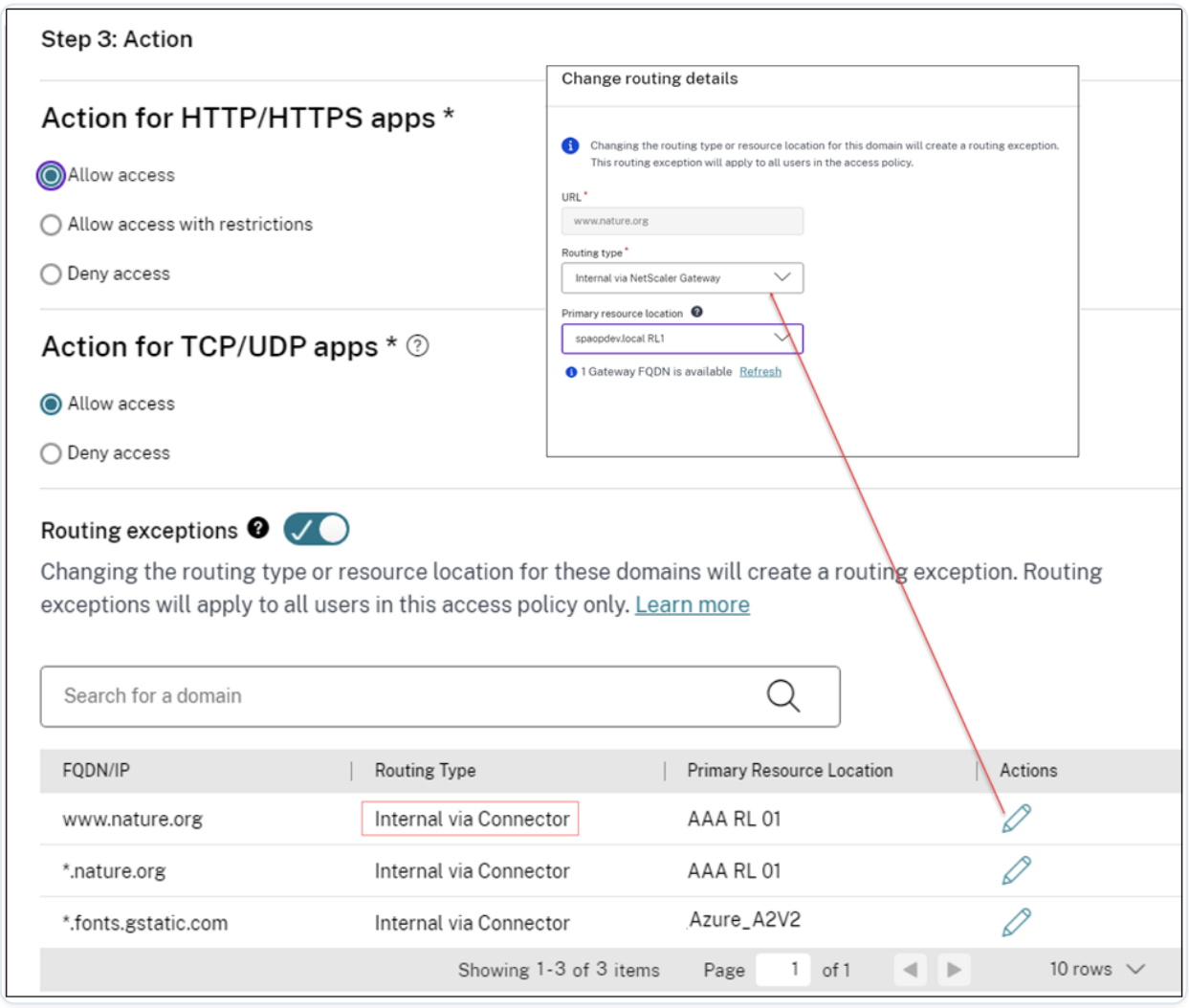
Routingdetails aus Zugriffsrichtlinien ändern

Sie können das Routingverhalten überschreiben, um es je nach spezifischem Kontext zu variieren. Diese Kontexte können Faktoren wie Benutzergruppen, geografischer Standort, Plattform und andere relevante Kriterien umfassen. Durch die Anpassung des Routingverhaltens basierend auf dem Kontext können Sie ein optimiertes Benutzererlebnis bieten.

Führen Sie die folgenden Schritte aus, um das Routing des Datenverkehrs über das lokale NetScaler Gateway aus der Zugriffsrichtlinie zu ändern.

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Aktivieren Sie auf der Seite **Schritt 3: Aktion** den Umschalter **Routing-Ausnahmen**. Der Umschalter **Routing-Ausnahmen** ermöglicht Ihnen die Bearbeitung der Ressourcenstandorte und Routinginformationen für Domänen der in der Zugriffsrichtlinie hinzugefügten Anwendungen.
3. Klicken Sie auf das Bearbeitungssymbol neben der Domäne, für die Sie den Routing-Typ ändern möchten.
4. Wählen Sie unter **Routing-Typ** die Option **Intern über NetScaler Gateway**.
5. Klicken Sie auf **Speichern**.

Einschränkungen

- Unterstützte NetScaler Gateway-Bereitstellungstypen – Der hybride Datenpfad wird derzeit nur für Umgebungen mit einer Hochverfügbarkeitskonfiguration unterstützt.
- Fallback-Mechanismus – In der aktuellen Version gibt es keinen Failover- oder Fallback-Mechanismus, der den Datenverkehr automatisch zur Cloud-Infrastruktur umleitet, falls das lokale Gateway ausfällt oder nicht verfügbar ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die folgenden Funktionen werden für den hybriden Datenpfad in der aktuellen Version nicht unterstützt:
  - Anwendungsermittlung
  - Richtlinienmodellierung
  - Sitzungsrichtlinien
  - Beobachtbarkeit
- Der Ordner /var/spa/scripts/ wird erstellt, wenn Sie das Skript `installns` zur Installation eines NetScaler-Builds ausführen. Dieser Ordner ist auf neu bereitgestellten NetScaler VPX-Instanzen nicht vorhanden und muss während des Installationsvorgangs erstellt werden. Weitere Informationen finden Sie in den folgenden Themen:
  - Upgrade einer eigenständigen NetScaler-Appliance
  - Upgrade eines Hochverfügbarkeitspaares

Problem mit dem Secure Private Access-Registrierungsskript

Das Secure Private Access-Registrierungsskript wird aufgrund eines Konfigurationsproblems mit einigen integrierten Befehlen nicht direkt auf einer neu bereitgestellten VPX-Instanz in Azure ausgeführt. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Stellen Sie eine neue VPX-Instanz in Azure bereit.
- Fügen Sie keine neue Konfiguration hinzu.
- Legen Sie mit dem Befehl `set system user nsroot <your-password>` ein neues Kennwort für den nsroot-Benutzer fest. Dieser Schritt ist wichtig, da der während der Bereitstellung erstellte benutzerdefinierte Benutzer nach Ausführung des Befehls `clear config` gelöscht wird. Sie können mit nsroot und diesem neuen Kennwort auf den NetScaler zugreifen.
- Speichern Sie die Konfiguration mit dem Befehl `save config`.
- Überprüfen Sie die Ausgabe von `show cache policylabel`. Sie muss leer sein.
- Führen Sie den Befehl `clear config basic` aus und geben Sie Y ein.
- Überprüfen Sie die Ausgabe von `show cache policylabel` erneut. Sie muss _reqBuiltinDefaults als Bezeichnung anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
show cache policylabel



Label Name: _reqBuiltinDefaults

Evaluates: REQ

Number of bound policies: 3

Number of times invoked: 02)  Label Name: _resBuiltinDefaults

Evaluates: RES

Number of bound policies: 8

Number of times invoked: 03)  Label Name: _httpquicReqBuiltinDefaults

Evaluates: HTTPQUIC_REQ

Number of bound policies: 3

Number of times invoked: 04)  Label Name: _httpquicResBuiltinDefaults

Evaluates: HTTPQUIC_RES

Number of bound policies: 8

Number of times invoked: 0Warning: Feature(s) not enabled [IC]
```

- Wenn Sie _reqBuiltinDefaults nicht in der Befehlsausgabe sehen, wenden Sie sich an den Citrix Support.
- Konfigurieren Sie den SNIP, den SSL-Zertifikatsschlüssel und den DNS-Namensserver.
- Speichern Sie die Konfiguration mit dem Befehl `save config`.
- Führen Sie das Registrierungsskript für Secure Private Access erneut aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungen, Domänen oder IP-Adressen in Ihrem Netzwerk ermitteln

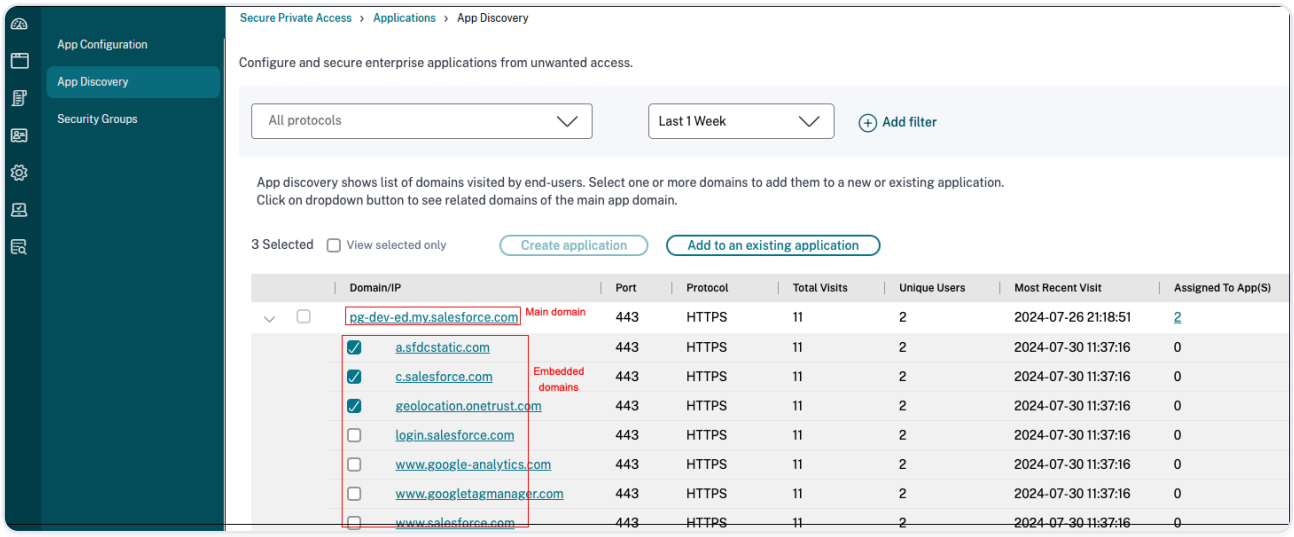
Die Funktion zur Anwendungserkennung (Application Discovery) hilft Administratoren, Einblick in die externen und internen Anwendungen (HTTP/HTTPS- und TCP/UDP-Apps) zu erhalten, auf die in einer Organisation zugegriffen wird. Diese Funktion erkennt und listet alle Domänen/IP-Adressen auf, ob veröffentlicht oder nicht. So können Administratoren sehen, auf welche Domänen/IP-Adressen von wem zugegriffen wird, und entscheiden, ob sie diese als Anwendungen veröffentlichen möchten, um diesen Benutzern Zugriff zu gewähren.

Die Funktion zur Anwendungserkennung bietet Administratoren die folgenden Funktionen:

- Bietet Einblick in interne und externe Domänen/IP-Adressen, auf die von Endbenutzern zugegriffen wird.
- Bietet einen umfassenden Einblick in alle Arten von Anwendungen, auf die zugegriffen wird (HTTP, HTTPS, TCP und UDP). Alle Zugriffsmethoden werden unterstützt, d. h. Zugriff über Citrix Enterprise Browser™, Secure Access Agent, Direct Access oder aus einem Store.
- Zeigt sowohl veröffentlichte als auch nicht veröffentlichte Domänen/IP-Adressen an, auf die von Endbenutzern zugegriffen wird.
- Zeigt sowohl die Hauptdomäne als auch die zugrunde liegenden eingebetteten Domänen an, die als zugehörige Domänen konfiguriert werden müssen, wenn die Anwendungen für den Zugriff über Citrix Enterprise Browser veröffentlicht werden.
- Zeigt die eingebetteten Domänen in einer Baumstruktur an. Administratoren können auf das erweitern-Zeichen (**>**) in der Zeile der Hauptdomäne klicken, um die eingebetteten Domänen anzuzeigen.
- Ermöglicht Administratoren das Erstellen neuer Anwendungen oder das Hinzufügen dieser Domänen zu einer vorhandenen Anwendung, wenn eine Hauptdomäne oder eine eingebettete Domäne (HTTP/HTTPS) oder die Ziel-IP-Adresse (TCP/UDP) keiner Anwendung zugeordnet ist.

Die folgende Abbildung zeigt eine Beispielseite für die **App-Erkennung**. Die Seite **App-Erkennung** ermöglicht das Filtern von Domänen basierend auf dem Protokoll (HTTP/HTTPS, TCP/UDP) sowie der Domänen-/IP-Adresse und den Portnummern. Sie zeigt auch die nicht veröffentlichten (keiner App zugewiesenen) Domänen an, auf die von Endbenutzern zugegriffen wird. Sie sehen eine Hauptdomäne mit einer Dropdown-Liste von eingebetteten Domänen darunter. Diese Domänen müssen beim Veröffentlichen der Anwendung als zugehörige Domänen konfiguriert werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

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

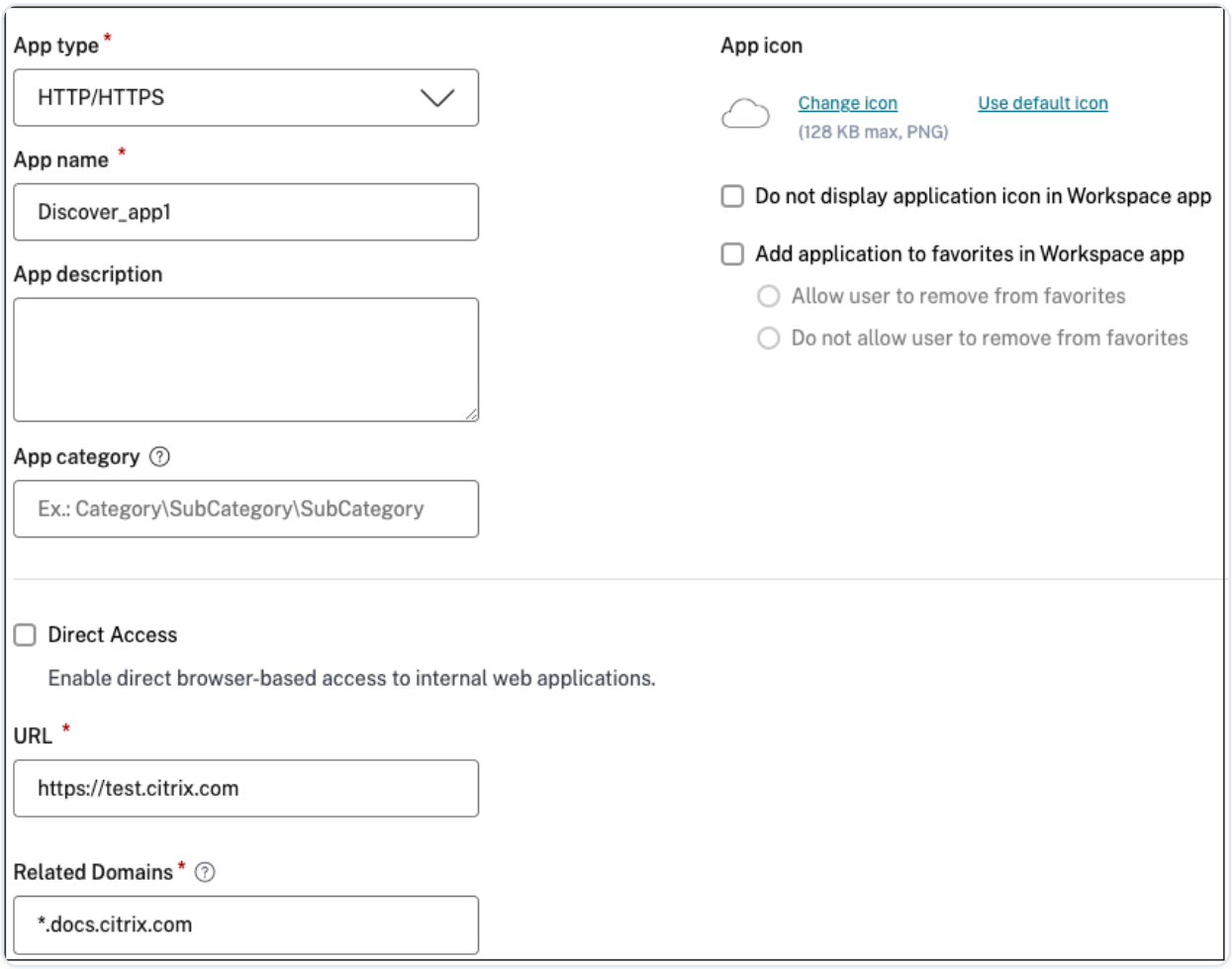
Anwendungserkennung für interne Domänen in einer neuen Umgebung

Die Funktion zur Anwendungsermittlung kann verwendet werden, wenn Sie eine neue Secure Private Access-Umgebung einrichten und Einblick in die zu konfigurierenden Anwendungen erhalten möchten. Diese Funktion ermittelt und listet alle Domänen/IP-Adressen auf, auf die Ihre Endbenutzer zugreifen, sodass Sie diese als Anwendungen konfigurieren können. Führen Sie die folgenden Schritte aus, um die Funktion zur Anwendungsermittlung zu aktivieren, wenn Sie Ihre Secure Private Access-Umgebung einrichten:

- Um interne Webanwendungen zu ermitteln, konfigurieren Sie eine Anwendung innerhalb von Secure Private Access und geben Sie die zugehörige Wildcard-Domäne an, die zur Domäne/Subdomäne der Anwendungen gehört, die Sie ermitteln möchten.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



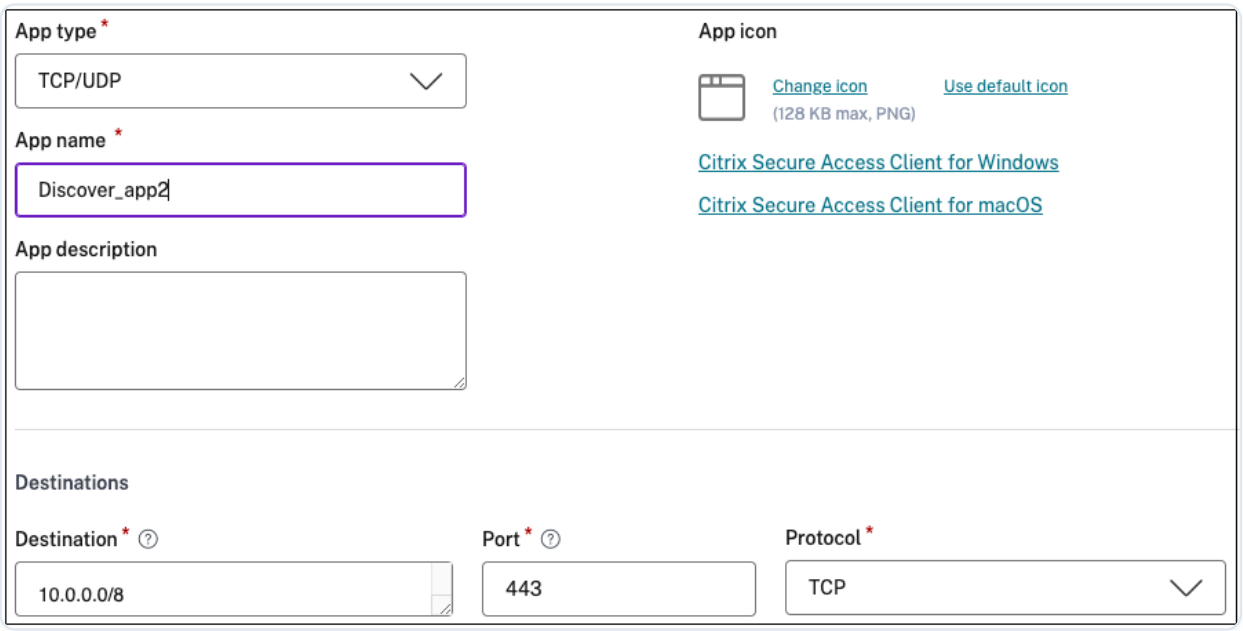
Web-App-URL: `https://test.citrix.com/` Zugehörige Domäne: `*.citrix.com`

- Für interne TCP/UDP-Apps konfigurieren Sie 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). Dies ermöglicht die Ermittlung aller TCP- und UDP-Apps vom Citrix Secure Access-Agent. Wenn Sie beispielsweise alle Anwendungen innerhalb des Subnetzes 10.0.0.0/8 ermitteln möchten, konfigurieren Sie die App mit den folgenden Details: Beispiel: 10.0.0.0/8:

  Port: (*)

  Protokoll: TCP

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Nachdem Sie die Anwendungen erstellt haben, müssen Sie auch Benutzer definieren, denen der Zugriff auf Apps mit den konfigurierten Domänen und IP-Subnetzen gestattet ist. Erstellen Sie eine Zugriffsrichtlinie und weisen Sie Benutzer zu, denen Sie Zugriff auf die in den erstellten Anwendungen konfigurierten FQDNs/IP-Adressen gewähren möchten. Dies kann ein anfänglicher Satz von Testbenutzern oder eine begrenzte Anzahl von Benutzern sein, denen Sie zunächst Zugriff gewähren möchten.
- Nachdem die Anwendungen und die entsprechenden Zugriffsrichtlinien erstellt wurden, können Benutzer weiterhin über die Citrix Workspace-App auf Anwendungen zugreifen und verschiedene Domänen aufrufen. Alle von den Endbenutzern aufgerufenen FQDN-/IP-Adressen werden auf der Seite „Anwendungsermittlung“ angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Sobald Sie die meisten Anwendungen über einige Tage/Wochen hinweg ermittelt und identifiziert haben, empfehlen wir, die ursprünglich erstellten Anwendungen zu löschen, damit der über die Wildcard-Domänen und IP-Subnetze gewährte breitere Zugriff eingeschränkt werden kann und nur bestimmten ermittelten Anwendungs-URLs und IP-Adressen über neue Anwendungen Zugriff gewährt werden muss.
- Fügen Sie das Präfix `Discover` im App-Namen hinzu, um anzuzeigen, dass dies eine spezielle App-Konfiguration zur Aktivierung der Ermittlungsüberwachung und -berichterstattung ist. Diese Benennung hilft Ihnen, die Wildcard-Domänen oder IP-Subnetze oder beides zu entfernen, sodass Sie die gesamte App-Zugriffszone später in Wochen oder einem Monat auf nur die spezifischen FQDNs und IP-/Port-Kombinationen reduzieren können.
- Um auf TCP/UDP-Apps zuzugreifen, müssen Benutzer den Citrix Secure Access-Agent verwenden. Der App-Zugriff von verschiedenen Zugriffsmethoden wird basierend auf der Konfiguration der App-Domänen und -Subnetze überwacht und auf der Seite **App-Ermittlung** gemeldet.
- Auch nachdem Sie die erkannten Anwendungen entfernt haben, erkennt diese Funktion weiterhin 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 erkannt wurden, die als Anwendungen konfiguriert werden müssen.

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

- Unterstützung für Enterprise-Webanwendungen
- Unterstützung für Software-as-a-Service-Anwendungen
- Unterstützung für Client-Server-Anwendungen

Eine Anwendung von der Seite App Discovery erstellen

Um eine Anwendung für eingebettete Domänen oder nicht veröffentlichte Domänen von der Seite **App Discovery** zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > App Discovery**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie eine Domäne aus der Liste aus. Wenn die Domäne eingebettete Domänen enthält, klicken Sie auf das erweitern-Zeichen (**>**) in der Zeile der Hauptdomäne und wählen Sie die eingebetteten Domänen aus.

   HINWEIS:

   - Sie können keine Domänen auswählen, die zu verschiedenen Protokollen gehören, um eine Anwendung zu erstellen. Eine Fehlermeldung wird angezeigt, wenn Sie Domänen auswählen, die zu verschiedenen Protokollen gehören.
   - Wenn eine Domäne bereits einer Anwendung zugeordnet ist, können Sie diese Domäne nicht erneut auswählen, um eine Anwendung zu erstellen. Das Kontrollkästchen für diese Domäne ist ausgegraut, und wenn Sie den Mauszeiger über das Kontrollkästchen bewegen, wird ein Tooltip angezeigt.
   - Sie können keine eingebetteten Domänen, die unter verschiedenen Hauptdomänen gruppiert sind, auswählen und einer Anwendung hinzufügen. Die Funktion Application Discovery erlaubt nur das Hinzufügen von eingebetteten Domänen, die unter einer einzigen Hauptdomäne gruppiert sind, zu einer App. Eine Fehlermeldung wird angezeigt, wenn eingebettete Domänen von verschiedenen Hauptdomänen ausgewählt und derselben App hinzugefügt werden.

3. Klicken Sie auf **Anwendung erstellen**. Einzelheiten zum Erstellen einer Anwendung finden Sie unter Unterstützung für Enterprise-Webanwendungen, Unterstützung für Software-as-a-Service-Anwendungen und Unterstützung für Client-Server-Anwendungen](/de-de/citrix-secure-private-access/service/spa-support-for-client-server-apps.html).

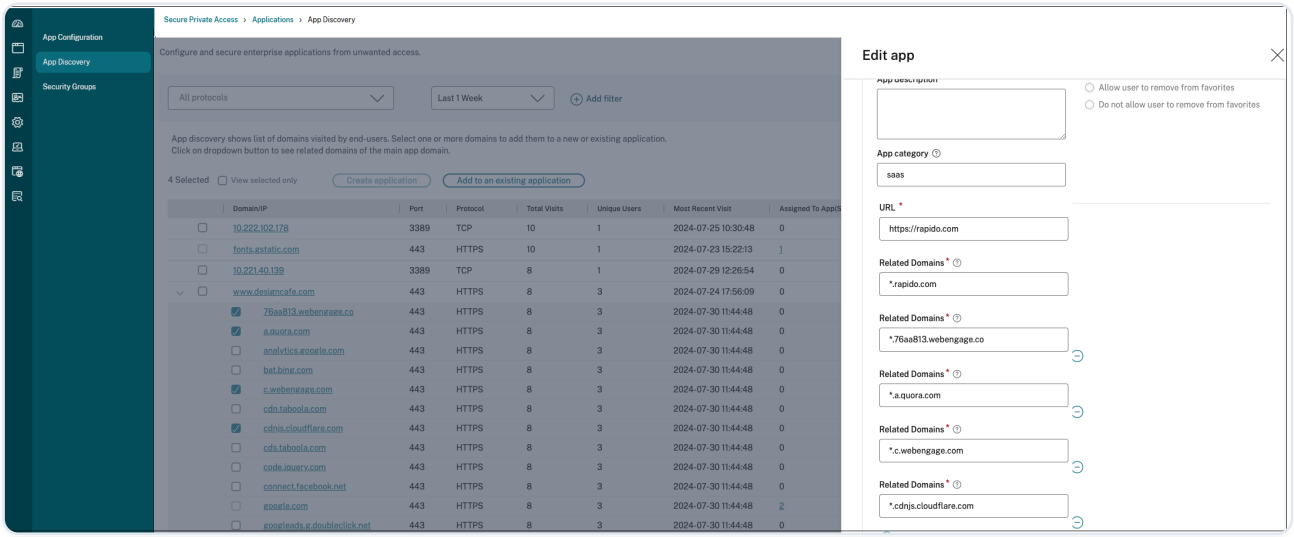
Eine vorhandene Anwendung aktualisieren

Um eine Domäne zu einer bestehenden Anwendung hinzuzufügen, wählen Sie die Domäne aus der Liste aus. Wenn die Domäne eingebettete Domänen enthält, klicken Sie auf das erweitern-Zeichen (**>**) in der Zeile 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 bestehenden Anwendung hinzufügen**.
3. Wählen Sie unter **Anwendungen** die Anwendung aus, der Sie diese Domänen hinzufügen möchten.
4. Klicken Sie auf **App-Details abrufen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Das Feld **Zugehörige Domänen** zeigt alle eingebetteten Domänen an, die Sie zuvor in separaten Zeilen ausgewählt haben.
6. Klicken Sie auf **Fertig stellen**.



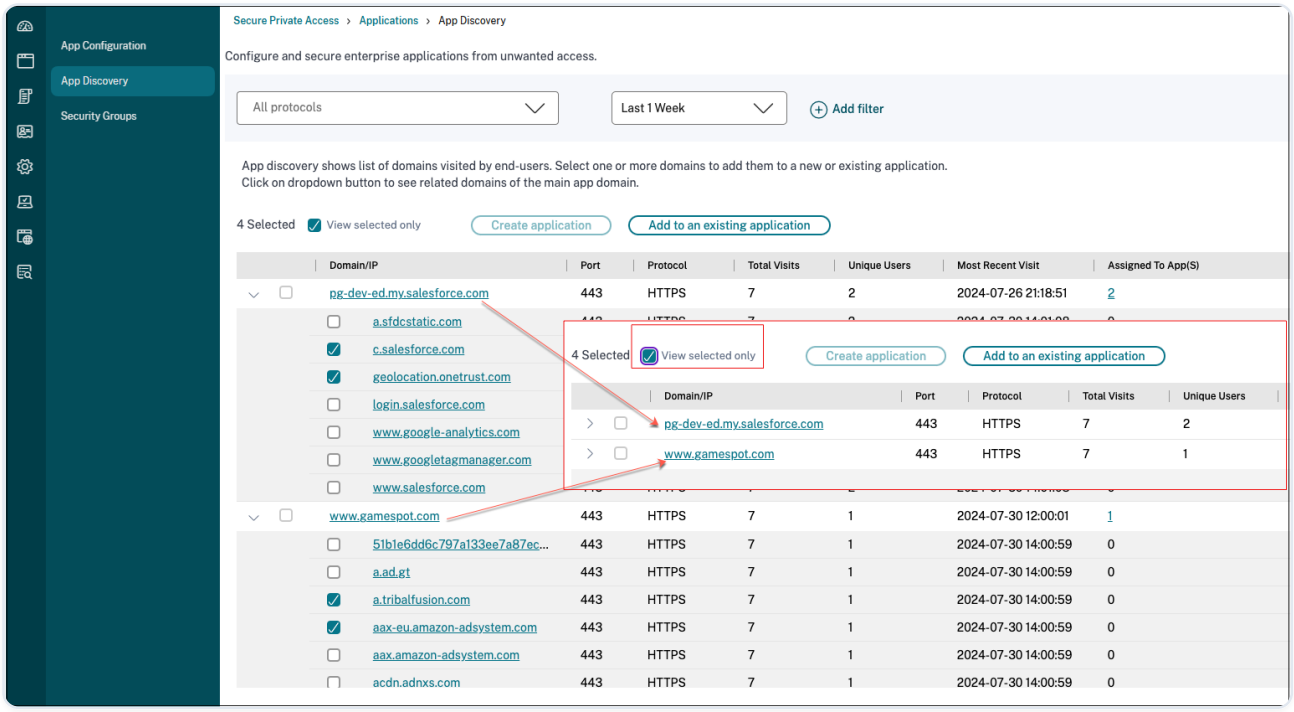
HINWEIS:

- Sie können eine TCP/UDP-Ziel-IP-Adresse nur zu einer bestehenden TCP/UDP-Anwendung hinzufügen. Das Feld Anwendungen listet nur die im System konfigurierten TCP/UDP-Apps auf.
- Sie können eine bestehende HTTP/HTTPS- oder TCP/UDP-App auswählen, um Domänen (Haupt-, Einzel- 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 die Liste der FQDN/IP-Adressen auf der Seite zur App-Erkennung mehrere Seiten umfasst, können Sie das Kontrollkästchen **Nur ausgewählte anzeigen** verwenden, um alle Haupt- und eingebetteten Domänen anzuzeigen, die Sie zum Erstellen oder Aktualisieren der Anwendung ausgewählt haben. Alle Hauptdomänen der ausgewählten eingebetteten Domänen werden angezeigt, wenn dieses Kontrollkästchen aktiviert ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Bekannte Einschränkungen

- Obwohl die Optionen **Anwendung erstellen** und **Zu bestehender Anwendung hinzufügen** im Secure Private Access-Dashboard (Diagramm **Top entdeckte Anwendungen nach Gesamtbesuchen**) verfügbar sind, wird empfohlen, eine Anwendung über die Seite **App-Erkennung** (**Anwendungen > App-Erkennung**) zu erstellen oder zu aktualisieren. Dies liegt daran, dass beim Hinzufügen oder Aktualisieren einer Anwendung über das Dashboard, wenn Sie den Vorgang abbrechen, die Seite neu geladen wird und infolgedessen alle Einstellungen zurückgesetzt werden.
- Manchmal bemerken Sie möglicherweise das erweitern-Zeichen (>) neben einer Hauptdomäne, aber die eingebetteten Domänen werden für diesen spezifischen FQDN nicht abgerufen. Dieses Problem kann in den folgenden Fällen auftreten:
  - Fehler beim Laden der Hauptwebseite aufgrund von Zugriffsbeschränkungen für die Benutzer.
  - Ein Fehler, der das Laden der Webseite verhindert.
  - Zwischenspeicherung der eingebetteten Domänenressourcen durch Citrix Enterprise Browser, wodurch die eingebetteten Domänen nicht von der Quelle abgerufen werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kontextbasiertes App-Routing und Auswahl des Ressourcenstandorts

Wenn eine App konfiguriert ist, werden die App-URL und die zugehörigen Domänen einem Routing-Typ und einem Ressourcenstandort zugewiesen. Dies geschieht während der App-Konfiguration. Diese Konfiguration für App-Routing und Ressourcenstandort gilt dann für alle Benutzer, die Zugriff auf die App haben. Es kann jedoch Szenarien wie die folgenden geben:

- Ein Administrator möchte dieselbe App für verschiedene Benutzer unterschiedlich routen. Beispielsweise muss eine interne App-URL für einige Benutzer extern geroutet werden, um zu verhindern, dass der Datenverkehr an den Secure Private Access-Dienst weitergeleitet wird.
- Es besteht die Notwendigkeit, verschiedene Ressourcenstandorte für verschiedene Benutzer zu verwenden, um Anfragen an das optimale Rechenzentrum weiterzuleiten und die Leistung zu verbessern.

Dies kann nun innerhalb der Zugriffsrichtlinien mithilfe von Routing-Ausnahmen erfolgen. Die Konfiguration der Routing-Ausnahmen in der Zugriffsrichtlinie ermöglicht es Administratoren, den internen Routing-Typ pro URL oder Ressourcenstandort basierend auf dem Benutzerkontext zu bearbeiten. Da diese Einstellung innerhalb der Zugriffsrichtlinien liegt, gilt sie nur für die Benutzer, die Teil dieser Zugriffsrichtlinie sind.

Sie können auch ganze Sitzungen dynamisch über **Sitzungsrichtlinien** routen. Weitere Informationen finden Sie unter Interne Unternehmensbenutzer direkt zu Backend-Anwendungen routen.

HINWEIS:

Wenn eine Routing- und Ressourcenstandortkonfiguration innerhalb einer Zugriffsrichtlinie vorhanden ist, überschreibt diese die App-Konfigurationen.

Die folgenden Beispiele veranschaulichen die Anwendungsfälle für Routing-Ausnahmen.

- Kontextbasiertes Routing
- Benutzerkontextbasierte Auswahl des Ressourcenstandorts
- Interne Unternehmensbenutzer direkt zu Backend-Anwendungen routen

Anwendungsfall: Kontextbasiertes Routing

Szenario:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Benutzer der Gruppe A: Mitarbeiter der Firma ABC, die über Secure Private Access auf die Outlook-App und die Microsoft Teams-App zugreifen, die intern geroutet wird.
- Benutzer der Gruppe B: Mitarbeiter eines Drittunternehmens, das mit ABC zusammenarbeitet. Sie greifen über Secure Private Access auf bestimmte Anwendungen (außer Outlook) zu. Sie verfügen auch über eine eigene Outlook-Anwendung, auf die über das Internet zugegriffen wird, und möchten ihren Outlook-Datenverkehr nicht über Secure Private Access leiten.

Problem:

- Benutzer der Gruppe B melden sich beim Secure Access Agent an, um auf ABC-Apps zuzugreifen.
- Ihre Anfragen für den Zugriff auf Outlook über ihren nativen Browser werden über Secure Private Access geleitet, was zu einer Zugriffsverweigerung führt.
- Die Zieldomäne für die Outlook-Anwendung ist für Benutzer der Gruppe A und der Gruppe B dieselbe.
- Die Zugriffsrichtlinie erlaubt den Zugriff nur für Benutzer der Gruppe A, was zu einer Zugriffsverweigerung für Benutzer der Gruppe B führt, wenn sie versuchen, Microsoft Teams oder Outlook zu starten.
- Benutzer der Gruppe B können aufgrund dieses Routing-Problems nicht auf ihr Firmen-Outlook zugreifen.

Lösung:

Der Administrator des Unternehmens ABC kann die folgenden Konfigurationsänderungen vornehmen, um dieses Problem zu beheben:

1. Definieren Sie eine neue Zugriffsrichtlinie speziell für Benutzer der Gruppe B, die auf die Office 365-App zugreifen.
2. In der Zugriffsrichtlinie aktivieren Sie die Option **Routing-Ausnahmen**.

   Der Administrator kann die Liste aller URLs und zugehörigen Domänen aller internen Apps einsehen, die mit der Zugriffsrichtlinie verknüpft sind.
3. Für alle Office365-App-URLs konfigurieren Sie das Routing so, dass es extern erfolgt.

   Dies stellt sicher, dass die Anfragen der Benutzer der Gruppe B für den Zugriff auf ihre Outlook-Anwendung über das Internet geleitet werden, wodurch Secure Private Access umgangen wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Durch die Implementierung dieser Änderungen können Benutzer der Gruppe B auf ihre Firmen-Outlook-Anwendung über das Internet zugreifen, ohne über Secure Private Access geleitet zu werden, während sie bei Bedarf weiterhin Zugriff auf andere ABC-Anwendungen haben.

Anwendungsfall: Auswahl des Ressourcenstandorts basierend auf dem Benutzerkontext

Szenarien:

- Unternehmen XYZ: Es hat zwei Benutzergruppen, die an der US-Ostküste und an der US-Westküste ansässig sind.
- Rechenzentren: Zwei Rechenzentren, eines an der Ostküste und eines an der Westküste, die beide dieselbe Jira-Anwendung hosten.
- Ziel: Der Administrator möchte die Zugriffsanfragen von Endbenutzern basierend auf dem Benutzerkontext (Geostandort, Netwerkstandort, Benutzername und Benutzergruppe) an die ausgewählten Ressourcenstandorte weiterleiten, um optimale Leistung und Routing zu gewährleisten.

Lösung:

1. Bearbeiten Sie die Zugriffsrichtlinie, die der Jira-Anwendung zugeordnet ist, um die neuen Routing-Anforderungen zu berücksichtigen.
2. Aktivieren Sie innerhalb der Zugriffsrichtlinie die Option **Routing-Ausnahmen**.
3. Ändern Sie die Ressourcenstandorte pro Benutzerkontext.

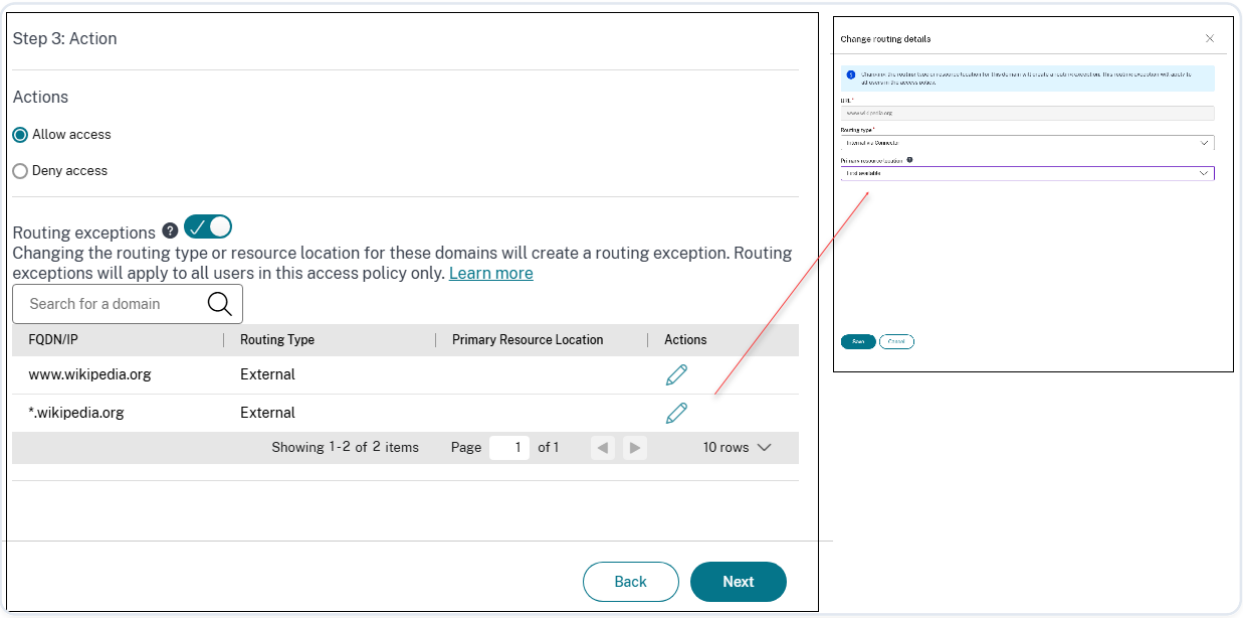
Der Administrator kann sicherstellen, dass Benutzeranfragen basierend auf ihrem Kontext an das optimale Rechenzentrum weitergeleitet werden, wodurch die Leistung verbessert und das Routing für alle Benutzer im Unternehmen effektiv verwaltet wird.

Schritte zum Ändern des Routing-Typs oder des Ressourcenstandorts

1. Erstellen oder bearbeiten Sie eine Zugriffsrichtlinie. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.
2. Aktivieren Sie auf der Seite **Schritt 3: Aktion** die Konfiguration der kontextbezogenen Routing-Domäne, indem Sie den Umschalter **Routing-Ausnahmen** betätigen. Der Umschalter **Routing-Ausnahmen** ermöglicht es Ihnen, die Ressourcenstandorte und Routing-Informationen für Domänen der in der Zugriffsrichtlinie hinzugefügten Anwendungen zu bearbeiten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Wenn der Umschalter auf EIN steht:** Eine Liste aller Anwendungs-URLs und zugehörigen Domänen wird in tabellarischer Form zusammen mit ihrer globalen Routing- und Ressourcenstandortkonfiguration angezeigt. Diese Liste enthält die URLs und zugehörigen Domänen aller in der Zugriffsrichtlinie hinzugefügten Anwendungen. Sie können auf das Bearbeitungssymbol neben einer Domäne klicken, um deren Ressourcenstandort und Routing-Typ zu ändern. Diese Routing-Ausnahme gilt nur für alle Benutzer in der Zugriffsrichtlinie.
- **Wenn der Umschalter auf AUS steht:** Bestehende Routing-Ausnahmen für die Domänen werden entfernt und sind nicht anwendbar. Endbenutzer werden nur basierend auf der globalen Konfiguration weitergeleitet, die während der Anwendungseinrichtung festgelegt wurde.



3. Klicken Sie auf das Bearbeitungssymbol neben der Domäne, für die Sie den Routingtyp ändern möchten.
4. Ändern Sie unter **Routingtyp** den Routingtyp:
   - **Intern:** Der Datenverkehr fließt über die Connector Appliance.
     - Bei einer Web-App fließt der Datenverkehr innerhalb des Rechenzentrums.
     - Bei einer SaaS-App wird der Datenverkehr außerhalb des Netzwerks über die Connector Appliance geleitet.
   - **Intern – Proxy umgehen:** Der Domänenverkehr wird über Citrix Cloud Connector™ Appliances geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
   - **Extern:** Der Datenverkehr fließt direkt ins Internet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Extern über Google Secure Gateway:** Der Datenverkehr fließt über das Google Secure Gateway ins Internet.

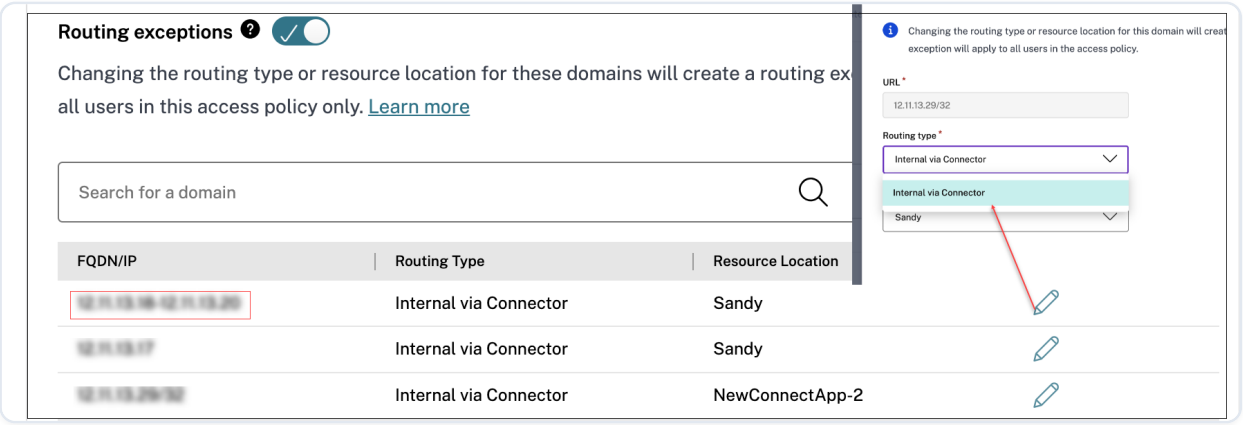
HINWEIS:

Dieser Routingtyp gilt nur für SaaS-Apps für Kunden, die in Google Chrome Enterprise Premium in Secure Private Access Cloud- und Hybridbereitstellungen integriert sind.

5. Ändern Sie unter **Ressourcenstandort** bei Bedarf den Ressourcenstandort. Diese Option gilt nur für intern geroutete Domänen.

HINWEIS:

Wenn eine App mit einer IP-Adresse erstellt wird, können Sie den Routingtyp nicht in **Extern** ändern, da in der Liste **Routingtyp** nur die Option **Intern über Connector** angezeigt wird. Sie können nur den Ressourcenstandort ändern. Diese Einschränkung gilt jedoch nicht für Apps, die mit einem FQDN erstellt wurden.



6. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Sie können nur das Routing und den Ressourcenstandort ändern, aber keine Routing-Domäne in der Routingtabelle hinzufügen oder löschen.
- Wenn Sie eine Domäne, für die kontextbezogenes Routing aktiviert ist, aus der Hauptroutingtabelle löschen, wird die Domäne nicht aus der Tabelle **Routingausnahmen** innerhalb der Zugriffsrichtlinie gelöscht. Dies bedeutet, dass die kontextbezogene Routingkonfiguration für diese Domäne in der Zugriffsrichtlinie intakt bleibt.
- Wenn Sie eine App löschen, für die kontextbezogenes Routing aktiviert ist, wird die Domäne aus der Tabelle **Routingausnahmen** innerhalb der Zugriffsrichtlinie gelöscht. Dies bedeutet, dass alle mit dieser App verbundenen kontextbezogenen Routingkonfigurationen aus der Zugriffsrichtlinie entfernt werden.
- Die ausgewählte zugehörige Domäne überschreibt die Standardeinstellung, wenn die Bedingung für die Benutzer erfüllt ist, die Teil dieser Zugriffsrichtlinie sind. Andernfalls wird das Standard-Routing angewendet.
- Wenn das Routing nicht geändert wird oder wenn die Funktion **Routingausnahmen** nicht aktiviert ist, erfolgt das Routing basierend auf den Standardeinstellungen in der Hauptroutingtabelle (**Einstellungen > Anwendungsdomäne**).

Anwendungsfall: Interne Unternehmensbenutzer direkt zu Back-End-Anwendungen leiten

Administratoren können Sitzungsrichtlinien konfigurieren, um interne Unternehmensbenutzer direkt zu Back-End-Apps zu leiten, ohne den Datenverkehr über Secure Private Access zu tunneln. Sitzungsrichtlinien bieten dynamisches Routing basierend auf Faktoren wie Netwerkstandort und Gerätestatus. Weitere Informationen finden Sie unter Sitzungsrichtlinien.

Einblicke in das kontextbezogene Routing in Monitor

Kontextbezogenes Routing kann zu dynamischen Änderungen der Anwendungsrouten führen. Beispielsweise kann eine Anwendung über den Secure Private Access-Dienst geleitet werden, wenn sich der Benutzer außerhalb des Unternehmensnetzwerks befindet, aber direkt zur App, wenn der Benutzer intern ist. Administratoren Einblick in diese Routing-Entscheidungen zu geben, ist entscheidend für die Fehlerbehebung bei Routing-Problemen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Seite **Anwendungstopologie** in DaaS Monitor bietet umfassende Einblicke in Routing-Entscheidungen und Richtliniendetails der Secure Private Access-Anwendungen, auf die über den Citrix Secure Access-Client zugegriffen wird. Diese Einblicke ermöglichen es den Administratoren, Routing-Probleme effizient zu beheben und so die Benutzererfahrung zu verbessern.

Die folgenden Details zum Anwendungsrouting werden auf der Seite **Anwendungstopologie** erfasst:

- **Routingkontext:** Das Feld **Routingkontext** im Abschnitt **Info** gibt den Richtlinientyp (Zugriffsrichtlinie, Sitzungsrichtlinie oder Anwendungsdomäne) an, der während des Routings angewendet wird. Der Routingkontext hilft, die Präzedenzhierarchie (Zugriffsrichtlinie > Sitzungsrichtlinie > Standardanwendungskonfiguration) zu identifizieren, die Routing-Entscheidungen beeinflusst.

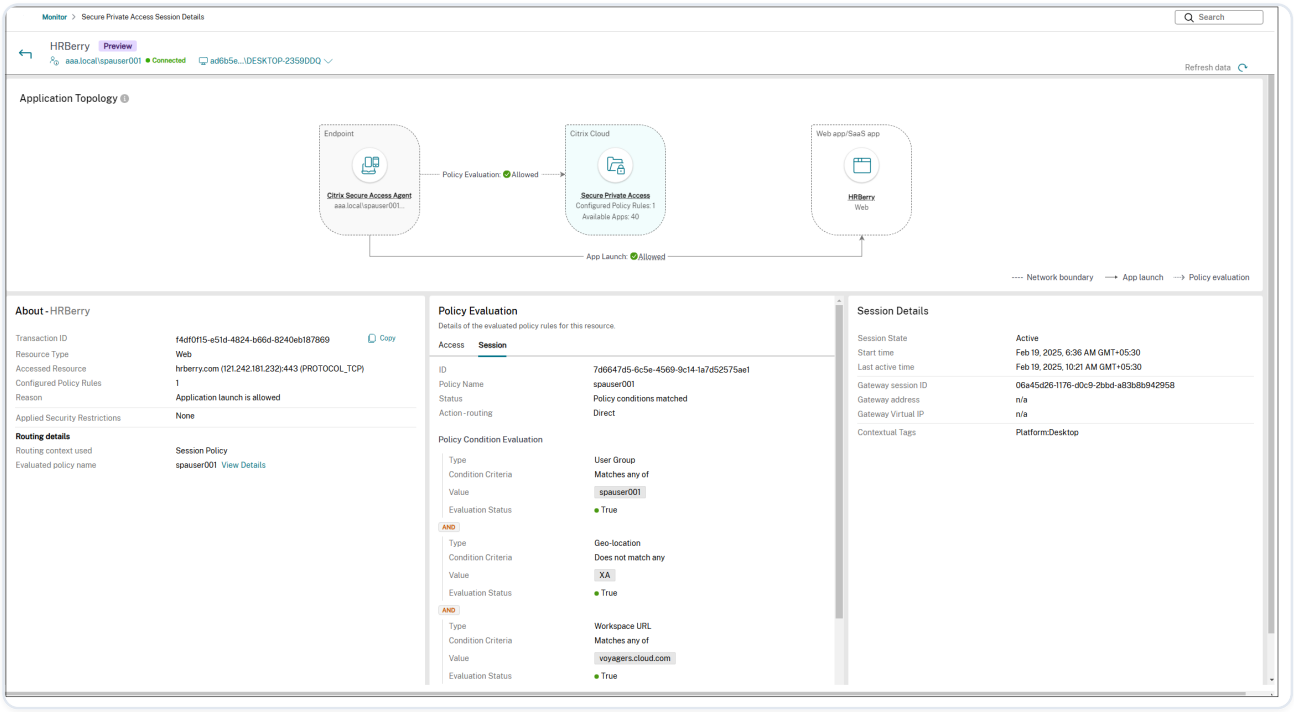
  Für die Sitzungsrichtlinie bietet der Link **Details anzeigen** zusätzliche Informationen zur Sitzungsrichtlinie.
- **Action-routing:** Das Feld **Action-routing** im Abschnitt **Policy Evaluation** zeigt den Routingpfad (**Direkt, Intern über Connector, Intern über Gateway**) an, den die Anforderung eines Benutzers über den Secure Private Access-Dienst nimmt.

HINWEIS:

Wenn das Standard-Anwendungsdomänen-Routing (Anwendungskonfiguration) angewendet wird, zeigt der Abschnitt **Policy Evaluation** die Richtliniendetails an, aber das Feld **Action-routing** zeigt den Wert **n/a** an, da in diesem Szenario keine Richtlinie erzwungen wird.

Die folgende Abbildung zeigt ein Topologiediagramm einer Anwendung, deren Routingtyp als direkt definiert ist und der Datenverkehr daher nicht über den Secure Private Access-Dienst geleitet wird.

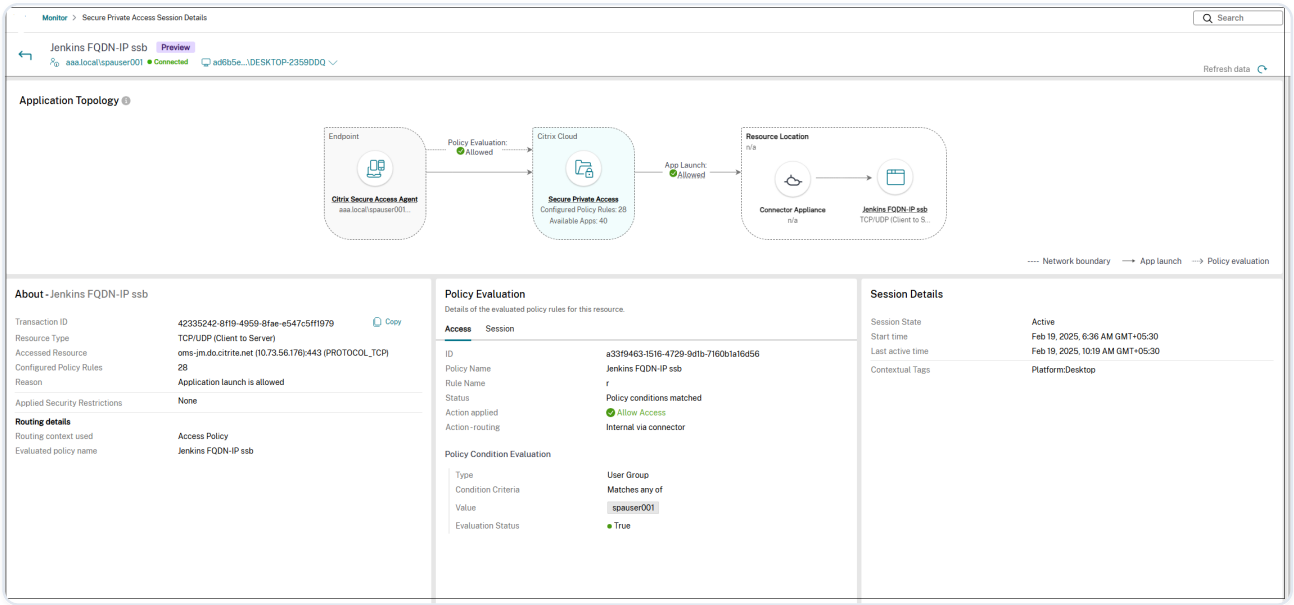
© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Für die Web-Apps, die über den Citrix Secure Access-Client getunnelt werden, zeigt das Topologiediagramm den Namen des Ressourcenstandorts und den Namen des Connectors an.

Die folgende Abbildung zeigt ein Topologiediagramm einer Anwendung, deren Routingtyp als intern über den Secure Private Access-Dienst unter Verwendung eines Connectors definiert ist.



Weitere Informationen finden Sie unter Integration mit DaaS Monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nahtloser Zugriff auf lokale LAN-Ressourcen (Drucker, Dateiserver)

Wenn Mitarbeiter über Secure Private Access von zu Hause oder von Remote-Standorten aus mit Citrix Secure Access Clients verbunden sind, können sie den Zugriff auf lokale Netzwerkressourcen verlieren, wenn der private IP-Adressbereich mit veröffentlichten Unternehmensanwendungen in Konflikt steht. Secure Private Access unterstützt den nahtlosen Zugriff auf lokale LAN-Ressourcen, während eine sichere Verbindung zu Unternehmensressourcen aufrechterhalten wird.

Wenn beispielsweise ein Heimdrucker mit der IP-Adresse 192.0.2.0 konfiguriert ist und Unternehmensanwendungen mit dem privaten IP-Adressbereich 192.0.2.0/30 konfiguriert sind, wird der Druckerdatenverkehr, wenn ein Benutzer versucht, auf den Drucker zuzugreifen, ebenfalls über SPA getunnelt, was zu einem Fehler führt. Durch die Aktivierung des lokalen LAN-Zugriffs kann der Benutzer Drucker über das lokale LAN erreichen, ohne den Citrix Secure Access Client zu trennen.

HINWEIS:

- Administratoren können die Funktion für den lokalen LAN-Zugriff in Sitzungsrichtlinien für alle Benutzer oder eine Gruppe von Benutzern aktivieren. Weitere Informationen finden Sie unter Direktes Routing innerhalb des Unternehmensnetzwerks mithilfe von Sitzungsrichtlinien konfigurieren.
- Wenn Benutzer die Funktion für den lokalen LAN-Zugriff aktivieren, wenn sie sich beim Citrix Secure Access Client anmelden, können sie auf lokale LAN-Ressourcen wie Heimdrucker und Network Attached Storage (NAS)-Geräte zugreifen, während sie mit Secure Private Access verbunden sind. Dies hilft dem Benutzer, grundlegende lokale Aufgaben mit minimaler Unterbrechung auszuführen.

Wichtige Überlegungen

- **Aktivieren des lokalen LAN-Zugriffs für alle Benutzer:** Sitzungsrichtlinien werden in der Reihenfolge ihrer Priorität ausgewertet. Wenn der lokale LAN-Zugriff für alle Benutzer erforderlich ist, muss die Option **Lokaler LAN-Zugriff** in jeder aktiven Sitzungsrichtlinie explizit aktiviert werden. Wenn ein Benutzer einer Sitzungsrichtlinie entspricht, stoppt die Auswertung bei der ersten anwendbaren Richtlinie. Wenn diese Richtlinie keinen lokalen LAN-Zugriff zulässt, wird der Benutzer nicht anhand anderer nachfolgender Richtlinien ausgewertet, selbst wenn diese Richtlinien die Option **Lokaler LAN-Zugriff** aktiviert haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

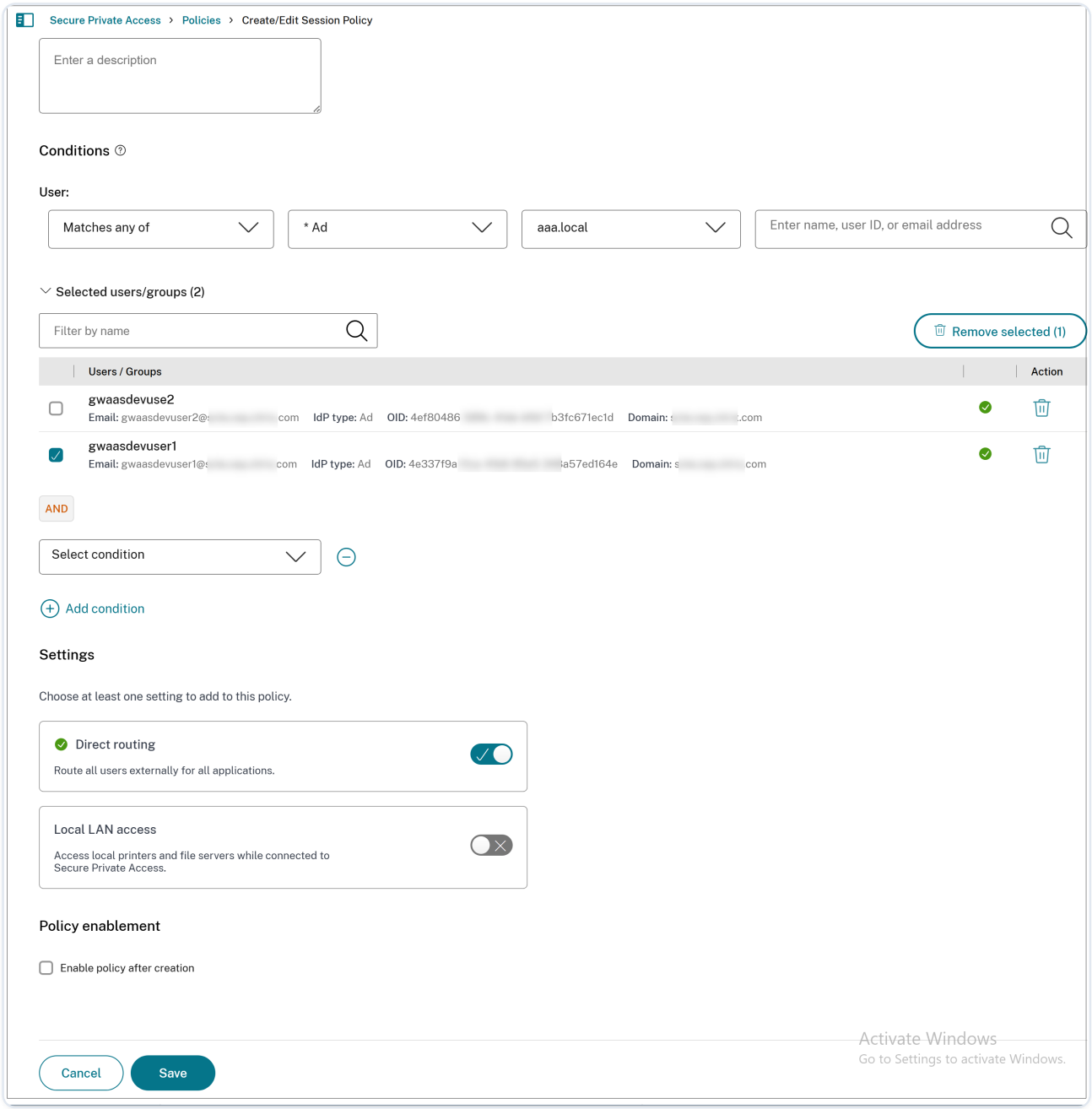
- **Unterschiede bei der Verarbeitung des Druckerdatenverkehrs durch den Citrix Secure Access Client für Windows und macOS:** Citrix Secure Access für Windows priorisiert den lokalen LAN-Zugriff. Das heißt, wenn die IP-Adresse eines Druckers mit der einer Unternehmensanwendung in Konflikt steht, sendet der Citrix Secure Access Client für Windows den Anwendungsdatenverkehr möglicherweise lokal, anstatt ihn über Secure Private Access zu senden. Im Gegensatz dazu kann der Citrix Secure Access Client für macOS den Druckerdatenverkehr an das lokale LAN senden, während gleichzeitig der Anwendungsdatenverkehr über Secure Private Access getunnelt wird.
- **Regelmäßige Aktualisierung:** Da die Funktion für den lokalen LAN-Zugriff sitzungsspezifisch ist, werden alle Konfigurationsänderungen an der lokalen LAN-Einstellung im Windows-Filter (WFP) bei der Anmeldung wirksam und bleiben bis zur Abmeldung erhalten. Eine regelmäßige Aktualisierung wird nicht unterstützt.

Funktion für den lokalen LAN-Zugriff aktivieren

Secure Private Access-Administratorkonsole:

1. Navigieren Sie zu **Richtlinien > Sitzungsrichtlinien** und klicken Sie auf Sitzungsrichtlinie erstellen.
2. Erstellen Sie eine Sitzungsrichtlinie. Weitere Informationen finden Sie unter Direktes Routing innerhalb des Unternehmensnetzwerks mithilfe von Sitzungsrichtlinien konfigurieren.
3. Stellen Sie sicher, dass Sie die Option **Lokaler LAN-Zugriff** auswählen.

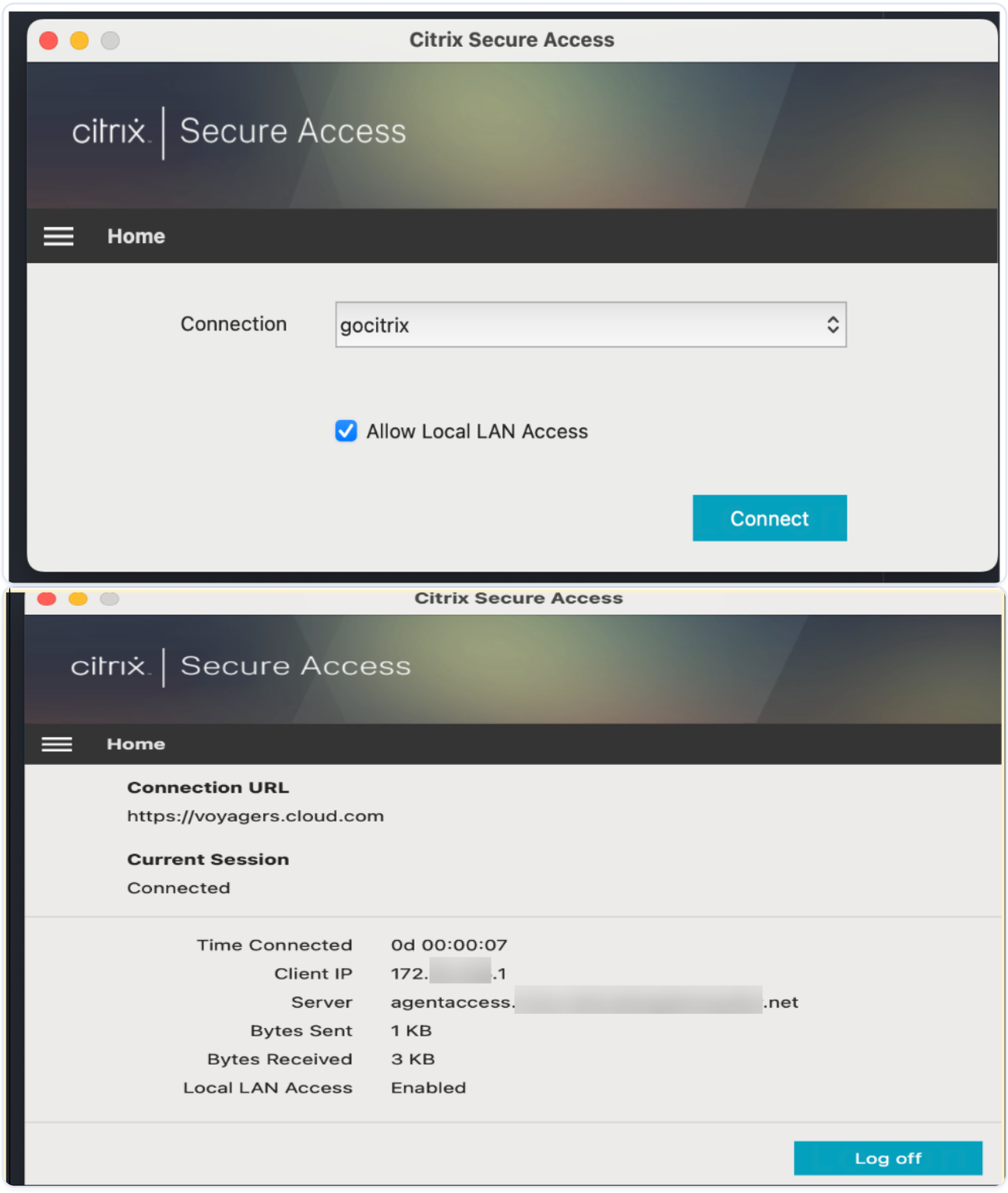
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Secure Access Client:

1. Im Fenster des Citrix Secure Access Clients wählen Sie **Lokalen LAN-Zugriff zulassen**.
2. Klicken Sie auf **Verbinden**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Richtlinienmodellierungstool

Beim Verwalten mehrerer Anwendungen und Zugriffsrichtlinien kann es für Administratoren schwierig sein, das genaue Zugriffsergebnis für Endbenutzer zu bestimmen. Dies betrifft, ob einem Benutzer der Zugriff auf eine Anwendung basierend auf allen aktuellen Konfigurationen erlaubt oder verweigert wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das Richtlinienmodellierungstool, das sich unter **Zugriffsrichtlinien > Richtlinienmodellierung** befindet, bietet Administratoren umfassende Transparenz über die erwarteten App-Zugriffsergebnisse (zugelassen, zugelassen mit Einschränkung oder verweigert) basierend auf den aktuellen Konfigurationen. Administratoren können die Zugriffsergebnisse für jeden Benutzer basierend auf Bedingungen wie Gerätetyp, Gerätestatus, Geo-Standort, Netwerkstandort und Store-URL überprüfen. Administratoren können auch die Zugriffsrichtlinien für bestimmte Anwendungsziele bewerten.

Zugriff auf das Richtlinienmodellierungstool

1. Klicken Sie in der Secure Private Access-Konsole auf **Zugriffsrichtlinien** und dann auf die Registerkarte **Richtlinienmodellierung**.
2. Die Benutzeroberfläche des Richtlinienmodellierungstools wird angezeigt.

    - Die Registerkarte **Alle Apps** ist standardmäßig ausgewählt. Diese Registerkarte kann zur Analyse von Richtlinien verwendet werden, die für mehrere Benutzer, Benutzergruppen oder Maschinen innerhalb der Umgebung gelten.
    - Um zu verstehen, wie Richtlinien für bestimmte Netzwerkziele durchgesetzt werden, wie z. B. eine bestimmte Website-Domain, eine IP-Adresse oder einen Netzwerkport, müssen Sie die Registerkarten **URL** oder **IP/Port** verwenden und die Zieldetails eingeben.

Richtlinien für eine Gruppe von Benutzern oder Maschinen analysieren

1. Wählen Sie die Registerkarte **Benutzer** oder **Maschinen** aus und geben Sie die folgenden Details ein.

    - **Gerätetyp:** Wählen Sie den Gerätetyp des Endbenutzers aus. (Desktop ist standardmäßig ausgewählt).
    - **Domäne:** Wählen Sie die dem Benutzer zugeordnete Domäne aus.
    - **Benutzername oder Benutzergruppe:** (Nur anwendbar, wenn Sie die Registerkarte **Benutzer** ausgewählt haben) Wählen Sie den Benutzernamen aus, für den Sie die Anwendungen und zugehörigen Richtlinien analysieren möchten.
    - **Maschinenname:** (Nur anwendbar, wenn Sie die Registerkarte **Maschinen** ausgewählt haben) Geben Sie den Maschinennamen ein, auf dessen Grundlage Sie die Anwendungen und zugehörigen Richtlinien analysieren möchten.

2. Um genaue Ergebnisse zu erhalten, fügen Sie die genauen Benutzer- oder Maschinenbedingungen hinzu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Klicken Sie auf **Bedingungen simulieren.**
- Wählen Sie die Bedingung (Gerätehaltung, Geo-Standort, Netwerkstandort, Benutzer-Risikobewertung und Store-URL) und anschließend den zugehörigen Wert aus.
- Klicken Sie auf das +-Zeichen, um weitere Bedingungen hinzuzufügen.
- Klicken Sie auf **Anwenden.**

Richtlinien für bestimmte Ziele analysieren

1. Klicken Sie auf die Registerkarte **URL** für Web-/SaaS-Anwendungen und auf die Registerkarte **IP/Port** für TCP/UDP-Anwendungen.
2. Geben Sie die folgenden Details ein:

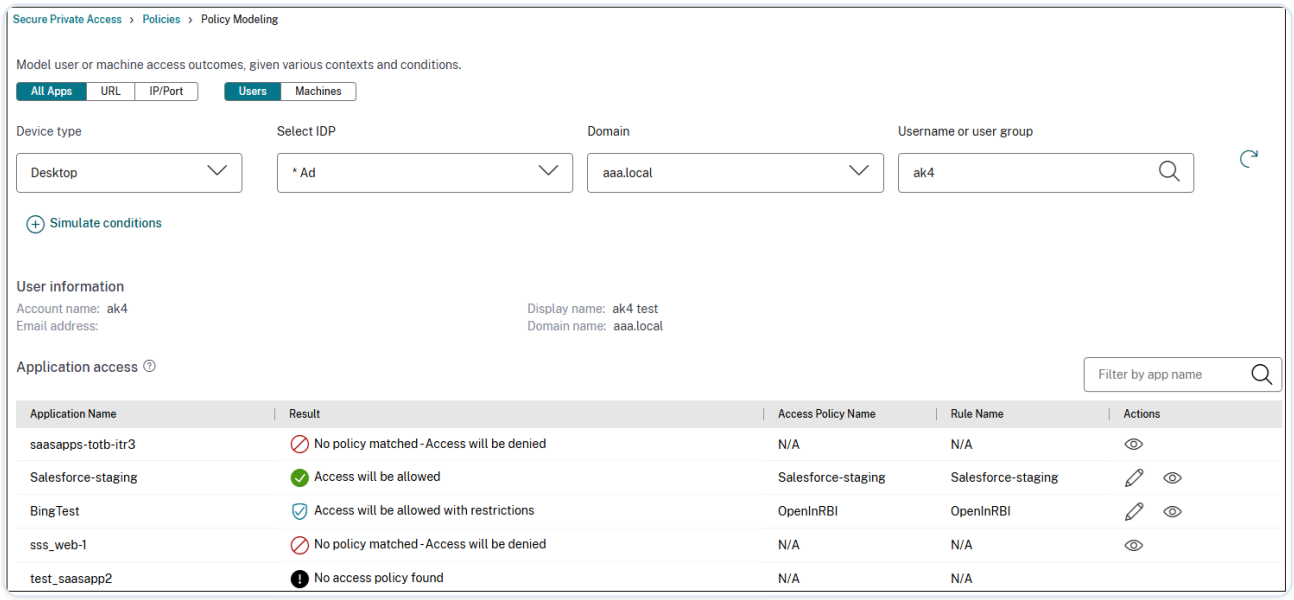
   - **URL:** Die URL der Anwendung, für die Sie die Zugriffsrichtlinien analysieren möchten.
   - **IP:Port:** Die IP-Adresse und Portnummer der TCP/UDP-App, für die Sie die Zugriffsrichtlinie analysieren möchten. Sie können auch den Hostnamen gefolgt von der Portnummer eingeben.

   Beispiele: 192.0.2.20:443; example.test.net:443
3. Klicken Sie auf **Anwenden.**

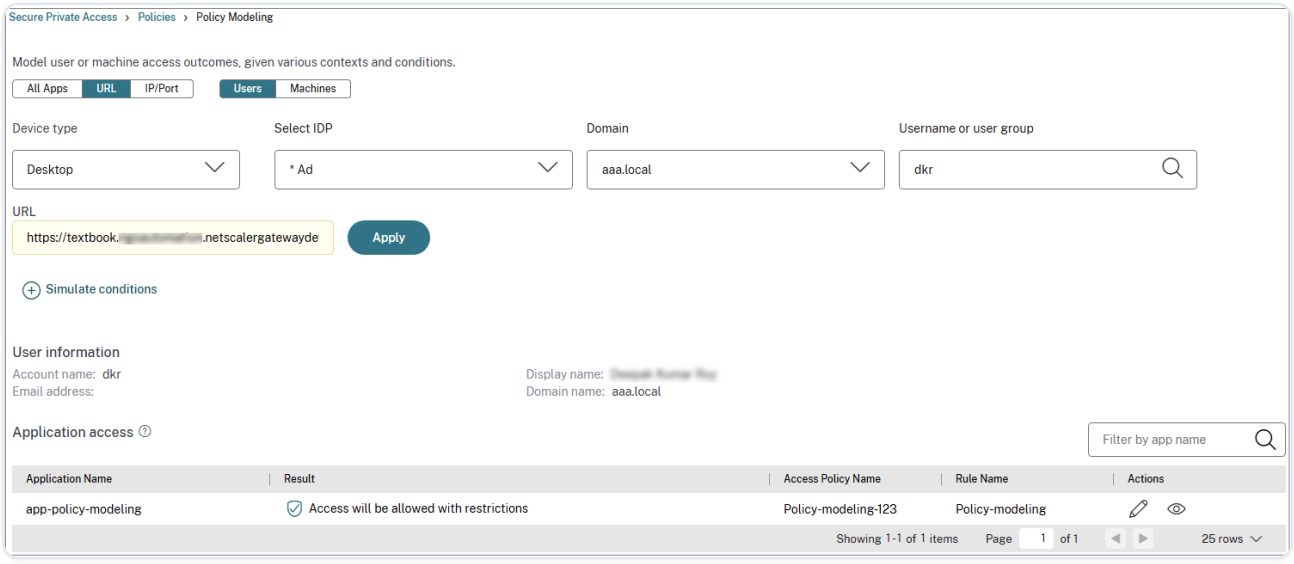
Der Abschnitt **Anwendungszugriff** zeigt die Liste der Anwendungen und die zugehörigen Richtlinien basierend auf Ihrer Suche an. Neben der Anwendung, für die eine exakte Richtlinienübereinstimmung oder keine Richtlinienübereinstimmung aufgetreten ist, wird ein Augensymbol angezeigt. Die Administratoren können auch eine Richtlinie für die Apps bearbeiten, für die der Zugriff erlaubt oder der Zugriff mit Einschränkung erlaubt ist.

Die folgende Abbildung zeigt den Richtlinienanalysator für alle Apps:

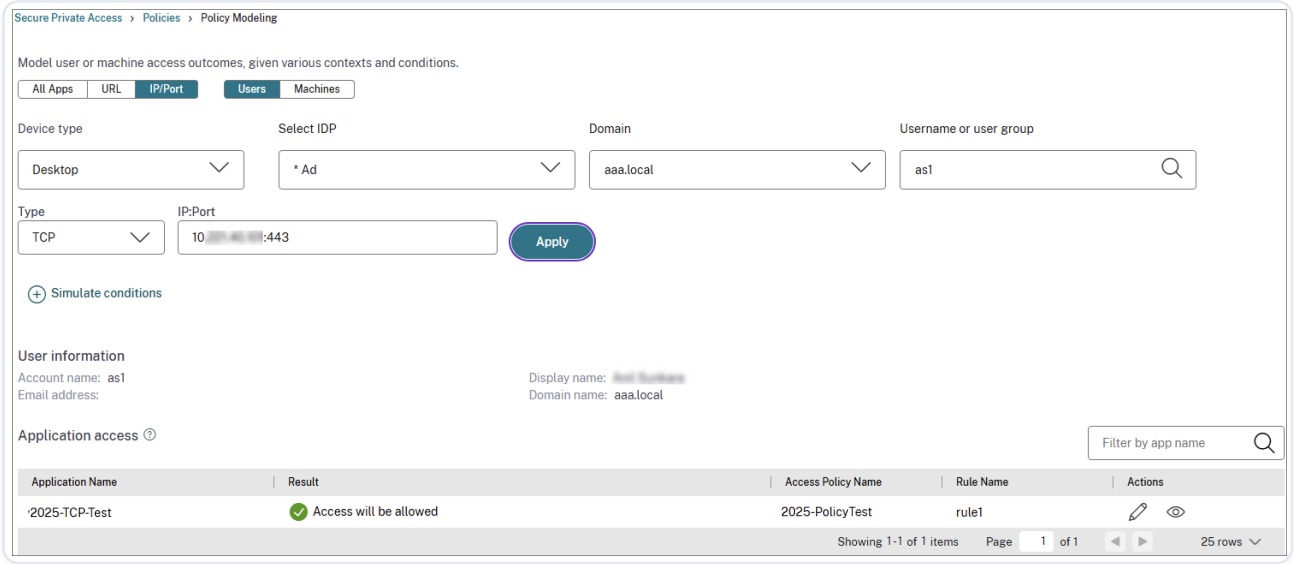
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Die folgende Abbildung zeigt den Richtlinienanalysator für eine Web-App:



Die folgende Abbildung zeigt den Richtlinienanalysator für eine TCP-App:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zugriffsrichtlinien detailliert anzeigen

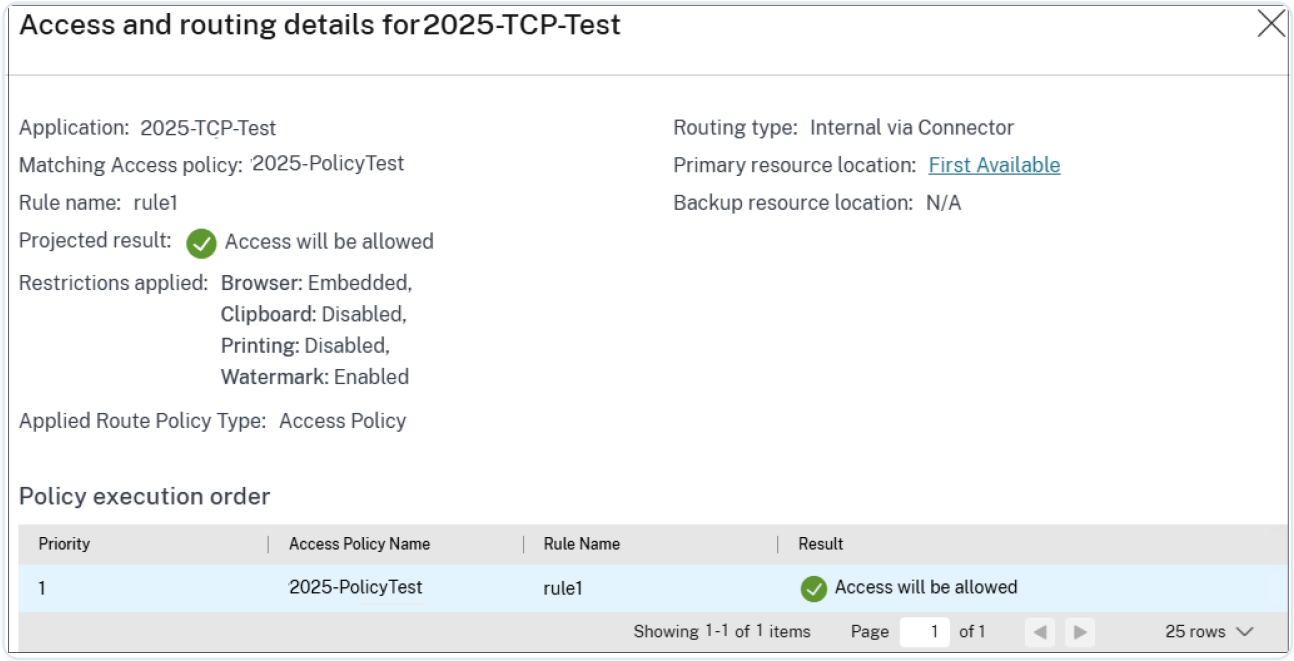
Klicken Sie im Abschnitt **Anwendungszugriff** auf das Augensymbol, um die Seite mit den Zugriffs- und Routingdetails anzuzeigen. Die Seite **Zugriffs- und Routingdetails** zeigt eine umfassende Liste aller relevanten Richtlinien an, die die Zugriffsentscheidungen für diese Anwendung beeinflusst haben. Diese Seite zeigt die folgenden Informationen an:

FELD	BESCHREIBUNG
Anwendung	Name der Anwendung.
Übereinstimmende Zugriffsrichtlinie	Der Name der Zugriffsrichtlinie, die eine exakte Übereinstimmung oder eine Hauptübereinstimmung mit der Anwendung aufweist.
Regelname	Die spezifische Regel, die der übereinstimmenden Richtlinie zugeordnet ist.
Prognostiziertes Ergebnis	Die Aktion, die basierend auf der Richtlinienauswertung bestimmt wurde (z. B. zulassen, verweigern, mit Einschränkung zulassen).
Angewendete Einschränkungen	Zugriffsbeschränkungen, falls vorhanden, die für die Anwendung erzwungen werden.
Angewendeter Routenrichtlinientyp	Gibt den Richtlinientyp an, der das Routingverhalten der Anwendungen bestimmt hat. Der Richtlinientyp ist Zugriffsrichtlinie, Sitzungsrichtlinie oder Anwendungsdomäne.
	Identifiziert die Hierarchie bei Routing-Entscheidungen. Die Rangfolge ist Zugriffsrichtlinie (höchste Priorität), gefolgt von Sitzungsrichtlinie und dann der Standard-Anwendungsdomäne (niedrigste Priorität).
Routing-Typ	Der Routing-Typ beschreibt den Pfad, den die Anfrage eines Benutzers durch den Secure Private Access-Dienst nimmt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

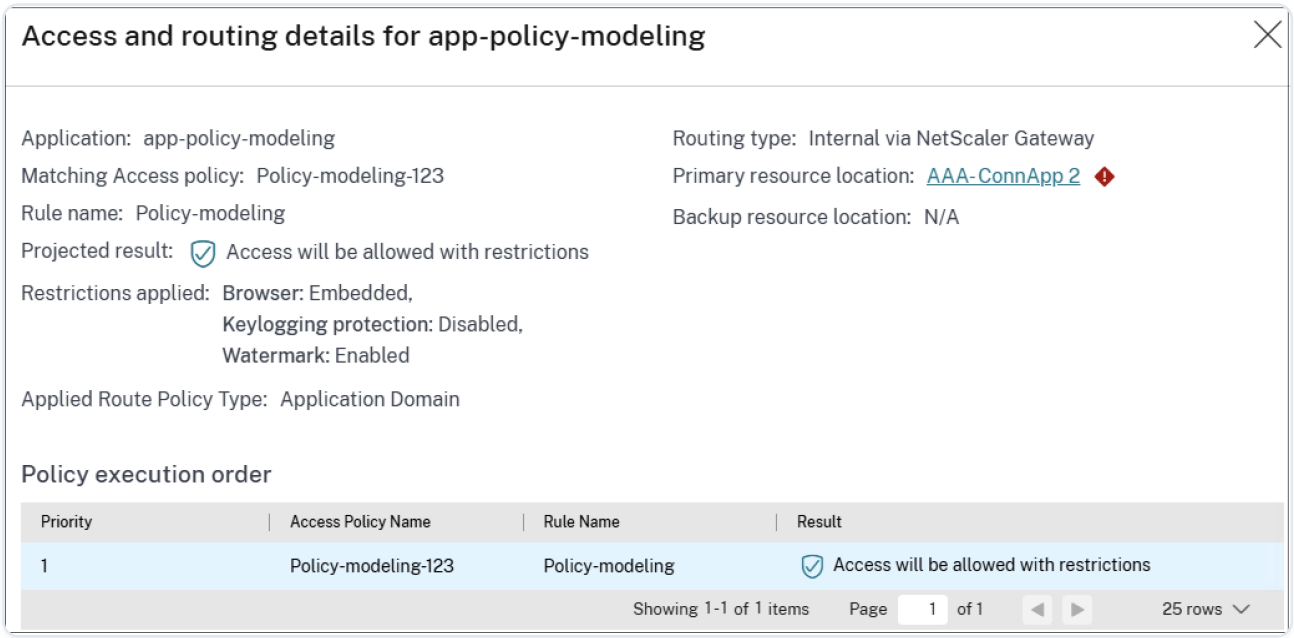
FELD	BESCHREIBUNG
	Extern Anfragen werden direkt an das beabsichtigte Ziel weitergeleitet.
	Intern über Connector Anfragen werden über einen Connector weitergeleitet.
	Intern über Gateway Anfragen werden über NetScaler Gateway weitergeleitet. Dieser Routing-Typ ist nur für hybride Datenpfade anwendbar, die mit dem Citrix Secure Access Client unterstützt werden. Einzelheiten finden Sie unter Hybrider Datenpfad für Secure Private Access-Dienste.
Primärer Ressourcenstandort	Name, der dem primären Standort der Anwendung zugeordnet ist.
Backup-Ressourcenstandort	Name des Sicherungsstandorts (falls konfiguriert).

Die folgende Abbildung zeigt die Ergebnisse des Policy-Drilldowns für eine TCP-Anwendung, für die der Zugriff erlaubt ist.

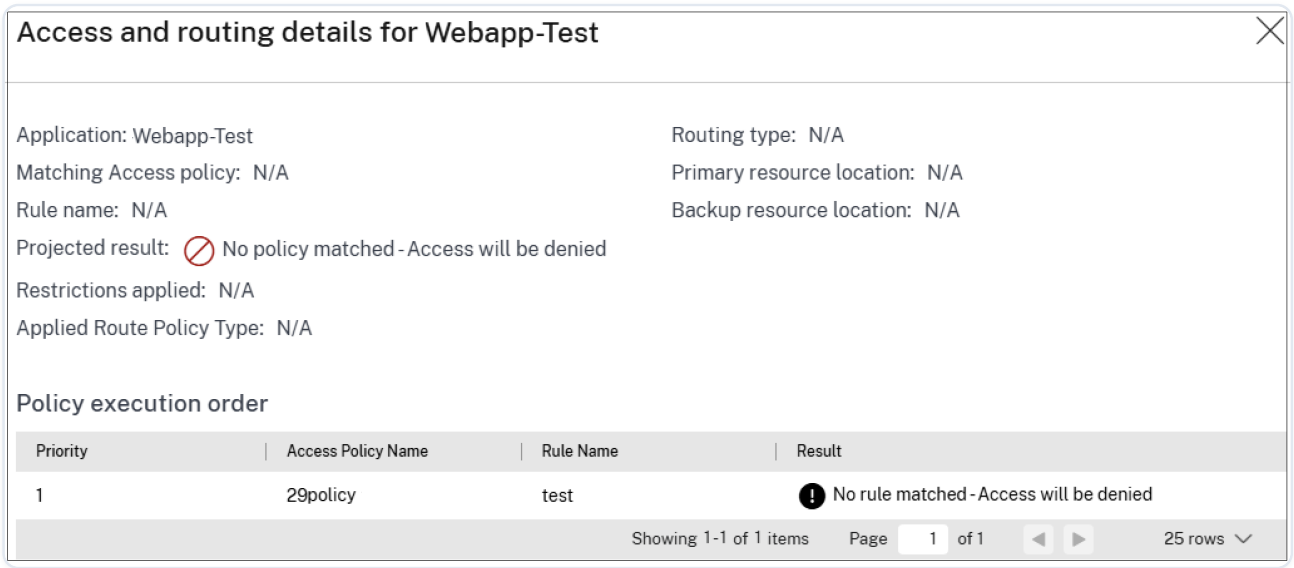


Die folgende Abbildung zeigt die Ergebnisse des Policy-Drilldowns für eine Webanwendung, für die der Zugriff mit Einschränkungen erlaubt ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Die folgende Abbildung zeigt die Ergebnisse des Policy-Drilldowns für eine Webanwendung, für die der Zugriff verweigert wird:



Anwendungen Import-Tool – Vorschau

The Secure Private Access admin console includes a file import tool that allows administrators to bulk import multiple applications into the system using a CSV file or the nsconfig file. This tool is especially useful for organizations shifting from a traditional VPN to a more advanced solution like Secure Private Access. For example, organizations can use this tool to migrate applications that were delivered over a VPN to Secure Private Access and shift to a ZTNA-based architecture. Bulk upload of apps enables the organizations to eliminate the need for manual configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **CSV-Datei:** Sie müssen sicherstellen, dass alle relevanten Anwendungsdetails in der CSV-Datei enthalten sind. Diese Details umfassen den Anwendungsnamen, den Routing-Typ, den Ressourcenstandort und alle anderen erforderlichen Konfigurationsparameter.
- **NetScaler-Dateien:** Sie können Anwendungen auch mithilfe einer vorab generierten CSV-Datei importieren. Diese CSV-Datei wird von einem Skript erstellt, das relevante Anwendungskonfigurationen aus den ns.conf- und ns.log-Dateien analysiert und extrahiert. Die vom Skript generierte CSV ermöglicht den effizienten und genauen Import von Anwendungskonfigurationen in die Citrix Secure Private Access-Konsole.

So funktioniert der Import

Hier sind die übergeordneten Schritte, die ein Administrator bei der Verwendung des CSV-basierten Anwendungsimport-Tools ausführen muss:

1. **CSV-Datei vorbereiten:** Wenn Sie die Apps manuell hinzufügen, füllen Sie die Anwendungsdetails in der CSV-Datei aus. Weitere Informationen finden Sie unter Vorbereiten der CSV-Datei.
2. **CSV-Datei importieren:** Importieren Sie die ausgefüllte CSV-Datei in die Secure Private Access-Konsole.
3. **App-Details überprüfen:** Überprüfen und validieren Sie die importierten Anwendungsdaten.
4. **Routing und Ressourcenstandort aktualisieren:** Überprüfen und aktualisieren Sie bei Bedarf den Routing-Typ und die Details des Ressourcenstandorts. Stellen Sie sicher, dass mindestens ein Connector am angegebenen Ressourcenstandort aktiv ist.
5. **Anwendungen auf der Seite „Anwendungen“ anzeigen:** Zeigen Sie die importierten Anwendungen auf der Seite „Anwendungen“ an. Überprüfen Sie, ob alle Anwendungen, die Sie für den Import ausgewählt haben, erfolgreich importiert wurden.

Dieser strukturierte Prozess gewährleistet eine gründliche Migration und ordnungsgemäße Konfiguration von Anwendungen für einen sicheren und nahtlosen Zugriff innerhalb der Secure Private Access-Umgebung.

Vorbereiten der CSV-Datei

Laden Sie die CSV-Datei von der Secure Private Access-Konsole herunter und fügen Sie die Anwendungsdetails hinzu.

1. Navigieren Sie zu **Anwendungen > App-Konfiguration**.
2. Klicken Sie auf **Anwendungen importieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie unter **Erfahren Sie, wie Sie mit CSV- und NetScaler-Dateien importieren**, auf **CSV** oder **NetScaler**.

   Die Seite **Importieren mit CSV** oder **Importieren mit NetScaler-Dateien** wird entsprechend angezeigt.

   - **CSV** – Laden Sie die CSV-Datei (CSV-Vorlage) herunter und füllen Sie die App-Details aus. Die Seite zeigt auch Beispielinformationen zu den einzugebenden App-Daten an.
   - **NetScaler**
     - Laden Sie das Python-Skript herunter und speichern Sie es im dafür vorgesehenen Ordner (/var/spa/scripts) in NetScaler.
     - Führen Sie das Skript als `python3 ztna-migration.py` aus, um eine CSV-Datei aus den Dateien ns.conf und ns.log zu generieren.
     - Sobald die CSV-Datei generiert wurde, laden Sie sie zum Import hoch.

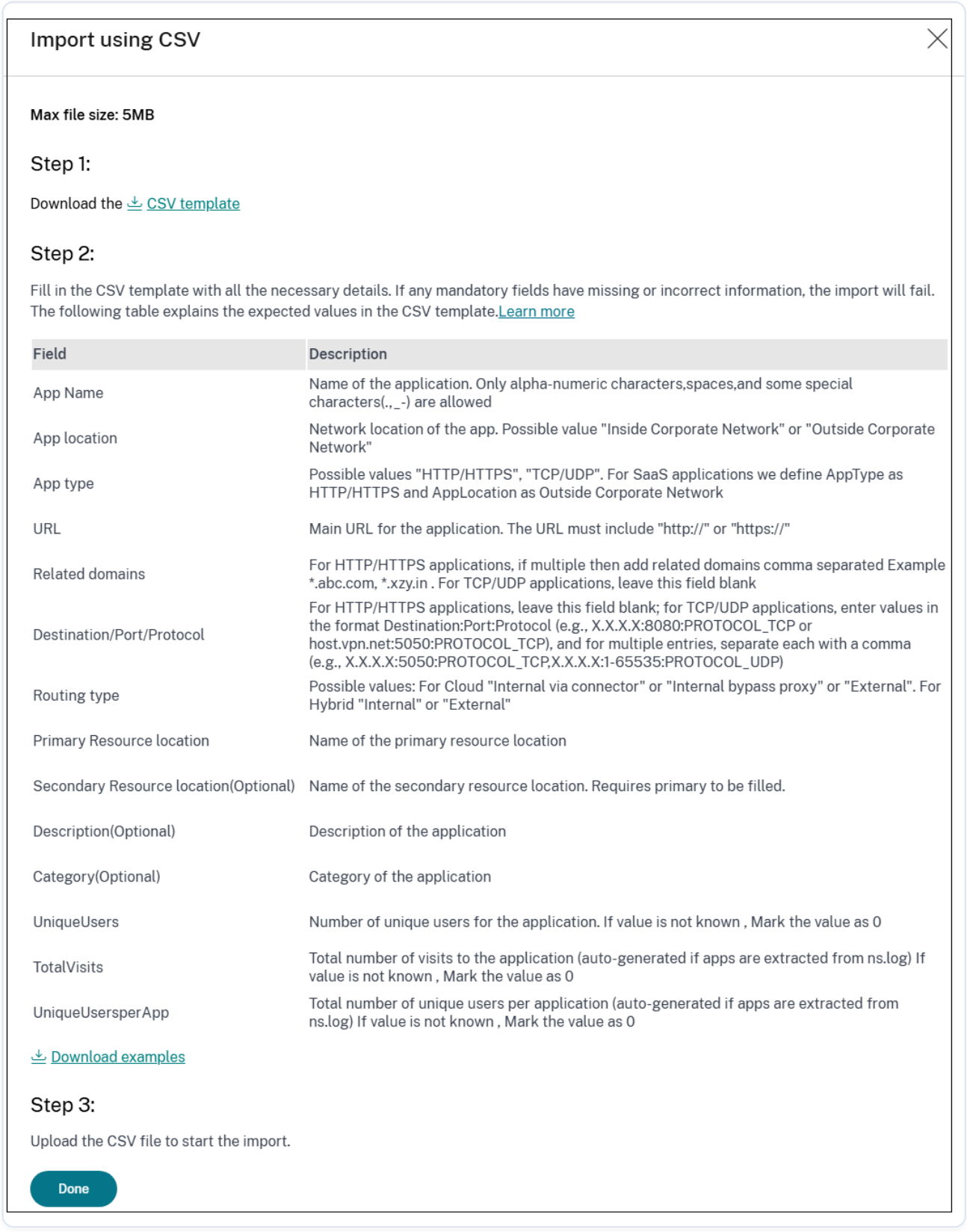
   HINWEIS:

   Wenn Sie eine große Anzahl von Anwendungen aus einer CSV-Datei importieren, verarbeiten Sie diese in Stapeln von 50. Wählen Sie nach dem Hochladen der CSV-Datei die ersten 50 Anwendungen aus und schließen Sie den Import ab, wählen Sie dann die nächsten 50 aus und wiederholen Sie den Vorgang, bis alle Anwendungen importiert sind.

   Klicken Sie auf **Beispiele herunterladen**, um eine Beispiel-CSV-Datei mit den Daten anzuzeigen.

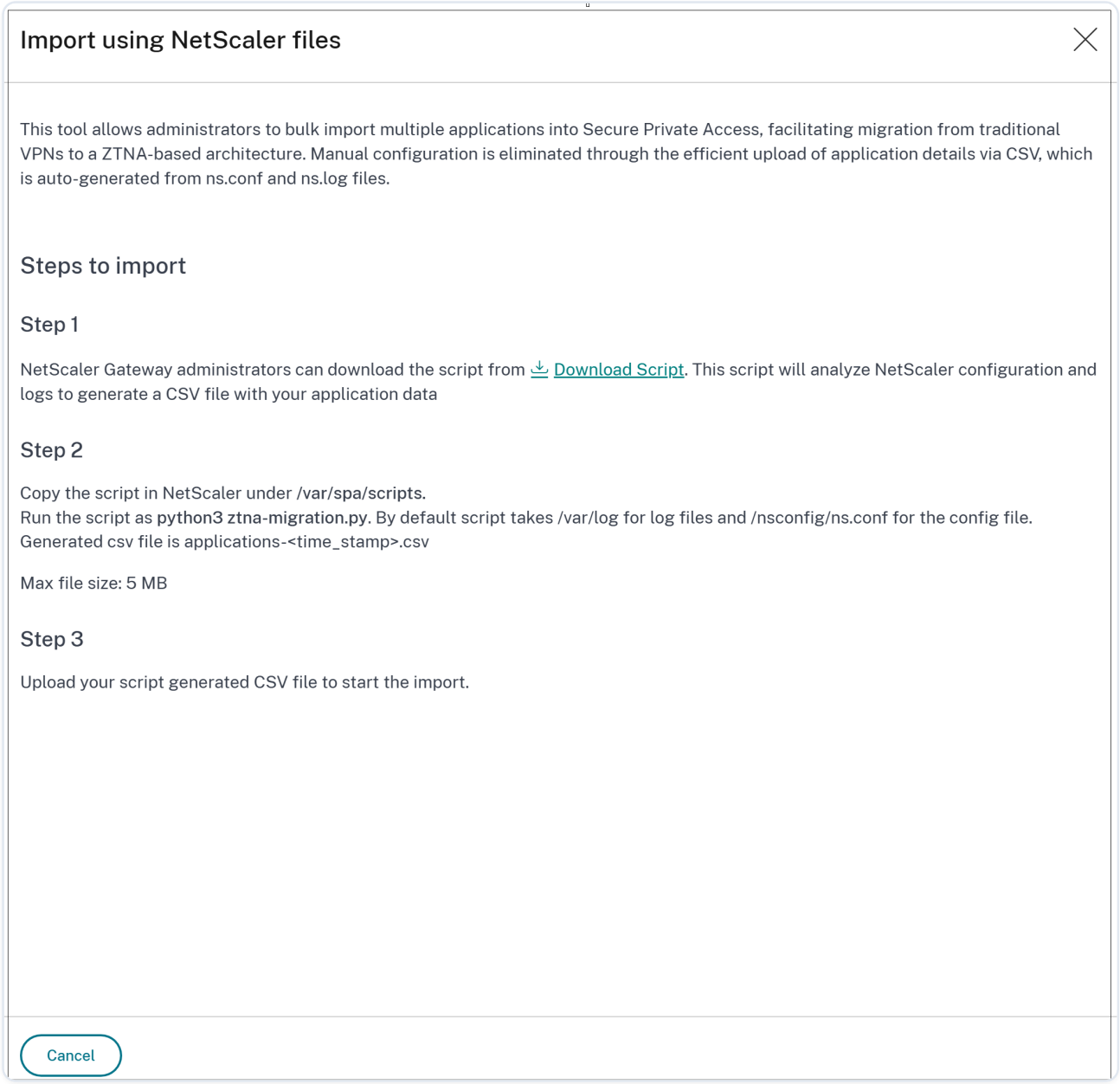
Richtlinien für den Import von Anwendungen mithilfe der CSV-Datei:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Richtlinien für den Import von Anwendungen mithilfe von NetScaler-Dateien:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Einzugebende Werte in der CSV-Datei

Die folgende Tabelle enthält Richtlinien zu den Werten, die für jede Spalte in der CSV-Datei eingegeben werden müssen, wenn die Anwendungen manuell erstellt werden:

SPALTENNAME	WERT
App-Speicherort	Innerhalb des Unternehmensnetzwerks (für interne Web-Apps, TCP-, UDP-Apps)
	Außerhalb des Unternehmensnetzwerks (für SaaS-Apps)
App-Typ	Muss einer der folgenden Werte sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SPALTENNAME	WERT
	HTTP/HTTPS
	TCP/UDP
URL	Nur für HTTP/HTTPS-Apps anwendbar. Die URL der Anwendung. Die URL muss „http://“ oder „https://“ enthalten.
Zugehörige Domänen	Nur für HTTP/HTTPS-Apps anwendbar. Sie können mehrere zugehörige Domänen durch ein Komma (,) getrennt hinzufügen.
	Für TCP/UDP-Apps lassen Sie dieses Feld leer.
DestinationPortProtocol	Nur für TCP/UDP-Apps anwendbar. Sie müssen alle IP-Adressen, IP-Adressbereiche oder IP/CIDR und Ports durch einen Doppelpunkt (:) getrennt auflisten.
	Für HTTP/HTTPS-Apps lassen Sie dieses Feld leer.
	Ziel, Port und Protokoll müssen bei manueller Dateneingabe wie folgt formatiert werden.
	Ziel:Port:Protokoll. Beispiel: 192.0.2.254:5050:PROTOCOL_TCP.
	Wenn es mehrere Ziele in der TCP/UDP-Anwendung gibt, werden mehrere Zieleinträge jeweils durch ein Komma getrennt (zum Beispiel X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP)
	Das Ziel kann eine IP-Adresse, ein IP-Adressbereich, CIDR, ein Hostname, eine Domäne oder ein FQDN sein. Der Port kann ein einzelner Port (Beispiel 5050) oder ein Portbereich (Beispiel 1–65335) sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SPALTENNAME	WERT
Routing-Typ (Cloud-Umgebung)	Wählen Sie je nach App-Typ einen der folgenden Werte aus.
	Intern – Proxy umgehen – Der Domänenverkehr wird über Citrix Cloud Connector™ geleitet, wobei der auf der Connector Appliance konfigurierte Webproxy des Kunden umgangen wird.
	Intern über Connector – Die Apps können extern oder intern sein, aber der Datenverkehr muss über die Connector Appliance fließen.
	Extern – Der Datenverkehr fließt direkt ins Internet.
Routing-Typ (Hybridumgebung)	**Intern** oder **Extern**.
Primärer Ressourcenstandort	Der Name des primären Ressourcenstandorts, an dem sich die Anwendung befindet.
	Hinweis: Nicht anwendbar für Hybridumgebungen.
Sekundärer Ressourcenstandort (optional)	Der Name des sekundären Ressourcenstandorts, an dem sich die Anwendung befindet. Der sekundäre Ressourcenstandort ist nur anwendbar, wenn der primäre Ressourcenstandort explizit angegeben ist.
	Hinweis: Nicht anwendbar für Hybridumgebungen.
Beschreibung	(Optional) Anwendungsbeschreibung.
Kategorie	(Optional) Anwendungskategorie.
UniqueUsers	Anzahl eindeutiger Benutzer für die Anwendung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SPALTENNAME	WERT
	Dieser Wert wird automatisch generiert, wenn die Anwendungen aus ns.log-Dateien extrahiert werden.
	Wenn Sie die CSV-Datei manuell aktualisieren, lassen Sie sie leer.
TotalVisits	Gesamtzahl der Zugriffe auf die Anwendung.
	Dieser Wert wird automatisch generiert, wenn die Apps aus ns.log-Dateien extrahiert werden.
	Wenn Sie die CSV-Datei manuell aktualisieren, lassen Sie dieses Feld leer.
UniqueUsersperApp	Gesamtzahl der eindeutigen Benutzer, die auf die Anwendung zugreifen.
	Dieser Wert wird automatisch generiert, wenn die Apps aus ns.log-Dateien extrahiert werden.
	Wenn Sie die CSV-Datei manuell aktualisieren, lassen Sie dieses Feld leer.

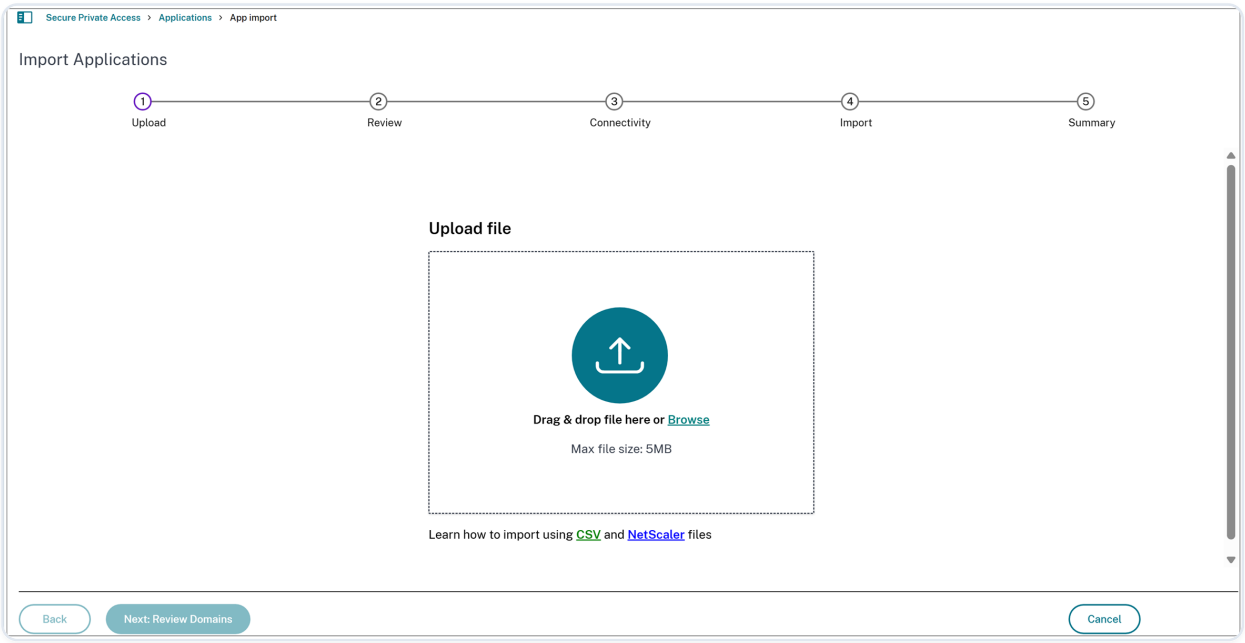
Schritte zur Migration von Anwendungen mit dem CSV-basierten Tool

Sie können Anwendungen während der Einrichtung von Secure Private Access oder nach Abschluss der Einrichtung importieren.

1. Klicken Sie auf der Dienstkachel Secure Private Access auf **Verwalten**.
2. Klicken Sie auf der Seite „Übersicht“ auf **Weiter**.
3. Richten Sie Identität und Authentifizierung für die Benutzer ein, damit diese sich bei ihren Stores anmelden können. Weitere Informationen finden Sie unter Identität und Authentifizierung einrichten.
4. Klicken Sie auf der Seite **Schritt 2: Anwendungen** auf **Anwendung importieren**.

   Alternativ, wenn Ihr Secure Private Access bereits eingerichtet ist, klicken Sie auf der Seite „Anwendungen“ (**Secure Private Access > Anwendungen**) auf **Die Anwendung importieren**.

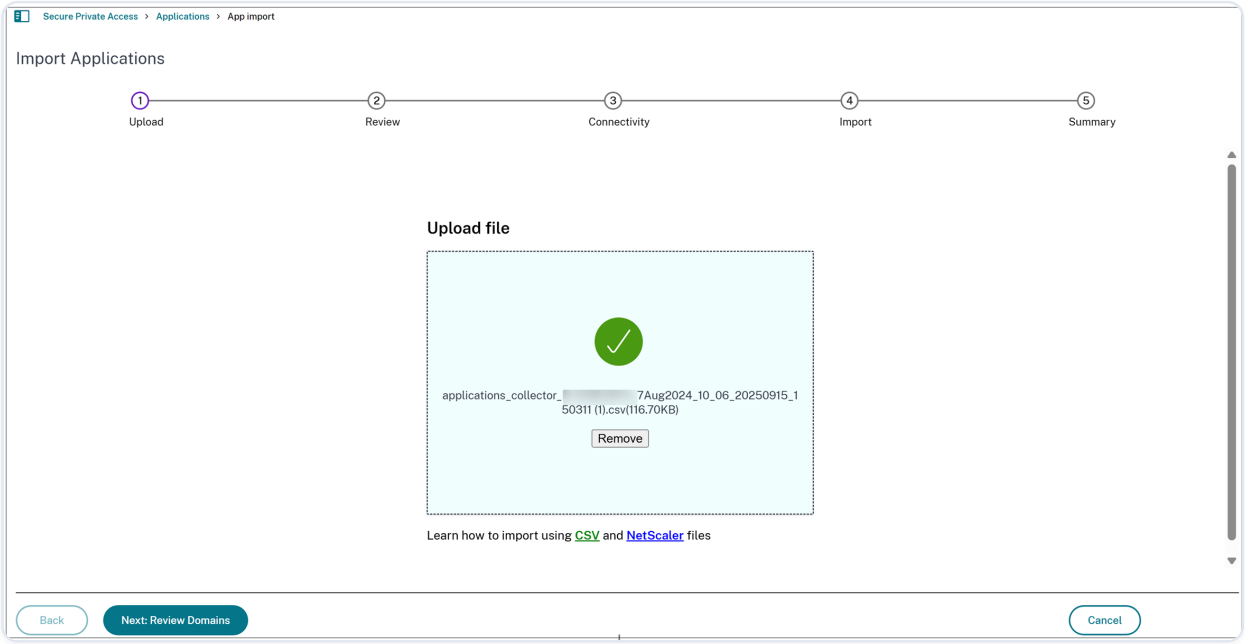
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Laden Sie die CSV-Datei hoch. Sie können die CSV-Datei entweder hierher ziehen oder nach ihr suchen, um sie auszuwählen.
6. Klicken Sie auf **Weiter: Domänen überprüfen**.

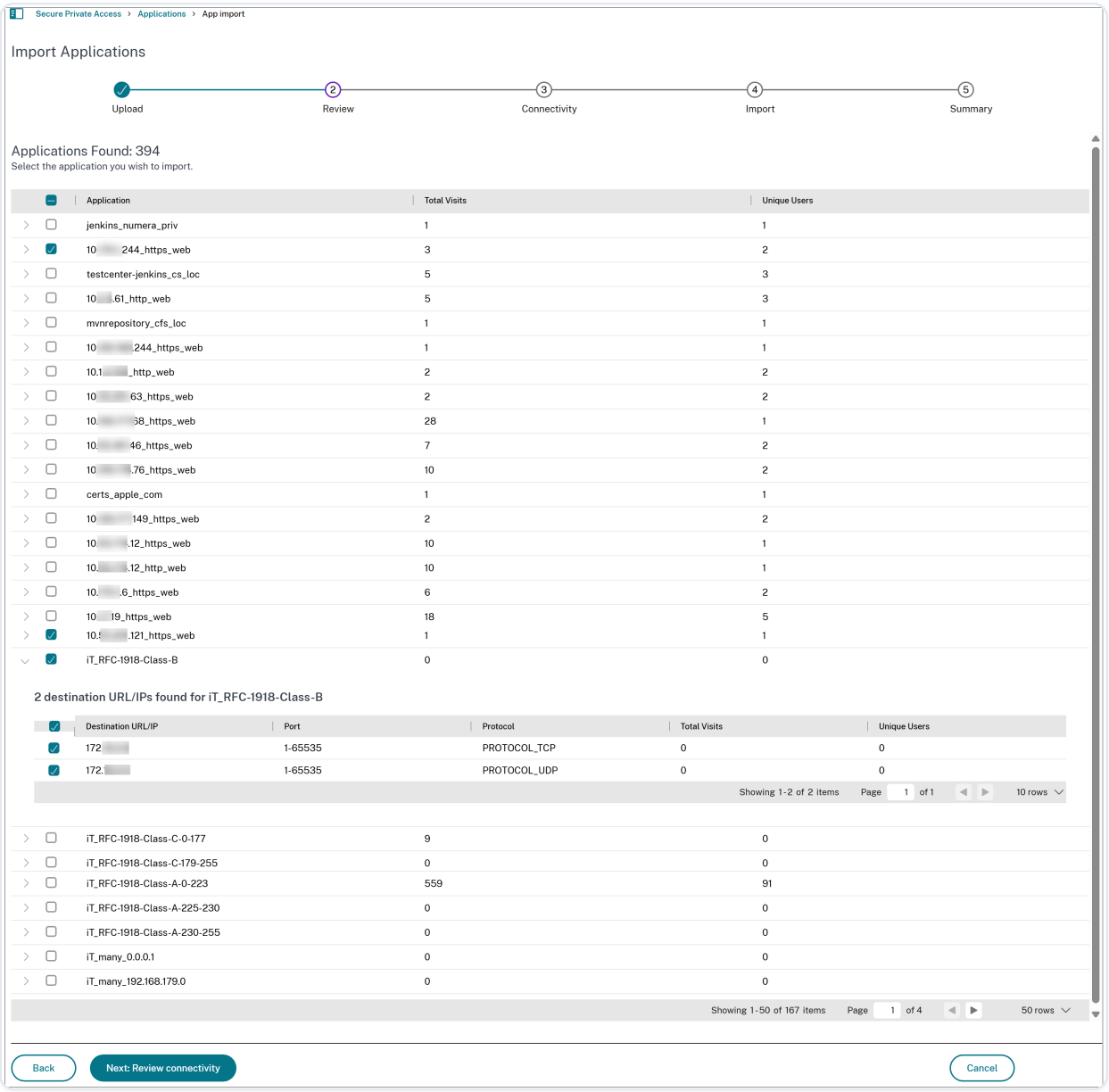
HINWEIS:

- Die Schaltfläche **Weiter: Domänen überprüfen** ist nur aktiviert, wenn die Datei keine Fehler enthält.
- Wenn Sie dieselbe CSV-/nsconfig-Datei mit zusätzlichen Anwendungen hochladen, wird nur die Differenz importiert.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Wählen Sie die Anwendungen aus, die Sie importieren möchten.



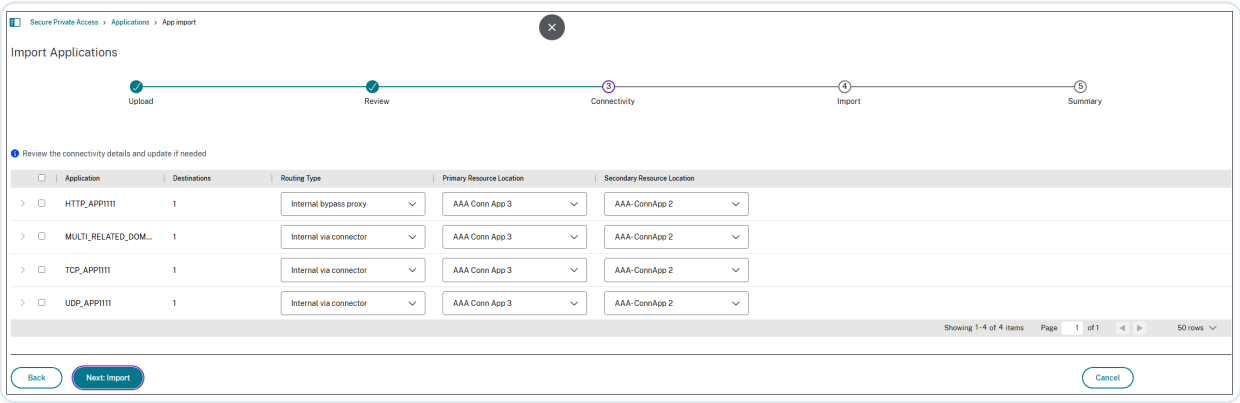
© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Wenn eine Anwendung mit derselben Domäne oder Wildcard-Domäne bereits existiert, ist diese Anwendung für den Import deaktiviert. Sie können diese Anwendungen nicht auswählen.
- Das erweitern-Symbol neben jeder Anwendung zeigt zusätzliche Details zur App an.
- Für SaaS-/Web- und TCP/UDP-Anwendungen zeigt die Seite **Anwendungen importieren** die gesamten Anwendungsbesuche und die Anzahl der eindeutigen Benutzer (einzelne Benutzer, die auf die Anwendung zugegriffen haben) an. Verwenden Sie das erweitern-Symbol, um die Port- und Protokolldetails der Anwendung anzuzeigen.
- Manuell über CSV hochgeladene SaaS-Apps (außerhalb des Unternehmensnetzwerks) werden als unveröffentlicht markiert und erscheinen trotz erfolgreichem Upload nicht in der Benutzeroberfläche „Anwendungen importieren“. Um daher eine SaaS-Anwendung durch manuelles Hinzufügen des Eintrags in der CSV-Datei zu erstellen, müssen Sie **App-Speicherort** auf **Außerhalb des Unternehmensnetzwerks** und **App-Typ** auf **HTTP/HTTPS** festlegen.
- Für TCP/UDP-Anwendungen listet das Tool alle zugehörigen Ziel-URLs und IP-Adressen auf. Standardmäßig werden beim Auswählen der Anwendung automatisch die zugehörigen URLs und IP-Adressen für den Import ausgewählt. Sie können einzelne Ziele nicht abwählen.

8. Klicken Sie auf **Weiter: Konnektivität überprüfen**.
9. Die Schaltfläche **Weiter: Konnektivität überprüfen** ist nur aktiviert, wenn mindestens eine Anwendung ausgewählt ist.
10. Überprüfen und aktualisieren Sie die Konnektivitätseinstellungen. Nehmen Sie bei Bedarf die erforderlichen Änderungen an Routing-Typ und Ressourcenstandorten vor und klicken Sie dann auf **Fertig**.

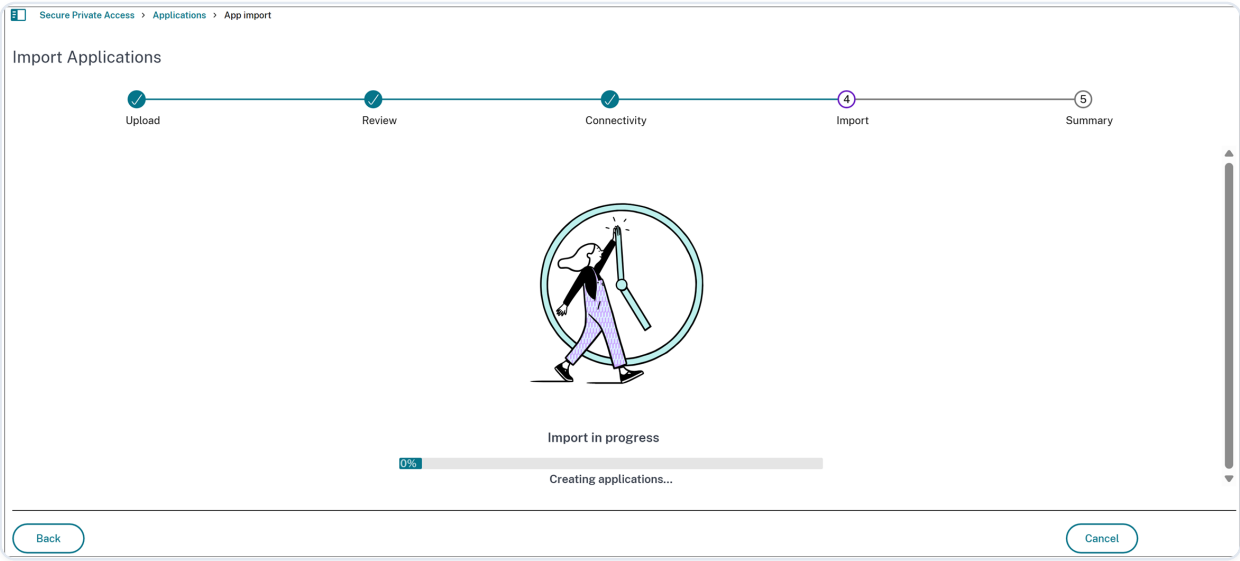
© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

- Wenn der angegebene Ressourcenstandort nicht existiert, wird standardmäßig der erste verfügbare Ressourcenstandort in der Liste der dem Kunden zugeordneten Ressourcenstandorte ausgewählt. Wenn die Connector Appliance am angegebenen Ressourcenstandort nicht aktiv ist, schlägt die Anwendungserstellung fehl.

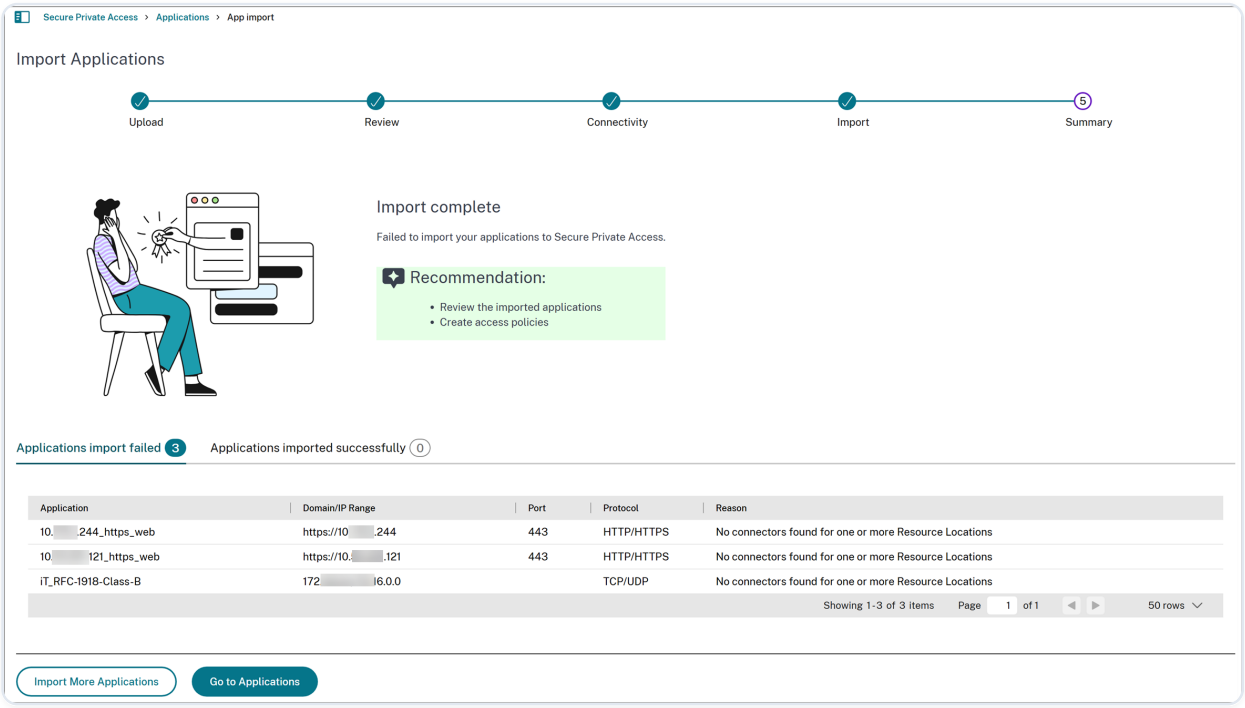
11. Klicken Sie auf: **Weiter: Importieren**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die Seite **Anwendungen importieren** zeigt die Details der importierten Anwendungen an. Diese Anwendungen werden auch der Liste der Anwendungen auf der Seite **Anwendungen** hinzugefügt.
- Bei fehlgeschlagenen Anwendungsimporten wird der Grund für den Fehler in der Spalte **Grund** angezeigt. Verwenden Sie diese Informationen, um die CSV-Datei zu korrigieren und diese Anwendungen erneut zu importieren.



12. Klicken Sie auf **Zu Anwendungen wechseln**, um die importierten Anwendungen auf der Seite **Anwendungen** anzuzeigen.

Fehler beim Importieren oder Erstellen von Anwendungen bei Verwendung der CSV-Datei

Die folgenden Probleme können zu Fehlern beim Importieren oder Erstellen von Anwendungen führen, wenn die CSV-Datei verwendet wird:

- Änderungen an den Spaltennamen oder deren Groß-/Kleinschreibung.
- Löschen oder Vertauschen der Spalten in der CSV-Datei.
- Fehlende obligatorische Anwendungsfelder in der CSV-Datei.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Eine leere CSV-Datei oder eine CSV-Datei, die nur Spaltennamen enthält, wird importiert. Bei einer leeren Datei wird eine Fehlermeldung angezeigt. Wenn die Datei nur Spaltennamen enthält, bleibt die Schaltfläche **Weiter** deaktiviert.
- Keine Connector Appliance ist am Ressourcenstandort verfügbar, der in der CSV-Datei angegeben ist.
- Ein sekundärer Ressourcenstandort ist angegeben, während der primäre Ressourcenstandort fehlt oder leer ist. Der Import schlägt mit einem Validierungsfehler fehl, der darauf hinweist, dass der primäre Ressourcenstandort erforderlich ist.

Referenzen

Beachten Sie die folgenden Themen für Informationen zum Erstellen von Anwendungen in Secure Private Access.

- Unterstützung für Enterprise-Web-Apps
- Unterstützung für SaaS-Apps
- Unterstützung für TCP/UDP-Apps

Interne IP-Adresspools für Clients – Vorschau

Die internen IP-Adresspools für Clients enthalten IP-Adressbereiche, die den angemeldeten Benutzern zugewiesen werden. Jeder Benutzer und sein Gerät erhalten eine eindeutige interne IP-Adresse, die für die Identifizierung und das Sitzungsmanagement innerhalb von Secure Private Access erforderlich ist. Diese interne Client-IP-Adresse ist nur innerhalb des Ressourcenstandorts des Kunden zugänglich.

Mithilfe dieser internen IP-Adressen können Geräte am Ressourcenstandort des Kunden den Datenverkehr direkt an das Gerät eines bestimmten angemeldeten Benutzers tunneln, wodurch Server-zu-Client-Verbindungen ermöglicht werden. Die interne Client-IP-Adresse unterstützt auch die Quell-IP-Persistenz für bestehenden Client-zu-Server-Tunnelverkehr und gewährleistet so stabile und konsistente Verbindungen.

HINWEIS:

Die Funktion der internen IP-Adresspools für Clients befindet sich in der Vorschauphase. Um diese Funktion zu aktivieren, wenden Sie sich an den Citrix® Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsfälle für interne IP-Adresspools für Clients

- **Server-zu-Client-Verbindungen ermöglichen:** Bestimmte Aufgaben wie das Pushen von Konfigurationen, die Bereitstellung von Remote-Unterstützung oder die Installation von Software erfordern, dass Server Verbindungen zu Client-Geräten initiieren. Interne IP-Adresspools für Clients ermöglichen dies, indem sie einen definierten Bereich von IP-Adressen zuweisen, die zur Identifizierung von Client-Geräten verwendet werden. Diese internen IP-Pools werden basierend auf dem Benutzerkontext und dem Standort zugewiesen. Zum Beispiel kann ein spezifischer IP-Adressbereich einer Benutzergruppe wie dem HR-Team zugewiesen werden.

  Um die Server-zu-Client-Kommunikation zu ermöglichen, müssen Sie eine Server-zu-Client-App erstellen und die Port- und Protokolldetails des Client-Geräts zusammen mit dem Backend-IP-Adressbereich angeben, der zum Erreichen des Clients verwendet wird. Weitere Informationen finden Sie unter Server-zu-Client-App-Konfiguration.

- **Client-interne IP-Adresspersistenz aktivieren:** Um konsistente Verbindungen aufrechtzuerhalten, erfordern einige Anwendungen eine kontinuierliche Sitzung mit demselben Client. Informationen zur Aktivierung der Client-IP-Adresspersistenz finden Sie unter Client-IP-Adresspersistenz.

  WICHTIG:

  Um die Quell-IP-Adresse als interne IP-Adresse oder die vom Server initiierte Verbindungsfunktionalität zu verwenden, stellen Sie Folgendes sicher:

  - Der Switch oder Router, der mit dem Subnetz der Connector Appliance verbunden ist, unterstützt Gratuitous ARP.
  - Die Konfiguration von Port Security und Dynamic ARP Inspection (DAI) beeinträchtigt nicht die Quell-IP-Adresse oder die vom Server initiierte Verbindungsfunktionalität.

Einschränkungen des IP-Adresspools

Im Folgenden sind einige der Einschränkungen des IP-Adresspools aufgeführt:

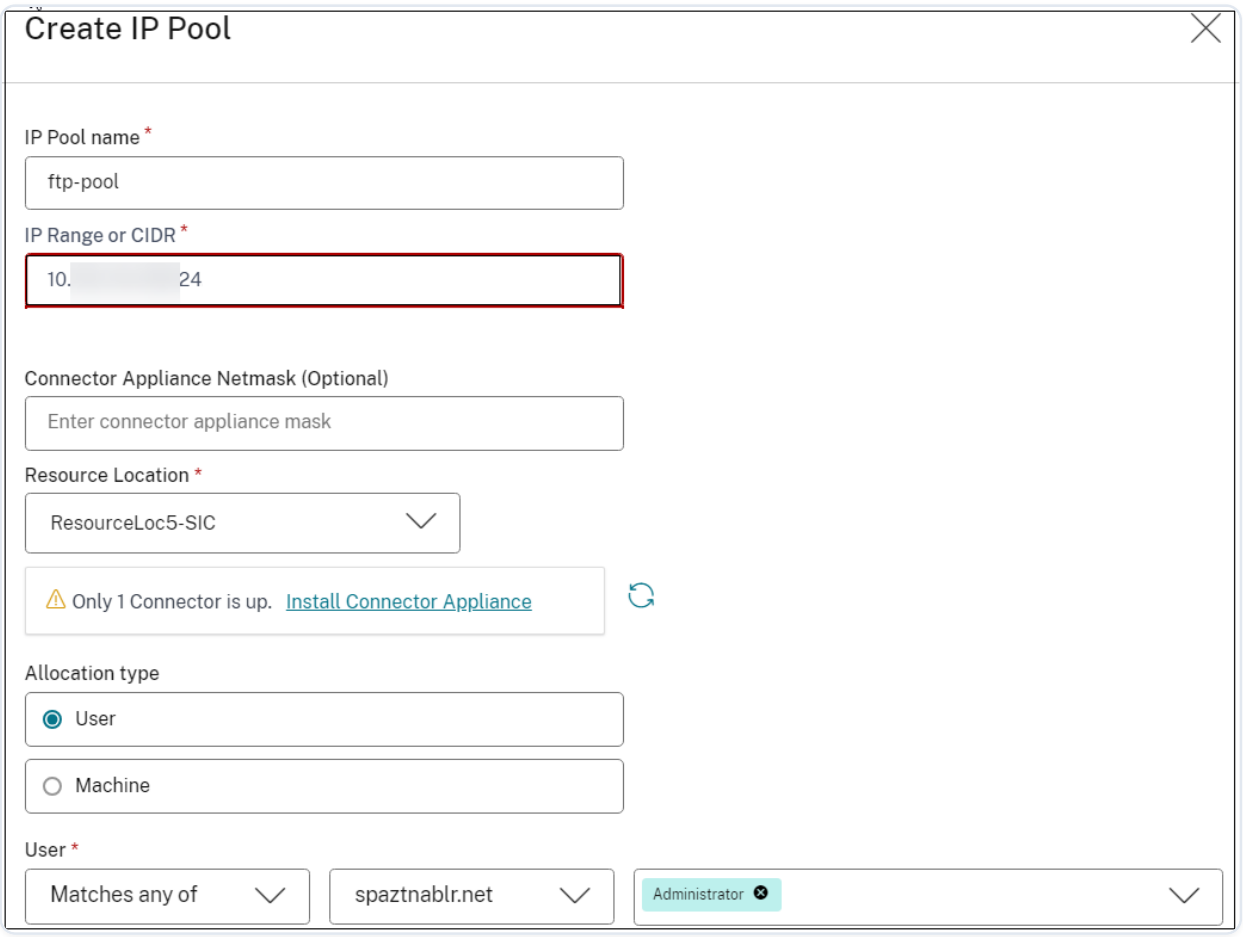
- Alle Connector Appliances an einem Ressourcenstandort müssen sich im selben IP-Subnetz befinden.
- Die internen IP-Adresspools müssen aus IP-Adressen des Connector Appliance-Subnetzes am selben Ressourcenstandort bestehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die IP-Adressen innerhalb der internen IP-Adresspools dürfen sich nicht mit verwendeten IP-Adressen der Connector Appliances oder anderer Geräte innerhalb desselben Subnetzes überschneiden.
- Wenn die IP-Adressen im Pool erschöpft sind, werden den Benutzern keine IP-Adressen zugewiesen, und daher können Server-zu-Client-Verbindungen und clientinterne IP-Stickiness-Funktionen nicht verwendet werden.
- Einem Benutzer können maximal 3 verschiedene IP-Adressen zugewiesen werden, was Anmeldungen von bis zu 3 verschiedenen Geräten ermöglicht. Wenn sich derselbe Benutzer von einem vierten Gerät anmeldet, wird keine IP-Adresse zugewiesen, wodurch die Verwendung von Server-zu-Client-initiierten Verbindungen und clientinterner IP-Stickiness verhindert wird.
- Die zugewiesene interne IP-Adresse ist persistent und bleibt für tägliche An- und Abmeldungen auf demselben Gerät gleich. Wenn ein Benutzer jedoch 15 aufeinanderfolgende Tage inaktiv ist, wird seine persistente interne IP-Adresse freigegeben und einem anderen Benutzer neu zugewiesen.

Einen Intranet-IP-Adresspool erstellen

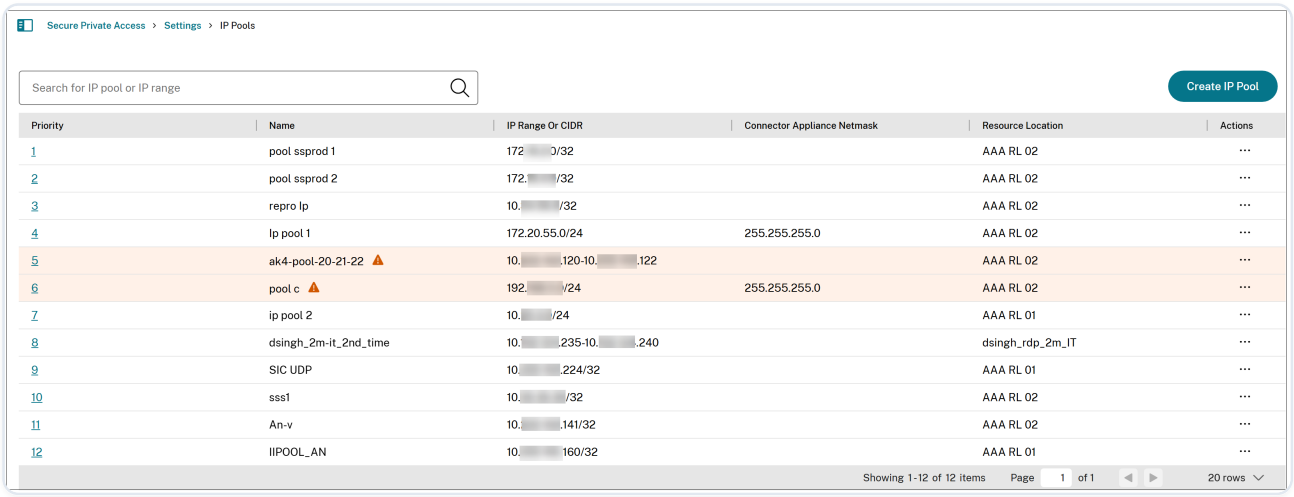
1. Navigieren Sie zu **Einstellungen > IP-Pools** und klicken Sie dann auf **IP-Pool erstellen**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **IP-Pool-Name**: Geben Sie einen Namen für den IP-Pool ein.
3. **IP-Bereich oder CIDR**: Geben Sie den Bereich der für Clients reservierten IP-Adressen ein. Eine dieser IP-Adressen wird den Client-Maschinen zugewiesen.
4. **Connector Appliance-Netzmaske**: (Optional). Falls das Netzwerk-Subnetz der Connector Appliance vom Subnetz der internen IP-Adresse abweicht, muss die Netzmaske der Connector Appliance eingegeben werden.
5. **Ressourcenstandort**: Wählen Sie den Ressourcenstandort aus, an dem sich der Back-End-Server befindet. Stellen Sie sicher, dass mindestens eine Connector Appliance aktiv ist.
6. **Zuweisungstyp**: Wählen Sie Benutzer aus und wählen Sie die Bedingung, Domäne und den Benutzer oder die Benutzergruppen aus, für die dieser Pool gilt.
7. Klicken Sie auf **Erstellen**.

Der von Ihnen erstellte IP-Adresspool wird auf der Seite „IP-Pools“ aufgeführt.



Sobald die Client-Anmeldung erfolgreich ist, wird dem Benutzer eine Intranet-IP-Adresse aus dem internen IP-Adresspool des Clients zugewiesen.

Wie in der vorhergehenden Abbildung gezeigt, können Administratoren den Priorisierungsmechanismus verwenden, um die Priorität des Pools zu steuern. Administratoren können explizite Prioritätsstufen für jeden IP-Pool definieren. Der Secure Private Access-Dienst weist IP-Adressen von der höchsten zur niedrigsten Priorität (von oben nach unten) zu, um eine vorhersehbare Zuweisung und operative Kontrolle zu gewährleisten.

HINWEIS:

Die Priorität mit einem niedrigeren Wert hat die höchste Präferenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einen IP-Adresspool löschen

IP-Adresspools können sofort oder im Laufe der Zeit mit einer der folgenden Optionen gelöscht werden.

- **IP-Pool zwangsweise löschen:** Stoppt die Zuweisung von IP-Adressen an neue Benutzer und gibt ungenutzte IP-Adressen sofort frei. Aktive Benutzersitzungen, die die gelöschten IP-Adressen verwenden, können beendet werden, was zu abrupten Schließungen und erzwungenen Abmeldungen führt. Benutzern mit beendeten Sitzungen werden erst dann neue IP-Adressen zugewiesen, wenn ein anderer IP-Adresspool erstellt wurde.
- **IP-Pool im Laufe der Zeit löschen:** Stoppt die Zuweisung von IP-Adressen an neue Benutzer und gibt ungenutzte IP-Adressen sofort frei. Das System wartet, bis die aktiven Sitzungen abgemeldet oder abgelaufen sind, bevor der Pool vollständig gelöscht wird. Benutzern mit beendeten Sitzungen werden erst dann neue IP-Adressen zugewiesen, wenn ein anderer IP-Adresspool erstellt wurde.

HINWEIS:

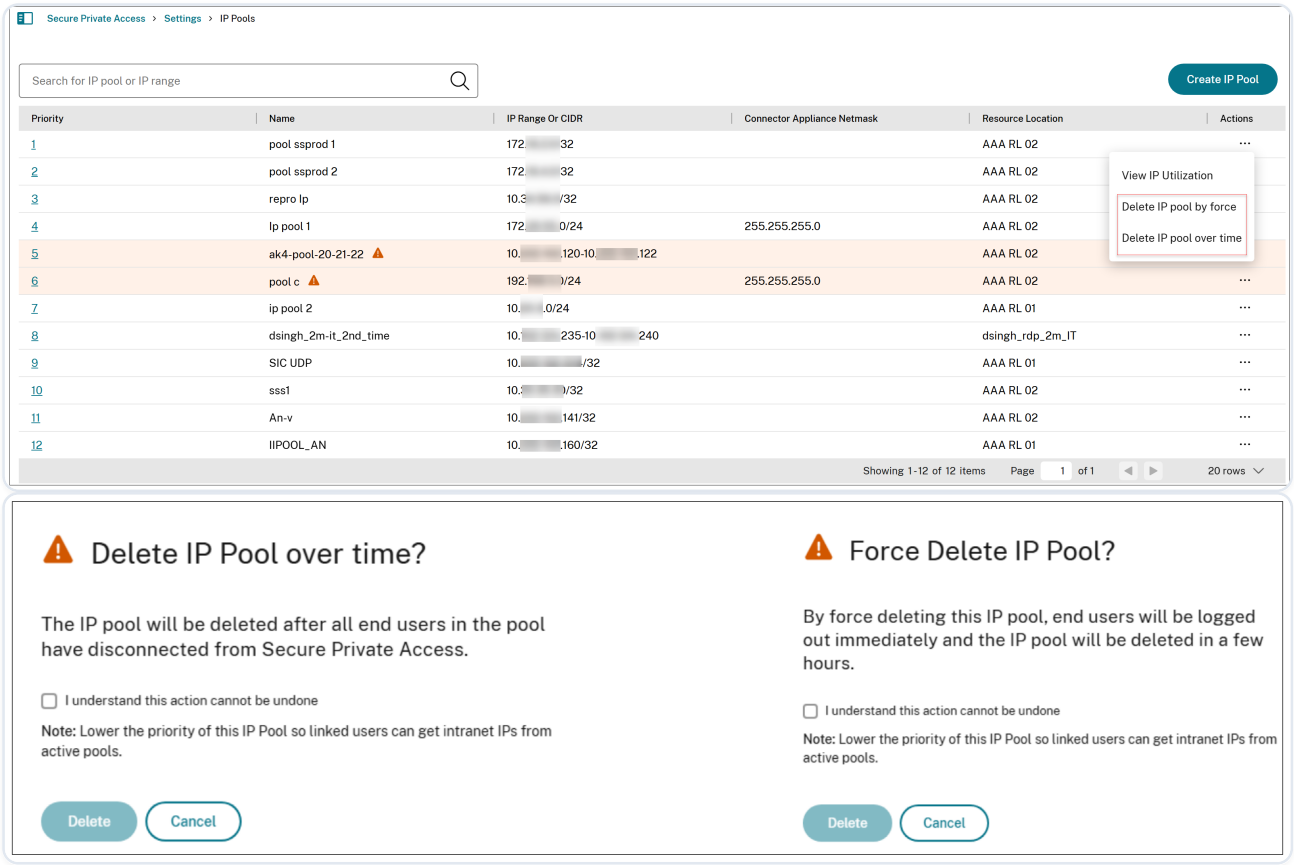
Wir empfehlen Ihnen, ein Wartungsfenster zu planen und die Benutzer zum Abmelden aufzufordern, bevor Sie die Löschung des IP-Pools im Laufe der Zeit einleiten. Wenn die meisten IP-Adressen nach der geplanten Zeit freigegeben wurden, können Sie die verbleibenden in Gebrauch befindlichen IP-Adressen zwangsweise löschen. Wir empfehlen jedoch, große IP-Adresspools nicht zwangsweise zu löschen.

Führen Sie die folgenden Schritte aus, um einen IP-Pool zu löschen:

1. Navigieren Sie zu **Einstellungen > IP-Pools**.

   Die Liste der IP-Adresspools und deren Details werden angezeigt.
2. Klicken Sie auf die Auslassungspunkte (…) neben dem Adresspool, den Sie löschen möchten, und wählen Sie dann entweder **IP-Pool zwangsweise löschen** oder **IP-Pool im Laufe der Zeit löschen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Wenn ein Pool gelöscht oder zur Löschung vorgesehen wird, muss der Administrator dessen Priorität senken. Die Priorität für diesen Pool muss niedriger sein als die der anderen aktiven Pools, um sicherzustellen, dass Secure Private Access keine neuen IP-Adressen mehr aus diesem Pool zuweist. Die IP-Adresszuweisung fällt automatisch auf die Pools mit höherer Priorität zurück.

Anzeigen der IP-Adressauslastungsdaten

Sie können die IP-Adressauslastungsdaten auf der Seite „IP-Pool-Auslastung“ überwachen. Diese Seite bietet einen Überblick über den Status der IP-Adressen.

- Eine Liste der Benutzer und der diesen Benutzern zugewiesenen IP-Adressen.
- Der Prozentsatz der verfügbaren IP-Adressen, die bereits zugewiesen sind, und die Gesamtzahl der zur Zuweisung verfügbaren IP-Adressen.

Administratoren können diese Daten verwenden, um den IP-Adressverbrauch zu überwachen und sicherzustellen, dass genügend IP-Adressen für die Benutzer verfügbar sind.

Führen Sie die folgenden Schritte aus, um die Details zur IP-Adressauslastung anzuzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Einstellungen > IP-Pools**.

   Die Liste der IP-Adresspools zusammen mit ihren Details wird in einem Tabellenformat angezeigt.

2. Klicken Sie auf die Auslassungspunkte (...) neben dem Adresspool und dann auf **IP-Auslastung anzeigen**.

Konsistente Verbindungen aufrechterhalten

Um persistente und konsistente Verbindungen für Anwendungen zu gewährleisten, die Sitzungskontinuität erfordern, können Administratoren entweder die Connector-Stickiness oder die Client-IP-Adress-Stickiness aktivieren, je nach Anwendungstyp (Web/SaaS oder TCP/UDP). Secure Private Access unterstützt sowohl die Connector-Stickiness als auch die Client-IP-Adress-Stickiness.

- **Connector-Stickiness** stellt sicher, dass, nachdem ein Client eine Verbindung mit der Connector Appliance hergestellt hat, alle nachfolgenden Anfragen von diesem Client an dieselbe Quelle (Connector Appliance) geleitet werden.
- **Client-IP-Adress-Stickiness** stellt sicher, dass Anfragen von einer bestimmten Client-IP-Adresse konsistent an denselben Back-End-Server weitergeleitet werden.

Connector- oder Client-IP-Adress-Stickiness kann beim Erstellen der Anwendungen aktiviert werden.

- Für Web-/SaaS-Anwendungen können Administratoren die Option **Konsistente Verbindungen aufrechterhalten** aktivieren.
- Für TCP/UDP-Anwendungen können Administratoren je nach Anforderung zwischen **Client-IP**- und **Connector-ID**-Stickiness wählen.

Weitere Informationen finden Sie in den folgenden Abschnitten:

- Connector-Stickiness
- Client-IP-Adress-Stickiness

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Die Funktion Client-IP-Adress-Stickiness befindet sich in der Vorschau.
- Um die Client-IP-Adress-Stickiness zu aktivieren, müssen Administratoren interne Client-IP-Adresspools konfigurieren. Der IP-Adresspool ist unerlässlich, um einem Benutzer und dem zugehörigen Gerät eine eindeutige IP-Adresse zuzuweisen. Die Geräte vom Ressourcenstandort des Kunden können den Datenverkehr über die interne IP-Adresse des Clients an das Gerät eines bestimmten angemeldeten Benutzers tunneln. Weitere Informationen finden Sie unter Interne Client-IP-Adresspools.

Connector-Stickiness

Einige Anwendungen erfordern Connector-Stickiness, was bedeutet, dass alle Anfragen für eine Benutzersitzung, einschließlich der ersten Anmeldung und der nachfolgenden Anfragen, von derselben Connector Appliance (derselben IP-Adresse) stammen. Wenn eine Anfrage über eine andere Connector Appliance geleitet wird, funktioniert die Anwendung möglicherweise nicht korrekt.

- Die Connector-Persistenz ist spezifisch für eine bestimmte Benutzersitzung. Wenn derselbe Benutzer die App erneut öffnet, kann der Datenverkehr an ein anderes Connector Appliance weitergeleitet werden.
- Connector Appliances werden zufällig aus den verfügbaren Connector Appliances an einem bestimmten Ressourcenstandort ausgewählt.
- Wenn ein Connector Appliance ausfällt, wird die Verbindung zu einem anderen Appliance am selben Ressourcenstandort umgeleitet.

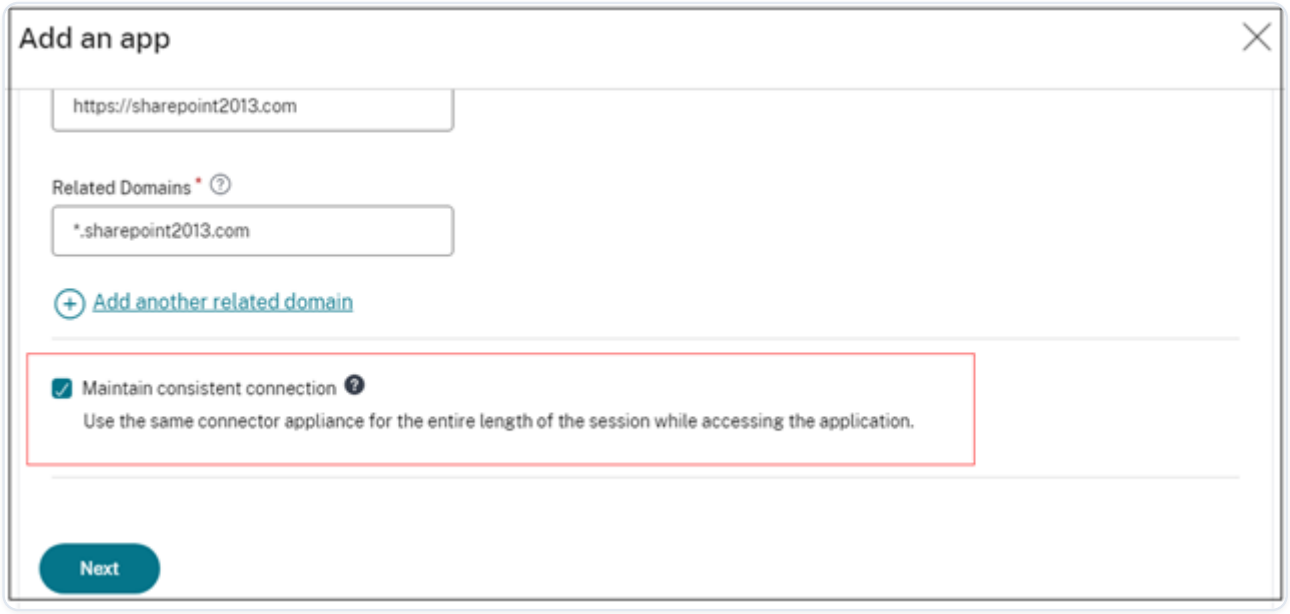
Die Connector-Persistenz ist in den folgenden Szenarien wichtig:

- NTLM-Protokolle, die von der IP-Adresse abhängen, um den Sitzungsstatus aufrechtzuerhalten. Wenn eine Anforderung über einen anderen Connector geleitet wird, kann die NTLM-Authentifizierung fehlschlagen, was zu Fehlern oder fehlgeschlagenen Anmeldungen führt.
- Anwendungen, die auf passivem FTP basieren und eine Verbindungspersistenz erfordern, um sicherzustellen, dass sowohl die Steuer- als auch die Datenverbindungen an denselben Back-End-Server weitergeleitet werden. Ohne diese Persistenz könnten die FTP-Sitzungen fehlschlagen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen zum Aktivieren der Connector-Persistenz für die Anwendungen finden Sie in den folgenden Themen:

- Eine Web-App konfigurieren
- Eine SaaS-App konfigurieren
- Eine TCP/UDP-App konfigurieren



Client-IP-Adressen-Persistenz – Vorschau

Wenn ein Client über Lastenausgleich über mehrere Connector Appliances an einem Ressourcenstandort eine Verbindung zum Back-End-Server herstellt, kann die Quell-IP-Adresse des Datenverkehrs als eine andere IP-Adresse des Connector Appliance erscheinen. Diese Diskrepanz bei den IP-Adressen kann zu Problemen wie den folgenden führen:

- **TCP/UDP-Anwendungen:** Bestimmte Anwendungen erfordern eine konsistente Sitzung zwischen einem bestimmten Client und Server. Wenn sich die Quell-IP-Adresse ändert, können diese Anwendungen möglicherweise nicht gestartet werden. Anwendungen wie passives FTP, aktives FTP und einige Webserver verlassen sich auf die IP-Adressaffinität (Persistenz), um korrekt zu funktionieren.
- **Sicherheits- und Überwachungssysteme:** Diese Systeme könnten Schwierigkeiten haben, den Datenverkehr zu verfolgen und zu analysieren, wenn sich die Quell-IP-Adressen häufig ändern.

Um die Affinität/Persistenz der Quell-IP-Adresse aufrechtzuerhalten, kann die Persistenz der internen Client-IP-Adresse für TCP/UDP-Anwendungen (Client-zu-Server) konfiguriert werden. Mit der Persistenz der Client-IP-Adresse wird der Benutzersitzung während der Anmeldung eine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

eindeutige interne IP-Adresse zugewiesen. Diese IP-Adresse wird anstelle der IP-Adresse der Connector Appliance am Ressourcenstandort verwendet. Diese Zuweisung stellt sicher, dass alle Verbindungen vom Client zum Back-End-Server die Quell-IP-Adresse als interne Client-IP-Adresse verwenden, die zum Zeitpunkt der Anmeldung zugewiesen wurde. Die Persistenz der Client-IP-Adresse gewährleistet die Sitzungspersistenz unabhängig von der Connector Appliance, die während der Verbindung verwendet wird.

Informationen zum Aktivieren der Client-IP-Adresspersistenz finden Sie unter Client-IP-Adresspersistenz für TCP/UDP-Anwendungen aktivieren.

Voraussetzungen

Stellen Sie sicher, dass die IP-Adresspools erstellt wurden. Der IP-Adresspool ist unerlässlich, um einem Benutzer und dem zugehörigen Gerät eine eindeutige IP-Adresse zuzuweisen. Weitere Informationen finden Sie unter Interne Client-IP-Adresspools.

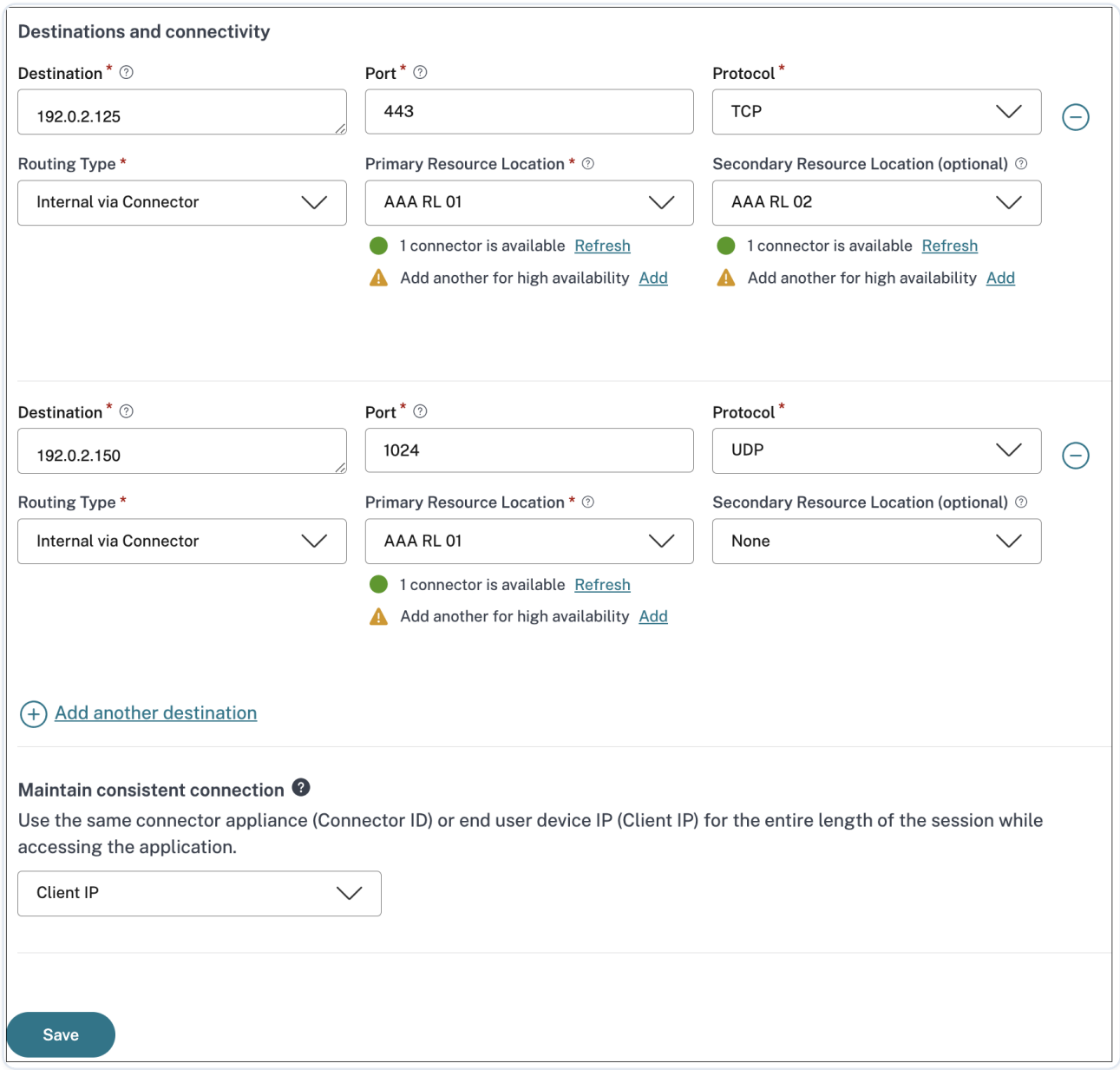
Client-IP-Adresspersistenz für TCP/UDP-Anwendungen aktivieren

Führen Sie die Schritte aus, die im Thema Unterstützung für TCP/UDP-Apps beschrieben sind.

Aktivieren oder deaktivieren Sie im Abschnitt **App-Details** die Client-IP-Persistenz, indem Sie einen der folgenden Werte unter **Konsistente Verbindung aufrechterhalten** auswählen.

- **Nicht verwenden:** Die Anwendung erfordert keine Persistenz. Die Anwendung kann mit jeder Quell-IP-Adresse arbeiten.
- **Client-IP:** Die Anwendung verwendet für den Client bei jeder Verbindung dieselbe Quell-IP-Adresse.
- **Connector-ID:** Die Anwendung stellt bei jeder Sitzung eine Verbindung zur selben Connector Appliance her.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

Um die Client-IP-Adresspersistenz zu aktivieren, wählen Sie denselben Ressourcenstandort aus, der beim Erstellen des internen IP-Adresspools verwendet wurde, und stellen Sie sicher, dass derselbe Ressourcenstandort im Abschnitt „App-Konnektivität“ festgelegt ist.

Aktive Sitzungen beenden und Benutzer/Maschinen zur Sperrliste hinzufügen

Administratoren können alle aktiven Sitzungen sofort beenden und die Benutzer/Maschinen zur Sperrliste hinzufügen. Das Hinzufügen eines Benutzers/einer Maschine zur Sperrliste beendet alle

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aktiven Secure Private Access-Anwendungssitzungen und blockiert den zukünftigen Anwendungszugriff.

Alle aktiven Anwendungssitzungen über den Chrome Enterprise Premium-Browser, den direkten Zugriff, die Citrix Workspace-App für HTML5 und den Secure Access-Agent werden beendet und blockiert. Alle über den Secure Access-Agent verbundenen Ressourcen wie Dateifreigaben, RDP- und SSH-Sitzungen werden ebenfalls beendet und blockiert. Benutzer können keine neuen Anwendungen starten, bis die Benutzer/Maschinen von der Sperrliste entfernt wurden.

Wenn die Anwendungen über den Chrome Enterprise Premium-Browser aufgerufen werden, werden auch alle aktiven browserbasierten Sitzungen beendet, und weitere Zugriffsanfragen des deaktivierten Benutzers werden gemäß der Secure Private Access-Sperrlistenrichtlinie abgelehnt.

HINWEIS:

- Das Hinzufügen eines Benutzers/einer Maschine zur Sperrliste ändert oder bearbeitet die konfigurierte Secure Private Access-Zugriffsrichtlinie nicht. Die Beendigung und Blockierung des Zugriffs erfolgt unabhängig von der konfigurierten Zugriffsrichtlinie. Sobald der Benutzer/die Maschine von der Liste entfernt wurde, werden die bestehenden Secure Private Access-Zugriffsrichtlinien für den Benutzer wiederhergestellt.
- Der Internetzugriff über den Citrix Enterprise Premium-Browser ist auch dann erlaubt, wenn ein Benutzer zur Sperrliste hinzugefügt wurde. Nur der Zugriff auf veröffentlichte Secure Private Access-Anwendungen wird blockiert.

Anwendungsfälle

Sie können diese Funktion in den folgenden Szenarien verwenden.

- Ein Mitarbeiter verlässt das Unternehmen oder wird aus dem Unternehmen entlassen. In diesem Fall widerruft der Administrator alle Secure Private Access-App-Zugriffe, 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 blockiert und alle aktuellen Sitzungen werden beendet. Der Benutzer kann von der Sperrliste entfernt werden, sobald die Situation unter Kontrolle ist.
- Ein Benutzer missbraucht den App-Zugriff. In diesem Fall kann der Zugriff für den Benutzer sofort widerrufen werden. Der Zugriff ist blockiert, bis der Benutzer zur Liste hinzugefügt wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen zum Blockieren von Benutzern bei Verwendung von Chrome Enterprise Premium

Um Benutzer zu blockieren, die Chrome Enterprise Premium mit Secure Private Access verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie beim Synchronisieren von Microsoft Entra ID-Benutzern über den Google Cloud / G Suite Connector von Microsoft sicher, dass die korrekte Attributzuordnung konfiguriert ist, damit die Benutzeridentität mit den Citrix Secure Private Access-Benutzerdatensätzen übereinstimmt.

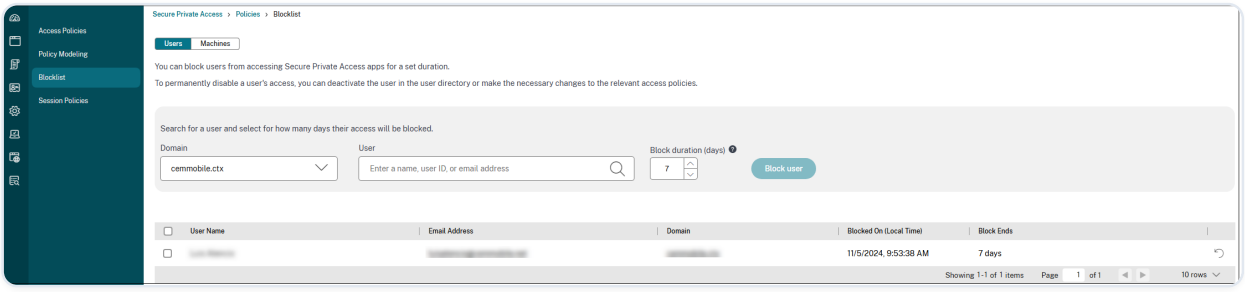
Wenn diese Konfiguration nicht festgelegt ist, wird die Richtlinie zum Sperren von Benutzern möglicherweise nicht für Benutzer erzwungen, die über den Chrome Enterprise Premium-Browser auf Anwendungen zugreifen.

Benutzer/Computer zur Sperrliste hinzufügen

1. Navigieren Sie zu **Secure Private Access > Richtlinien > Sperrliste**.
2. Wählen Sie unter **Domäne** die Domäne aus, für die der Zugriff deaktiviert werden soll.
3. Suchen Sie unter **Benutzer** nach dem Benutzernamen, der zur Sperrliste hinzugefügt werden soll. Alle Benutzernamen, die den Suchkriterien entsprechen, werden angezeigt. Wenn der Benutzer aus dem Verzeichnisdienst entfernt wird, wird dieser Benutzername nicht in der Liste **Benutzer** angezeigt.

   HINWEIS:

   Das Feld **Benutzer** wird nur angezeigt, wenn die Registerkarte **Benutzer** ausgewählt ist.

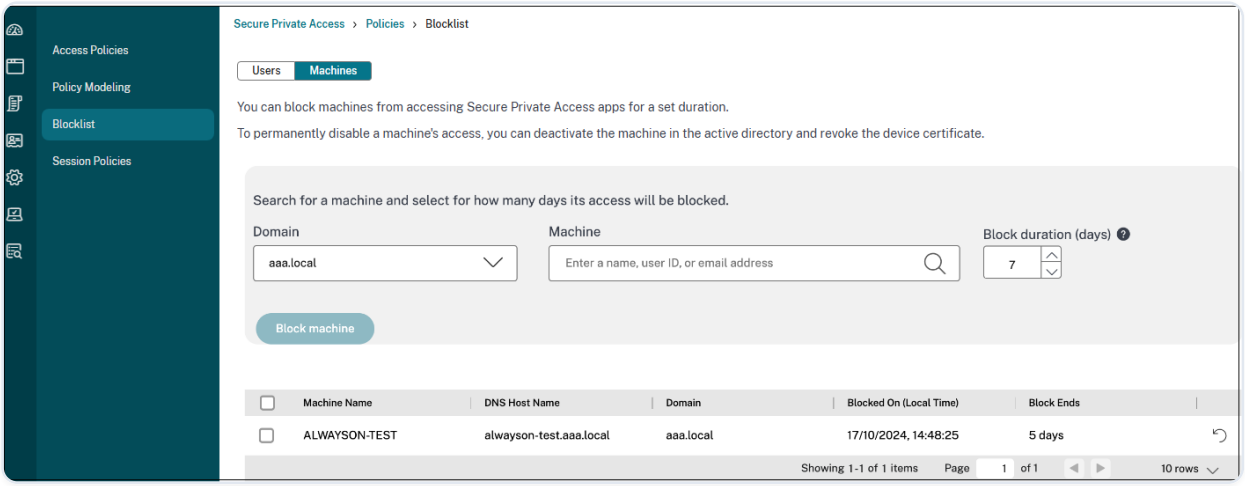


4. Suchen Sie unter **Computer** nach dem Computernamen, der zur Sperrliste hinzugefügt werden soll. Alle Computernamen, die den Suchkriterien entsprechen, werden angezeigt. Wenn der Computer aus dem Verzeichnisdienst entfernt wird, wird dieser Computername nicht in der Liste **Benutzer** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Das Feld **Computer** wird nur angezeigt, wenn die Registerkarte **Computer** ausgewählt ist.



5. Geben Sie unter **Sperrdauer (Tage)** die Anzahl der Tage ein, für die dieser Benutzer/Computer gesperrt werden soll. Sobald Sie den Benutzer/Computer zur Sperrliste hinzufügen, wird er standardmäßig für 7 Tage gesperrt. Sie können die Dauer jedoch auf 1 bis 99 Tage ändern. Nach Ablauf der Dauer wird der Zugriff basierend auf dem Benutzerverzeichnis und der Richtlinienkonfiguration wiederhergestellt. Dieser Wert bleibt auch für zukünftige Ergänzungen für den Benutzer erhalten. Wenn ein Administrator beispielsweise die Sperrdauer für einen Benutzer/Computer auf 30 Tage festlegt, bleibt diese Einstellung für den Benutzer/Computer bei zukünftigen Ergänzungen bestehen.
6. Klicken Sie entsprechend auf **Benutzer sperren** oder **Computer sperren**.

HINWEIS:

Das Feld **Benutzer blockieren** oder **Maschine blockieren** scheint von der ausgewählten Registerkarte (**Benutzer** oder **Maschinen**) abzuhängen.

Der Benutzer/die Maschine wird zur Sperrliste hinzugefügt.

Empfehlungen:

- Sie können den Zugriff noch vor Ablauf der Sperrdauer wiederherstellen, indem Sie einen der folgenden Schritte ausführen.
  - Wählen Sie den Zugriff aus, für den Sie den Zugriff wiederherstellen müssen, und klicken Sie dann auf **Zugriff wiederherstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Klicken Sie auf das Wiederherstellungssymbol in der Zeile des Benutzers, für den Sie den Zugriff wiederherstellen möchten.

      In beiden Fällen wird ein Bestätigungsdialogfeld angezeigt.

- Um den Zugriff für einen Benutzer/eine Maschine auf unbestimmte Zeit zu widerrufen, entfernen Sie den Benutzer/die Maschine aus Ihrem jeweiligen Verzeichnisdienst, z. B. Active Directory, und fügen Sie sie dann der Sperrliste hinzu. Dadurch werden die aktiven Secure Private Access-Sitzungen beendet, zukünftiger App-Zugriff blockiert, und sobald der Benutzer/die Maschine vom Store abgemeldet ist, kann sich der Benutzer/die Maschine aufgrund inaktiver Verzeichnisanmeldeinformationen nicht erneut anmelden.

Endbenutzererfahrung, nachdem ein Benutzer/eine Maschine zur Sperrliste hinzugefügt wurde

Die folgenden Abschnitte enthalten weitere Informationen zur Endbenutzererfahrung, nachdem ein Benutzer/eine Maschine zur Sperrliste hinzugefügt wurde.

Über die Cloud aufgerufene Anwendungen

Wenn ein Benutzer blockiert ist:

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

Wenn ein Gerät blockiert wird:

- Sobald ein Gerät zur Sperrliste hinzugefügt wird, wird der Zugriff des Benutzers auf alle aktuell ausgeführten Anwendungen blockiert.
- Jeder Versuch, auf neue Anwendungen zuzugreifen, löst eine Abmeldeanforderung aus.

Anwendungen, auf die über ein lokales NetScaler® Gateway zugegriffen wird (hybrider Datenpfad)

- Wenn eine Cloud-Sitzung beendet wird (entweder durch Benutzeraktion oder aufgrund eines Widerrufs), werden die entsprechenden aktiven NetScaler Gateway-Sitzungen automatisch beendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn ein blockierter Benutzer versucht, über NetScaler Gateway auf neue Anwendungen zuzugreifen, löst das System eine Abmeldeanforderung aus.

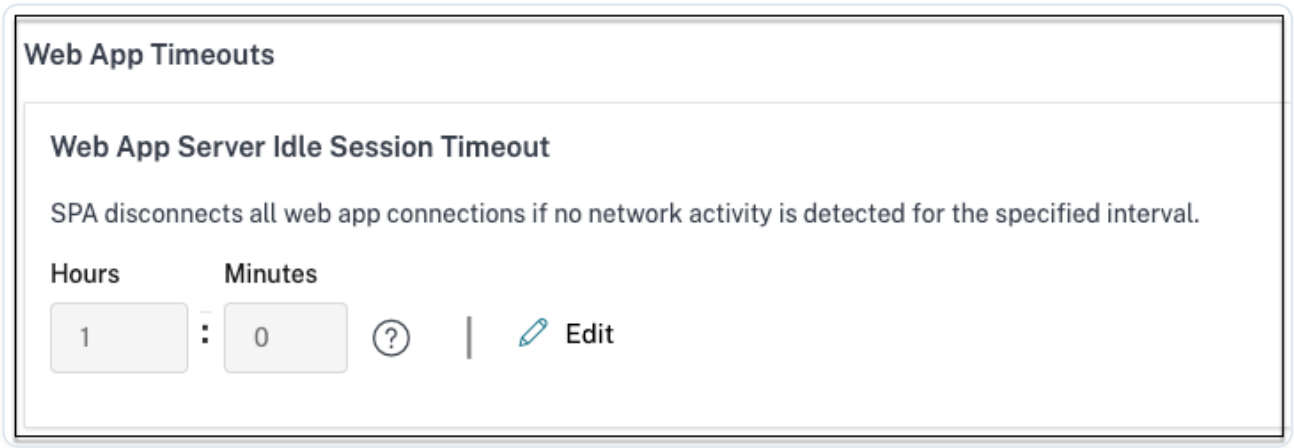
Timeouts für Benutzersitzungen

Sie können eine Timeout-Periode für die Web-Apps und den Citrix Secure Access™ Client konfigurieren, um Benutzersitzungen zu beenden, wenn für den angegebenen Zeitraum keine Netzwerkaktivität stattfindet. Für den Citrix Secure Access Client können Sie auch konfigurieren, dass der Citrix Secure Access Client eine Sitzung beendet, wenn für den angegebenen Zeitraum keine Benutzeraktivität stattfindet. Außerdem können Sie eine erzwungene Trennung auf dem Citrix Secure Access Client konfigurieren, unabhängig von der Benutzer- und Netzwerkaktivität, sobald der konfigurierte Zeitraum abläuft.

Timeout für die Web-App-Server

1. Navigieren Sie zu **Einstellungen > Timeouts**.
2. Wählen Sie unter **Leerlauf-Sitzungs-Timeout des Web-App-Servers** die Dauer in Stunden und Minuten aus, für die die Web-App-Sitzung im Leerlauf sein darf. Der Secure Private Access-Dienst beendet die Sitzung, nachdem diese Zeit abgelaufen ist, wenn die Sitzung im Leerlauf bleibt.

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



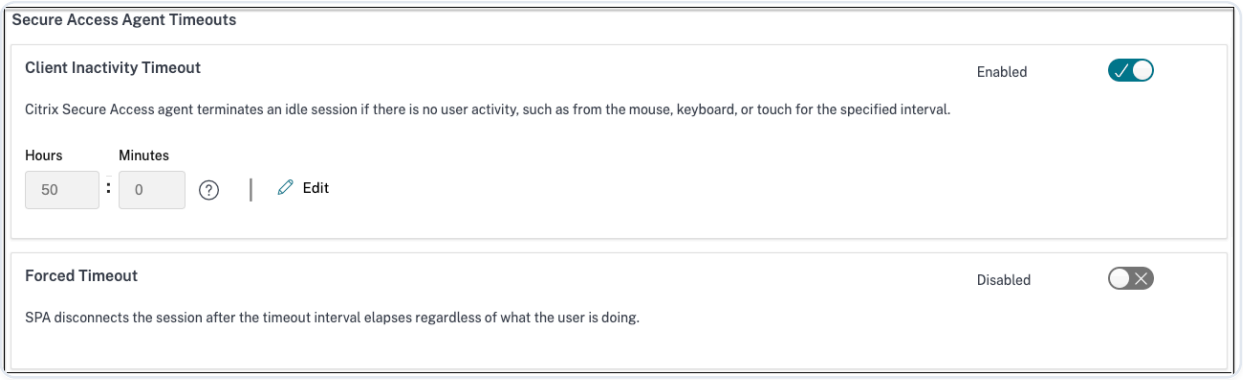
Timeouts für den Citrix Secure Access Client

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

- Client-Inaktivität
- Erzwungenes Timeout

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie 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.

   - **Client-Inaktivitätstimeout**: Die Dauer, nach der der Citrix Secure Access Client eine Sitzung beendet, wenn für den konfigurierten Zeitraum keine Benutzeraktivität (Maus oder Tastatur) stattfindet. Diese Option ist standardmäßig deaktiviert. Sie müssen die Option mithilfe des Umschalters aktivieren, um den konfigurierten Timeout-Zeitraum zu erzwingen. Wenn Sie den Umschalter jedoch nach dem Speichern der Konfiguration deaktivieren, initiiert der Client kein Timeout.

     Die Mindestdauer beträgt 5 Minuten und die maximale Dauer kann 168 Stunden betragen. Der Standardwert ist 8 Stunden.
   - **Erzwungenes Timeout**: Die Dauer, nach der der Citrix Secure Access Client eine Sitzung beendet, unabhängig von Benutzer- oder Netzwerkaktivitäten. Diese Option ist standardmäßig deaktiviert. Sie müssen die Option über den Umschalter aktivieren, um die konfigurierte Timeout-Periode zu erzwingen. Wenn Sie den Umschalter jedoch nach dem Speichern der Konfiguration deaktivieren, leitet der Client kein Timeout ein.

     Eine Benachrichtigung wird 15 Minuten vor dem Sitzungsende angezeigt.

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

HINWEIS:

Wenn Sie mehr als eine dieser Einstellungen aktivieren, schließt das erste ablaufende Timeout-Intervall die Benutzerverbindung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsberichte

Kundenadministratoren können Konfigurationsberichte generieren, um Einblicke in die Secure Private Access-Einrichtung zu erhalten. Der Konfigurationsbericht enthält Informationen für die folgenden Kategorien:

- Zugriffsrichtlinien, die den Zugriff auf Anwendungen und Ressourcen regeln.
- Anwendungen, die in Secure Private Access konfiguriert sind.
- Routing-Domänen, die für die Anwendungen eingerichtet wurden.
- Ressourcenstandorte, die dem Kunden zugeordnet sind.
- Authentifizierungsdomäne, die zur Überprüfung von Benutzeridentitäten verwendet wird.
- Identitätsanbieter (IdP), der für die Benutzeridentität verwendet wird.
- Kundenparameter, die für einen bestimmten Kunden definiert sind.
- Store-Konfigurationen im Zusammenhang mit Cloud-Stores.

Die Konfigurationsberichte können in den folgenden Szenarien verwendet werden:

- Konfigurationsprobleme identifizieren und beheben.
- Zur Untersuchung und Fehlerbehebung mit dem Citrix Support-Team teilen.
- Verwenden Sie den Bericht als Referenz für eine neue Einrichtung oder ändern Sie vorhandene Einrichtungsdetails.

Einen Konfigurationsbericht generieren

Führen Sie die folgenden Schritte aus, um einen Konfigurationsbericht zu erstellen.

1. Gehen Sie in der Secure Private Access-Administratorkonsole zu **Einstellungen > Globale Konfiguration**.
2. Klicken Sie auf **Bericht erstellen**, um den Berichtserstellungsprozess zu starten.

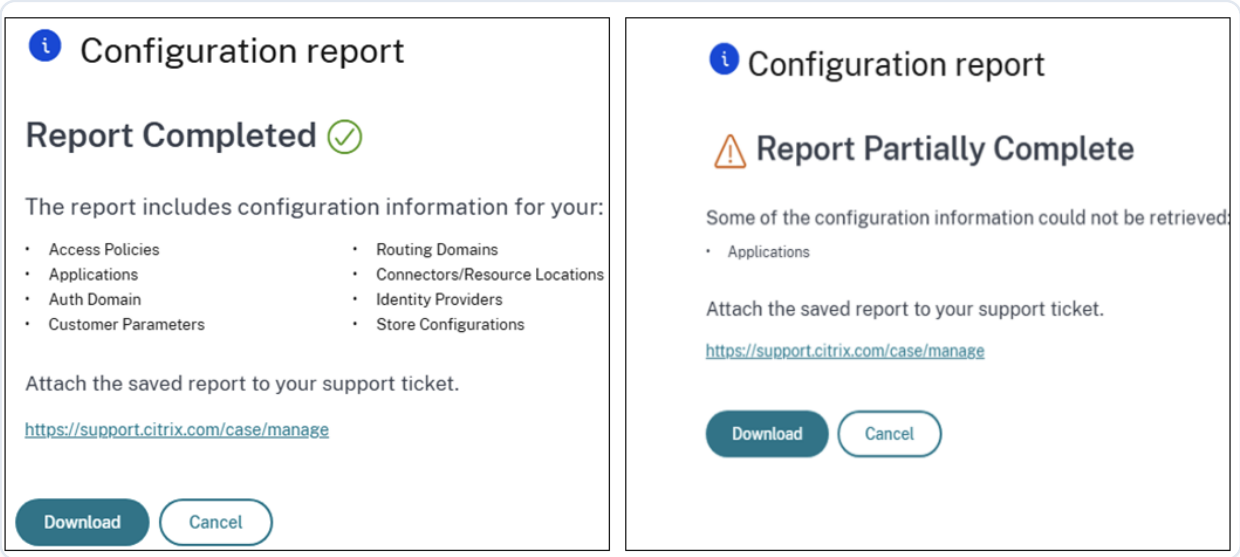
   Sobald der Bericht generiert wurde, zeigt das Dialogfeld **Konfigurationsbericht** den folgenden Status an:

   - **Bericht abgeschlossen:** Zeigt an, dass alle erforderlichen Details erfolgreich in den Bericht aufgenommen wurden.
   - **Bericht teilweise abgeschlossen:** Zeigt an, dass einige Details fehlen oder nicht generiert wurden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das Dialogfeld listet auch die Kategorien auf, für die die Berichtserstellung unvollständig war.

Die folgende Abbildung zeigt ein Beispiel für ein Dialogfeld „Konfigurationsbericht“ mit vollständigem und teilweise vollständigem Status.



3. Klicken Sie auf **Herunterladen**, um den Bericht manuell auf Ihr lokales Laufwerk zu exportieren.

WICHTIG:

Das Generieren von Konfigurationsberichten ist auf Administratoren mit den folgenden Secure Private Access-Rollen beschränkt:

- Administrator mit Vollzugriff
- Administrator mit Lesezugriff
- Administrator mit vollständiger Überwachung

Administratoren mit der Rolle des Helpdesk-Administrators können keine Konfigurationsberichte generieren.

ADFS-Integration mit Secure Private Access

Anspruchsregeln sind notwendig, um den Fluss von Ansprüchen durch die Anspruchspipeline zu steuern. Anspruchsregeln können auch verwendet werden, um den Anspruchsfluss während des Ausführungsprozesses der Anspruchsregel anzupassen. Weitere Informationen zu Ansprüchen finden Sie in der Microsoft-Dokumentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

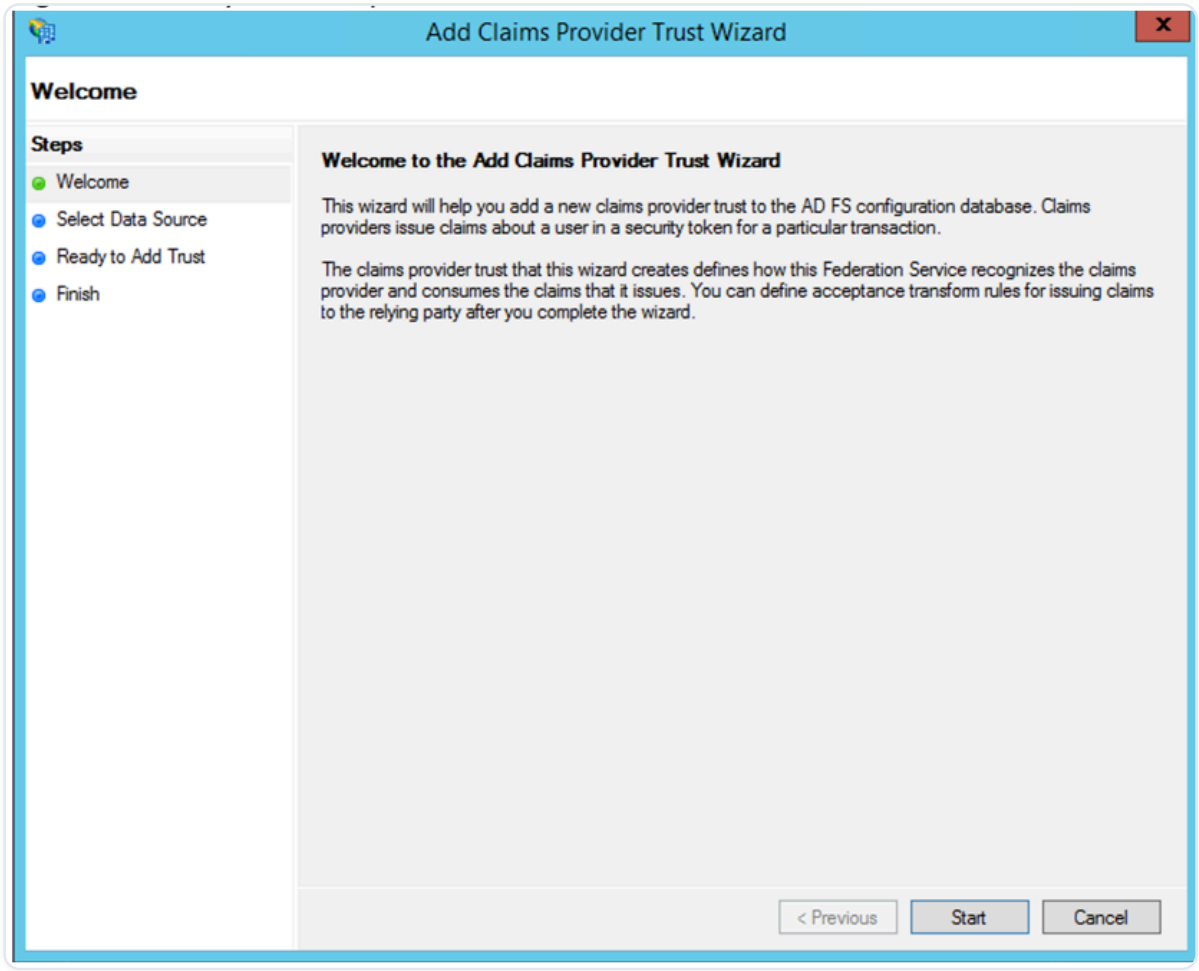
Um ADFS so einzurichten, dass es Ansprüche von Citrix Secure Private Access™ akzeptiert, müssen Sie die folgenden Schritte ausführen:

1. Anspruchsanbieter-Vertrauensstellung in ADFS hinzufügen.
2. Schließen Sie die App-Konfiguration auf Citrix Secure Private Access ab.

Anspruchsanbieter-Vertrauensstellung in ADFS hinzufügen

1. Öffnen Sie die ADFS-Verwaltungskonsole. Gehen Sie zu **ADFS > Vertrauensstellungen > Anspruchsanbieter-Vertrauensstellungen**.

   a. Klicken Sie mit der rechten Maustaste und wählen Sie **Anspruchsanbieter-Vertrauensstellung hinzufügen**.

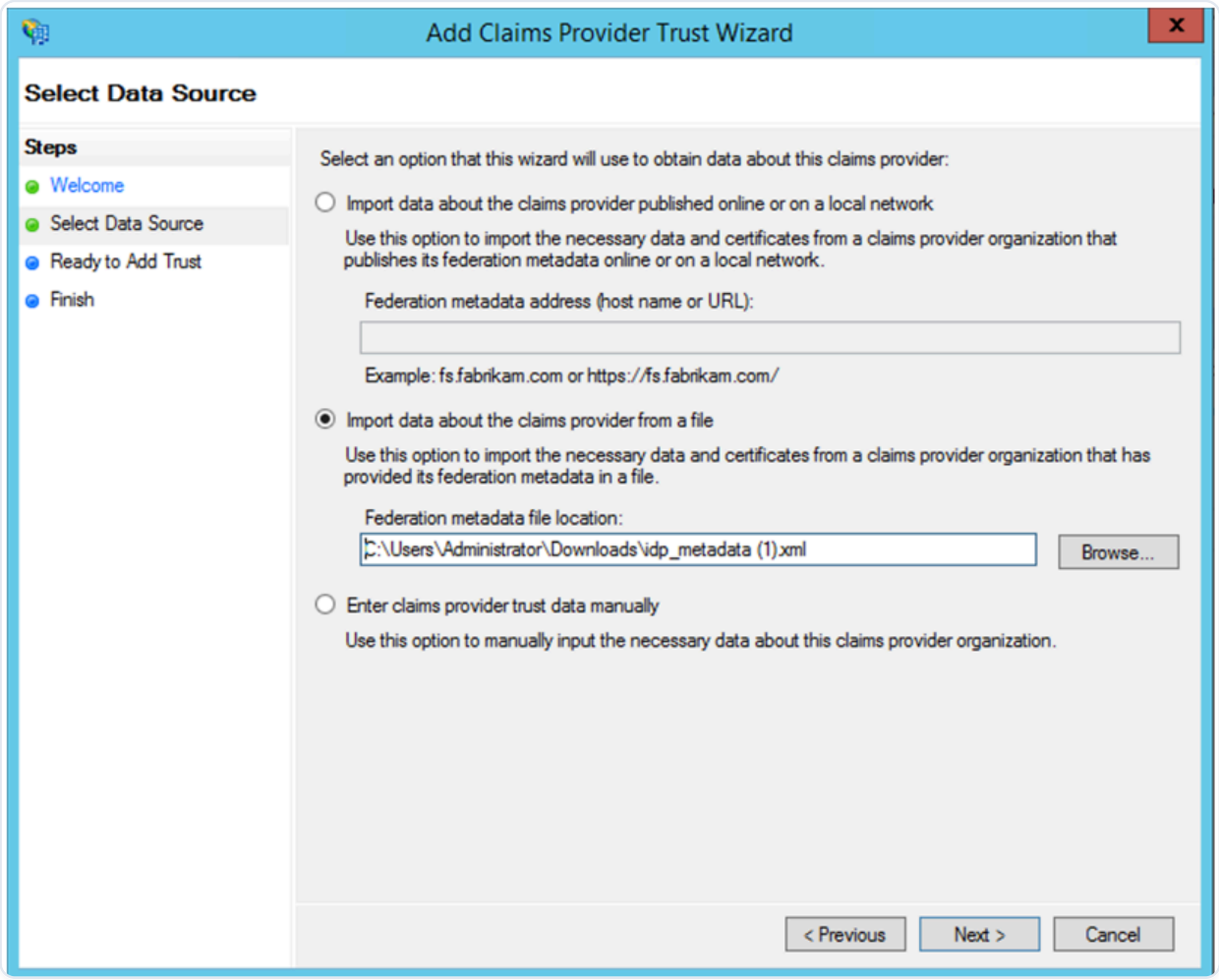


   b. Fügen Sie eine App in Secure Private Access hinzu, die zur Föderation mit ADFS verwendet wird. Weitere Informationen finden Sie unter App-Konfiguration auf Citrix Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

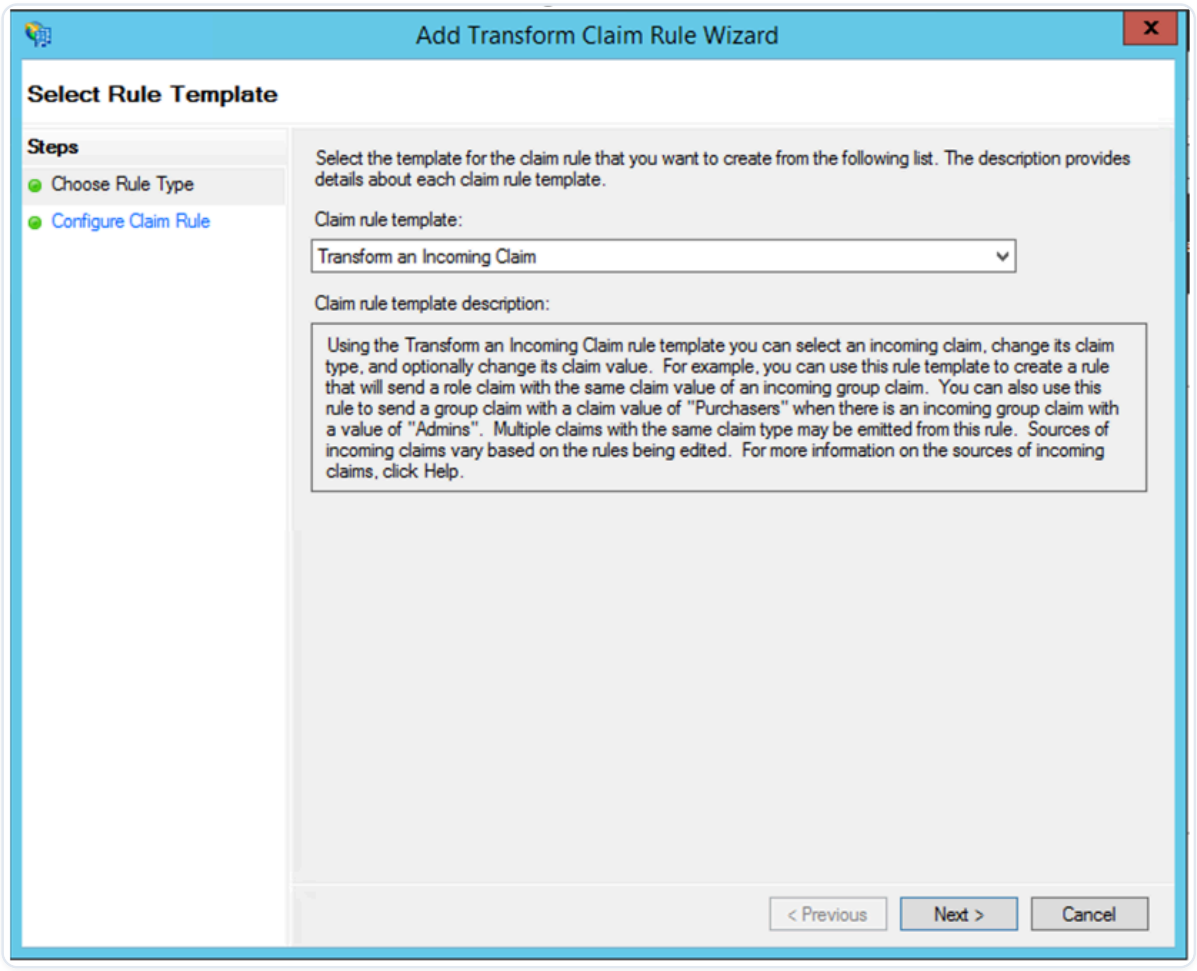
Fügen Sie zuerst die App hinzu, und aus dem SSO-Konfigurationsbereich der App können Sie die SAML-Metadatendatei herunterladen und die Metadatendatei dann in ADFS importieren.



a. Schließen Sie die Schritte ab, um die Anspruchsanbieter-Vertrauensstellung hinzuzufügen. Nachdem Sie die Anspruchsanbieter-Vertrauensstellung hinzugefügt haben, wird ein Fenster zum Bearbeiten der Anspruchsregel angezeigt.

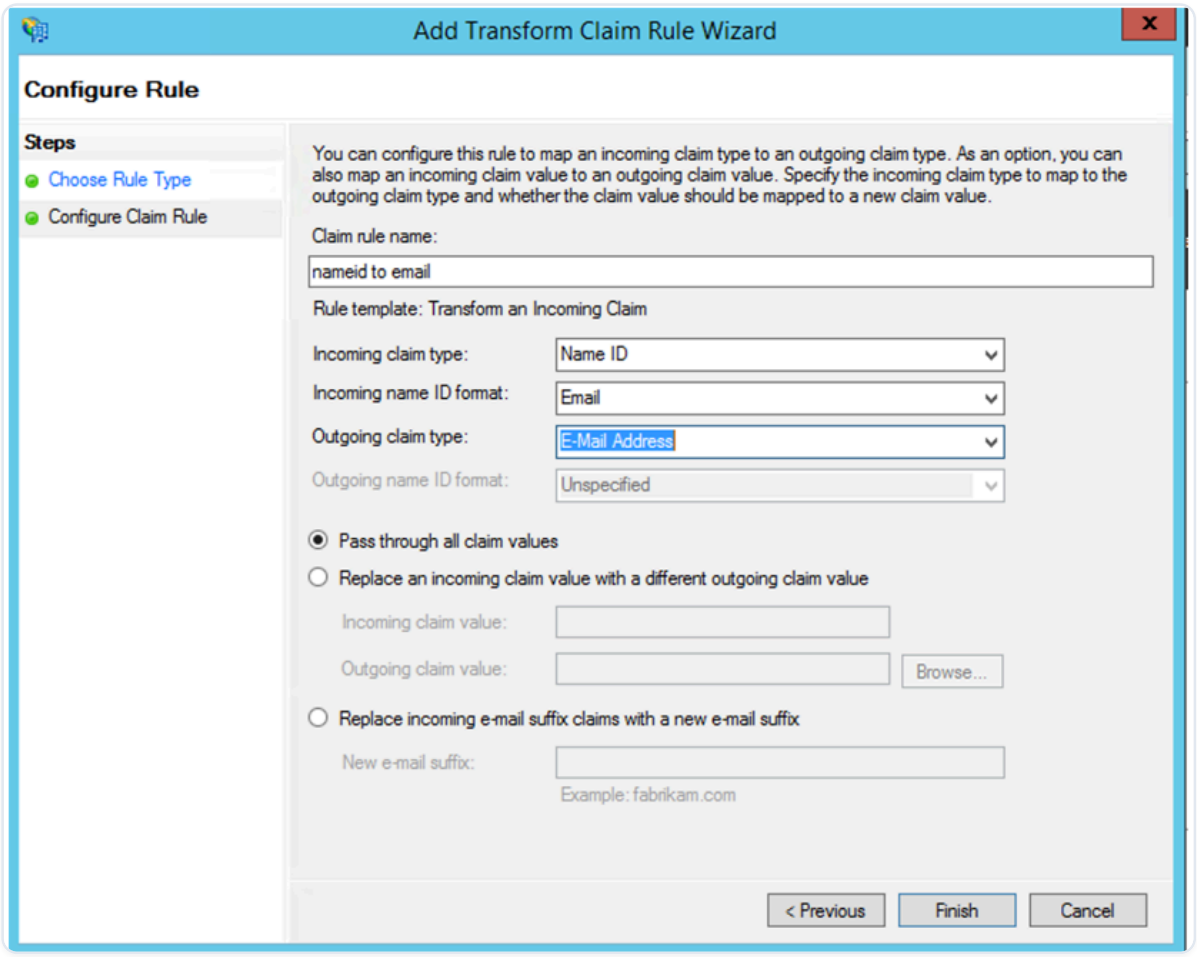
b. Fügen Sie eine Anspruchsregel mit **Eingehenden Anspruch transformieren** hinzu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. Schließen Sie die Einstellungen ab, wie in der folgenden Abbildung gezeigt. Wenn Ihr ADFS andere Ansprüche akzeptiert, verwenden Sie diese Ansprüche und konfigurieren Sie SSO in Secure Private Access entsprechend.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

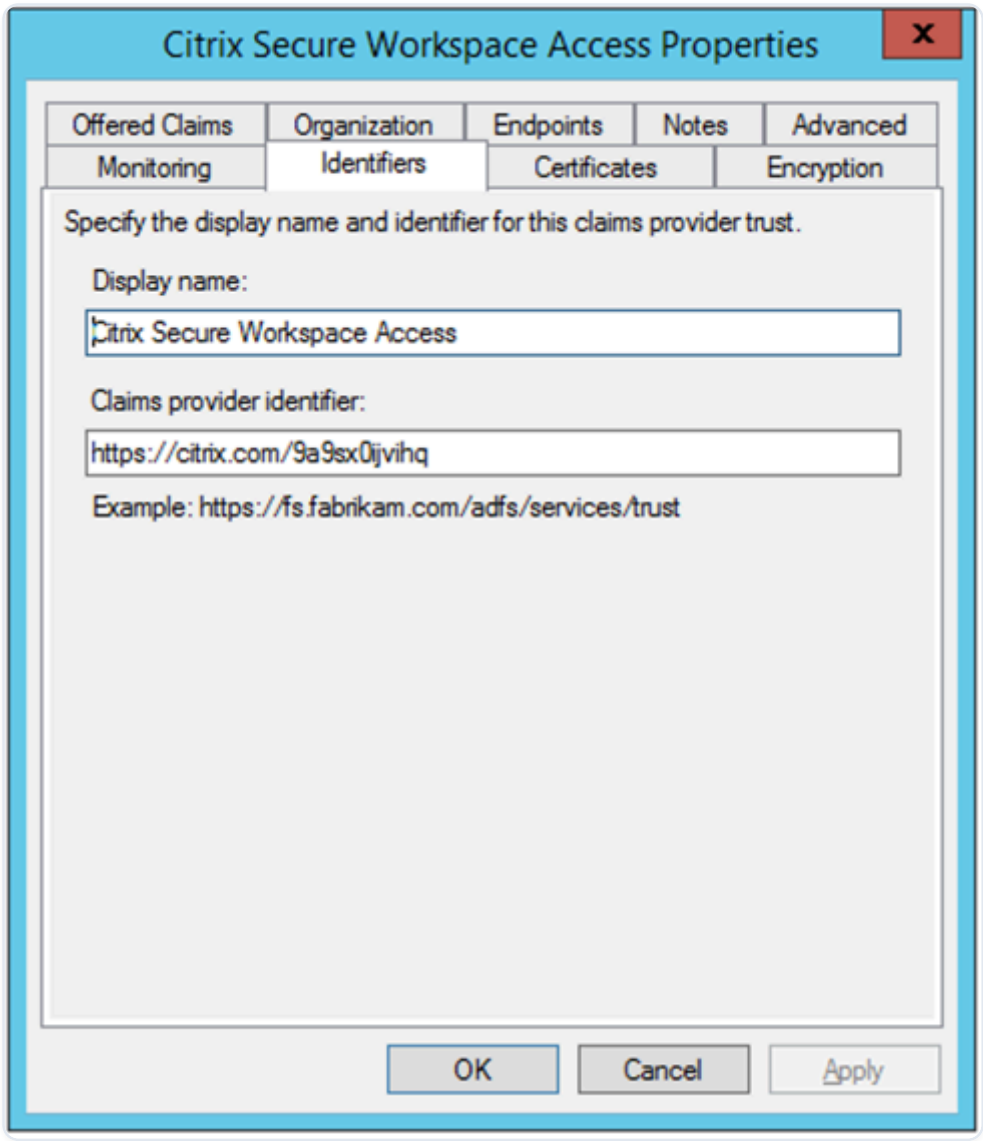


Sie haben nun die Anspruchsanbieter-Vertrauensstellung konfiguriert, die bestätigt, dass ADFS Citrix Secure Private Access für SAML vertraut.

ID der Anspruchsanbieter-Vertrauensstellung

Notieren Sie sich die ID der Anspruchsanbieter-Vertrauensstellung, die Sie hinzugefügt haben. Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.

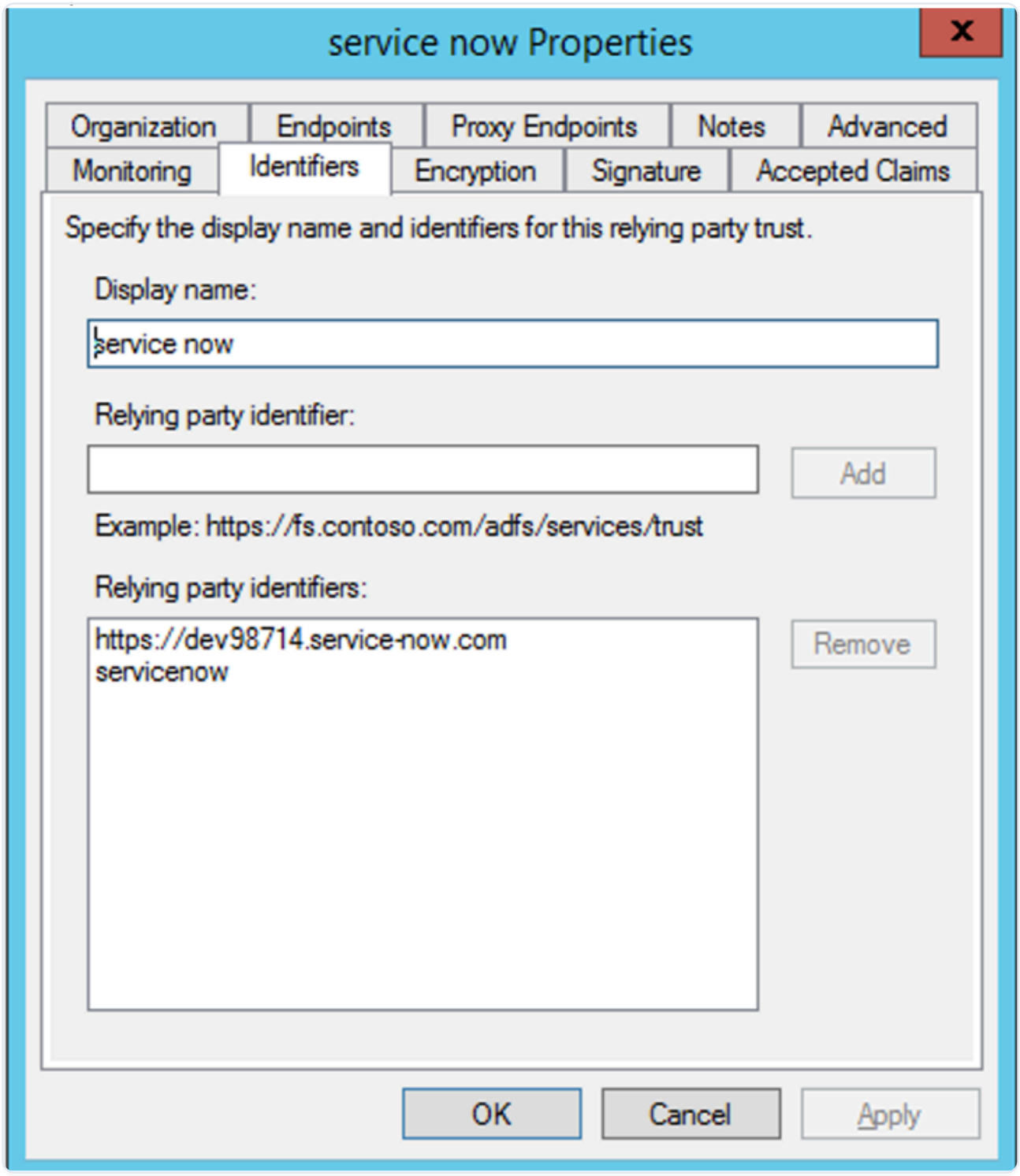
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Bezeichner der vertrauenden Seite

Wenn Ihre SaaS-App bereits mit ADFS authentifiziert wird, müssen Sie bereits die Vertrauensstellung der vertrauenden Seite für diese App hinzugefügt haben. Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Relay-Status im IdP-initiierten Fluss aktivieren

RelayState ist ein Parameter des SAML-Protokolls, der verwendet wird, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und zum Verbundserver der vertrauenden Seite weitergeleitet wurden. Wenn RelayState in ADFS nicht aktiviert ist, sehen Benutzer einen Fehler, nachdem sie sich bei den Ressourcenanbietern authentifiziert haben, die dies erfordern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für ADFS 2.0 müssen Sie das Update KB2681584 (Update Rollup 2) oder KB2790338 (Update Rollup 3) installieren, um RelayState-Unterstützung bereitzustellen. ADFS 3.0 verfügt über integrierte RelayState-Unterstützung. In beiden Fällen muss RelayState weiterhin aktiviert sein.

So aktivieren Sie den RelayState-Parameter auf Ihren ADFS-Servern

1. Öffnen Sie die Datei.
    - Geben Sie für ADFS 2.0 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.IdentityServer.Servicehost.exe.config
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 `IISReset` aus, um IIS neu zu starten.
3. Starten Sie für beide Plattformen die Active Directory-Verbunddienste `(adfssrv) service.` **Hinweis:** Wenn Sie Windows 2016 oder Windows 10 verwenden, verwenden Sie den folgenden PowerShell-Befehl, um es zu aktivieren. `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

Link zu Befehlen

App-Konfiguration in Citrix Secure Private Access

Sie können entweder den IdP-initiierten Flow oder den SP-initiierten Flow konfigurieren. Die Schritte zur Konfiguration des IdP- oder SP-initiierten Flows in Citrix Secure Private Access sind dieselben, außer dass Sie für den SP-initiierten Flow das Kontrollkästchen **App über die angegebene URL starten (SP-initiiert)** in der Benutzeroberfläche aktivieren müssen.

IdP-initiierter Flow

1. Beim Einrichten des IdP-initiierten Flows konfigurieren Sie 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 Ihrer ADFS-Einrichtung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **RP-ID** – Die RP-ID ist die ID, die Sie von Ihrem vertrauenden Parteienvertrauen erhalten. Sie ist identisch mit dem Bezeichner der vertrauenden Partei. Wenn es sich um eine URL handelt, erfolgt eine URL-Kodierung.
- **IdP-ID** – Die IdP-ID ist identisch mit der Vertrauens-ID des Anspruchsanbieters. Wenn es sich um eine URL handelt, erfolgt eine URL-Kodierung.

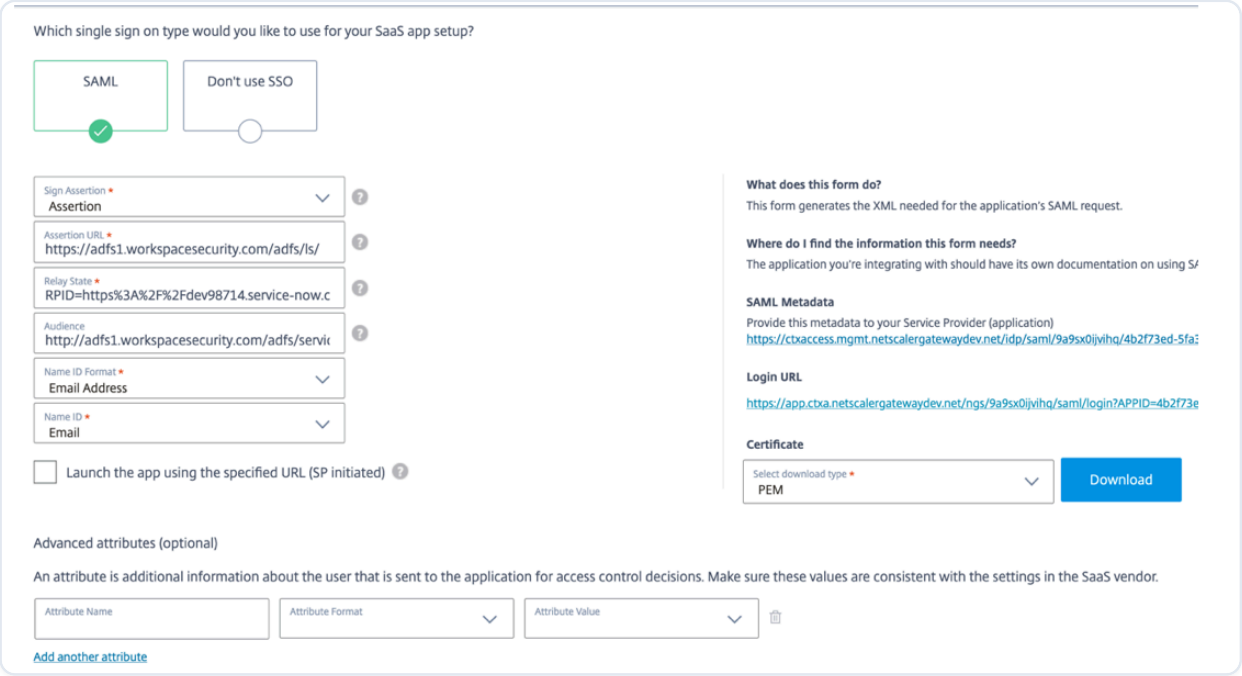
  Beispiel

2. SAML-SSO-Konfiguration.

   Dies sind die Standardwerte des ADFS-Servers. Wenn Werte geändert werden, rufen Sie die korrekten Werte aus den Metadaten des ADFS-Servers ab. Die Verbundmetadaten des ADFS-Servers können von seinem Verbundmetadaten-Endpunkt heruntergeladen werden, dessen Endpunkt unter **ADFS > Dienst > Endpunkte** ermittelt werden kann.

   - **Assertions-URL** – `https://<adfs fqdn>/adfs/ls/`
   - **Relay-Status** – Der Relay-Status ist wichtig für den IdP-initiierten Flow. Folgen Sie diesem Link, um ihn korrekt zu erstellen - Relay-Status

     Beispiel: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
   - **Zielgruppe** – `http://<adfsfqdn>/adfs/services/trust`
   - Die anderen SAML-SSO-Konfigurationseinstellungen finden Sie in der folgenden Abbildung. Weitere Informationen finden Sie unter Support für SaaS-Apps.



3. Speichern Sie die App und abonnieren Sie sie für den Benutzer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SP-initiierter Flow

Für den SP-initiierten Flow konfigurieren Sie die Einstellungen wie im Abschnitt **IDP-initiierter Flow** beschrieben. Aktivieren Sie zusätzlich das Kontrollkästchen **App über die angegebene URL starten (SP-initiiert)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Private Access Terraform-Provider

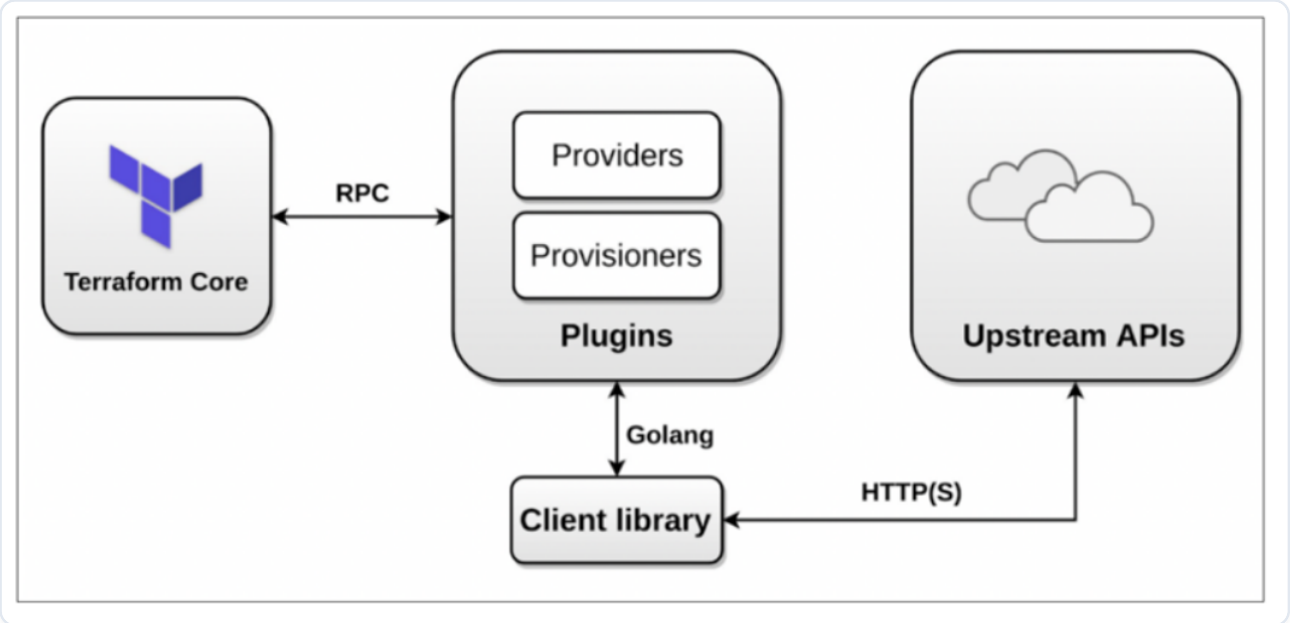
Die manuelle Verwaltung von Secure Private Access™-Konfigurationen über eine Benutzeroberfläche kann zeitaufwändig, fehleranfällig und schwierig über verschiedene Umgebungen hinweg zu skalieren sein. Kunden, die Infrastructure-as-Code-Praktiken anwenden, benötigen eine Möglichkeit, die Secure Private Access-Konfiguration zu automatisieren, Konsistenz zu gewährleisten und Secure Private Access-Änderungen in CI/CD-Pipelines zu integrieren.

Der Citrix Secure Private Access Terraform-Provider ermöglicht es Kunden, Secure Private Access-Ressourcen programmgesteuert mit Terraform bereitzustellen, zu konfigurieren und zu verwalten. Er ermöglicht die konsistente, wiederholbare und skalierbare Verwaltung von Secure Private Access-Umgebungen als Teil eines Infrastructure-as-Code-Workflows.

Der Citrix Secure Private Access Terraform-Provider ist anwendbar für:

- Citrix Secure Private Access Cloud-Bereitstellungen.
- Kunden, die Terraform für die Infrastruktur- oder Konfigurationsverwaltung verwenden.

Das folgende Diagramm zeigt die Architektur des Terraform-Providers:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hauptvorteile

Der Citrix Secure Private Access Terraform-Provider stellt Secure Private Access-Ressourcen als von Terraform verwaltete Objekte bereit. Kunden können die Secure Private Access-Konfiguration deklarativ definieren, sie zusammen mit der Anwendungsinfrastruktur versionieren und Änderungen auf vorhersehbare Weise anwenden.

Die Hauptvorteile der Verwendung dieser Lösung sind:

- Infrastructure-as-Code-Verwaltung für Secure Private Access.
- Konsistente Konfiguration über Umgebungen hinweg (Entwicklung, Test, Produktion).
- Reduzierter manueller Aufwand und Konfigurationsdrift.
- Einfache Integration in CI/CD-Pipelines und GitOps-Workflows.
- Schnelleres Onboarding und wiederholbare Bereitstellungen.

Anwendungsfall

Sie können den Citrix Secure Private Access Terraform-Provider für die folgenden Anwendungsfälle verwenden:

- Automatisieren Sie das Onboarding neuer Anwendungen/Richtlinien in Secure Private Access.
- Standardisieren Sie die Secure Private Access-Konfiguration über mehrere Umgebungen hinweg.
- Erstellen oder stellen Sie Secure Private Access-Umgebungen mithilfe des versionierten Terraform-Zustands wieder her.
- Integrieren Sie Secure Private Access-Konfigurationsänderungen in bestehende Terraform-Workflows.
- Ermöglichen Sie DevOps-Teams, Zugriffsrichtlinien zusammen mit der Infrastruktur zu verwalten.
- Migrieren Sie die Secure Private Access-Konfiguration von einem Test-Tenant zu einem Produktions-Tenant.
- Führen Sie die Secure Private Access-Konfiguration von 2 Kunden für Akquisitionsszenarien zusammen.

Systemanforderungen

Stellen Sie sicher, dass die folgenden Systemanforderungen erfüllt sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Terraform v1.3 oder höher.
- Zugriff auf einen Citrix Secure Private Access-Tenant.
- Netzwerkkonnektivität zu Citrix Cloud™ APIs.

Voraussetzungen

Bevor Sie den Citrix Secure Private Access Terraform Provider verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie verfügen über ein aktives Citrix Secure Private Access-Abonnement.
- Sie haben die Berechtigung, Secure Private Access-Ressourcen in Ihrem Citrix Tenant zu verwalten.
- Terraform ist in Ihrer Umgebung installiert und verfügbar.
- API-Anmeldeinformationen oder eine Authentifizierungsmethode für Citrix Cloud sind konfiguriert.

Berechtigungen

Das vom Terraform verwendete Service Principal Authentication-Konto muss über Berechtigungen verfügen, um:

- Secure Private Access-Ressourcen zu erstellen, zu aktualisieren und zu löschen.
- Die vorhandene Secure Private Access-Konfiguration für den Statusabgleich zu lesen.

Installation

Siehe Installieren von Terraform und Konfigurieren des Citrix Terraform Providers.

Terraform-Konfiguration

Mit dem Terraform-Provider kann die Secure Private Access-Konfiguration außerhalb der Citrix-Benutzeroberfläche verwaltet werden. Kunden können die Benutzeroberfläche bei Bedarf weiterhin verwenden, aber Terraform ist der empfohlene Ansatz für automatisierte und groß angelegte Bereitstellungen.

Um den Terraform-Provider für Secure Private Access zu verwenden, müssen Sie den Provider in Ihrer Terraform-Konfiguration wie folgt definieren:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
terraform {

  required_providers {

    citrixspa = {

      source = "citrix/citrixspa"

      version = `<version>`

    }

  }

}



provider "citrixspa" {

  base_url      = "<https://api.cloud.com/accessSecurity>"  # for
commercial deployment

  customer_id   = "xxxxxxxxxxxxx" # the CC customer id

  client_id     = "xxxxxxxxxxxxx" # client id of service principal

  client_secret = "xxxxxxxxxxxxx" # client secret of service principal

}
```

Nachdem der Provider konfiguriert ist, können Sie Secure Private Access-Ressourcen mithilfe von Terraform-Ressourcenblöcken definieren und diese mit Standard-Terraform-Befehlen anwenden, wie zum Beispiel:

- `terraform plan`
- `terraform apply`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Der Terraform-Provider ist standardmäßig aktiviert, nachdem er in der Terraform-Konfiguration deklariert und initialisiert wurde.

Fehlerbehebung

- **Der Vorgang `terraform apply` schlägt mit Authentifizierungsfehlern fehl.**

  Ursache: Ungültige oder fehlende Citrix Cloud-Anmeldeinformationen.

  Lösung: Überprüfen Sie die Authentifizierungskonfiguration und Berechtigungen des Providers.

- **Unerwartete Änderungen in `terraform plan` erkannt.**

  Ursache: Konfigurationsabweichungen aufgrund manueller UI-Änderungen.

  Lösung: Änderungen über Terraform abstimmen und bei Bedarf den Status aktualisieren.

Einschränkungen

- Möglicherweise sind nicht alle Secure Private Access-Funktionen in der ersten Provider-Version verfügbar.
- Direkt in der Benutzeroberfläche vorgenommene Änderungen können zu einer Abweichung des Terraform-Status führen.
- Die `terraform destroy`-Vorgänge entfernen möglicherweise nicht alle abhängigen Ressourcen automatisch.

Wichtige Überlegungen

- Terraform-Statusdateien können vertrauliche Konfigurationsdaten enthalten und müssen sicher gespeichert werden (z. B. Remote-Backends).
- Wir empfehlen, Secure Private Access-Ressourcen nach der Einführung ausschließlich mit Terraform zu verwalten.
- Wir empfehlen dringend, die Provider-Version festzulegen, um unerwartete Änderungen zu vermeiden.
- Überprüfen Sie immer die `terraform plan`-Ausgabe, bevor Sie Änderungen anwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Referenzen

- Terraform Registry-Dokumentation
- Terraform-Dokumentation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sichtbarkeit und Überwachung

Administratoren können die folgenden Funktionen/Ressourcen für die Sichtbarkeit und Überwachung von Secure Private Access nutzen.

Monitor

Secure Private Access ist in Monitor integriert, die Überwachungs- und Fehlerbehebungskonsole für Citrix DaaS. Administratoren und Helpdesk-Mitarbeiter können Web-/SaaS- und TCP/UDP-App-Sitzungen und -Ereignisse vom DaaS Monitor aus überwachen und Fehler beheben, zusätzlich zum Secure Private Access-Dashboard. Weitere Informationen finden Sie unter Integration mit DaaS Monitor.

Secure Private Access-Nutzungs-Dashboard

Die Sichtbarkeit der Secure Private Access-Benutzer, -Anwendungen, -Richtlinien und des Connector-Status ist im Secure Private Access-Dashboard verfügbar. Administratoren können das Dashboard verwenden, um diese Ereignisse zu überwachen. Weitere Informationen finden Sie unter Dashboard.

Secure Private Access-Anwendungs- und Sitzungsüberwachung

Überwachen Sie Ihre Secure Private Access-Sitzungen und Anwendungstrends in Ihrem gesamten Unternehmen mithilfe von Citrix Monitor. Weitere Informationen finden Sie in den folgenden Themen:

- Monitor bietet Filterfunktionen für die Sitzungen und Anwendungen, was die Analyse von Benutzeraktivitäten und die Behebung von Problemen mit der Anwendungsleistung erleichtert. Weitere Informationen finden Sie unter Sitzungs- und Anwendungsüberwachung.
- Administratoren können die Sitzungs- und Fehlertrends in Monitor anzeigen, die helfen, Muster zu erkennen und Probleme zu beheben. Weitere Informationen finden Sie unter Fehler- und Sitzungstrends.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connector Appliance-Zustandsüberwachung

Die Connector Appliance-Komponente wird automatisch als Teil der Infrastrukturüberwachung hinzugefügt, wenn Sie Secure Private Access bereitstellen. Jede Connector Appliance, die mit der Citrix DaaS-Site verbunden ist, wird automatisch für eine umfassende Überwachung integriert, was Administratoren Echtzeit-Einblicke in den Zustand und die Leistung dieser kritischen Infrastrukturkomponenten bietet.

Weitere Informationen zur Connector Appliance-Zustandsüberwachung finden Sie unter Connector Appliance-Zustandsmetriken.

Secure Private Access Nutzungs-Dashboard

Das Secure Private Access-Dienst-Dashboard zeigt die Diagnose- und Nutzungsdaten der SaaS-, Web-, TCP- und UDP-Apps an. Das Dashboard bietet Administratoren einen vollständigen Überblick über ihre Apps, Benutzer, den Integritätsstatus der Konnektoren und die Bandbreitennutzung an einem einzigen Ort zur Nutzung. 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. Für einige der Entitäten können Sie Details anzeigen, indem Sie einen Drilldown durchführen.

Die Metriken werden grob in die folgenden Kategorien eingeteilt.

- **Protokollierung und Fehlerbehebung**
  - Diagnoseprotokolle: Protokolle im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Enumeration und Geräteintegritätsprüfungen.
- **Benutzer**
  - Aktive Benutzer: Gesamtzahl der eindeutigen Benutzer, die während des ausgewählten Zeitintervalls auf die Anwendungen (SaaS, Web und TCP) zugreifen.
  - Uploads: Gesamtes Datenvolumen, das über den Secure Private Access-Dienst für das ausgewählte Zeitintervall hochgeladen wurde.
  - Downloads: Gesamtes Datenvolumen, das über den Secure Private Access-Dienst für das ausgewählte Zeitintervall heruntergeladen wurde.
- **Anwendungen:**
  - Anwendungen: Gesamtzahl der aktuell konfigurierten Anwendungen (unabhängig vom Zeitintervall).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

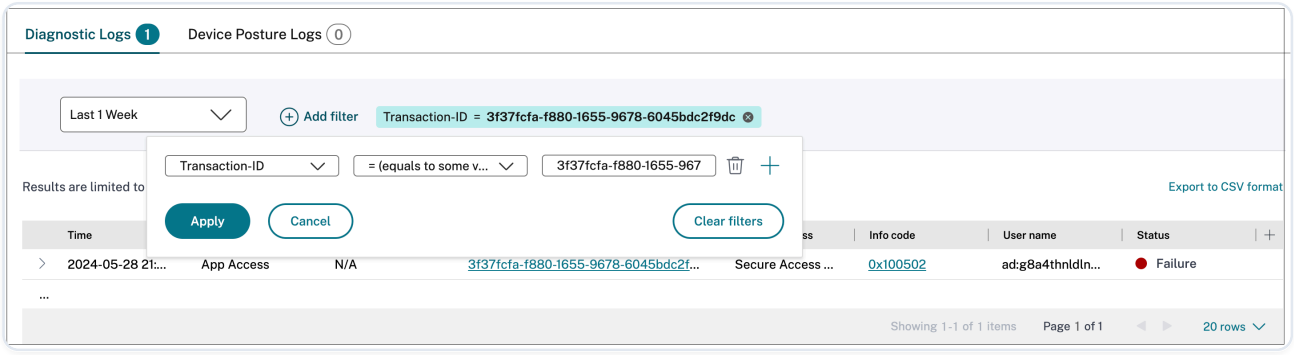
- Anwendungsstartanzahl: Gesamtzahl der Anwendungen (App-Sitzungen), die von jedem Benutzer für das ausgewählte Zeitintervall gestartet wurden.
- Konfigurierte Domänen: Gesamtzahl der für das ausgewählte Zeitintervall konfigurierten Domänen.
- Erkannte Anwendungen: Gesamtzahl der eindeutigen, einzelnen Domänen, auf die zugegriffen wurde, die aber keiner App zugeordnet sind.

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

Diagnoseprotokolle

Verwenden Sie das Diagramm **Diagnoseprotokolle**, um die Protokolle bezüglich Authentifizierung, Anwendungsstart, App-Aufzählung und auch Protokolle bezüglich des Gerätestatus anzuzeigen. Sie können auf den Link **Mehr anzeigen** klicken, um die Details der Protokolle anzuzeigen. Die Details werden in einem Tabellenformat dargestellt. Sie können die Protokolle für die voreingestellte Zeit oder für einen benutzerdefinierten Zeitraum 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.

- Sie können die Option **Filter hinzufügen** verwenden, um Ihre Suche basierend auf verschiedenen Kriterien wie App-Typ, Kategorie, Beschreibung zu verfeinern. Zum Beispiel können Sie in den Suchfeldern `Transaction ID`, `= (equals to some value)` auswählen und `7456c0fb-a60d-4bb9-a2a2-edab8340bb15` in dieser Reihenfolge eingeben, um alle Protokolle zu suchen, die mit dieser Transaktions-ID zusammenhängen. Details zu Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.

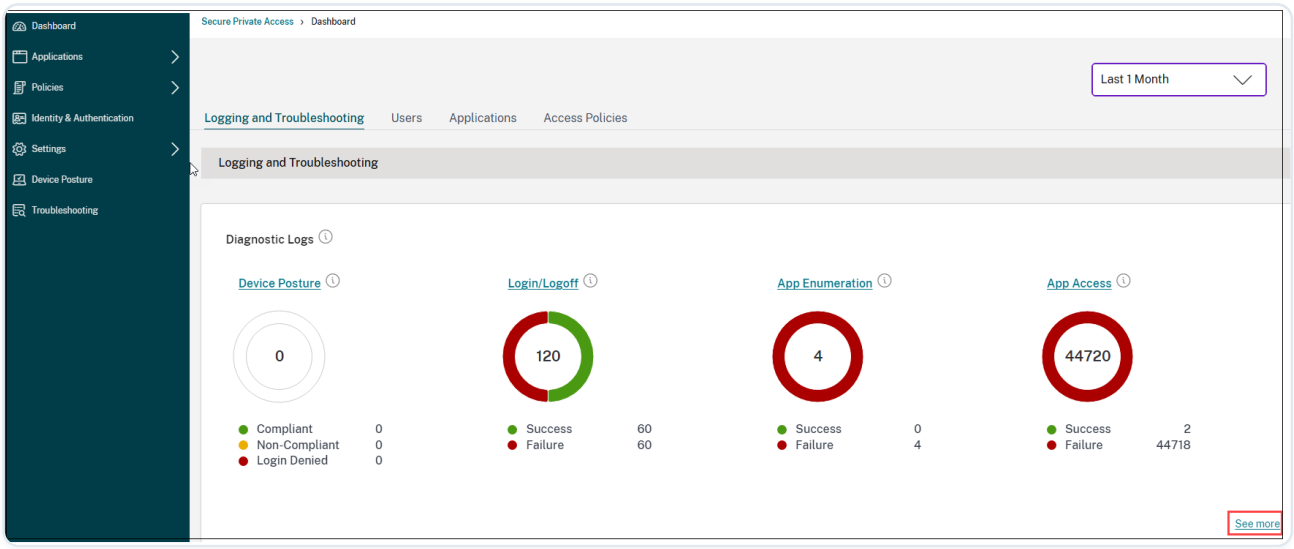


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Protokolle zum Gerätestatus:** Sie können Ihre Suche basierend auf den Richtlinienergebnissen (**Konform, Nicht konform und Anmeldung verweigert**) verfeinern. Details zum Gerätestatus finden Sie unter Gerätestatus.

HINWEIS:

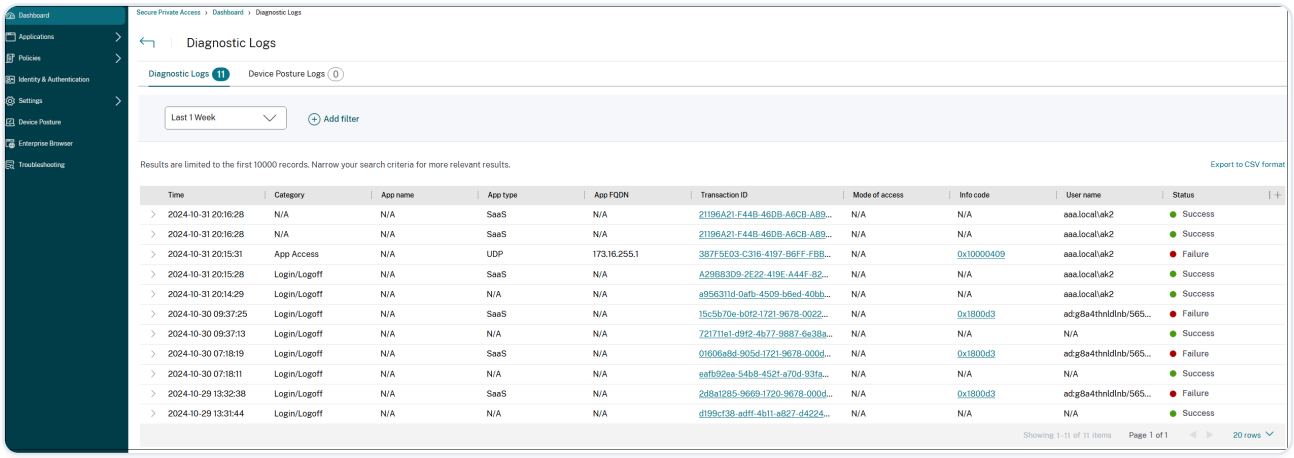
- Jedes Fehlerereignis im Dashboard der Secure Private Access-Diagnoseprotokolle hat einen zugehörigen Infocode. Details finden Sie unter Infocode.
- Die Transaktions-ID korreliert alle Secure Private Access-Protokolle für eine Zugriffsanforderung. Details finden Sie unter Transaktions-ID.



- Sie können auf das erweitern-Symbol (>) klicken, um die vollständigen Details der Protokolle anzuzeigen.
- Die Seite **Diagnoseprotokolle** zeigt die eingebetteten Domänen für jede der aufgerufenen Haupt-URLs an. Administratoren können die eingebetteten Domänen anzeigen, indem sie auf das erweitern-Symbol (>) der Haupt-URL klicken. Administratoren können die Liste der eingebetteten Domänen verwenden, um Probleme im Zusammenhang mit dem App-Zugriff oder der App-Darstellung zu beheben. Wenn beispielsweise eine Domäne in der Anwendungskonfiguration fehlte, kann die spezifische App vom Endbenutzer nicht aufgerufen werden. 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.

Standardmäßig zeigt die Seite **Diagnoseprotokolle** die Daten der aktuellen Woche und nur die letzten 10000 Datensätze an. Verwenden Sie die benutzerdefinierte Datumssuche und Filter, um Ihre Suchergebnisse weiter zu verfeinern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

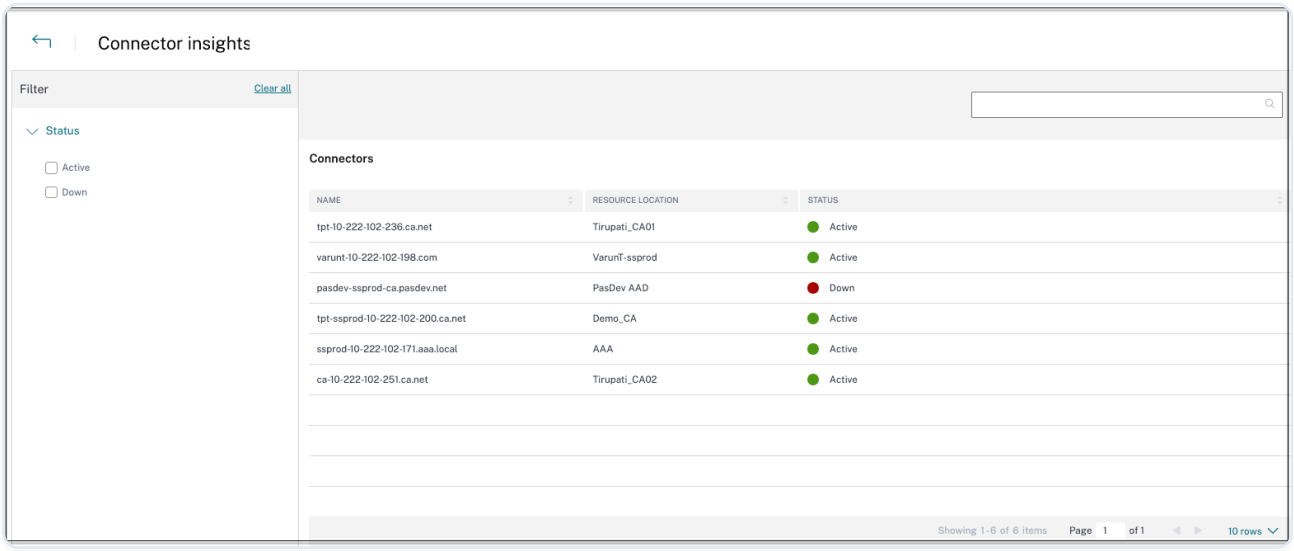


WICHTIG:

Eine umfassende Liste der Fehler, die Benutzern bei der Verwendung des Secure Private Access-Dienstes begegnen können, finden Sie unter Info-Code-Nachschlagetabelle.

Konnektorstatus

Verwenden Sie das Diagramm **Konnektorstatus**, um den Status der Konnektoren und der Ressourcenstandorte anzuzeigen, an denen die Konnektoren bereitgestellt werden. Klicken Sie auf den Link **Mehr anzeigen**, um die Details anzuzeigen. Auf der Seite **Konnektor-Einblicke** können Sie die Filter **Aktiv** oder **Inaktiv** verwenden, um die Konnektoren nach ihrem Status zu filtern.

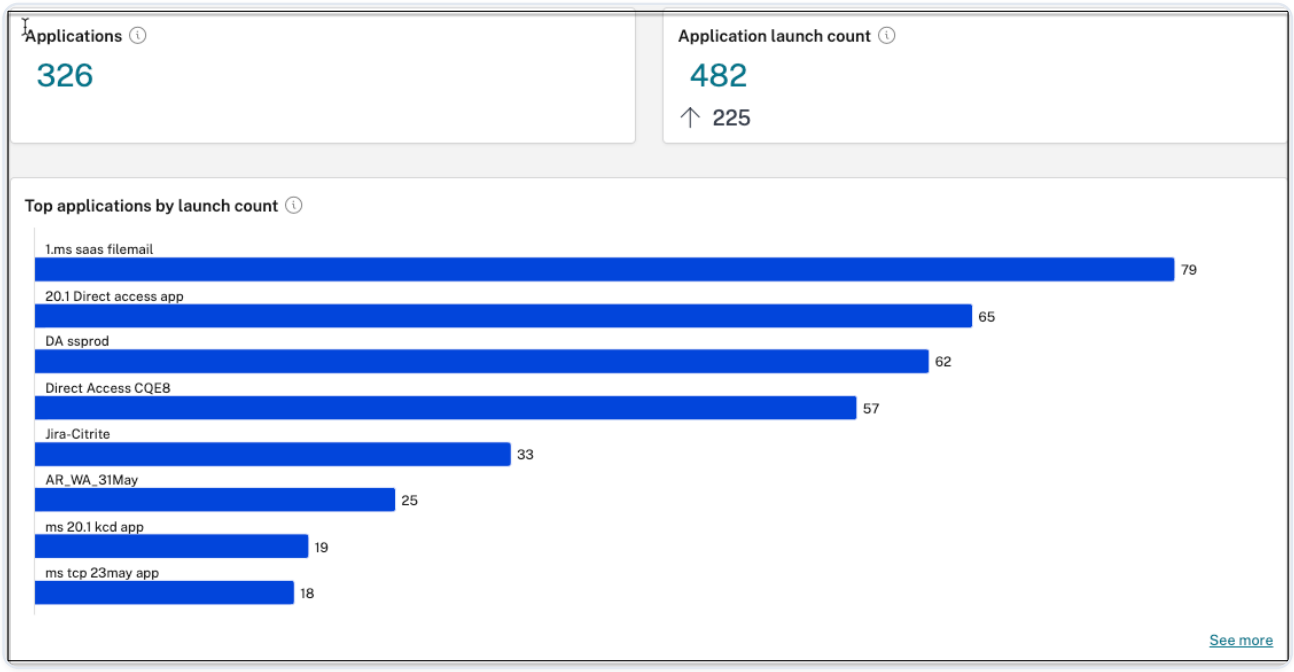


Top-Anwendungen nach Startanzahl

Verwenden Sie das Diagramm **Top-Anwendungen nach Startanzahl**, um die Liste der Top-Anwendungen anzuzeigen, basierend auf der Häufigkeit des App-Starts, dem gesamten Datenvolumen, das auf den App-Server hochgeladen wurde, und dem gesamten Datenvolumen,

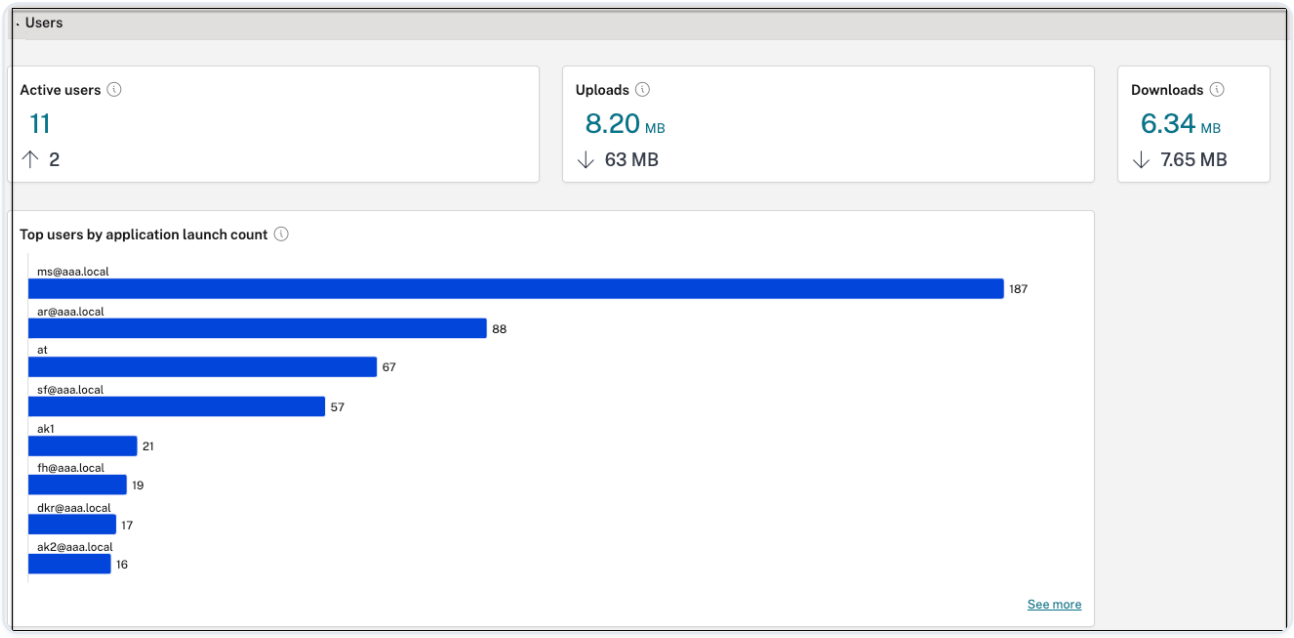
© 1997–2026 Citrix Systems, Inc. All rights reserved.

das vom App-Server heruntergeladen wurde. Sie können die Filter **SaaS-Apps**, **Web-Apps** oder **TCP/UDP-Apps** anwenden, um Ihre Suche auf bestimmte Apps einzugrenzen. Sie können die Daten für einen voreingestellten oder einen benutzerdefinierten Zeitrahmen filtern.



Top-Benutzer nach Anwendungsstartanzahl

Verwenden Sie das Diagramm **Top-Benutzer nach Anwendungsstartanzahl**, um die Daten pro Benutzer anzuzeigen. Zum Beispiel die Häufigkeit, mit der ein Benutzer die TCP-App gestartet hat, das gesamte Datenvolumen, das auf den App-Server hochgeladen wurde, und das gesamte Datenvolumen, das vom App-Server heruntergeladen wurde. Sie können die Daten für einen voreingestellten oder einen benutzerdefinierten Zeitrahmen filtern.



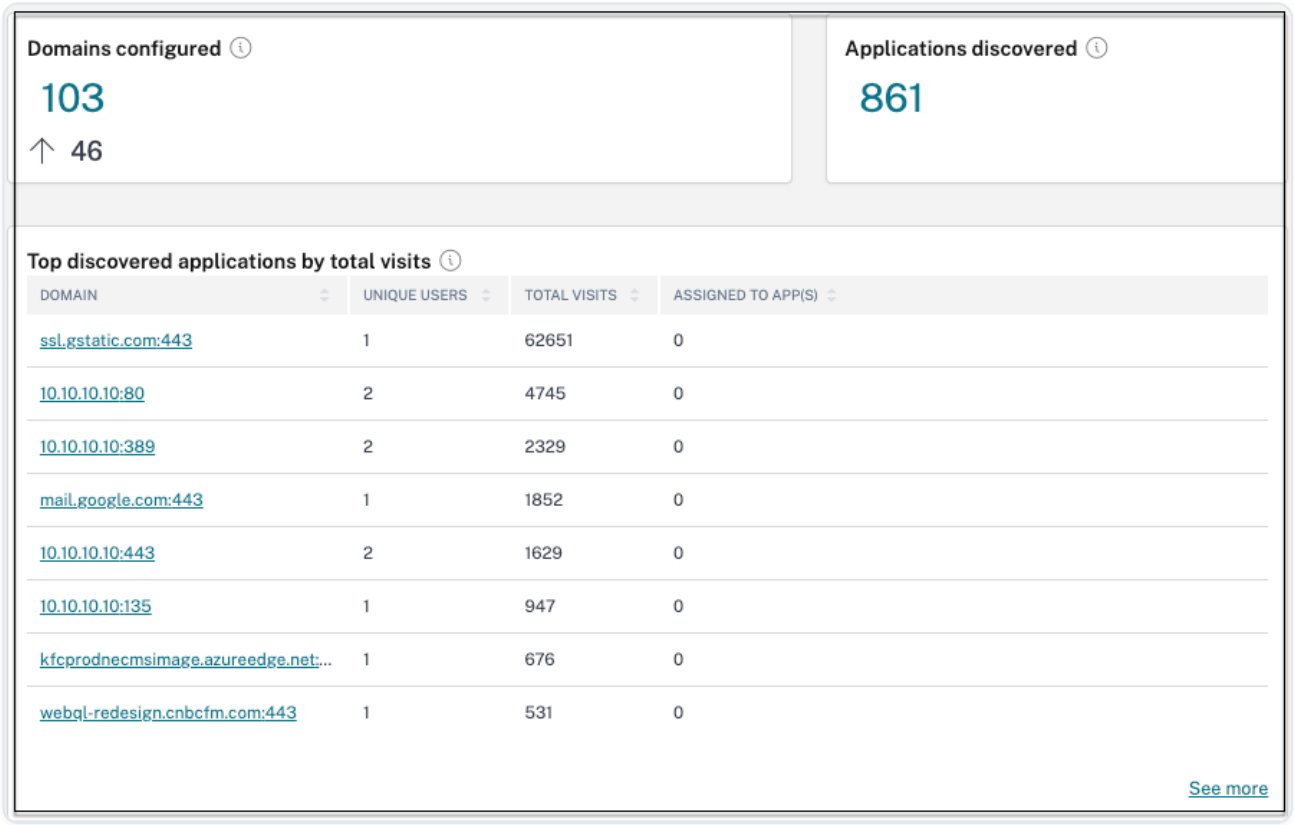
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Top-Zugriffsrichtlinien nach Durchsetzung

Verwenden Sie das Diagramm **Top-Zugriffsrichtlinien nach Durchsetzung**, um die Liste der Zugriffsrichtlinien anzuzeigen, die für die Apps erzwungen werden. Klicken Sie auf den Link **Mehr anzeigen**, um die Liste der Richtlinien anzuzeigen, die den Apps zugeordnet sind, und wie oft die Richtlinien erzwungen werden. Sie können auch die Option **Suchen** auf der Seite Zugriffsrichtlinien verwenden, um die Richtlinien nach dem Richtliniennamen zu filtern. Sie können auch nach bestimmten Richtlinien suchen, indem Sie die Suchoperatoren verwenden, um Ihre Suche weiter zu verfeinern. Weitere Informationen finden Sie unter Suchoperatoren.

Top-erkannte Anwendungen

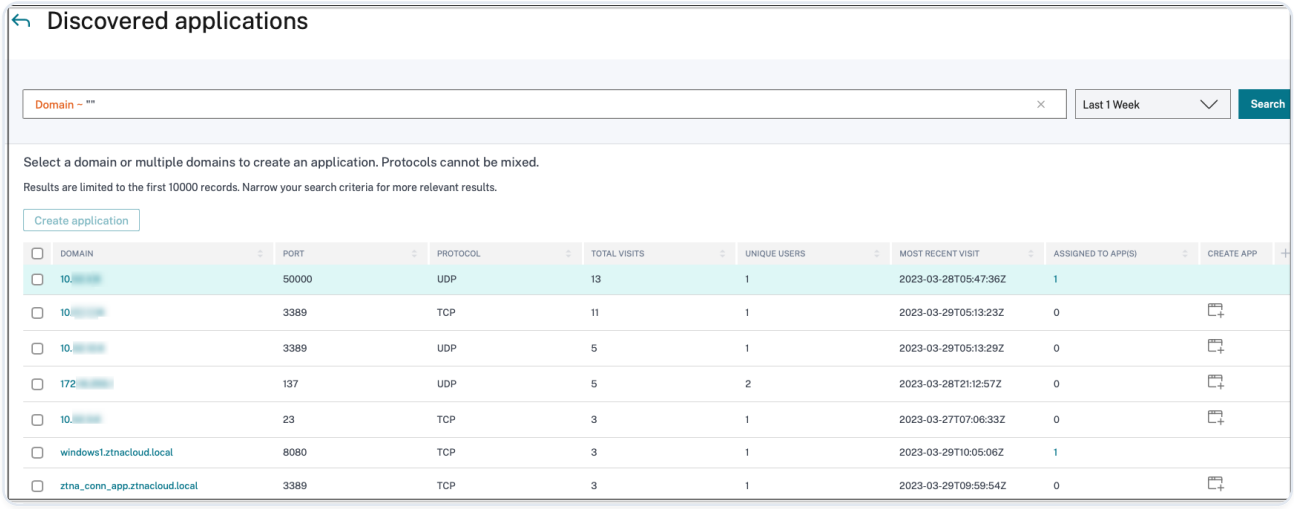
Verwenden Sie die **Top-erkannten Anwendungen nach Gesamtbesuchen**, um die Liste der eindeutigen, einzelnen Domänen anzuzeigen, auf die irgendwann zugegriffen wurde, die aber keiner App zugeordnet sind. Diese Domänen werden basierend auf der Gesamtzahl der Besuche dieser Domänen aufgelistet. Administratoren können dieses Diagramm verwenden, um zu sehen, ob eine Domäne von besonderem Interesse von vielen Benutzern aufgerufen wird. In solchen Fällen können Administratoren eine App mit dieser Domäne für einen einfachen Zugriff erstellen.



In der Tabelle zeigt die Spalte **ZU APPS ZUGEWIESEN** die Gesamtzahl der Anwendungen an, für die diese Domäne als Teil ihrer zugehörigen URL- oder Ziel-URL-Werte konfiguriert ist. Durch Klicken auf die Zahl werden die Apps angezeigt, die dieser Domäne zugewiesen sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



Die Seite **Entdeckte Anwendungen** zeigt die Details der Domänen an, wie Domänenname, Port, Protokoll, Gesamtbesuche, eindeutige Benutzer und das Datum des letzten Besuchs. Alle Spalten in der Tabelle sind sortierbar. Sie können die Suchleiste verwenden, um nach Domäne zu suchen.

HINWEIS:

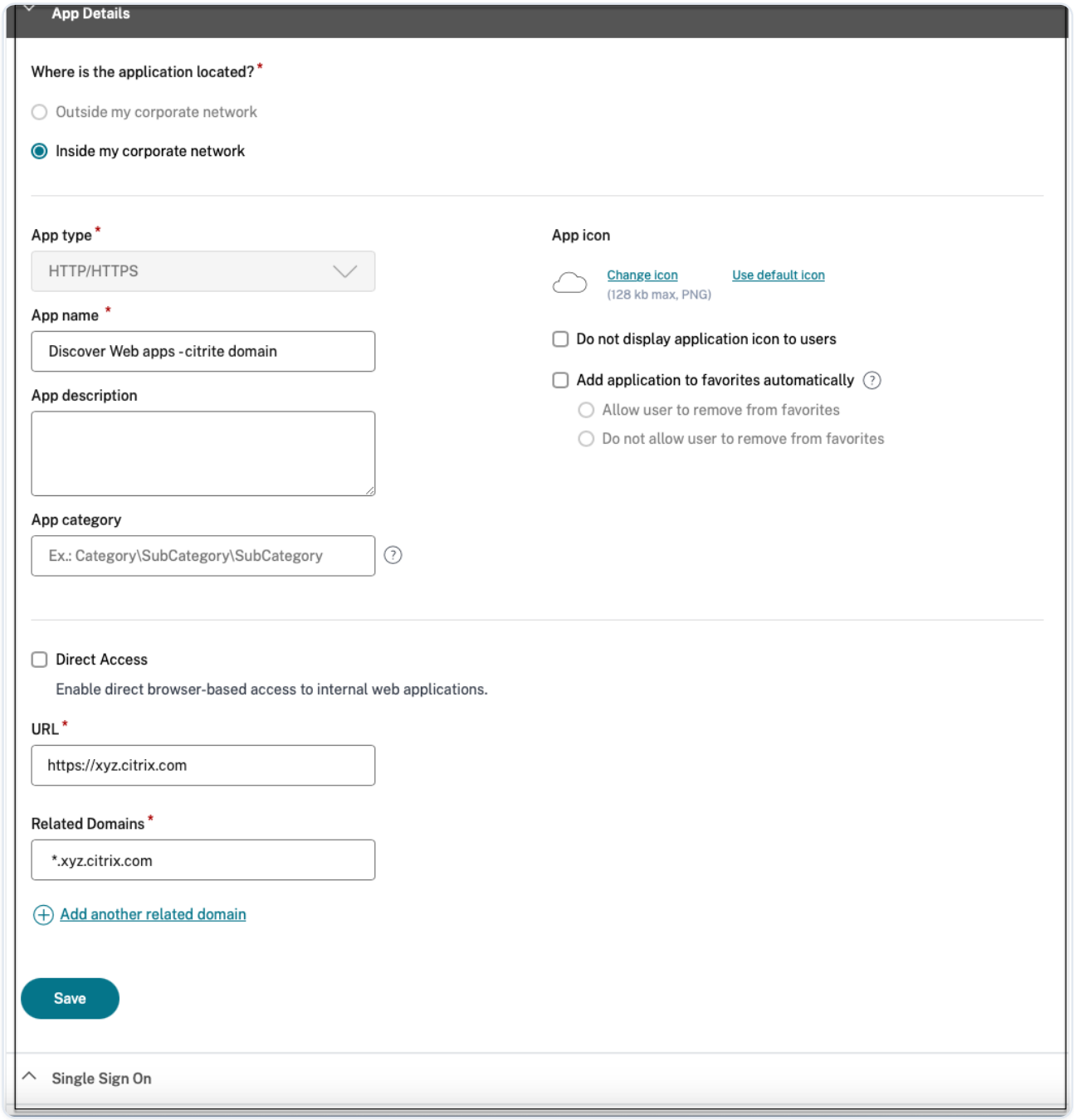
- Die Protokolle werden basierend auf den von Kunden verwendeten Standardports abgeleitet.
- Die Liste der entdeckten Domänen ist auf 10000 Einträge begrenzt.

Erstellen einer App aus der Tabelle

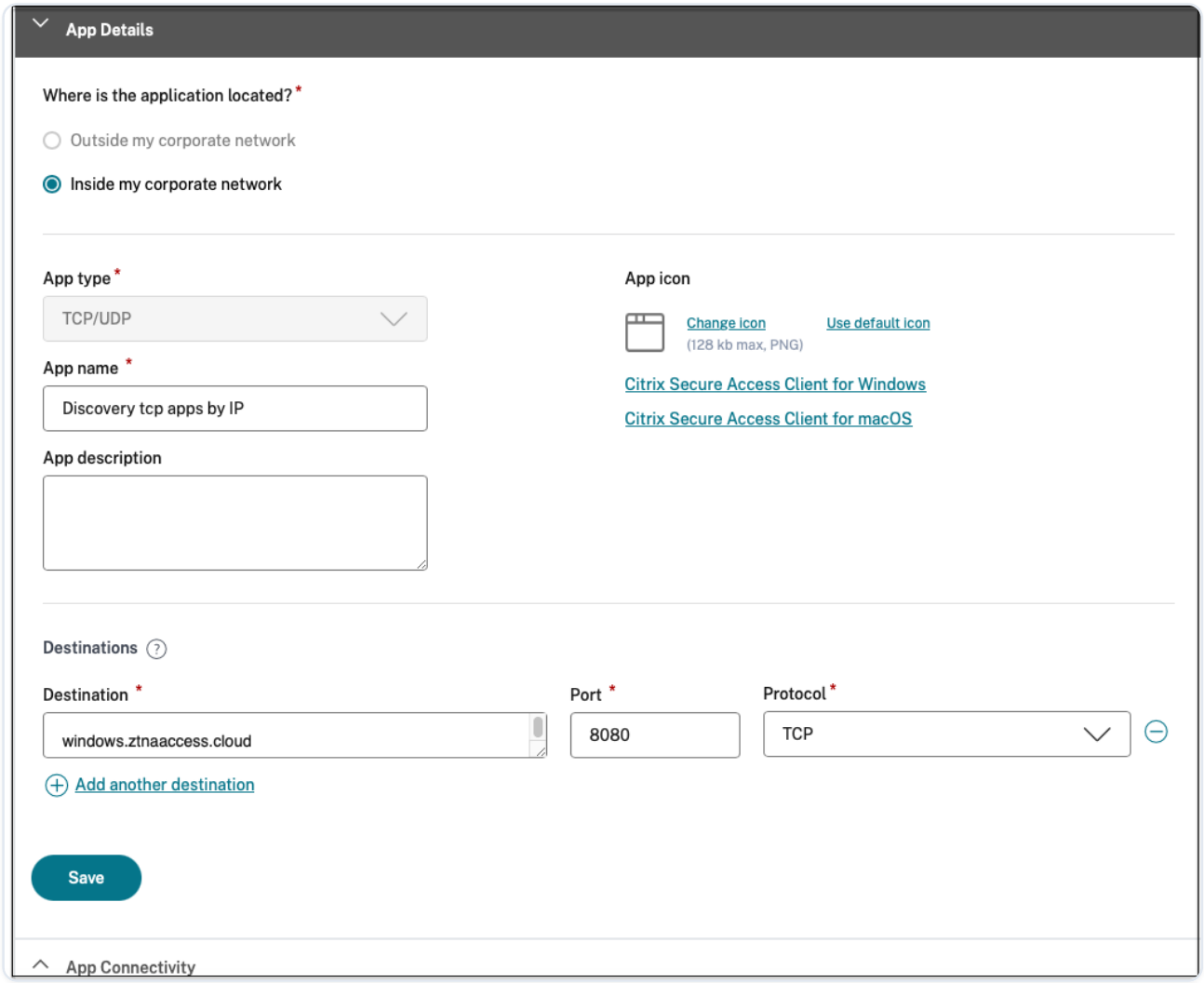
Klicken Sie auf das **+**-Symbol in der Zeile der jeweiligen Domäne, um eine App zu erstellen. Der App-Konfigurationsassistent wird angezeigt. Das Symbol zum Erstellen einer App wird nicht für Zeilen angezeigt, in denen bereits eine App mit derselben Domänen-, Port- und Protokollkombination erstellt wurde und sich im vollständigen Zustand 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 Informationen finden Sie unter Administratorgeführter Workflow für einfaches Onboarding und Einrichtung.

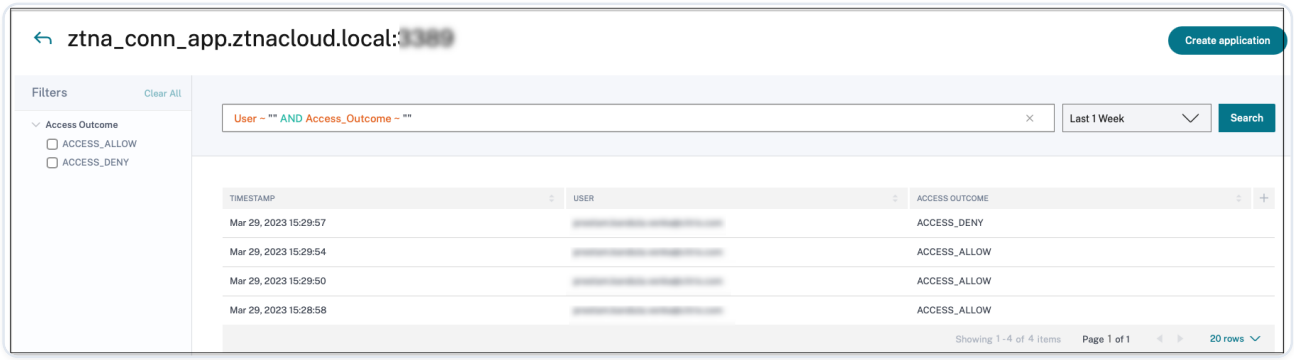
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sie können auch auf den Link der eindeutigen Domäne 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

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

- **= (entspricht einem Wert)**: Zum Suchen nach Protokollen/Richtlinien, die genau den Suchkriterien entsprechen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Secure Private Access-Anwendungen, -Sitzungen und -Trends

Secure Private Access ist in Monitor integriert, die Überwachungs- und Fehlerbehebungskonsole für Citrix DaaS. Administratoren und Helpdesk-Mitarbeiter können diese Integration nutzen, um Web/SaaS- und TCP/UDP-Anwendungssitzungen und -Ereignisse über die DaaS Monitor-Konsole zu überwachen und Fehler zu beheben. Dies bietet zusätzliche Überwachungsfunktionen, die das Secure Private Access-Dashboard ergänzen.

Um die DaaS Monitor-Funktion mit Secure Private Access zu verwenden, müssen Sie sowohl Secure Private Access- als auch DaaS-Berechtigungen besitzen.

Sie können über das Secure Private Access-Dashboard (**Zu Monitor wechseln**) oder über die Citrix DaaS-Dienstkachel auf Monitor zugreifen.

Weitere Informationen zur Integration mit Monitor finden Sie unter Secure Private Access.

Anwendungen, Sitzungen und Trends

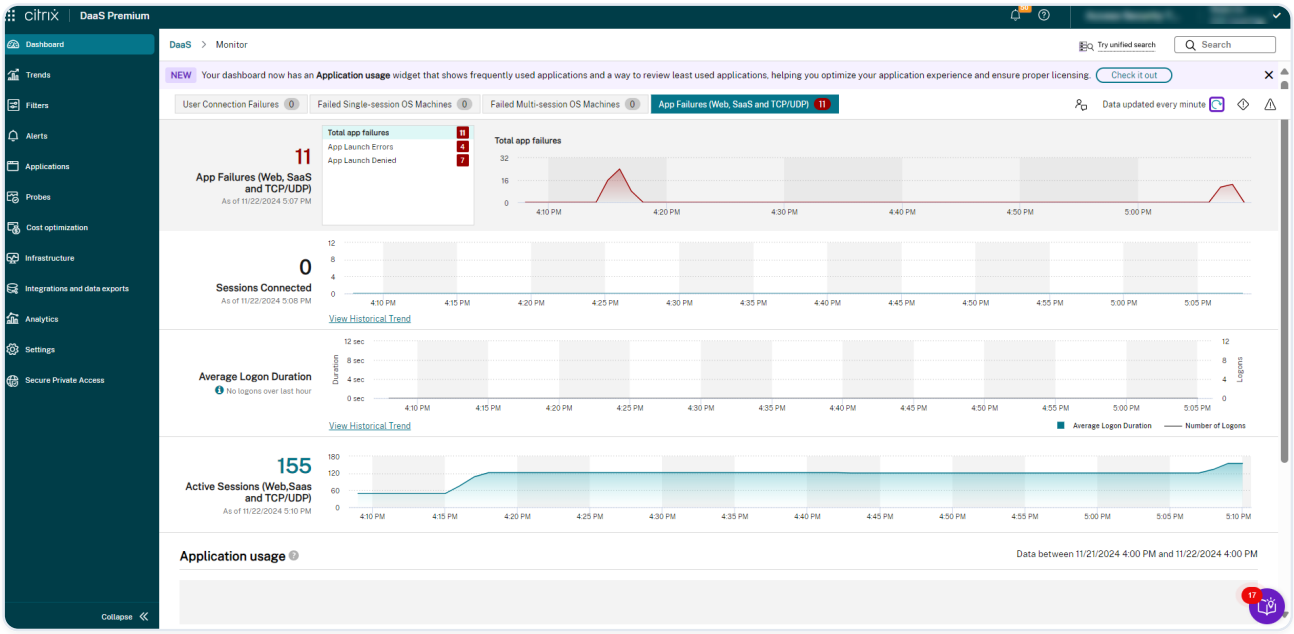
Monitor bietet eine verbesserte Transparenz für Secure Private Access-Sitzungen und die damit verbundenen Trends. Diese umfassende Überwachungsfunktion bietet detaillierte Einblicke in die Art und Weise, wie Anwendungen aufgerufen und genutzt werden, sowie detaillierte Informationen über die individuellen Benutzeraktivitäten innerhalb dieser Sitzungen. Dies ermöglicht Administratoren ein tieferes Verständnis des Benutzerverhaltens und der Anwendungsleistung, was ein proaktives Management und die Optimierung der Secure Private Access-Umgebung ermöglicht.

Um die Sitzungsdefinitionen im Kontext von Secure Private Access zu verstehen, siehe Sitzungsdefinitionen.

Um eine Secure Private Access-Sitzung nach Benutzer anzuzeigen, siehe Benutzersitzung anzeigen.

Um die Sitzungsdetails anzuzeigen, siehe Transparenz für den Secure Private Access-Dienst.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Zustandsüberwachung

Die folgenden Abschnitte enthalten weitere Informationen zur Zustandsüberwachung.

Connector Appliance

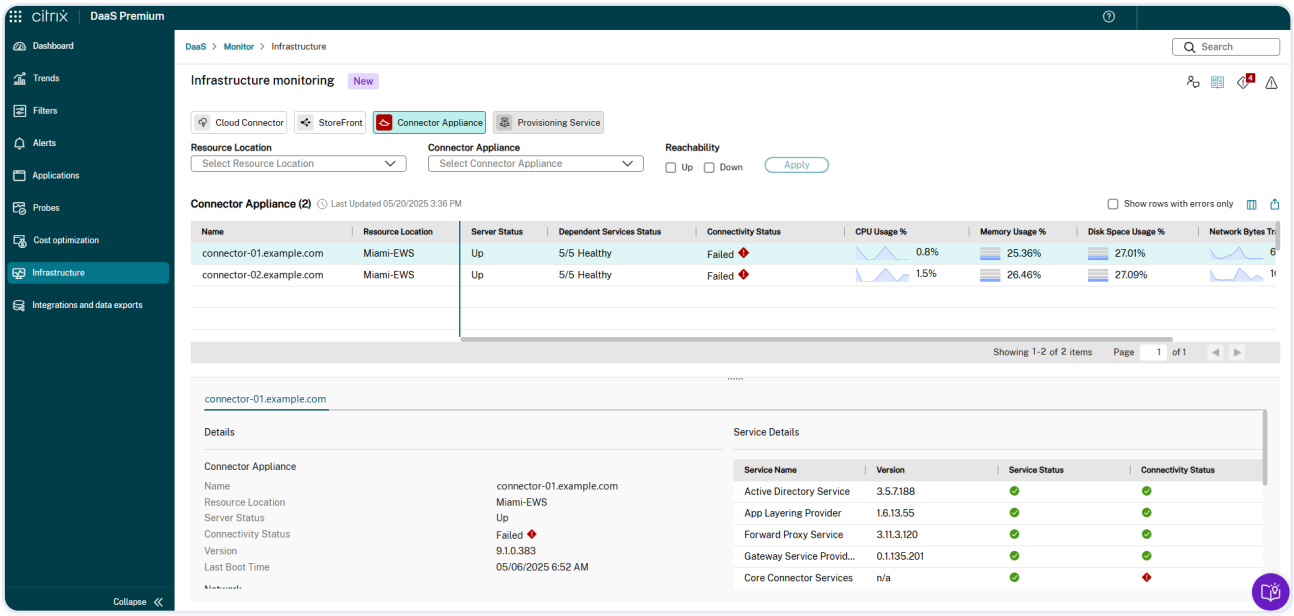
Die Connector Appliance ist eine Citrix-Komponente, die in Ihrem Hypervisor gehostet wird. Sie dient als Kommunikationskanal zwischen Citrix Cloud und Ihren Ressourcenstandorten und ermöglicht die Cloud-Verwaltung, ohne dass eine komplexe Netzwerk- oder Infrastrukturkonfiguration erforderlich ist. Mit der Connector Appliance können Sie die Ressourcen verwalten und sich auf diese konzentrieren, die Ihren Benutzern einen Mehrwert bieten. Weitere Informationen finden Sie unter Connector Appliance für Secure Private Access.

Die Funktion für Zustandsmetriken der Connector Appliance bietet eine wesentliche Möglichkeit zur Überwachung des Zustands und der Leistung der Connector Appliance-Komponente innerhalb der Citrix-Infrastruktur. Diese Komponente wird bei der Verbindung mit einer Citrix DaaS-Site automatisch für die Überwachung integriert, wodurch eine nahtlose Integration in das Dashboard für die Infrastrukturüberwachung gewährleistet ist.

Die Zustandsmetriken werden im Dashboard für die Infrastrukturüberwachung angezeigt und bieten eine zentralisierte Ansicht des Status der Connector Appliance. Administratoren können auf detaillierte Metriken und Trends zugreifen, um Probleme proaktiv zu identifizieren und zu beheben.

Die folgende Abbildung zeigt ein Beispiel für den Zustand der Connector Appliance in Monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sitzungs- und Anwendungstrends

Administratoren können Sitzungs- und Anwendungstrends in ihren Organisationen über den DaaS Monitor überwachen. Dies umfasst die Verfolgung von Rollouts, das Verständnis der Funktionsweise von Richtlinien und Konfigurationen sowie die Analyse potenzieller Probleme.

Weitere Informationen finden Sie unter Sichtbarkeit für den Secure Private Access Service.

Sitzungen und Anwendungstrends

Überwachen Sie Ihre Secure Private Access-Sitzungen und Anwendungstrends in Ihrem gesamten Unternehmen mit Citrix Monitor. Verfolgen Sie den Rollout-Fortschritt, verstehen Sie, wie Ihre Richtlinien und Konfigurationen funktionieren, und identifizieren Sie, ob sie weitreichende Benutzerprobleme verursachen. Citrix Monitor bietet umfassende Einblicke in Benutzeraktivitäten und Anwendungsmuster, um Ihre Bereitstellung zu optimieren.

Citrix Monitor liefert Echtzeit- und historische Einblicke in Ihre Secure Private Access-Umgebung, wodurch Administratoren datengestützte Entscheidungen über Ressourcenzuweisung, Richtlinienanpassungen und Verbesserungen der Benutzererfahrung treffen können. Die Überwachungsfunktionen helfen Ihnen, eine optimale Leistung aufrechtzuerhalten und gleichzeitig die Einhaltung der Sicherheitsvorschriften zu gewährleisten.

Sitzungsüberwachung

Administratoren können aktive Benutzersitzungen in Echtzeit mit Monitor überwachen. Sie können App-Fehler für Web-/SaaS- und TCP/UDP-Apps überwachen und aktive Sitzungen für Web-/SaaS-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apps im Dashboard anzeigen. Weitere Informationen finden Sie unter Sichtbarkeit für den Secure Private Access Service.

Anwendungstrends

Überwachen Sie die Zugriffstrends von Secure Private Access-Anwendungen, zeigen Sie aktive Anwendungssitzungen an und identifizieren Sie Anwendungen, die Probleme oder Fehler aufweisen. Citrix Monitor bietet umfassende Analysen, die Ihnen helfen, Anwendungsmuster zu verstehen, die Leistung zu optimieren und einen zuverlässigen Zugriff auf die kritischen Anwendungen Ihres Unternehmens zu gewährleisten.

Detaillierte Informationen zum Zugriff auf diese Überwachungsfunktionen und zur Interpretation der Daten finden Sie unter Sichtbarkeit für den Secure Private Access Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Triage und Fehlerbehebung

Dieses Thema beschreibt die wesentlichen Überlegungen und Verfahren zur effektiven Fehlerbehebung und Triage von Problemen im Zusammenhang mit Citrix Secure Private Access. Administratoren können dieses Dokument als Leitfaden zur Identifizierung, Diagnose und Behebung von Problemen verwenden, um einen nahtlosen und sicheren Zugriff für Benutzer zu gewährleisten.

Weitere Informationen finden Sie in den folgenden Themen:

Fehlerbehebung bei anwendungsbezogenen Problemen

Zeigen Sie die Probleme an, die sich auf den Gerätestatus (Device Posture), Anmelde-/Abmeldestatus, Anwendungsaufzählung und den Anwendungszugriff beziehen. Weitere Informationen finden Sie unter Fehlerbehebung bei anwendungsbezogenen Problemen.

Secure Private Access-Sitzungscodes in DaaS Monitor

Zeigen Sie die Liste der Fehlercodes an, die sich auf Anwendungsaufzählung, Anwendungsstart und Sitzungen in Citrix Monitor beziehen. Weitere Informationen finden Sie unter Secure Private Access-Sitzungscodes in DaaS Monitor.

Fehlerbehebung bei sitzungsbezogenen Problemen in Monitor

Verwenden Sie die Helpdesk-Ansicht von Monitor (Seite „Aktivitätsmanager“), um Informationen über den Benutzer oder Endpunkt anzuzeigen. Weitere Informationen finden Sie unter Fehlerbehebung bei sitzungsbezogenen Problemen in Monitor.

Fehlerbehebung bei Problemen im Zusammenhang mit dem Gerätestatus (Device Posture)

Sie können die Probleme/Fehler des Gerätestatus (Device Posture) in DaaS Monitor mithilfe der Transaktions-ID beheben, die für jede Sitzung generiert wird, wenn ein Benutzer über Secure Private Access oder DaaS eine Verbindung herstellt. Wenn Sie die Transaktions-ID finden, zeigt der DaaS Monitor Informationen über die Sitzung und die angewendete zugehörige Device

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Posture-Richtlinie an. Monitor zeigt auch die Richtlinienergebnisse an, einschließlich der Information, ob das Gerät die Posture-Prüfungen bestanden oder nicht bestanden hat. Weitere Informationen finden Sie unter Fehlerbehebung beim Device Posture-Dienst.

Fehlerbehebung bei authentifizierungsbezogenen Problemen

Wenn eine bedingte Authentifizierung fehlschlägt, können Sie die in der Fehlermeldung verfügbare Transaktions-ID verwenden und im Monitor nach den Fehlerdetails suchen. Monitor hilft Ihnen bei der Fehlerbehebung bei Fehlern bei der bedingten Authentifizierung, indem er Fehlerursachen und bedingte Richtlinien in der Monitor-Benutzeroberfläche anzeigt. Weitere Informationen finden Sie unter Fehlerbehebung bei der Authentifizierung.

Fehlerbehebung mithilfe von Protokollen

Die Secure Private Access- und Device Posture-Protokolle helfen Administratoren, Konfigurationsprobleme, Konnektivitätsprobleme, Fehlkonfigurationen von Richtlinien und Probleme mit der Gerätekonformität zu identifizieren, was eine schnellere Identifizierung und Behebung von Problemen ermöglicht.

Secure Private Access-Protokolle

Sie können die Secure Private Access-Protokolle über das Secure Private Access-Dashboard anzeigen. Informationen zu den verschiedenen in Diagnoseprotokollen erfassten Ereignissen finden Sie unter Ereignisse.

Weitere Informationen zu den Secure Private Access-Diagnoseprotokollen finden Sie unter Diagnoseprotokolle.

Die verschiedenen Fehlercodes, die jedem Ereignis zugeordnet sind, finden Sie unter Diagnoseprotokoll-Infocodes.

Device Posture-Protokolle

Die Diagnoseprotokolle im Device Posture-Dashboard bieten Einblicke in die Gerätekonformität (konform, nicht konform und Anmeldung verweigert). Diese Protokolle ermöglichen es Administratoren, die Endpunktsicherheit zu überwachen, die Einhaltung von Organisationsrichtlinien sicherzustellen und Geräte zu identifizieren, die Umweltrisiken darstellen könnten.

Sie können die Device Posture-Protokolle und -Ereignisse im Secure Private Access-Dashboard und in der Identity and Access Management-Konsole anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Device Posture-Protokolle und -Ereignisse.

Echtzeit-Sitzungsfehlerbehebung mit Monitor

Administratoren können Secure Private Access-Sitzungen in Echtzeit über die Monitor-Konsole überwachen und Fehler beheben.

Weitere Informationen finden Sie in den folgenden Themen:

- Informationen zur Integration von Secure Private Access mit Monitor finden Sie unter Integration mit DaaS Monitor.
- Sie können im Monitor nach Secure Private Access-Benutzersitzungen suchen, um bestimmte Sitzungen für die Fehlerbehebung und Berichterstellung schnell zu finden. Weitere Informationen finden Sie unter Eine Secure Private Access-Sitzung nach Benutzer anzeigen.
- Weitere Informationen zu Monitor finden Sie unter DaaS Monitor.

Fehlercodes für Diagnoseprotokolle

Die folgende Tabelle enthält eine umfassende Liste der verschiedenen Fehler, die Benutzern bei der Verwendung des Secure Private Access-Dienstes möglicherweise begegnen können, sowie die entsprechende Lösung.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x180022	App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist	App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist
0x1800B7	App-Start fehlgeschlagen, weil die Länge des App-FQDN überschritten wurde	App-Start fehlgeschlagen, weil die Länge des App-FQDN überschritten wurde
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7	Start der Web-App fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte	Start der Web-App fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte
0x18001A, 0x18001B	Benutzerdetails nicht gefunden	Benutzerdetails nicht gefunden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x1800AA	Start der Web-/SaaS-App ist fehlgeschlagen, da Benutzerattribute während der Vorbereitung des SAML-Tokens nicht gefunden wurden	Start der Web-/SaaS-App ist fehlgeschlagen
0x180010	Start der Web-/SaaS-App ist fehlgeschlagen, da der Anwendungs-FQDN nicht identifiziert werden konnte	Start der Web-/SaaS-App ist fehlgeschlagen, da der Anwendungs-FQDN nicht identifiziert werden konnte
0x180040	Der Start der Web-/SaaS-App ist aufgrund einer ungültigen App-ID, die vom SAML-Dienstanbieter bereitgestellt wurde, fehlgeschlagen.	App-Start fehlgeschlagen aufgrund einer ungültigen App-ID, die vom SAML-Dienstanbieter bereitgestellt wurde
0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048	Der Start der Web-/SaaS-App ist aufgrund einer ungültigen App-Zugriffsanforderung fehlgeschlagen.	Start der Web-/SaaS-App fehlgeschlagen aufgrund einer ungültigen App-Zugriffsanforderung
0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC	Der App-Start ist während der Richtlinienauswertung aufgrund eines internen Fehlers fehlgeschlagen.	App-Start fehlgeschlagen während der Richtlinienauswertung aufgrund eines internen Fehlers
0x1800D9	Der App-Start ist beim Parsen der Richtlinienauswertungsantwort fehlgeschlagen.	App-Start fehlgeschlagen beim Parsen der Richtlinienauswertungsantwort
0x1800DA	Der App-Start ist mit einem ungültigen Ergebnis während der Richtlinienauswertung fehlgeschlagen.	App-Start fehlgeschlagen mit ungültigem Ergebnis während der Richtlinienauswertung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x1800DB	App-Start ist mit ungültiger Ressourcenstandortkonfiguration fehlgeschlagen	App-Start ist mit ungültiger Ressourcenstandortkonfiguration fehlgeschlagen
0x1800E0	App-Start fehlgeschlagen, da der Name der App zu lang ist	App-Start fehlgeschlagen, da der Name der App zu lang ist
0x1800EE	App-Start ist während des Verbindungsaufbaus zum privaten TCP-Server aufgrund einer ungültigen App-ID fehlgeschlagen	App-Start ist während des Verbindungsaufbaus zum privaten TCP-Server aufgrund einer ungültigen App-ID fehlgeschlagen
0x1800E3	App-Start wurde während der Richtlinienauswertung verweigert	App-Start wurde während der Richtlinienauswertung verweigert
0x1800EA	App-Start ist fehlgeschlagen, da der Ziel-FQDN zu lang ist	App-Start ist fehlgeschlagen, da der Ziel-FQDN zu lang ist
0x1800ED	App-Start ist aufgrund einer ungültigen Ziel-IP fehlgeschlagen	App-Start ist aufgrund einer ungültigen Ziel-IP fehlgeschlagen
0x180102	App-Start ist fehlgeschlagen, da keine Antwort von der Connector Appliance empfangen wurde	App-Start ist fehlgeschlagen, da keine Antwort von der Connector Appliance empfangen wurde
0x10000005	Der Start der Web-/SaaS-Anwendung ist aufgrund eines Fehlers beim Herstellen einer Verbindung mit dem Backend-App-Server fehlgeschlagen	Der Start der Web-/SaaS-Anwendung ist aufgrund eines Fehlers beim Herstellen einer Verbindung mit dem Backend-App-Server fehlgeschlagen
0x10000101, 0x10000102, 0x10000103, 0x10000104	Web-/SaaS-FormFill-SSO ist aufgrund einer ungültigen Anwendungskonfiguration fehlgeschlagen	Web-/SaaS-FormFill-SSO ist aufgrund einer ungültigen Anwendungskonfiguration fehlgeschlagen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x10000202	Kerberos-SSO für Web/SaaS ist fehlgeschlagen	Kerberos-SSO für Web/SaaS ist fehlgeschlagen
0x10000203	Web/SaaS SSO fehlgeschlagen aufgrund eines internen Serverfehlers	Web/SaaS SSO fehlgeschlagen aufgrund eines internen Serverfehlers
0x10000303, 0x10000304	Start der Web-/SaaS-App fehlgeschlagen, da der konfigurierte Proxy nicht erreichbar ist	Start der Web-/SaaS-App fehlgeschlagen, da der konfigurierte Proxy nicht erreichbar ist
0x10000305	Start der Web-/SaaS-App fehlgeschlagen, da die Authentifizierung beim konfigurierten Proxy fehlgeschlagen ist	Start der Web-/SaaS-App fehlgeschlagen, da die Authentifizierung beim konfigurierten Proxy fehlgeschlagen ist
0x10000414	Anwendungsstart fehlgeschlagen, da eine Anforderung über eine ungültige IP/einen ungültigen Hostnamen oder Port erfolgte	Anwendungsstart fehlgeschlagen, da eine Anforderung über eine ungültige IP/einen ungültigen Hostnamen oder Port erfolgte
0x10000415	Anwendungsstart fehlgeschlagen, da der Zielserver die Verbindung verweigert hat	Anwendungsstart fehlgeschlagen, da der Zielserver die Verbindung verweigert hat
0x10000416	Anwendungsstart fehlgeschlagen, da das Ziel nicht gefunden wurde	Anwendungsstart fehlgeschlagen, da das Ziel nicht gefunden wurde
0x10000417	Anwendungsstart fehlgeschlagen, da das Zielnetzwerk nicht erreichbar war	Anwendungsstart fehlgeschlagen, da das Zielnetzwerk nicht erreichbar war
0x10000405	Anwendungsstart fehlgeschlagen, da keine	Anwendungsstart fehlgeschlagen, da keine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
	Verbindung zum Ziel hergestellt werden konnte	Verbindung zum Ziel hergestellt werden konnte
0x10000301	Verbindung des Connectors zum SPA-Dienst fehlgeschlagen	Verbindung des Connectors zum Secure Private Access-Dienst fehlgeschlagen
0x10000302	Connector konnte die Proxy-Details nicht lesen	Connector konnte die Proxy-Details nicht lesen
0x10000306	Konfigurierte Proxys sind nicht erreichbar	Konfigurierte Proxys sind nicht erreichbar
0x10000401	Connector Appliance kann FR nicht erreichen	Connector Appliance kann FR (Edge-Knoten) nicht erreichen
0x10000403, 0x10000404, 0x10000407	Anwendungsstart aufgrund eines internen Verbindungsfehlers fehlgeschlagen	Anwendungsstart aufgrund eines internen Verbindungsfehlers fehlgeschlagen
6003, 6007	Citrix Secure Access Client konnte SSO nicht durchführen	Citrix Secure Access Client konnte SSO nicht durchführen

App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist

Infocode: 0x180022

Secure Private Access ermöglicht Administratoren die Konfiguration eines Authentifizierungsdienstes von Drittanbietern, wie z. B. das traditionelle Active Directory, AAD, Okta oder SAML. Ausfälle dieser Authentifizierungsdienste können dieses Problem verursachen.

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

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

Infocode: 0x1800B7

App-FQDNs dürfen 512 Zeichen nicht überschreiten. Überprüfen Sie den Anwendungs-FQDN auf der App-Konfigurationsseite, um sicherzustellen, dass er dieses Limit nicht überschreitet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Gehen Sie zur Registerkarte **Anwendungen** in der Admin-Konsole.
2. Suchen Sie nach der Anwendung, deren FQDN 512 Zeichen überschreitet.
3. Bearbeiten Sie die Anwendung und korrigieren Sie die Länge des App-FQDN.

Start der Web-App fehlgeschlagen, da keine Verbindung zur Backend-Web-App hergestellt werden konnte

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

Fehlerhafte Browser-Erfahrung bei Webanwendungen, die innerhalb des Unternehmensnetzwerks ausgeführt werden.

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

Benutzerdetails nicht gefunden

Infocode: 0x18001A, 0x18001B

Domänenbenutzerdetails werden nicht gefunden, während der Secure Private Access-Dienst die Anforderung verarbeitet. Dieses Problem kann auftreten, wenn die erforderlichen Domänenbenutzerattribute von Citrix Cloud™ fehlen.

1. Stellen Sie sicher, dass der Citrix Cloud Connector™ keine Probleme beim Synchronisieren der Benutzer mit Citrix Cloud hat.
2. Stellen Sie sicher, dass die Domänen in **Citrix Cloud > Identity and Access Management** erreichbar sind.
3. Melden Sie sich ab und wieder bei Citrix Workspace an.

Der Start der Web-/SaaS-App ist fehlgeschlagen, weil Benutzerattribute während der Vorbereitung des SAML-Tokens nicht gefunden wurden

Infocode: 0x1800AA

Erforderliche Benutzerattribute wurden nicht gefunden, während der Secure Private Access-Dienst das SAML-Token vorbereitet. Dieses Problem kann auftreten, wenn die erforderlichen Domänenbenutzerattribute aus Citrix Cloud fehlen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Stellen Sie sicher, dass der Citrix Cloud Connector keine Probleme beim Synchronisieren der Benutzer mit Citrix Cloud hat.
2. Stellen Sie sicher, dass die Domänen in **Citrix Cloud > Identity and Access Management** erreichbar sind.
3. Melden Sie sich ab und wieder bei Citrix Workspace an.

Der Start der Web-/SaaS-App ist fehlgeschlagen, weil die Anwendungs-FQDN nicht identifiziert werden konnte

Infocode: 0x180010

Keine Anwendung für den angegebenen Domänennamen gefunden.

Stellen Sie sicher, dass die Länge des Domänennamens das Konfigurationslimit nicht überschreitet.

Der Start der Web-/SaaS-App ist fehlgeschlagen, weil eine ungültige appId vom SAML-Dienstanbieter bereitgestellt wurde

Infocode: 0x180040

Die vom SAML-Dienstanbieter bereitgestellte App-ID ist ungültig. Die App mit der angegebenen App-ID des SAML-Dienstanbieters konnte nicht gefunden werden.

1. Überprüfen Sie die Konfiguration des SAML-Dienstanbieters.
2. Stellen Sie sicher, dass die beim SAML-Dienstanbieter konfigurierte IdP-URL geeignet ist.
3. Diese App-ID muss der im Secure Private Access-Dienst konfigurierten App zugeordnet sein.

Start der Web-/SaaS-App ist aufgrund einer ungültigen App-Zugriffsanforderung fehlgeschlagen

Infocode: 0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048

Der App-Zugriff ist aufgrund einer ungültigen Anforderung, die vom Secure Private Access-Dienst empfangen wurde, fehlgeschlagen.

Die vom Secure Private Access-Dienst empfangene Anwendung kann nicht identifiziert werden. Empfangene Anforderungsparameter sind möglicherweise ungültig.

1. Starten Sie die Anwendung neu oder melden Sie sich ab und wieder bei Citrix Workspace an.
2. Wenn das Problem weiterhin besteht, wenden Sie sich an den Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App-Start ist während der Richtlinienauswertung aufgrund eines internen Fehlers fehlgeschlagen

Infocode: 0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC

Wenden Sie sich mit der Transaktions-ID und den vom Client gesammelten Debug-Protokollen an den Citrix Support.

App-Start ist beim Parsen der Richtlinienauswertungsantwort fehlgeschlagen

Infocode: 0x1800D9

Die Anwendungskonfiguration enthält möglicherweise Sonderzeichen, oder es liegt ein Problem bei der Richtlinienkonfiguration vor.

Stellen Sie sicher, dass die TCP/UDP/HTTP-Anwendungskonfiguration keine nicht unterstützten Zeichen enthält.

1. Klicken Sie in der Secure Private Access-Administratorkonsole auf **Anwendungen**.
2. Überprüfen Sie, ob der Anwendungsname oder die Ziele Sonderzeichen enthalten.

Überprüfen Sie, ob die Richtlinien korrekt konfiguriert und den richtigen Anwendungen zugewiesen sind.

1. Klicken Sie im Secure Private Access-Administratorportal auf **Zugriffsrichtlinien**.
2. Überprüfen Sie die Richtlinienkonfiguration, den Richtliniennamen und die Bedingungen.
3. Überprüfen Sie, ob die Richtlinie der richtigen Anwendung zugewiesen ist.

Wenn die Konfigurationen in Ordnung sind, wenden Sie sich mit der Transaktions-ID und den Client-Debug-Protokollen an den Citrix Support.

Der App-Start ist während der Richtlinienauswertung mit einem ungültigen Ergebnis fehlgeschlagen

Infocode: 0x1800DA

Es liegt möglicherweise ein Problem mit der Anwendungs- oder Richtlinienkonfiguration vor. Stellen Sie sicher, dass die TCP/UDP/HTTP-Anwendungskonfiguration keine nicht unterstützten Zeichen enthält.

1. Klicken Sie in der Secure Private Access-Administratorkonsole auf **Anwendungen**.
2. Überprüfen Sie, ob der Anwendungsname oder die Zieldomäne/FQDN Sonderzeichen enthält.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Überprüfen Sie auch, ob die Ziel-IP/der IP-Bereich/die IP-CIDRs gültig sind.

Stellen Sie sicher, dass in der Tabelle **Anwendungsdomäne** (**Secure Private Access > Einstellungen > Anwendungsdomäne**) der Eintrag für das Anwendungsziel aktiviert ist.

Überprüfen Sie, ob die Richtlinien korrekt konfiguriert und den richtigen Anwendungen zugewiesen sind.

1. Klicken Sie im Secure Private Access-Administratorportal auf **Zugriffsrichtlinien**.
2. Überprüfen Sie die Richtlinienkonfiguration, den Richtliniennamen und die Bedingungen.
3. Überprüfen Sie, ob die Richtlinie der richtigen Anwendung zugewiesen ist.

App-Start ist fehlgeschlagen aufgrund von ungültiger Ressourcenstandortkonfiguration

Infocode: 0x1800DB

Es liegt möglicherweise ein Problem mit dem Ressourcenstandort und der Konfiguration vor.

Stellen Sie sicher, dass der Ressourcenstandort konfiguriert ist.

1. Melden Sie sich beim Citrix Cloud-Portal an und klicken Sie im Menü auf **Ressourcenstandorte**.
2. Überprüfen Sie, ob der erwartete Ressourcenstandort konfiguriert ist.

Stellen Sie sicher, dass der Ressourcenstandort fehlerfrei und aktiv ist.

1. Melden Sie sich beim Citrix Cloud-Portal an und klicken Sie im Menü auf **Ressourcenstandorte**.
2. Überprüfen Sie, ob der erwartete Ressourcenstandort aktiv und fehlerfrei ist.

Stellen Sie sicher, dass der richtige Ressourcenstandort für das Ziel in der Tabelle **Anwendungsdomäne** (**Secure Private Access > Einstellungen > Anwendungsdomäne**) ausgewählt ist.

1. Klicken Sie in der Secure Private Access-Administrationskonsole auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte **Anwendungsdomäne**.
3. Überprüfen Sie, ob für das aufgerufene Ziel der richtige Ressourcenstandort konfiguriert ist.
4. Überprüfen Sie, ob der Eintrag des aufgerufenen Ziels in der Tabelle **Anwendungsdomäne** aktiv ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden automatisch zur Tabelle **Anwendungsdomäne** hinzugefügt. Es wird empfohlen, die Ziele/URLs aktiver TCP/UDP/HTTP-Anwendungen nicht zu löschen/deaktivieren.

App-Start fehlgeschlagen, da der App-Name zu lang ist

Infocode: 0x1800E0

Wenden Sie sich mit der Transaktions-ID und den vom Client gesammelten Debug-Protokollen an den Citrix Support.

App-Start ist während des Verbindungsaufbaus zum privaten TCP-Server aufgrund einer ungültigen App-ID fehlgeschlagen

Infocode: 0x1800EE

Wenden Sie sich mit der Transaktions-ID und den vom Client gesammelten Debug-Protokollen an den Citrix Support.

App-Start wurde während der Richtlinienauswertung verweigert

Infocode: 0x1800E3

Wenden Sie sich mit der Transaktions-ID und den vom Client gesammelten Debug-Protokollen an den Citrix Support.

App-Start ist fehlgeschlagen, da der Ziel-FQDN zu lang ist

Infocode: 0x1800EA

Stellen Sie sicher, dass die FQDN-Länge unter 256 Zeichen liegt.

App-Start aufgrund ungültiger Ziel-IP fehlgeschlagen

Infocode: 0x1800ED

Greifen Sie von den Clients nur auf gültige private IP-Adressen zu.

App-Start fehlgeschlagen, da keine Antwort von der Connector Appliance empfangen wurde

Infocode: 0x180102

Überprüfen Sie die Erreichbarkeit der Connector Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsstart fehlgeschlagen aufgrund einer Anforderung an eine ungültige IP/einen ungültigen Hostnamen oder Port

Infocode: 0x10000414

Überprüfen Sie die Gültigkeit von Hostnamen, IP-Adresse oder Portnummer.

Anwendungsstart fehlgeschlagen, da der Zielserver die Verbindung verweigerte

Infocode: 0x10000415

Überprüfen Sie den Status des Zielservers.

Anwendungsstart fehlgeschlagen, da das Ziel nicht gefunden wurde

Infocode: 0x10000416

Überprüfen Sie den Hostnamen des Zielservers.

Anwendungsstart fehlgeschlagen, da das Zielnetzwerk nicht erreichbar war

Infocode: 0x10000417

Die Connector Appliance hat ein Verbindungsproblem mit den Back-End Private TCP/UDP-Servern. Überprüfen Sie die Netzwerkeinstellungen für Ihre Connector Appliance.

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv und betriebsbereit ist und Anfragen empfangen kann.
- Überprüfen Sie die Erreichbarkeit der Back-End-Server innerhalb des Unternehmensnetzwerks.
- Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector am Erreichen des Back-End-Servers gehindert wird.
- Wenn es sich um eine Anfrage für eine FQDN-basierte App handelt, überprüfen Sie den DNS-Eintrag für die entsprechende App auf dem DNS-Server.

Anwendungsstart fehlgeschlagen aufgrund der Unfähigkeit, eine Verbindung zum Ziel herzustellen

Infocode: 0x10000405

Die Connector Appliance hat ein Verbindungsproblem mit den Back-End Private TCP/UDP-Servern. Überprüfen Sie die Netzwerkeinstellungen für Ihre Connector Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv und betriebsbereit ist und Anfragen empfangen kann.
- Überprüfen Sie die Erreichbarkeit der Back-End-Server innerhalb des Unternehmensnetzwerks.
- Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector am Erreichen des Back-End-Servers gehindert wird.
- Wenn die Anforderung für eine FQDN-basierte App erfolgt, überprüfen Sie den DNS-Eintrag für die entsprechende App im DNS-Server.

Verbindung des Connectors zum Secure Private Access-Dienst fehlgeschlagen

Infocode: 0x10000301

- Suchen Sie die Transaktions-ID für den Fehlercode.
- Filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Secure Private Access-Dashboard.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Falls ja, führen Sie die entsprechende Problemumgehung für diesen Fehlercode durch.
- Wenn in anderen Komponenten kein Fehler gefunden wird, gehen Sie wie folgt vor:
  - Gehen Sie zur Admin-Seite der Connector Appliances.
  - Laden Sie den Diagnosebericht herunter. Weitere Informationen finden Sie unter Generieren eines Diagnoseberichts.
  - Erfassen Sie die Paketverfolgung. Weitere Informationen finden Sie unter Überprüfen Ihrer Netzwerkverbindung.
- Wenden Sie sich mit diesem Diagnosebericht und der Paketverfolgung zusammen mit dem Fehlercode und der Transaktions-ID an den Citrix Support.

Connector konnte die Proxy-Details nicht lesen

Infocode: 0x10000302

Die Connector Appliance hat Verbindungsprobleme mit den privaten TCP/UDP-Back-End-Servern. Überprüfen Sie die Netzwerkeinstellungen für Ihre Connector Appliance.

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv ist und Anforderungen empfangen kann.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 es sich um eine Anfrage für eine FQDN-basierte App handelt, überprüfen Sie den DNS-Eintrag für die entsprechende App im DNS-Server.

Konfigurierte Proxys sind nicht erreichbar

Infocode: 0x10000306

Die Connector Appliance hat Verbindungsprobleme mit den privaten TCP/UDP-Back-End-Servern. Überprüfen Sie die Netzwerkeinstellungen für Ihre Connector Appliance.

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv ist und läuft und Anfragen 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 es sich um eine Anfrage für eine FQDN-basierte App handelt, überprüfen Sie den DNS-Eintrag für die entsprechende App im DNS-Server.

Connector Appliance kann FR (Edge-Knoten) nicht erreichen

Infocode: 0x10000401

Überprüfen Sie die Netzwerkkonnektivität mit dem Citrix Secure Private Access-Dienst.

Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Anwendungsstart fehlgeschlagen aufgrund eines internen Verbindungsfehlers

Infocode: 0x10000403, 0x10000404, 0x10000407

- Suchen Sie die Transaktions-ID für den Fehlercode.
- Filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Secure Private Access-Dashboard.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Wenn ein Fehler gefunden wird, führen Sie die entsprechende Problemumgehung für diesen Fehlercode durch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn in anderen Komponenten kein Fehler gefunden wird, gehen Sie wie folgt vor:
  - Gehen Sie zur Administratorseite der Connector Appliances.
  - Laden Sie den Diagnosebericht herunter. Weitere Informationen finden Sie unter Generieren eines Diagnoseberichts.
  - Erfassen Sie die Paketverfolgung. Weitere Informationen finden Sie unter Überprüfen Ihrer Netzwerkverbindung.
- Wenden Sie sich mit diesem Diagnosebericht und der Paketverfolgung zusammen mit dem Fehlercode und der Transaktions-ID an den Citrix Support.

Start der Web-/SaaS-Anwendung fehlgeschlagen

Der Start der Web-/SaaS-Anwendung ist aufgrund eines Fehlers beim Herstellen einer Verbindung mit dem Back-End-App-Server fehlgeschlagen.

Infocode: 0x10000005

Überprüfen Sie die Ziel-URL oder die Netzwerkeinstellungen der Connector Appliance. Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Web-/SaaS-FormFill-SSO fehlgeschlagen aufgrund ungültiger Anwendungskonfiguration

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

Überprüfen Sie die SSO-Formular-App-Konfiguration und stellen Sie sicher, dass die Felder für Benutzername, Kennwort, Aktion und Anmelde-URL in den App-Einstellungen korrekt konfiguriert sind.

Kerberos-SSO für Web/SaaS fehlgeschlagen

Infocode: 0x10000202

Kerberos-SSO für Web/SaaS ist entweder aufgrund eines internen Serverfehlers mit der Connector Appliance oder aufgrund der Unfähigkeit, das Token vom Domänencontroller abzurufen, fehlgeschlagen.

Überprüfen Sie die Kerberos-SSO-Einstellungen auf dem Back-End-Server und dem Domänencontroller. Überprüfen Sie auch die Fallback-NTLM-Authentifizierungseinstellungen.

Weitere Informationen finden Sie unter Überprüfen Ihrer Kerberos-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web/SaaS-SSO aufgrund eines internen Serverfehlers fehlgeschlagen

Infocode: 0x10000203

Überprüfen Sie die SSO-Einstellungen im Secure Private Access-Dienst und auf dem Back-End-Server. Informationen zum Secure Private Access-Dienst finden Sie unter Festlegen der bevorzugten Anmeldemethode.

Start der Web/SaaS-App fehlgeschlagen, da der konfigurierte Proxy nicht erreichbar ist

Infocode: 0x10000303, 0x10000304

Überprüfen Sie die Proxy-Server-Einstellungen und stellen Sie sicher, dass er für die Connector Appliance erreichbar ist. Weitere Informationen finden Sie unter Registrieren Ihrer Connector Appliance bei Citrix Cloud.

Start der Web/SaaS-App fehlgeschlagen, da die Authentifizierung mit dem konfigurierten Proxy fehlgeschlagen ist

Infocode: 0x10000305

Überprüfen Sie die Proxy-Server-Anmeldeinformationen und stellen Sie sicher, dass sie in der Connector Appliance korrekt konfiguriert sind. Weitere Informationen finden Sie unter Nach der Registrierung Ihrer Connector Appliance.

Citrix Secure Access™ Client konnte SSO nicht durchführen

Infocode: 6003

Fehler beim Abrufen des Secure Private Access Single Sign-On-Handles vom Broker-Agent-Dienst.

Überprüfen Sie, ob das Secure Private Access SSO-Flag in der Bereitstellungsgruppe aktiviert ist. Weitere Informationen finden Sie unter Nahtlose Anmeldung vom Citrix Secure Access Client auf VDA.

Infocode: 6007

Anmeldung bei Secure Private Access fehlgeschlagen.

Starten Sie den VDA neu, wenn die Citrix Secure Access Client-Sitzung abgelaufen ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sitzungscodes

CODE	STATUS	BESCHREIBUNG
2101	Fehler	Sitzungsfehler
2102	aktiv/inaktiv/Fehler	Die Sitzung ist aktiv oder beendet, oder mindestens ein App-Start in der Sitzung ist fehlgeschlagen.
2000	Aktiv	Die Sitzung ist aktiv.
2001	Inaktiv	Sitzung ist beendet/inaktiv.

Meldungscodes für die App-Aufzählung

CODE	STATUS	BESCHREIBUNG
1000	Erfolg	Die Aufzählung war erfolgreich. Mindestens eine App wurde aufgezählt.
1001	Erfolg	Es wurden keine Anwendungen aufgelistet, da sie alle durch Richtlinien abgelehnt wurden.
1002	Erfolg	Es wurden keine Anwendungen aufgelistet, da keine Richtlinien übereinstimmten.
1003	Erfolg	Es wurden keine Anwendungen aufgelistet, da einige abgelehnt wurden und für andere keine Richtlinien übereinstimmten.
1004	Erfolg	Es wurden keine Anwendungen aufgelistet, da keine Richtlinien zur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	STATUS	BESCHREIBUNG
		Auswertung vorhanden waren.
1101	Fehler	Während der Auflistung ist ein interner Fehler aufgetreten.
1102	Fehler	Einige Anwendungen wurden aufgelistet, aber mindestens eine App-Evaluierung ist fehlgeschlagen
1103	Fehler	Es wurden keine Anwendungen aufgelistet, und mindestens eine App-Evaluierung ist fehlgeschlagen
3000	Zulassen	Die Anwendungsauflistung ist zugelassen
3001	Verweigern	Die Anwendungsauflistung wird durch die Richtlinie verweigert
3002	Verweigern	Die Anwendung wurde nicht aufgelistet, da keine Richtlinien übereinstimmten
3003	Unbekannt	Der Status der Anwendungsaufzählung ist unbekannt
3004	Anwendungsstart von CEB	Anwendungsstartversuch vom Citrix Enterprise Browser™
3101	Fehler	Anwendungsaufzählung – Ein interner Fehler ist aufgetreten (derzeit ungenutzt)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	STATUS	BESCHREIBUNG
3102	Fehler	Die Anwendung wurde nicht aufgezählt, da während der Richtlinienauswertung eine Ausnahme aufgetreten ist
3103	Fehler	Der Status der Anwendungsaufzählung ist null – Während der Richtlinienauswertung ist ein interner Fehler aufgetreten
3104	Zulassen/Verweigern/Fehler	Fehler beim Abrufen der Richtliniendetails für die App

Meldungscodes für den App-Start

CODE	STATUS	BESCHREIBUNG
4000	Zulassen	Anwendungsstart ist zugelassen
4001	Verweigern	Der Anwendungsstart wurde aufgrund einer Richtlinie verweigert
4002	Verweigern	Der Anwendungsstart wurde verweigert, da keine Richtlinie übereinstimmte
4101	Fehler	Fehler beim Anwendungsstart – Während des Anwendungsstarts ist ein interner Fehler aufgetreten
4102	Fehler	Fehler beim Anwendungsstart (intern)
4103	Zulassen/Verweigern/Fehler	Fehler beim Abrufen der Richtliniendetails für die App

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	STATUS	BESCHREIBUNG
4104	Fehler	Fehler beim Anwendungsstart – Keine Anwendungskonfiguration gefunden

Fehlercodes für den App-Start

CODE	BESCHREIBUNG	LÖSUNG/ PROBLEMUMGEHUNG
5001	TCP – Verbindung fehlgeschlagen	Überprüfen Sie die Netzwerkerreichbarkeit zum Ziel (pingen Sie `-S <SNIP>` vom NetScaler Gateway).
5003	TCP – Sondierung fehlgeschlagen	
5002	TCP – Proxyserver ausgefallen	Stellen Sie sicher, dass der Proxy-Host aktiv ist.
5004	TCP – Speicherzuweisung im Gateway fehlgeschlagen	Aktivieren Sie die Protokollierung auf Debug-Ebene und erfassen Sie das Support-Bundle vom NetScaler.
5005	TCP – Server ausgefallen	Überprüfen Sie die Netzwerkerreichbarkeit zum Ziel (pingen Sie `-S <SNIP>` vom NetScaler Gateway aus) und prüfen Sie, ob der Server AUSGEFALLEN ist.
5006	TCP – Proxy-Verbindung fehlgeschlagen	Stellen Sie sicher, dass der Proxy-Host VERFÜGBAR ist und Verbindungen akzeptiert.
5007	TCP – Proxy-Prüfung fehlgeschlagen	Überprüfen Sie die Netzwerkerreichbarkeit zum Ziel (pingen Sie `-S <SNIP>` vom NetScaler Gateway aus). Aktivieren Sie die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	BESCHREIBUNG	LÖSUNG/ PROBLEMUMGEHUNG
		Protokollierung auf Debug-Ebene und sammeln Sie das Support-Paket vom NetScaler.
5008	SPA – Server ausgefallen	Überprüfen Sie, ob die URL der Secure Private Access-Site VERFÜGBAR ist. (Verwenden Sie den CLI-Befehl `show vpn securePrivateAccessProfile` auf der NetScaler CLI, um den URL-Status zu überprüfen).
5009	SPA – Callout-Anforderungsfehler	Überprüfen Sie, ob die URL der Secure Private Access-Site VERFÜGBAR ist. Aktivieren Sie die Protokollierung auf Debug-Ebene und sammeln Sie das Support-Paket vom NetScaler.
5010	SPA – Callout-Antwortfehler	
5011	TCP – Sitzung abgelaufen	Dies weist darauf hin, dass auf die App zugegriffen wurde, als die Benutzersitzung nicht mehr aktiv war. Starten Sie eine neue aktive Benutzersitzung.
5013	TCP – Interner Gateway-Fehler	Aktivieren Sie die Debug-Protokollierung und erfassen Sie das Support-Bundle von NetScaler.
5014	TCP – DNS-Server ausgefallen	Stellen Sie sicher, dass der DNS-Server aktiv ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE	BESCHREIBUNG	LÖSUNG/ PROBLEMUMGEHUNG
5015	TCP – Interner Gateway-DNS-Fehler	Stellen Sie sicher, dass der DNS-Server aktiv ist. Aktivieren Sie die Debug-Protokollierung und erfassen Sie das Support-Bundle von NetScaler.
5016	Verbindung zum Zielserver fehlgeschlagen	Überprüfen Sie die Netzwerkerreichbarkeit zum Ziel (ping -S `<SNIP>` von NetScaler Gateway).
5017	DNS-Auflösung des Zielservers fehlgeschlagen	Stellen Sie sicher, dass der Hostname, den Ihre Anwendung verwendet, von den vorgesehenen DNS-Servern (intern vs. öffentlich) aufgelöst wird.
5018	Interner Gateway-Fehler	Aktivieren Sie die Protokollierung auf Debug-Ebene und erfassen Sie das Support-Bundle von NetScaler.
0x1300000C	DNS-Auflösung für Anwendungsdomäne fehlgeschlagen	Stellen Sie sicher, dass der Hostname, den Ihre Anwendung verwendet, von den vorgesehenen DNS-Servern (intern vs. öffentlich) aufgelöst wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access-Protokolle und -Ereignisse

Die Protokolle und Ereignisse sind entscheidend für Überwachung, Fehlerbehebung und die Sicherstellung der Compliance. Die dienstbezogenen Protokolle und Ereignisse des Citrix Secure Private Access-Dienstes können aus den folgenden Quellen abgerufen werden:

Diagnose-Dashboard

Das Diagnose-Dashboard bietet eine zentrale Schnittstelle zum Anzeigen und Analysieren von Protokollen und Ereignissen. Administratoren können dieses Dashboard zur Überwachung und Fehlerbehebung bei Problemen im Zusammenhang mit Secure Private Access verwenden. Weitere Informationen finden Sie unter Secure Private Access-Dashboard.

Liste der Fehler

Eine umfassende Liste der Fehler, die Benutzern bei der Verwendung des Secure Private Access-Dienstes begegnen können, finden Sie unter Diagnoseprotokoll-Infocodes.

Audit-Protokolle

Audit-Protokolle erfassen detaillierte Aufzeichnungen von Benutzeraktivitäten und Systemänderungen. Diese Protokolle sind für Compliance- und Sicherheitszwecke unerlässlich, da sie dabei helfen, nachzuverfolgen, wer auf das System zugegriffen hat, welche Änderungen vorgenommen wurden und wann diese Aktionen stattfanden. Weitere Informationen finden Sie unter Audit- und Systemprotokolle.

Systemprotokolle

Systemprotokolle enthalten Informationen über die internen Vorgänge des Secure Private Access-Dienstes. Diese Protokolle sind nützlich zur Diagnose von Problemen auf Systemebene, wie z. B. Leistungsproblemen oder Fehlern in der Dienstfunktionalität. Weitere Informationen finden Sie unter Systemprotokoll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geräte-Posture-Protokolle

Geräte-Posture-Protokolle bieten Einblicke in die Sicherheitslage von Geräten, die auf den Secure Private Access-Dienst zugreifen. Diese Protokolle tragen dazu bei, dass Geräte die erforderlichen Sicherheitsstandards erfüllen, bevor der Zugriff gewährt wird, wodurch die Gesamtsicherheit verbessert wird. Weitere Informationen finden Sie unter Geräte-Posture-Protokolle.

Diagnoseprotokolle

Die folgenden Abschnitte enthalten weitere Informationen zu den Diagnoseprotokollen.

FAQ

Die folgenden Abschnitte enthalten weitere Informationen zu den häufig gestellten Fragen.

Was sind Secure Private Access-Diagnoseprotokolle?

Secure Private Access-Diagnoseprotokolle erfassen alle Ereignisse, die auftreten, wenn ein Benutzer auf eine beliebige Anwendung (Web/SaaS/TCP/UDP) zugreift. Diese Protokolle erfassen Gerätestatus, App-Authentifizierung, App-Enumeration und App-Zugriffsprotokolle. Die Details werden in einem Tabellenformat dargestellt. Sie können die Protokolle für die voreingestellte Zeit oder für einen benutzerdefinierten Zeitrahmen 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 in das CSV-Format exportieren.

Wo finde ich Secure Private Access-Protokolle?

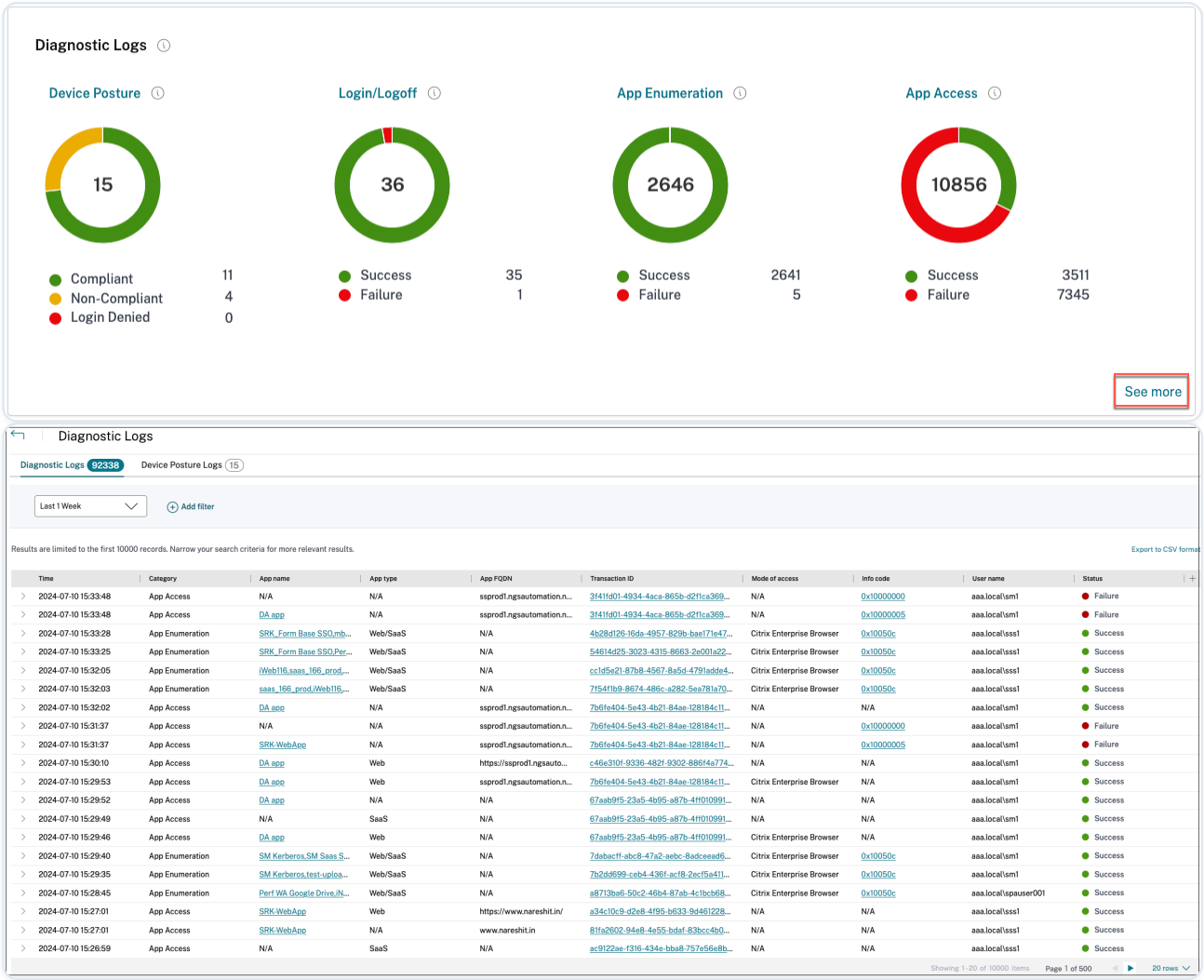
1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Dienstkachel für Secure Private Access auf **Verwalten**.
3. Klicken Sie in der linken Navigation der Administratorbenutzeroberfläche auf **Dashboard**.
4. Klicken Sie im Diagramm **Diagnoseprotokolle** auf den Link **Mehr anzeigen**.

Welches Widget zeigt die Secure Private Access-Diagnoseprotokolle an?

Das Widget **Diagnoseprotokolle** im Abschnitt **Protokollierung und Fehlerbehebung** zeigt eine Tortendiagrammansicht aller Secure Private Access-Ereignisse im Zusammenhang mit Authentifizierung, Anwendungsstart, App-Enumeration sowie Protokolle zum Gerätestatus an. Die Secure Private Access-Diagnoseprotokolle rufen Ereignisse von mehreren internen Komponenten ab, wobei jede ein Ereignis sendet, wenn ein Endbenutzer auf eine Anwendung zugreift. Diese Ereignisse sind in Kategorien unterteilt: **Anmeldung/Abmeldung**, **App-Enumeration** und **App-Zugriff**. Das Tortendiagramm zeigt das Gesamtverhältnis von Erfolgen/Fehlern jeder Kategorie an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie auf das farbige Tortenstück in einem beliebigen Diagramm klicken, gelangen Sie zu den Diagnoseprotokollen, wo Sie die entsprechenden Ereignisse finden können. Es gibt auch Gerätestatusprotokolle, wenn Sie den Device Posture-Dienst aktiviert haben. 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 für Benutzerprotokolle von Secure Private Access bietet standardmäßig die folgenden Details.

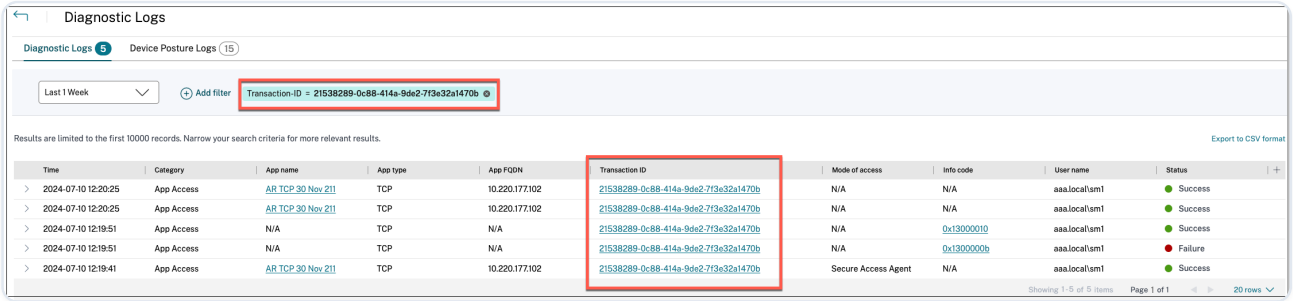
- **Zeitstempel** – Zeitpunkt des Ereignisses in UTC.
- **Benutzername** – Benutzername des Endbenutzers, der auf die App zugreift.
- **App-Name** – Name der App/Apps, auf die zugegriffen wurde.
- **Richtlinieninformationen** – Name der Zugriffsrichtlinie oder -richtlinien, die während des Ereignisses ausgelöst wurden.
- **Status** – Status des Ereignisses, Erfolg oder Fehler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

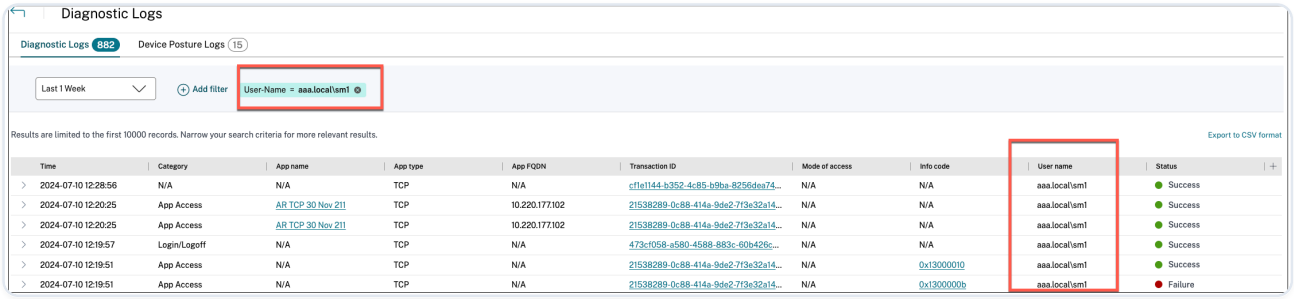
- **Infocode** – Code, der jedem Fehlerereignis im Dashboard der Diagnoseprotokolle von Secure Private Access zugeordnet ist. Weitere Informationen zum Infocode finden Sie hier.
- **Beschreibung** – Grund für den Fehler oder weitere Details zum Ereignis.
- **APP-FQDN**: FQDN der aufgerufenen Anwendung.
- **Ereignistyp** – Ereignistyp, der dem ausgeführten Vorgang zugeordnet ist.
- **Vorgangstyp** – Vorgang, für den das Protokoll generiert wird.
- **Kategorie** – Verfügbare Kategorie, abhängig vom Ereignistyp. Verfügbare Optionen sind: App-Authentifizierung, App-Enumeration oder App-Zugriff. Diese Optionen sind auch als Filteroptionen verfügbar. Sie können diese Optionen verwenden, um Protokolle nach der Art des Problems zu 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-ID verwenden. Die folgenden Details können durch Klicken auf die Schaltfläche „+“ ganz rechts im Dashboard abgerufen werden:
- **SPA PoP-Standort** – Name/ID des Secure Private Access Service PoP-Standorts, der während des App-Zugriffs verwendet wurde. Siehe Secure Private Access PoP-Standorte.

Wie filtere ich die Diagnoseprotokolle?

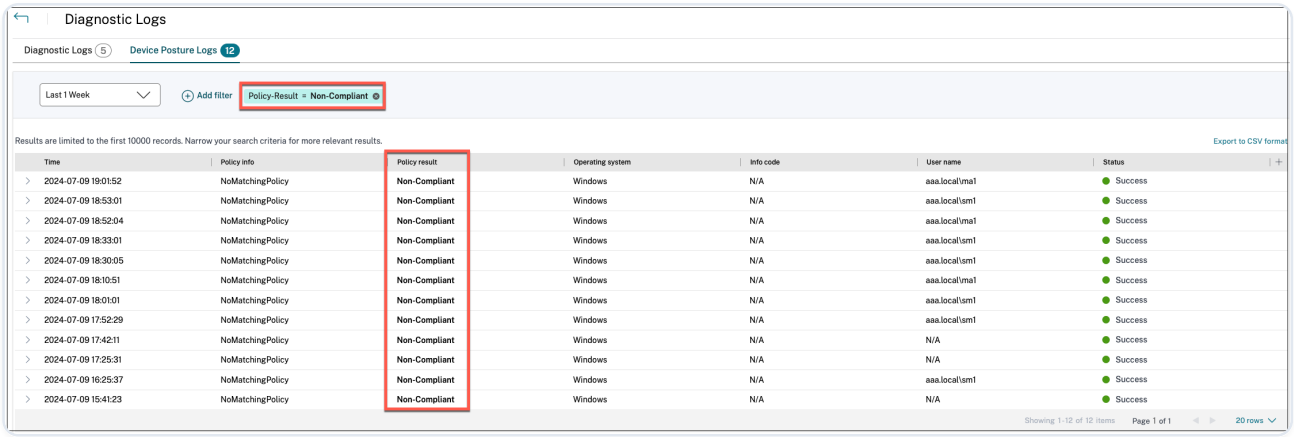
Sie können die Option **Filter hinzufügen** verwenden, um Ihre Suche basierend auf verschiedenen Kriterien wie App-Typ, Kategorie und Beschreibung zu verfeinern. Beispielsweise können Sie im Feld **Suchen** auf **Transaktions-ID, = (gleich einem Wert), und geben Sie 21538289-0c88-414a-9de2-7f3e32a1470b ein** klicken, um alle Protokolle zu suchen, die sich auf diese Transaktions-ID beziehen. Details zu Suchoperatoren, die mit der Filteroption verwendet werden können, finden Sie unter Suchoperatoren.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



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

Die Diagnoseprotokolle von Secure Private Access erfassen die folgenden Ereignisse:

- **Gerätepostur:** Gerätestatus des Endbenutzers. Diese Protokolle erfassen Informationen zu den Gerätepostur-Ergebnissen, ob das Gerät als konform, nicht konform oder der Zugriff verweigert wurde, basierend auf Ihrer Gerätepostur-Richtlinie.
- **Anmeldung/Abmeldung**: Ereignisse im Zusammenhang mit dem An- oder Abmeldestatus des Endbenutzers beim Citrix Secure Access-Client und der Authentifizierung bei Stores (internen oder externen Anbietern).
- **App-Aufzählung**: Im Secure Private Access-Dienst legen von Administratoren konfigurierte Zugriffsrichtlinien fest, welcher Benutzer auf welche App zugreifen darf. Verweigerte Anwendungen sind für Endbenutzer in der Citrix Workspace-App nicht sichtbar (werden nicht aufgezählt). Diese Ereignisse helfen Ihnen zu erfahren, welche Anwendungen einem Benutzer basierend auf den im Secure Private Access-Dienst konfigurierten Zugriffsrichtlinien erlaubt oder verweigert wurden.
- **App-Zugriff**: Ereignisse des Endbenutzer-Anwendungs-/Endpunktzugriffs, Zulassungs-/Verweigerungsstatus, Single Sign-On-Status und Konnektivitätsstatus gemäß den konfigurierten Zugriffsrichtlinien für das ausgewählte Zeitintervall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Liste der Fehler

Eine umfassende Liste der Fehler, die Benutzern bei der Verwendung des Secure Private Access-Dienstes begegnen können, finden Sie unter Diagnoseprotokoll-Infocodes.

Infocodes für Diagnoseprotokolle

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 Diagnoseprotokollen von Secure Private Access und suchen Sie dann auf dieser Seite nach diesem Code, um die entsprechenden Schritte zur Fehlerbehebung zu finden. Im Folgenden finden Sie einige häufig gestellte Fragen, die Ihnen helfen, dieses Thema besser zu nutzen.

Weitere Informationen zu den Diagnoseprotokollen finden Sie unter Diagnoseprotokolle.

Die folgende Fehlerübersichtstabelle bietet einen umfassenden Überblick über die verschiedenen Fehler, auf die Benutzer bei der Verwendung des Secure Private Access-Dienstes stoßen können.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x180006, 0x1800B7	App-Start fehlgeschlagen, da die Länge des App-FQDN überschritten wurde	App-Start fehlgeschlagen, da die Länge des App-FQDN überschritten wurde
0x180022	App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist	App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist
0x180001, 0x18001A, 0x18001B, 0x18008A	Single Sign-On-Fehler, Fehler beim Verbindungsaufbau zwischen Citrix Cloud und lokalen Konnektoren, SAML-SSO-Fehler, Ungültiger App-FQDN	App-Zugriff verweigert
0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC		
0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0		
0x1800B1, 0x1800B2, 0x1800B3, 0x180048		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x1800EF	Problem beim Herstellen einer Verbindung zur Connector Appliance	Problem beim Herstellen einer Verbindung zur Connector Appliance
0x18009D	DNS-Lookup/Verbindung fehlgeschlagen	Secure Browser Service – DNS-Lookup-/ Verbindungsfehler
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5	Start der Web-App fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte	Start der Web-App fehlgeschlagen, da keine Verbindung zur Back-End-Web-App hergestellt werden konnte
0x1800A6, 0x1800A7		
0x1800BC, 0x1800BF	Der Benutzer ist nicht berechtigt, auf die Web-/ SaaS-App zuzugreifen	Der Benutzer ist nicht berechtigt, auf die Web-/ SaaS-App zuzugreifen
0x1800BD	Der Benutzer ist nicht berechtigt, auf die Web-/ SaaS-App für DirectAccess zuzugreifen	Der Benutzer ist nicht berechtigt, auf die Web-/ SaaS-App für DirectAccess zuzugreifen
0x1800D0	Der Start der Citrix Secure Access Agent-Sitzung ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen	Citrix Secure Access Agent: Sitzungsstart ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Citrix Secure Access Agent: Sitzungsstart ist beim Abrufen der Anwendungskonfiguration fehlgeschlagen, Citrix Secure Access Agent: App-Start ist während der Richtlinienauswertung fehlgeschlagen, Citrix Secure Access Agent: App-Start ist fehlgeschlagen	Fehlerhafte Client-Anfragen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x1800DE	Citrix Secure Access Agent: App-Start ist während der Richtlinienauswertung fehlgeschlagen	Citrix Secure Access Agent: App-Start ist während der Richtlinienauswertung fehlgeschlagen
0x180055, 0x1800DF, 0x1800E3	Apps durch kontextbezogene Richtlinie eingeschränkt, Zugriff aufgrund von Richtlinienkonfiguration verweigert	Eine oder mehrere Apps sind nicht im Benutzer-Dashboard aufgeführt
0x1800EB	Citrix Secure Access Agent: App-Start ist fehlgeschlagen, da IPv6 nicht unterstützt wird	Citrix Secure Access Agent: App-Start ist fehlgeschlagen, da IPv6 nicht unterstützt wird
0x1800EC, 0x1800ED	Citrix Secure Access Agent: App-Start ist aufgrund einer ungültigen IP-Adresse fehlgeschlagen	Der Start der Citrix Secure Access Agent-App ist aufgrund einer ungültigen IP-Adresse fehlgeschlagen
0x10000001, 0x10000002, 0x10000003, 0x10000004	Anmeldung des Citrix Secure Access Clients aufgrund eines Netzwerkproblems fehlgeschlagen	Problem mit der Netzwerkkonnektivität des Citrix Secure Access Clients
0x10000006	Anmeldung des Citrix Secure Access Clients aufgrund eines Proxys in der Mitte fehlgeschlagen	Proxyserver stört die Client-Konnektivität mit dem Dienst
0x10000007	Anmeldung des Citrix Secure Access Clients aufgrund einer nicht vertrauenswürdigen Zertifizierungsstelle fehlgeschlagen	Problem mit nicht vertrauenswürdigem Serverzertifikat festgestellt
0x10000008	Anmeldung des Citrix Secure Access Clients aufgrund eines ungültigen Zertifikats fehlgeschlagen	Problem mit ungültigem Serverzertifikat festgestellt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x1000000A	Anmeldung des Citrix Secure Access Clients aufgrund eines Konfigurationsproblems fehlgeschlagen	Anmeldung fehlgeschlagen, da die Konfiguration für den Benutzer leer ist(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#login-failed-as-configuration-is-empty-for-the-user)
0x1000000B	Citrix Secure Access Client-Anmeldefehler aufgrund eines Verbindungsfehlers	Verbindung durch das Netzwerk oder den Endbenutzer beendet(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#connection-terminated-by-the-network-and-or-end-user)
0x10000010	Citrix Secure Access Client-Anmeldefehler aufgrund einer abgelaufenen Sitzung	Konfigurations-Download fehlgeschlagen, da die Sitzung abgelaufen ist(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#configuration-download-failed-as-session-is-expired)
0x10000013	Citrix Secure Access Client-Anmeldefehler aufgrund einer umfangreichen Konfigurationsliste	Citrix Secure Access Client konnte sich nicht anmelden(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#citrix-secure-access-client-failed-to-log-in)
0x11000003	Citrix Secure Access Client-Anmeldefehler aufgrund	Einrichtung des Steuerkanals fehlgeschlagen, da die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
	eines Fehlers bei der Erstellung des Steuerkanals	Sitzung abgelaufen ist(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-as-the-session-expired)
0x11000004	Citrix Secure Access Client-Anmeldefehler aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Einrichtung des Steuerkanals fehlgeschlagen(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed)
0x11000005	Fehler bei der Anmeldung des Citrix Secure Access Clients aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Einrichtung des Steuerkanals fehlgeschlagen(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-1)
0x11000006	Fehler bei der Anmeldung des Citrix Secure Access Clients aufgrund eines Fehlers bei der Erstellung des Steuerkanals	Einrichtung des Steuerkanals aufgrund eines Netzwerkproblems fehlgeschlagen(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#control-channel-establishment-failed-due-to-network-issue)
0x12000001	Fehler bei der Abmeldung des Citrix Secure Access Clients, da die Sitzung bereits abgelaufen ist	Abmeldung nicht möglich, da die Sitzung beendet wurde(/de-de/citrix-secure-private-access/service/secure-private-access-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
		troubleshooting.html#unable-to-logoff-as-session-is-terminated)
0x12000002	Fehler bei der Abmeldung des Citrix Secure Access Clients, da die Sitzung bereits abgelaufen ist	Sitzung wurde zwangsweise beendet(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#session-is-forcefully-terminated)
0x13000001	App-Zugriff fehlgeschlagen, da die Sitzung abgelaufen ist	Anwendungsstart fehlgeschlagen, da die Sitzung abgelaufen ist
0x13000002	App-Zugriff fehlgeschlagen, da Lizenz unzureichend ist	Anwendungsstart fehlgeschlagen aufgrund eines Lizenzproblems
0x13000003, 0x13000008, 0x001800DF	App-Zugriff fehlgeschlagen, da der Zugriff verboten ist; der Start der TCP/UDP-App wird gemäß Richtlinie verweigert	Anwendungsstart fehlgeschlagen, da der Zugriff vom Dienst verweigert wird
0x13000004, 0x13000005	App-Zugriff fehlgeschlagen, da der Server nicht verfügbar ist	Anwendungsstart fehlgeschlagen, da der Client den Dienst nicht erreichen kann
0x13000007	App-Zugriff fehlgeschlagen, da die Zugriffsrichtlinie deaktiviert ist oder der Benutzer nicht abonniert ist	Anwendungsstart fehlgeschlagen, da die Richtlinienauswertung und Konfigurationsvalidierung fehlgeschlagen sind
0x13000009	App-Zugriff fehlgeschlagen, da der Routing-Eintrag fehlt	Anwendungsstart fehlgeschlagen aufgrund von Problemen in der Anwendungsdomänentabelle(/de-de/citrix-secure-private-access/service/secure-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
		private-access-troubleshooting.html#application-launch-failed-because-of-issues-in-application-domain-table)
0x1300000B	Der Client hat die Verbindung geschlossen	Der Client hat die Verbindung mit dem Secure Private Access-Dienst geschlossen(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#client-closed-the-connection-with-secure-private-access-service)
0x1300000C	Die FQDN-Auflösung über ZTNA ist fehlgeschlagen	FQDN konnte vom DNS-Server nicht aufgelöst werden(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#unable-to-resolve-fqdn-by-the-dns-server)
0x1300000E	App-Start fehlgeschlagen, da ein Nicht-Chrome-Browser verwendet wurde	App-Start fehlgeschlagen, da ein Nicht-Chrome-Browser verwendet wurde(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#app-launch-failed-due-to-use-of-non-chrome-browser)
0x001800D3	Fehler beim Herunterladen der Anwendungskonfiguration während der Anmeldung	Fehler beim Abrufen der Liste der konfigurierten Anwendungsziele(/de-de/citrix-secure-private-access/service/secure-private-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
		access-troubleshooting.html#failed-to-fetch-configured-application-destinations-list)
0x001800D9, 0x001800DA	Der Start der TCP/UDP-App ist während der Analyse der Richtlinienauswertungsantwort fehlgeschlagen, der Start der TCP/UDP-App ist mit einem ungültigen Ergebnis während der Richtlinienauswertung fehlgeschlagen	Problem mit der Anwendungskonfiguration
0x001800DB	Der Start der TCP/UDP-App ist aufgrund einer ungültigen Konfiguration des Ressourcenstandorts fehlgeschlagen.	Problem mit dem Ressourcenstandort
0x13000006, 0x001800DC, 0x001800DD	Der Start der TCP-App ist aufgrund einer nicht unterstützten erweiterten Sicherheitsrichtlinie für die App fehlgeschlagen, der Start der TCP-App ist aufgrund einer nicht unterstützten Umleitung des Secure Browser Service für die TCP-App fehlgeschlagen.	Erweiterte Sicherheitsrichtlinie ist an die HTTP-Anwendung gebunden
0x001800DE	Der Start der TCP/UDP-App ist fehlgeschlagen, da keine Anwendungskonfiguration für das Ziel gefunden wurde.	Anwendung kann nicht gefunden werden
0x001800EA	Der Start der TCP-App ist fehlgeschlagen, da der Ziel-FQDN zu lang ist.	Hostname-Länge überschreitet 256 Zeichen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x001800ED	Der Start der TCP-App ist aufgrund einer ungültigen Ziel-IP fehlgeschlagen.	Ungültige IP-Adresse
0x001800EF	Der Start der TCP-Anwendung ist während des Verbindungsaufbaus zum privaten TCP-Server fehlgeschlagen	End-to-End-Verbindung kann nicht hergestellt werden
0x001800F5	Der Start der UDP-Anwendung ist aufgrund der IPv6-Adresse fehlgeschlagen	IPv6 in der Anwendungsanfrage empfangen
0x001800F9	UDP-Verkehr konnte nicht zugestellt werden, da die Client-Verbindung verloren ging	UDP-Verkehr konnte nicht zugestellt werden
0x001800FF	Zustellung des UDP-Datenverkehrs fehlgeschlagen	Zustellung des UDP-Datenverkehrs fehlgeschlagen
0x10000401	Verbindungsaufbau zum Citrix Rendezvous-Server fehlgeschlagen	Anwendungsstart aufgrund von Netzwerkverbindungsproblemen fehlgeschlagen
0x10000402, 0x1000040C	Registrierung der Connector Appliance nicht möglich, Initialisierungsfehler der UDP-Netzwerkverbindung	Registrierung der Connector Appliance beim Secure Private Access-Dienst fehlgeschlagen
0x10000403, 0x10000404, 0x10000407, 0x1000040A	Verbindungsfehler, Fehler bei der Übertragung von Steuerpaketen, Fehler beim Lesen des Gateway-Dienstes, Fehler beim Parsen von Steuerpaketen, Fehler beim Schreiben des Gateway-Dienstes	Verbindungsproblem mit der Connector Appliance
0x1000040B, 0x1000040F, 0x10000410		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x10000405, 0x10000408, 0x10000409, 0x1000040D	Back-End nicht erreichbar, Fehler bei der UDP-Paketübertragung, Fehler beim UDP-Paketempfang, Fehler beim Schreiben ins Back-End, Back-End hat die Verbindung geschlossen	Verbindungsprobleme mit der Connector Appliance und privaten TCP/UDP-Back-End-Servern
0x1000040E, 0x10000412		
0x10000406	DNS-Auflösung fehlgeschlagen	Connector-Appliance kann DNS für FQDNs nicht auflösen
0x10000411	Gateway-Dienst hat die Verbindung geschlossen	Private Serververbindung beendet
0x10000413	Fehler beim Ermitteln des Grundes für den Verbindungsabbau	Verbindung zum privaten Dienst-IP oder FQDN konnte nicht hergestellt oder Daten gesendet werden
0x100508	Benutzerkontext stimmt nicht mit den Zugriffsregelbedingungen überein	Keine übereinstimmende Richtlinienbedingung
0x100509	Zugriffsrichtlinie ist der Anwendung nicht zugeordnet	Keine Zugriffsrichtlinie der Anwendung zugeordnet
0x10050C	Ergebnisse der Richtlinienauswertung mehrerer Anwendungen, für die der Benutzer möglicherweise berechtigt ist	Informationen zur App-Aufzählung
0x00180101	Start der TCP/UDP-App fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt	Start der TCP/UDP-App fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x00180102	Start der TCP/UDP-App fehlgeschlagen, da Konnektoren nicht fehlerfrei sind	Start der TCP/UDP-App fehlgeschlagen, da Konnektoren nicht fehlerfrei sind
0x00180103	UDP/DNS-Anfrage fehlgeschlagen, da der Connector nicht erreichbar ist	UDP/DNS-Anfrage fehlgeschlagen, da der Connector nicht erreichbar ist
0x20580001	Fehler beim Laden der Seite, da das NGS-Cookie abgelaufen ist	Fehler beim Laden der Seite, da das NGS-Cookie abgelaufen ist
0x20580002	Abruf der Zugriffsrichtlinie aufgrund eines Netzwerkfehlers fehlgeschlagen	Abruf der Zugriffsrichtlinie aufgrund eines Netzwerkfehlers fehlgeschlagen
0x20580003	Abruf der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens fehlgeschlagen	Abruf der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens fehlgeschlagen
0x20580004	Netzwerkfehler beim Abrufen der Details zur Zugriffsrichtlinie	Netzwerkfehler beim Abrufen der Details zur Zugriffsrichtlinie
0x20580005	Richtlinienabruf beim Abrufen des öffentlichen Zertifikats fehlgeschlagen	Richtlinienabruf beim Abrufen des öffentlichen Zertifikats fehlgeschlagen
0x20580007	Richtlinienabruf bei der Validierung der JWT-Signatur fehlgeschlagen	Richtlinienabruf fehlgeschlagen bei der Validierung der JWT-Signatur
0x20580008	Richtlinienabruf fehlgeschlagen bei der Validierung des öffentlichen Zertifikats	Richtlinienabruf fehlgeschlagen bei der Validierung des öffentlichen Zertifikats
0x2058000A	Speicherumgebung konnte nicht ermittelt werden, um	Speicherumgebung konnte nicht ermittelt werden, um

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
	eine Richtlinien-URL zu erstellen	eine Richtlinien-URL zu erstellen
0x2058000B	Antwort auf die Abrufanfrage für Zugriffsrichtlinien konnte nicht abgerufen werden	Antwort auf die Abrufanfrage für Zugriffsrichtlinien konnte nicht abgerufen werden
0x2058000C	Abruf der Zugriffsrichtlinie fehlgeschlagen aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens	Abruf der Zugriffsrichtlinie fehlgeschlagen aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens
0x10200002	Connector-Appliance ist nicht registriert	Connector Appliance ist nicht registriert
0x10200003	Verbindung zur Connector Appliance nicht möglich	Verbindung zur Connector Appliance nicht möglich
0x10000301	Verbindung zum Citrix SPA-Dienst fehlgeschlagen	Verbindung zum Citrix Secure Private Access-Dienst fehlgeschlagen
0x10000303, 0x10000304	Der Proxyserver ist nicht erreichbar	Proxyserver ist nicht erreichbar
0x10000305	Authentifizierung am Proxyserver fehlgeschlagen	Authentifizierung am Proxyserver fehlgeschlagen
0x10000306	Konfigurierte Proxyserver sind nicht erreichbar	Konfigurierte Proxyserver sind nicht erreichbar(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#configured-proxy-servers-are-not-reachable)
0x10000307	Fehlerantwort vom Backend-Server erhalten	Fehlerantwort vom Backend-Server erhalten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFOCODE	BESCHREIBUNG	LÖSUNG
0x10000005	Anfrage konnte nicht an die Ziel-URL gesendet werden	Anfrage konnte nicht an die Ziel-URL gesendet werden
0x10000107	Fehler bei der SSO-Verarbeitung	Fehler bei der SSO-Verarbeitung
0x10000108, 0x1000010B	Fehler bei der SSO-Verarbeitung, SSO-Einstellungen konnten nicht ermittelt werden	Fehler bei der SSO-Verarbeitung, SSO-Einstellungen konnten nicht ermittelt werden
0x10000101, 0x10000102, 0x10000103, 0x10000104	FormFill-SSO fehlgeschlagen, falsche Formular-App-Konfiguration	FormFill-SSO fehlgeschlagen, falsche Formular-App-Konfiguration
0x1000010A	FormFill-SSO fehlgeschlagen, falsche Formular-App-Konfiguration	FormFill-SSO fehlgeschlagen, falsche Formular-App-Konfiguration
0x10000202	Kerberos-SSO fehlgeschlagen	Kerberos-SSO fehlgeschlagen
0x10000203	SSO-Verarbeitung für Authentifizierungstyp fehlgeschlagen	SSO-Verarbeitung für Authentifizierungstyp fehlgeschlagen
0x10000204	Kerberos-SSO fehlgeschlagen, aber Rückgriff auf NTLM	Kerberos-SSO fehlgeschlagen, aber Rückgriff auf NTLM
0x14000001	Mehrere ZTNA-berechtigte Konten in der Citrix Workspace-Anwendung konfiguriert	Mehrere ZTNA-berechtigte Konten in der Citrix Workspace-Anwendung konfiguriert(/de-de/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#multiple-ztna-entitled-accounts-configured-in-citrix-workspace-application)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lösungsschritte

Die folgenden Abschnitte enthalten Lösungsschritte für die meisten Infocodes. Für Codes, für die keine Lösungsschritte erfasst wurden, wenden Sie sich an den Citrix Support.

Eine oder mehrere Apps werden nicht im Benutzer-Dashboard aufgeführt

Infocode: 0x180055, 0x1800DF, 0x1800E3

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

1. Kopieren Sie die Transaktions-ID aus der Spalte `reasons` für den Fehlercode `0x18005C` in der CSV-Datei der Diagnoseprotokolle.
2. Ändern Sie den Spaltenfilter `prod` in der CSV-Datei, um Ereignisse von der Komponente `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 `reason` nach der ausgewerteten Richtlinien-Payload. Diese Payload zeigt die ausgewertete Richtlinie für den Benutzerkontext für alle Apps an, die der Benutzer abonniert hat.
4. Wenn die Richtlinienauswertung anzeigt, dass die App für den Benutzer verweigert wurde, können die möglichen Gründe sein:

    - 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 Standardübereinstimmungsregel in der Richtlinie – dies ist ein Fallback-Szenario. Passen Sie die Bedingungen entsprechend an.

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 hat.

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

1. Gehen Sie im Verwaltungsportal zur Anwendung.
2. Bearbeiten Sie die App und gehen Sie zur Registerkarte **Abonnement**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Stellen Sie sicher, dass der Zielbenutzer in der Abonnementliste aufgeführt ist.

Langsame Leistung der Back-End-App

Infocode: 0x18000F

Es gibt Fälle, in denen das Kundennetzwerk aufgrund von Konnektoren an einem Ressourcenstandort, die ausgefallen sein können, oder weil der Back-End-Server selbst nicht reagiert, instabil ist.

1. Stellen Sie sicher, dass die Connector Appliance geografisch nahe am Back-End-Server positioniert ist, um Netzwerklatenzen auszuschließen.
2. Überprüfen Sie, ob die Firewall des Back-End-Servers die Connector Appliance nicht blockiert.
3. Überprüfen Sie, ob der Client eine Verbindung zum nächstgelegenen Cloud-POP herstellt.

   Zum Beispiel zeigt `nslookup nssvc.dnsdiag.net` auf dem Client der kanonische Name in der Antwort den geospezifischen Server an, wie `aws-us-w.g.nssvc.net.`.

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

Infocode: 0x180006, 0x1800B7

App-FQDNs dürfen eine Länge von 512 Zeichen nicht überschreiten. Überprüfen Sie den Anwendungs-FQDN auf der App-Konfigurationsseite. Stellen Sie sicher, dass die Länge 512 Byte nicht überschreitet.

1. Gehen Sie auf der Verwaltungskonsole zur Registerkarte **Anwendungen**.
2. Suchen Sie nach der Anwendung, deren FQDN 512 Zeichen überschreitet.
3. Bearbeiten Sie die Anwendung und korrigieren Sie die Länge des Anwendungs-FQDN.

Länge der Anwendungsdetails 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.

App-Zugriff verweigert

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dies bezieht sich auf kontextbezogene Richtlinien, bei denen Richtlinien die App für einen bestimmten Benutzer verweigern.

Überprüfen Sie die Richtlinien, ob sie den App-Zugriff blockieren.

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

Anwendungen nicht aufgelistet

Anwendungen können in der aufgelisteten Liste fehlen, weil Richtlinien verweigert wurden oder die Secure Private Access-Integration nicht aktiviert ist.

- Wenn der Zugriff für einige der Apps aktiviert werden muss, Sie aber keine Apps sehen, versuchen Sie, die Secure Private Access-Integration zu aktivieren.
  - Melden Sie sich bei Citrix Cloud an.
  - Wählen Sie **StoreFront Cloud** aus dem Hamburger-Menü und klicken Sie dann auf **Service Integrations**.
  - Klicken Sie auf die Schaltfläche mit den Auslassungspunkten in Secure Private Access und dann auf **Aktivieren**.
- Wenn die Secure Private Access-Integration bereits aktiviert ist, deaktivieren Sie sie und aktivieren Sie sie dann erneut, um zu sehen, ob Sie Apps haben.

Problem beim Verbinden mit Connector Appliance

Infocode: 0x1800EF

Das App-Routing schlägt aufgrund der Nichtverfügbarkeit von TCP-Verbindungen mit lokalen Konnektoren fehl.

EREIGNISSE DER CONTROLLER-KOMPONENTE ÜBERPRÜFEN

1. Suchen Sie nach dem `transaction ID` für den Fehlercode `0x1800EF` in der CSV-Datei der Diagnoseprotokolle.
2. Filtern Sie alle Ereignisse, die der Transaktions-ID in der CSV-Datei entsprechen.
3. Filtern Sie auch die Spalte `prod` in der CSV-Datei, die `SWA.GOCTRL` entsprechen.

   Wenn Sie Ereignisse mit der Meldung `connectType` `multiconnect::success` sehen, dann:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Dies weist darauf hin, dass die Anforderung zur Tunnelherstellung erfolgreich an den Controller weitergeleitet wurde.
- Überprüfen Sie, ob `Resource Location` in der Protokollmeldung korrekt ist. Wenn dies nicht der Fall ist, korrigieren Sie den Ressourcenstandort im Abschnitt zur App-Konfiguration im Citrix Management Portal.
- Überprüfen Sie, ob `VDA Ip and Port` in der Protokollmeldung korrekt ist. Die VDA-IP und der Port geben die IP und den Port der Back-End-Anwendung an. Wenn dies nicht der Fall ist, korrigieren Sie den App-FQDN oder die IP-Adresse im Abschnitt zur App-Konfiguration im Citrix Management Portal.
- Fahren Sie mit der Überprüfung der Connector-Ereignisse fort, wenn Sie keine der zuvor genannten Probleme finden.

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

- Überprüfen Sie, ob die empfohlene Lösung für diese Protokollmeldung lautet: `Check if connector is still connected to same pop`. Dies weist darauf hin, dass der Connector am Ressourcenstandort möglicherweise ausgefallen ist. Fahren Sie mit der Überprüfung der Connector-Ereignisse fort.
- 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.

EREIGNISSE DER CONNECTOR-KOMPONENTE ÜBERPRÜFEN

1. Suchen Sie `transaction ID` für den Fehlercode `0x1800EF` in der CSV-Datei der Diagnoseprotokolle.
2. Filtern Sie alle Ereignisse, die der Transaktions-ID in der CSV-Datei entsprechen.
3. Filtern Sie auch die Spalte `prod` in der CSV-Datei, die `SWA.ConnectorAppliance.WebApps` entspricht.
4. Wenn Sie Ereignisse mit `status` als `failure` sehen, dann:
   - Überprüfen Sie die Meldung `reason` für jedes dieser Fehlerereignisse.
   - `UnableToRegister` zeigt an, dass der Connector sich nicht erfolgreich bei Citrix Cloud registrieren konnte. Wenden Sie sich an den Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `IsProxyRequiredCheckError` oder `ProxyDialFailed` oder `ProxyConnectionFailed` oder `ProxyAuthenticationFailure` oder `ProxiesUnReachable` zeigt an, dass der Connector die Back-End-URL über die Proxy-Konfiguration nicht auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Korrektheit.
- Weitere Informationen zur Fehlerbehebung finden Sie unter Connector-SSO-Ereignisse.

Fehler bei der einmaligen Anmeldung

Für die einmalige Anmeldung werden verschiedene SSO-Attribute aus der App-Konfiguration extrahiert und während des App-Starts angewendet. Wenn dieser bestimmte Benutzer die Attribute nicht besitzt oder wenn 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 eine Berechtigung hat.
3. Überprüfen Sie die Richtlinienregeln und -bedingungen für den Endbenutzer.

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

SSO-EREIGNISSE DER CONNECTOR-KOMPONENTE ÜBERPRÜFEN

1. Filtern Sie die `component name` in der CSV-Datei, die `SWA.ConnectorAppliance.WebApps` entsprechen.
2. Sehen Sie Ereignisse mit dem Status „Fehler“?
   - 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 über die Proxy-Konfiguration nicht auflösen konnte. Überprüfen Sie die Proxy-Konfiguration auf Korrektheit.
   - `FailedToReadRequest` oder `RequestReceivedForNonSecureBrowse` oder `UnableToRetrieveUserCredentials` oder `CCSPolicyIsNotLoaded` oder `FailedToLoadBaseClient` oder `ProcessConnectionFailure` oder `WebAppUnSupportedAuthType` zeigt einen Tunneling-Fehler an. Wenden Sie sich an den Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `UnableToConnectTargetServer` zeigt an, dass der Back-End-Server vom Connector aus nicht erreichbar ist. Überprüfen Sie die Back-End-Konfiguration erneut.
- `IncorrectFormAppConfiguration` oder `NoLoginFormFound` oder `FailedToConstructForLoginActionURL` oder `FailedToLoginViaFormBasedAuth` weist auf einen Fehler bei der formularbasierten Authentifizierung hin. Überprüfen Sie den Abschnitt zur Formular-SSO-Konfiguration in der App-Konfiguration im Citrix Management Portal.
- `NTLMAuthNotFound` weist auf einen Fehler bei der NTLM-basierten Authentifizierung hin. Überprüfen Sie den Abschnitt zur NTLM-SSO-Konfiguration in der App-Konfiguration im Citrix Management Portal.
- Weitere Informationen zum Debugging finden Sie unter Connector-Ereignisse.

App-Start fehlgeschlagen, da der Authentifizierungsdienst nicht verfügbar ist

Infocode: 0x180022

Secure Private Access ermöglicht Administratoren die Konfiguration eines Authentifizierungsdienstes von Drittanbietern, wie z. B. das traditionelle 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

Benutzer stoßen beim Starten der App auf einen Authentifizierungsfehler, wenn dieser IdP-initiiert ist, oder sehen möglicherweise unzugängliche Links, wenn dieser SP-initiiert ist. Überprüfen Sie die SAML-App-Konfiguration auf der Secure Private Access-Dienstseite sowie die Dienstanbieterkonfiguration.

Secure Private Access-Konfiguration:

1. Gehen Sie zur Registerkarte **Anwendungen**.
2. Suchen Sie nach der problematischen SAML-App.
3. Bearbeiten Sie die Anwendung und gehen Sie zur Registerkarte **Single Sign-On**.
4. Überprüfen Sie die folgenden Felder.
    - Assertions-URL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Relay-Status
- Zielgruppe
- Name-ID-Format, Name-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 die App über das Netzwerk zugänglich ist.

WEB-APP-VALIDIERUNG

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

Fehlerhafte Browser-Erfahrung über den Remote Browser Isolation-Dienst. Überprüfen Sie den Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte.

1. Gehen Sie zum Back-End-Server und prüfen Sie, ob er läuft und Anfragen empfangen kann.
2. Überprüfen Sie die Proxy-Einstellungen, falls diese die Verbindung zum Back-End-Server blockieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Der Dienst Citrix Remote Browser Isolation™ war früher als Secure Browser Service bekannt.

CWA Web – DNS-Suche/Verbindungsfehler für Web-Apps

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

Beschädigtes Browser-Erlebnis von 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 – als Web-App falsch konfiguriert

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

Überprüfen Sie die widersprüchliche Konfiguration zwischen der Routing-Domänentabelle und der App-Konfiguration.

1. Gehen Sie im Verwaltungsportal zur Anwendung.
2. Bearbeiten Sie die App und prüfen Sie, ob der direkte Zugriff aktiviert ist.
3. Überprüfen Sie den FQDN der App in der Routing-Domänentabelle, ob er als intern markiert wurde.

Benutzer ist nicht berechtigt, auf die Web-/SaaS-App für DirectAccess zuzugreifen

Infocode: 0x1800BD

Die App-Konfiguration deaktiviert den direkten Zugriff für Datenverkehr, der von browserbasierten Clients stammt.

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

1. Gehen Sie im Verwaltungsportal zur Anwendung.
2. Bearbeiten Sie die App und überprüfen Sie die agentenlose Zugriffskonfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erweiterte Sicherheitsrichtlinien – Fehlkonfiguration des Secure Browser Service

Infocode: 0x1800C3

Es wurde ein falsches Verhalten beobachtet, das nicht den Richtlinienregeln entsprach. Überprüfen Sie die kontextbezogenen Zugriffsrichtlinien.

1. Gehen Sie zur Registerkarte **Richtlinien**.
2. Überprüfen Sie die der Anwendung zugeordneten Richtlinien.
3. Überprüfen Sie die Regeln für diese Richtlinien.

Erweiterte Sicherheitsrichtlinien – Richtlinienfehlkonfiguration

Es wurde ein falsches Verhalten beobachtet, das nicht den Richtlinienregeln entsprach. Überprüfen Sie die erweiterten Sicherheitseinstellungen.

1. Gehen Sie zur Anwendung.
2. Klicken Sie auf die Registerkarte **Zugriffsrichtlinien**.
3. Überprüfen Sie die Einstellungen im Abschnitt **Verfügbare Sicherheitseinschränkungen:**.

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

Infocode: 0x1800D0

Die Citrix Secure Access App kann keinen vollständigen Tunnel zu Citrix Cloud erfolgreich herstellen.

1. Überprüfen Sie die Routing-Domain-Konfiguration für die TCP/UDP-Anwendungen.
2. Stellen Sie sicher, dass die maximale Anzahl der Einträge innerhalb des 16k-Limits liegt.

TCP/UDP-Anwendungen – fehlerhafte Client-Anfragen

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

Entweder ist der VPN-Tunnel nicht eingerichtet, oder bestimmte FQDNs werden möglicherweise nicht getunnelt.

1. Stellen Sie sicher, dass die Anfragen nicht von Proxys in der Mitte gefälscht oder rekonstruiert werden.
2. Vermutete Man-in-the-Middle-Angriffe.

TCP/UDP-Anwendungen – Fehlkonfiguration der Umleitung des Secure Browser Service

Infocode: 0x1800DD

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Umleitungen des Remote Browser Isolation-Dienstes können nur für Web-Apps und nicht für 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 Routing-Domain-Tabelle haben.

Start der Citrix Secure Access Agent-App fehlgeschlagen, da IPv6 nicht unterstützt wird

Infocode: 0x1800EB

Überprüfen Sie die Routing-Domain-Einträge. Stellen Sie sicher, dass keine IPv6-Einträge in der Tabelle vorhanden sind.

Start der Citrix Secure Access Agent-App aufgrund einer ungültigen IP-Adresse fehlgeschlagen

Infocode: 0x1800EC, 0x1800ED

Überprüfen Sie die Routing-Domain-Einträge. Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Backend verweisen.

Problem mit der Netzwerkkonnektivität des Citrix Secure Access Clients

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

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

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So sammeln Sie Client-Protokolle.

Proxy-Server stört die Client-Konnektivität mit dem Dienst

Infocode: 0x10000006

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Überprüfen Sie, ob das Netzwerk des Client-Computers erreichbar ist.
2. Überprüfen Sie, ob der Proxy im Client korrekt konfiguriert ist.
3. Wenn es bei beiden keine Probleme gibt, wenden Sie sich mit den Client-Debug-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter Sammeln von Client-Protokollen.

Problem mit nicht vertrauenswürdigem Serverzertifikat festgestellt

Infocode: 0x10000007

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

Problem mit ungültigem Serverzertifikat festgestellt

Infocode: 0x10000008

Wenden Sie sich an den Citrix Support, um zu überprüfen, ob das Serverzertifikat selbstsigniert, abgelaufen oder von einer nicht vertrauenswürdigen Quelle stammt.

Anmeldung fehlgeschlagen, da die Konfiguration für den Benutzer leer ist

Infocode: 0x1000000A

1. Stellen Sie sicher, dass mindestens eine TCP/UDP/HTTP-App konfiguriert ist. Weitere Informationen finden Sie unter Anwendungen hinzufügen und verwalten.
2. Stellen Sie sicher, dass die Tabelle Anwendungsdomäne (**Secure Private Access > Einstellungen > Anwendungsdomäne**) nicht leer ist oder 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 die URL einer aktiven TCP/UDP/HTTP-Anwendung nicht zu löschen oder zu deaktivieren.

Verbindung durch das Netzwerk und/oder den Endbenutzer beendet

Infocode: 0x1000000B

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsdownload fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode: 0x10000010

Die VPN-Sitzung ist möglicherweise während der ZTNA-Sitzungskonfigurations-Downloadanforderung abgelaufen. Versuchen Sie, sich erneut beim Citrix Secure Access Client anzumelden.

Citrix Secure Access Client konnte sich nicht anmelden

Infocode: 0x10000013

Der Citrix Secure Access Client konnte sich nicht anmelden, da die Konfigurationsgröße das maximale Konfigurationslimit überschreitet.

1. Überprüfen Sie die Routing-Domain-Konfiguration für die TCP/UDP-Anwendungen unter **Secure Private Access > Settings > Application Domain**
2. Stellen Sie sicher, dass die Anzahl der Einträge nicht zu groß ist. Wenn die Einträgeliste zu groß ist, deaktivieren oder entfernen Sie ungenutzte Ziele.

   Wenn die Zielliste voraussichtlich mehr als 1000 Einträge enthält, versuchen Sie, die maximale Konfigurationsdownloadgröße zu erhöhen, indem Sie den Registrierungsschlüssel ConfigSize aktualisieren. Weitere Informationen finden Sie unter Citrix Gateway VPN client registry keys.

Einrichtung des Steuerkanals fehlgeschlagen, da die Sitzung abgelaufen ist

Infocode: 0x11000003

Der Steuerkanal für die DNS-Anforderungsherstellung 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.

Einrichtung des Steuerkanals fehlgeschlagen

Infocode: 0x11000004

Die Einrichtung des Steuerkanals für DNS-Anfragen ist fehlgeschlagen.

- **Ressourcenstandort intakt halten:**

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie im Hamburger-Menü auf **Ressourcenstandort**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Führen Sie eine Integritätsprüfung für die Connector Appliances am jeweiligen Ressourcenstandort durch.
4. Wenn dies das Problem nicht behebt, versuchen Sie, die virtuelle Connector-Maschine neu zu starten.

- **HA-Connector-Appliance intakt halten:**

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie im Hamburger-Menü auf **Ressourcenstandort**.
3. Stellen Sie sicher, dass der erwartete Ressourcenstandort mindestens zwei Connector Appliances aufweist.

Stellen Sie Folgendes sicher:

- Das LAN des Ressourcenstandorts ist funktionsfähig.
- Keine Firewall oder kein Proxy blockiert die Connector Appliance auf dem Weg zum Dienst oder zu den Back-End-Servern.
- Das Client-Netzwerk ist fehlerfrei.
- Die privaten Back-End-Server sind betriebsbereit.
- Die DNS-Server sind betriebsbereit.
- FQDNs sind auflösbar.

Wenn Sie die vorstehenden Empfehlungen erfüllen, gehen Sie wie folgt vor.

1. Rufen Sie die Transaktions-ID für diesen Fehler aus dem Diagnoseprotokoll ab.
2. Filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Secure Private Access Dashboard.
3. Überprüfen Sie, ob in den Diagnoseprotokollen des Clients, der Connector Appliance oder des Dienstes ein Fehler aufgetreten ist, der der Transaktions-ID entspricht. Ergreifen Sie dann die entsprechenden Maßnahmen.
4. Überprüfen Sie, ob der Ressourcenstandort für das Ziel in der Anwendungsdomänentabelle (**Secure Private Access > Einstellungen > Anwendungsdomäne**) korrekt ausgewählt ist.
5. Überprüfen Sie, ob die Anwendung mit dem richtigen Port, 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 an den Citrix Support mit dem Fehlercode, der der Transaktions-ID und den Client-Protokollen entspricht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter Sammeln von Client-Protokollen.

Einrichtung des Steuerkanals fehlgeschlagen

Infocode: 0x11000005

Einrichtung des Steuerkanals (für DNS-Anfrage) fehlgeschlagen.

1. Überprüfen Sie die Lizenzberechtigung für den Secure Private Access-Dienst.
2. Falls nicht berechtigt, wenden Sie sich an den Citrix Support, um die Lizenz zu überprüfen.

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

Einrichtung des Steuerkanals aufgrund eines Netzwerkproblems fehlgeschlagen

Infocode: 0x11000006

Einrichtung des Steuerkanals (für DNS-Anfrage) aufgrund eines Netzwerkproblems fehlgeschlagen.

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

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So sammeln Sie Client-Protokolle.

Einrichtung des Steuerkanals aufgrund unzureichender IIPs fehlgeschlagen

Infocode: 0x11000007

Einrichtung des Steuerkanals (für DNS-Anfrage) aufgrund unzureichender IIPs fehlgeschlagen.

Wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So sammeln Sie Client-Protokolle.

Abmeldung nicht möglich, da die Sitzung beendet wurde

Dieses Problem könnte aufgetreten sein, weil die Clientmaschine (Tastatur oder Maus) länger als die konfigurierte Zeitüberschreitung inaktiv war.

Infocode: 0x12000001

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Sitzung wird zwangsweise beendet

Die Sitzung wird zwangsweise beendet, da die konfigurierte erzwungene Zeitüberschreitung erreicht wurde.

Infocode: 0x12000002

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

Anwendungsstart 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.

Anwendungsstart fehlgeschlagen aufgrund eines Lizenzproblems

Infocode: 0x13000002

1. Überprüfen Sie die Berechtigung für die Secure Private Access-Dienstlizenz.
2. Wenn Sie nicht berechtigt sind, wenden Sie sich an den Citrix Support, um die Lizenz zu überprüfen.

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

Anwendungsstart fehlgeschlagen, da der Zugriff vom Dienst verweigert wird

Infocode: 0x13000003, 0x13000008, 0x001800DF

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

Stellen Sie Folgendes sicher:

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

Überprüfen Sie auch die Bedingungen und Aktionen der für die verweigerte Anwendung konfigurierten Richtlinien. Überprüfen Sie anschließend die Richtlinienbedingungen und -aktionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Zugriffsrichtlinien.

Anwendungsstart 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 Clientprotokollen an den Citrix Support.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So sammeln Sie Client-Protokolle.

Anwendungsstart fehlgeschlagen, da Richtlinienauswertung und Konfigurationsvalidierung fehlgeschlagen sind

Infocode: 0x13000007

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

Anwendung für das aufgerufene Ziel konnte nicht gefunden werden.

Anwendungsstart fehlgeschlagen, da der Zugriff vom Dienst verweigert wurde.

Anwendungsstart fehlgeschlagen aufgrund von Problemen in der Anwendungsdomänentabelle

Infocode: 0x13000009

Der Anwendungsstart ist fehlgeschlagen, da die Anwendungsdomänentabelle keinen Eintrag für das aufgerufene Ziel enthält.

Überprüfen Sie, ob der Routeneintrag für die Anwendung unter **Secure Private Access > Einstellungen > Anwendungsdomäne** korrekt konfiguriert ist.

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. Falls nicht, wenden Sie sich mit dem Fehlercode und den Client-Protokollen an den Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So sammeln Sie Client-Protokolle.

FQDN kann vom DNS-Server nicht aufgelöst werden

Infocode: 0x1300000C

Dieses Problem tritt auf, wenn die Connector Appliance die DNS-Auflösung für FQDNs nicht durchführen kann.

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

Start der Anwendung fehlgeschlagen aufgrund der Verwendung eines Nicht-Chrome-Browsers

Infocode: 0x1300000E

Der Anwendungsstart schlägt fehl, weil der Browsermodus auf Google Chrome Enterprise Premium eingestellt ist und ein Nicht-Chrome-Browser verwendet wird.

Verwenden Sie den Chrome-Browser, um die Anwendung zu starten.

- Überprüfen Sie, ob der Standard-Systembrowser im System des Benutzers auf Chrome eingestellt ist.
- Überprüfen Sie, ob der Benutzer nicht versucht, die App manuell mit einem Nicht-Chrome-Browser zu starten.

Anwendung nicht auffindbar

Infocode: 0x001800DE

Möglicherweise können Sie die Anwendung für das aufgerufene Ziel für den Benutzer nicht finden. Dies kann auftreten, wenn die Zuordnung von Ziel zu 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 ein Abonnement für die Anwendung für das aufgerufene Ziel hat.

1. Gehen Sie im Verwaltungsportal zur Anwendung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Ressourcenstandort enthält.

Fehler beim Abrufen der Liste der konfigurierten Anwendungsziele

Infocode: 0x001800D3

- Stellen Sie sicher, dass mindestens eine TCP/UDP/HTTP-App konfiguriert ist. Weitere Informationen finden Sie unter Anwendungen hinzufügen und verwalten.
- Stellen Sie sicher, dass die Seite der Tabelle Anwendungsdomäne (**Secure Private Access > Einstellungen > Anwendungsdomäne**) nicht leer ist oder 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 Tabelle Anwendungsdomäne nicht zu löschen oder zu deaktivieren.

Problem bei der Anwendungskonfiguration

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

Infocode: 0x001800D9, 0x001800DA

Stellen Sie Folgendes sicher:

- Die App-Konfiguration enthält keine nicht unterstützten Zeichen.
- Die Ziel-IP-Adresse oder der IP-Adressbereich oder der IP-CIDR sind gültig.
- Das Anwendungsziel ist in der Tabelle „Anwendungsdomäne“ aktiviert (**Secure Private Access > Einstellungen > Anwendungsdomäne**).
- Die Richtlinien sind konfiguriert und der jeweiligen Anwendung zugewiesen.
- Die Konfiguration der Zugriffsrichtlinie ist korrekt.

Problem mit dem Ressourcenstandort

Infocode: 0x001800DB

- Stellen Sie sicher, dass ein Ressourcenstandort konfiguriert ist.
    a. Wählen Sie im Hamburger-Menü von Citrix Cloud die Option **Ressourcenstandort** aus.
    b. Stellen Sie sicher, dass der erwartete Ressourcenstandort konfiguriert und der Ressourcenstandort aktiv ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Stellen Sie sicher, dass in der Tabelle „Anwendungsdomäne“ (**Secure Private Access > Einstellungen > Anwendungsdomäne**) ein korrekter Ressourcenstandort für das Ziel ausgewählt ist.

Die in der TCP/UDP/HTTP-Anwendung konfigurierten Ziele werden automatisch zu dieser Tabelle hinzugefügt. Es wird empfohlen, die Ziele oder URLs der aktiven TCP/UDP/HTTP-Anwendung in der Tabelle „Anwendungsdomäne“ nicht zu löschen oder zu deaktivieren.

Erweiterte Sicherheitsrichtlinie ist an die HTTP-Anwendung gebunden

Infocode: 0x001800DC, 0x001800DD, 0x13000006

Die HTTP-Anwendung, an die eine erweiterte Sicherheitsrichtlinie gebunden ist, wird über den Citrix Secure Access Client aufgerufen.

- Stellen Sie sicher, dass dasselbe Ziel nicht sowohl für TCP/UDP- als auch für HTTP-Anwendungen verwendet wird.
- Wenn die erweiterte Sicherheitsrichtlinie für HTTP/HTTPS-Anwendungen aktiviert ist, wird empfohlen, die App nur über die Citrix Workspace-App oder den Citrix Remote Browser Isolation-Dienst aufzurufen.
- 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-Administratorportal.
    - 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 identifizierten Richtliniennamen.
    - Wählen Sie die Richtlinie aus und klicken Sie auf **Bearbeiten**.
    - Ändern Sie die Aktion von **Zugriff mit Einschränkung zulassen** in **Zugriff zulassen.**

Weitere Informationen zur Konfiguration finden Sie unter Anwendungen hinzufügen und verwalten.

HINWEIS:

Der Citrix Remote Browser Isolation-Dienst war früher als Secure Browser-Dienst bekannt.

Länge des Hostnamens überschreitet 256 Zeichen

Infocode: 0x001800EA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der im Anwendungsstart-Request empfangene Hostname überschreitet 256 Zeichen.

Es wird empfohlen, dass die FDQN-Zeichen 256 Zeichen nicht überschreiten.

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.

End-to-End-Verbindung kann nicht hergestellt werden

Infocode: 0x001800EF

End-to-End-Verbindung zwischen dem Client und dem in der Ressourcenstandort konfigurierten Server kann nicht hergestellt werden.

- Stellen Sie sicher, dass der Ressourcenstandort aktiv ist.
  - Wählen Sie im Hamburger-Menü von Citrix Cloud die Option **Ressourcenstandort**.
  - Führen Sie eine Integritätsprüfung für die Connector Appliances am jeweiligen Ressourcenstandort durch.
  - Wenn dies das Problem nicht behebt, starten Sie die virtuelle Connector-Maschine neu.
- Halten Sie eine hochverfügbare Connector Appliance bereit
  - Wählen Sie im Hamburger-Menü von Citrix Cloud die Option **Ressourcenstandort**.
  - Stellen Sie sicher, dass der Ressourcenstandort mindestens zwei Connector Appliances hat.
- Stellen Sie Folgendes sicher:
  - Das LAN des Ressourcenstandorts ist funktionsfähig.
  - Keine Firewalls oder Proxys blockieren die Connector Appliance zum Dienst oder zu den Back-End-Servern.
  - Client-Netzwerk ist fehlerfrei.
  - Private Back-End-Server sind fehlerfrei.
  - DNS-Server sind fehlerfrei.
  - FQDNs sind auflösbar.

Wenn es damit keine Probleme gibt, gehen Sie wie folgt vor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Rufen Sie die Transaktions-ID für diesen Fehler aus den Diagnoseprotokollen ab.
2. Filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Dashboard des Secure Private Access-Dienstes.
3. Überprüfen Sie die Diagnoseprotokolle, die der Transaktions-ID im Dashboard des Secure Private Access-Dienstes entsprechen, und ergreifen Sie dann entsprechende Maßnahmen.
4. Überprüfen Sie, ob in der Tabelle „Anwendungsdomäne“ (**Secure Private Access > Einstellungen > Anwendungsdomäne**) ein korrekter Ressourcenstandort als Ziel ausgewählt ist.
5. Überprüfen Sie, ob die Anwendung (**Secure Private Access > Anwendungen**) mit der korrekten IP-Adresse, dem Port und dem FQDN konfiguriert ist.

Wenn keiner dieser Schritte das Problem löst, wenden Sie sich an den Citrix Support mit dem Fehlercode, der der Transaktions-ID entspricht, und erfassen Sie Clientprotokolle.

Informationen zum Sammeln von Client-Debug-Protokollen finden Sie unter So erfassen Sie Clientprotokolle.

IPv6 in der App-Anfrage empfangen

Infocode: 0x001800F5

In der App-Anfrage wurde eine nicht unterstützte IPv6-Adresse empfangen. 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-Administratorportal.
2. Klicken Sie auf die Registerkarte **Anwendungen**.
3. Suchen Sie nach der App und klicken Sie auf **Bearbeiten**.

Weitere Informationen finden Sie unter Apps hinzufügen und verwalten.

UDP-Datenverkehr konnte nicht zugestellt werden

Infocode: 0x001800F9

UDP-Datenverkehr konnte nicht zugestellt werden, da die Clientverbindung unterbrochen ist

1. Überprüfen Sie, ob die Clientsitzung aktiv ist.
2. Melden Sie sich ab und dann wieder an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UDP-Datenverkehr konnte nicht zugestellt werden

Infocode: 0x001800FF

- Suchen Sie die Transaktions-ID für den Fehlercode und filtern Sie alle Ereignisse, die der Transaktions-ID entsprechen, im Secure Private Access-Dienst-Dashboard.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Wenn ein Problem in anderen Komponenten gefunden wird, ergreifen Sie entsprechende Maßnahmen.
- Wenn dies das Problem nicht löst, wenden Sie sich mit dem Fehlercode und der entsprechenden Transaktions-ID an den Citrix Support.

Anwendungsstart fehlgeschlagen aufgrund von Netzwerkverbindungsproblemen

Infocode: 0x10000401

Fehler beim Starten der Anwendung aufgrund von Netzwerkverbindungsproblemen zwischen der Connector Appliance und dem Secure Private Access-Dienst

1. Überprüfen Sie die öffentliche Internetkonnektivität der Connector Appliance.
2. Überprüfen Sie, ob Proxy- oder Firewallregeln die Verbindung blockieren.
3. Wenn ein Proxy das Problem verursacht, umgehen Sie den Proxy und versuchen Sie den App-Start erneut.
4. Überprüfen Sie den Integritätsstatus der Connector Appliance (**Citrix Cloud > Resource Location**).

Details zu den Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Connector Appliance konnte sich nicht beim Secure Private Access-Dienst registrieren

Infocode: 0x10000402, 0x1000040C

1. Gehen Sie zur Admin-Seite 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 virtuelle Connector-Maschine neu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Überprüfen Sie die Connector-Zusammenfassung und führen Sie die Integritätsprüfung erneut durch.

Details zu den Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Konnektivitätsproblem mit der Connector Appliance

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

- Suchen Sie die Transaktions-ID für den Fehlercode.
- Filtern Sie alle Ereignisse, die der Transaktions-ID im Secure Private Access-Dashboard entsprechen.
- Überprüfen Sie, ob in der anderen Komponente, die der Transaktions-ID entspricht, ein Fehler aufgetreten ist. Falls ja, führen Sie die entsprechende Problemumgehung für diesen Fehlercode durch.
- Wenn in anderen Komponenten kein Fehler gefunden wird, gehen Sie wie folgt vor:
  - Gehen Sie zur Administratorseite der Connector Appliance.
  - Laden Sie den Diagnosebericht herunter. Details finden Sie unter Generieren eines Diagnoseberichts.
  - Erfassen Sie den Paket-Trace. Details finden Sie unter Überprüfen Sie Ihre Netzwerkverbindung.
- Wenden Sie sich mit diesem Diagnosebericht und Paket-Trace sowie dem Fehlercode und der Transaktions-ID an den Citrix Support.

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

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

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

- Überprüfen Sie, ob der Back-End-Server, mit dem der Endbenutzer eine Verbindung herstellen möchte, aktiv ist und ausgeführt wird und Anfragen empfangen kann.
- Überprüfen Sie die Erreichbarkeit der Back-End-Server innerhalb des Unternehmensnetzwerks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Überprüfen Sie die Proxy-Einstellungen, um festzustellen, ob der Connector daran gehindert wird, den Back-End-Server zu erreichen.
- Wenn es sich um eine Anforderung für eine FQDN-basierte App handelt, überprüfen Sie den DNS-Eintrag für die entsprechende App auf dem DNS-Server.

Connector Appliance kann DNS für FQDNs nicht auflösen

Infocode: 0x10000406

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

Verbindung zum privaten Server beendet

Infocode: 0x10000411

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

1. Überprüfen Sie, ob der Endbenutzer die Anwendung geschlossen hat.
2. Überprüfen Sie andere Diagnoseprotokolle, die der Transaktions-ID dieses Protokolls entsprechen, und ergreifen Sie entsprechende Maßnahmen.
3. Starten Sie die App erneut.
4. Wenn dies das Problem nicht löst, wenden Sie sich mit dem Fehlercode und der Transaktions-ID an den Citrix Support.

Verbindung zum oder Senden von Daten an die private Dienst-IP oder den FQDN fehlgeschlagen

Infocode: 0x10000413

- Verbindung zum privaten Server beendet
- Konnektivitätsprobleme mit der Connector Appliance und privaten TCP/UDP-Backend-Servern. Überprüfen Sie die Routing-Domäneneinträge. Stellen Sie sicher, dass die IP-Adressen gültig sind und auf das richtige Backend verweisen.

Keine übereinstimmende Richtlinienbedingung

Infocode: 0x100508

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Benutzerkontext stimmt nicht mit den Zugriffsregelbedingungen überein, die in den der App zugewiesenen Richtlinien definiert sind.

Aktualisieren Sie die Richtlinienkonfiguration, um sie an den Benutzerkontext anzupassen.

Keine Zugriffsrichtlinie der Anwendung zugeordnet

Infocode: 0x100509

1. Klicken Sie in der GUI des Citrix Secure Private Access™-Dienstes in der linken Navigation 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. Weitere Informationen finden Sie unter Zugriffsrichtlinien erstellen.
4. Wenn dies das Problem nicht löst, wenden Sie sich an den Citrix Support.

Keine Anwendungskonfiguration für den FQDN oder die IP-Adresse gefunden

Infocode: 0x10050A

Für die eingehende FQDN- oder IP-Adressanfrage 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 Secure Private Access Service-Administratorportal.
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 Wildcard-Domäne hinzufügen.

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

Informationen zur App-Aufzählung

Infocode: 0x10050C

Dieser Code erfasst die Richtlinienauswertungsergebnisse mehrerer Anwendungen, für die der Benutzer möglicherweise berechtigt ist. Der App-Zugriff kann aus folgenden Gründen verweigert werden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Benutzerkontext stimmt nicht mit den Zugriffsregelbedingungen überein, die in den der App zugewiesenen Richtlinien definiert sind – Details finden Sie unter Keine passende Richtlinienbedingung.
- Der Anwendung ist keine Zugriffsrichtlinie zugeordnet – Details finden Sie unter Keine Zugriffsrichtlinie der Anwendung zugeordnet.
- Eine der Anwendung zugeordnete Richtlinie ist so konfiguriert, dass der Zugriff verweigert wird – In diesem Fall ist keine Aktion erforderlich, da dies beabsichtigt ist.
- Unerwarteter interner Fehler bei der Durchsetzung der Zugriffsrichtlinie. Für Details wenden Sie sich an den Citrix Support.

TCP/UDP-App-Start fehlgeschlagen, da der Routing-Eintrag in der Anwendungsdomänentabelle fehlt

Infocode: 0x00180101

Dieses Problem kann auftreten, wenn die Anwendungskonfiguration vorhanden ist, der Routing-Eintrag jedoch fehlt oder zuvor gelöscht wurde.

Fügen Sie einen Routing-Eintrag (**Secure Private Access > Settings > Application Domain**) für das Ziel hinzu, auf das zugegriffen wird.

Start der TCP/UDP-App fehlgeschlagen, da 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-Anfrage fehlgeschlagen, da Konnektor nicht erreichbar ist

Infocode: 0x00180103

Dieses Problem kann auftreten, wenn der UDP/DNS-Verkehr den Konnektor nicht erreichen kann.

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

Laden der Seite fehlgeschlagen, da das NGS-Cookie abgelaufen ist

Infocode: 0x20580001

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Abruf der Zugriffsrichtlinie 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.

Fehler beim Abrufen der Zugriffsrichtlinie beim Parsen des JSON-Web-Tokens

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 von 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.

Fehler beim Abrufen der Richtlinie beim Abrufen des öffentlichen Zertifikats

Infocode: 0x20580005

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

Richtlinienabruf fehlgeschlagen bei der Validierung der Signatur des JSON-Web-Tokens

Infocode: 0x20580007

1. Überprüfen Sie, ob die Netzwerkzeit und die Gerätezeit des Benutzers synchron sind.
2. Starten Sie den Browser neu und versuchen Sie, die App erneut zu öffnen.
3. Wenn dies das Problem nicht löst, wenden Sie sich an den Citrix Support.

Richtlinienabruf fehlgeschlagen bei der Validierung des öffentlichen Zertifikats

Infocode: 0x20580008

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Fehler beim Bestimmen der Store-Umgebung zum Erstellen einer Richtlinien-URL

Infocode: 0x2058000A

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

Fehler beim Abrufen einer Antwort für die Anforderung zum Abrufen der Zugriffsrichtlinie

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.

Fehler beim Abrufen der Zugriffsrichtlinie aufgrund eines abgelaufenen sekundären DS-Authentifizierungstokens

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 Registrierung der Connector Appliance.

Weitere Informationen finden Sie unter Registrieren Ihrer Connector Appliance bei Citrix Cloud.

Verbindung zur Connector Appliance nicht möglich

Infocode: 0x10200003

Die Connector Appliance kann nicht zwischen Citrix Cloud und Ressourcenstandorten kommunizieren.

Überprüfen Sie die Connector-Registrierung.

Weitere Informationen finden Sie unter Registrieren Sie Ihre Connector Appliance bei Citrix Cloud.

Verbindung zum Citrix Secure Private Access-Dienst fehlgeschlagen

Infocode: 0x10000301

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Überprüfen Sie die Netzwerkeinstellungen der Connector Appliance. Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Proxyserver ist nicht erreichbar

Infocode: 0x10000303, 0x10000304

Überprüfen Sie die Proxyserver-Einstellungen und stellen Sie sicher, dass er für die Connector Appliance erreichbar ist. Weitere Informationen finden Sie unter Registrieren Sie Ihre Connector Appliance bei Citrix Cloud.

Proxyserver-Authentifizierung fehlgeschlagen

Infocode: 0x10000305

Überprüfen Sie die Proxyserver-Anmeldeinformationen und stellen Sie sicher, dass sie in der Connector Appliance korrekt konfiguriert sind. Weitere Informationen finden Sie unter Nach der Registrierung Ihrer Connector Appliance.

Konfigurierte Proxyserver sind nicht erreichbar

Infocode: 0x10000306

Überprüfen Sie die Netzwerkeinstellungen, Firewall-Einstellungen oder Proxyserver-Einstellungen der Connector Appliance. Weitere Informationen finden Sie in den folgenden Themen:

- Netzwerkeinstellungen für Ihre Connector Appliance
- Registrieren Sie Ihre Connector Appliance bei Citrix Cloud
- Kommunikation der Connector Appliance

Fehlerantwort vom Backend-Server erhalten

Infocode: 0x10000307

Überprüfen Sie den HTTP-Statuscode des Backend-Webservers, falls es sich nicht um einen erwarteten Code handelt.

Anfrage an die Ziel-URL konnte nicht gesendet werden

Infocode: 0x10000005

Überprüfen Sie die Ziel-URL oder die Netzwerkeinstellungen der Connector Appliance. Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

SSO-Verarbeitung fehlgeschlagen

Infocode: 0x10000107

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fehler beim Abrufen der App-Konfigurationsdaten aus Citrix Cloud.

Überprüfen Sie die Netzwerkeinstellungen der Connector Appliance und stellen Sie sicher, dass der NTP-Server konfiguriert ist und keine Zeitverschiebungsprobleme vorliegen. Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

Verbindung zum Citrix Secure Private Access-Dienst fehlgeschlagen

Infocode: 0x10000108, 0x1000010B

Überprüfen Sie die Netzwerkeinstellungen der Connector Appliance. Weitere Informationen finden Sie unter Netzwerkeinstellungen für Ihre Connector Appliance.

SSO-Verarbeitung fehlgeschlagen, SSO-Einstellungen können nicht ermittelt werden

Infocode: 0x1000010A

Überprüfen Sie die SSO-Konfiguration und stellen Sie sicher, dass der Server für die Connector Appliance erreichbar ist.

FormFill-SSO fehlgeschlagen, falsche Formular-App-Konfiguration

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

Überprüfen Sie die SSO-Formular-App-Konfiguration und stellen Sie sicher, dass die Felder für Benutzername, Kennwort, Aktion und Anmelde-URL in den App-Einstellungen korrekt konfiguriert sind.

Kerberos-SSO 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 Kerberos-SSO-Einstellungen finden Sie unter Validieren Ihrer Kerberos-Konfiguration.

SSO-Verarbeitung für Authentifizierungstyp fehlgeschlagen

Infocode: 0x10000203

Überprüfen Sie die SSO-Einstellungen im Secure Private Access-Dienst und auf dem Backend-Server. Informationen zum Secure Private Access-Dienst finden Sie unter Festlegen der bevorzugten Anmeldemethode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kerberos-SSO fehlgeschlagen, aber Fallback auf NTLM

Infocode: 0x10000204

Das Abrufen des Kerberos-Tickets vom Domänencontroller ist fehlgeschlagen. Als sekundäre Authentifizierung hat die 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 Informationen finden Sie unter Validieren Ihrer Kerberos-Konfiguration.

Mehrere ZTNA-berechtigte Konten in der Citrix Workspace™-App konfiguriert

Infocode: 0x14000001

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

So erfassen Sie Client-Protokolle

- **Windows-Client:**
  a. Öffnen Sie die App und stellen Sie sicher, dass die Protokollierung aktiviert ist.
  b. Stellen Sie nun eine Verbindung zum Secure Private Access-Dienst her und reproduzieren Sie das Problem, das bei Ihnen auftritt.
  c. Gehen Sie in der App zu **Protokollierung** und klicken Sie auf **Protokolldateien sammeln**. Dadurch wird die Protokolldatei generiert.
  d. Speichern Sie die Protokolldatei auf dem Desktop des Client-Computers.
- **Mac-Client:**
  a. Öffnen Sie die App und gehen Sie zu **Protokolle > Ausführlich**.
  b. Löschen Sie die Protokolle und reproduzieren Sie das Problem.
  c. Gehen Sie zurück zu **Protokolle > Protokolle exportieren**. Dadurch wird eine Zip-Datei erstellt, die Protokolldateien enthält.

FAQs

Die folgenden Abschnitte enthalten weitere Informationen zu den häufig gestellten Fragen.

Wo finde ich weitere Informationen zu Diagnoseprotokollen?

Weitere Informationen zu den Diagnoseprotokollen finden Sie im Thema Diagnoseprotokolle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

1. Rufen Sie den Infocode für den Fehler ab, den Sie beheben möchten.
2. Suchen Sie den Infocode in der Fehlersuchttabelle.
3. Befolgen Sie die für diesen Infocode bereitgestellten Lösungsschritte.

Was ist ein Infocode? Wo finde ich sie?

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

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

Zugriffsfehler/-probleme über den Citrix Enterprise Browser zeigen dem Endbenutzer eine Transaktions-ID an. 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, wodurch sie das genaue Problem identifizieren können. Sobald die Administratoren Ereignisse mit der Transaktions-ID filtern, werden nur die Ereignisse angezeigt, die sich auf das vorliegende Problem beziehen, und den Administratoren alle Details darüber geliefert, 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?

Im Folgenden finden Sie die Liste der Secure Private Access Daten-PoP-Standorte.

POP-NAME	ZONE	REGION
az-us-e	Azure Ost-USA	Virginia
az-us-w	Azure West-USA	Kalifornien
az-us-sc	Azure Süd-Zentral-USA	Texas
az-aus-e	Azure Ostaustralien	New South Wales
az-eu-n	Azure Nordeuropa	Irland
az-eu-w	Azure Westeuropa	Niederlande
az-jp-e	Azure Japan, Osten	Tokio, Saitama

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POP-NAME	ZONE	REGION
az-bz-s	Azure Brasilien, Süden	Bundesstaat São Paulo
az-asia-se	Azure Südostasien	Singapur
az-uae-n	Azure VAE Nord	Dubai
az-in-s	Azure Südindien	Chennai
az-asia-hk	Azure Ostasien	Hongkong

Im Folgenden ist die Liste der Secure Private Access Management PoP-Standorte aufgeführt.

POP-NAME	ZONE	REGION
aws-us-e-mgmt	AWS us-east-1	Nord-Virginia
aws-in-w-mgmt	AWS ap-south-1	Mumbai
aws-eu-c-mgmt	AWS eu-central-1	Frankfurt

Was mache ich, wenn ich meinen Fehler nicht mithilfe des Infocodes und der Fehler-Nachschlagetabelle beheben kann?

Wenden Sie sich an den Citrix Support.

Referenzen

- **Eine Web-App hinzufügen**
  - Support für Unternehmens-Web-Apps
  - Direkten Zugriff auf Web-Apps konfigurieren
- **Eine SaaS-App hinzufügen**
  - Support für Software-as-a-Service-Apps
  - SaaS-App-Server-spezifische Konfiguration
- **Client-Server-Apps konfigurieren**
  - Unterstützung für Client-Server-Apps
- **Zugriffsrichtlinien erstellen**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Zugriffsrichtlinien erstellen

- **Routingtabellen**
    - Routingtabellen

Audit- und Systemprotokolle

Ereignisse im Zusammenhang mit dem Secure Private Access-Dienst werden in **Citrix Cloud > Systemprotokoll** erfasst. Alle Ereignisse, die ein Administrator im Citrix Secure Private Access™-Dienst ausführt, werden an Citrix Cloud gesendet und im **Systemprotokoll** erfasst. Die Administratorereignisse können unter anderem folgende sein:

- Erstellen oder Aktualisieren einer App
- Löschen einer App
- Konfigurieren oder Löschen einer adaptiven Zugriffsrichtlinie
- Connector-Upgrade
- Erstellung von zugelassenen oder blockierten Websites

Standardmäßig zeigt das **Systemprotokoll** Ereignisse an, die in den letzten 30 Tagen aufgetreten sind. Die neuesten Ereignisse werden zuerst angezeigt.

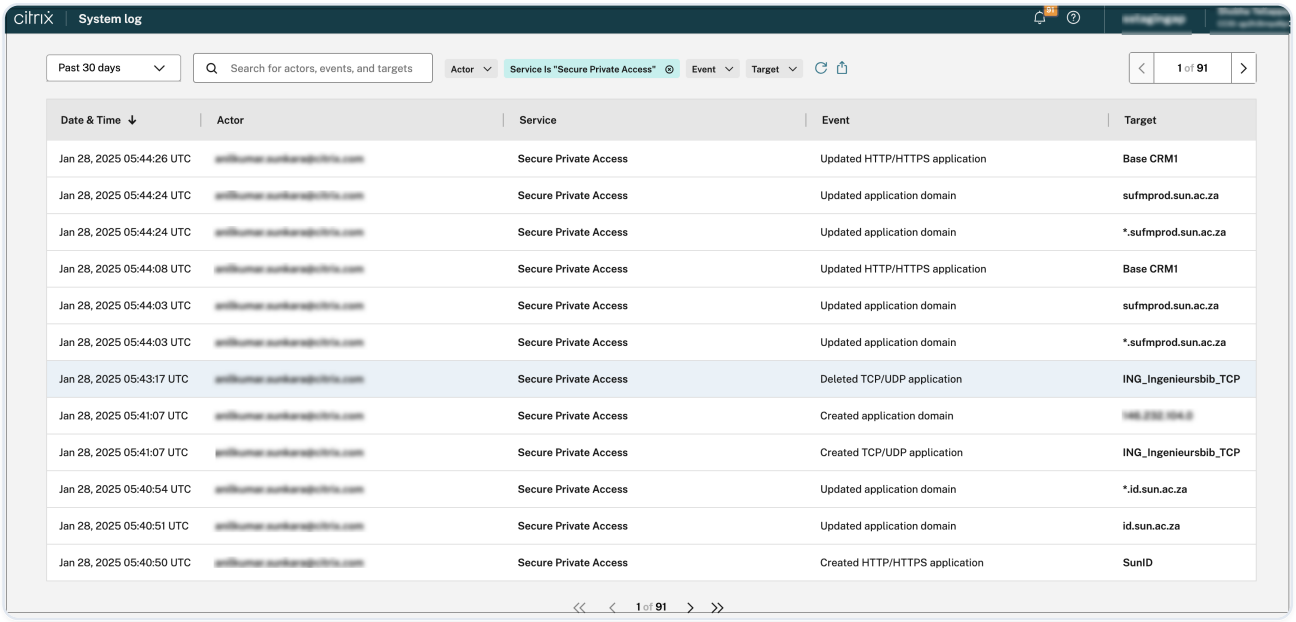
Die Protokolle zeigen Details zu Ereignissen und können nach folgenden Kriterien gefiltert werden:

- **Datum und Uhrzeit:** Das Datum und die Uhrzeit (UTC-Format), zu der das Ereignis aufgetreten ist.
- **Akteur:** Der Benutzer oder das System, das das Ereignis ausgelöst hat. Zum Beispiel: Administrator, sicherer Client, Dienstprinzipal.
- **Dienst:** Der Dienst, in dem das Ereignis protokolliert wurde. Die Secure Private Access-Ereignisse müssen **Secure Private Access** als Dienst aufweisen.
- **Ereignis:** Eine kurze Beschreibung des Ereignisses. Zum Beispiel: SaaS-Anwendung erstellt, TCP/UDP-Anwendung gelöscht, adaptive Zugriffsrichtlinie aktualisiert, Anwendungsdomäne aktualisiert.
- **Ziel:** Das Objekt, das durch das Ereignis betroffen oder geändert wurde. Zum Beispiel die für eine Anwendung verwendete Domäne.

  Der Zielbezeichner liegt in einem menschenlesbaren Format vor und ist nicht die tatsächliche ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



Weitere Informationen zum Exportieren von Ereignissen, zum Abrufen von Ereignissen für einen bestimmten Zeitraum, zum Weiterleiten von Protokollereignissen und zur Datenaufbewahrung finden Sie unter Systemprotokoll.

Gerätehaltungs-Protokolle und -Ereignisse

Administratoren können die Gerätekonformität über das Gerätehaltungs-Dashboard überwachen. Sie können alle konfigurierten Gerätehaltungsrichtlinien einsehen, die die Konformitätsanforderungen für Endpunkte definieren, die auf Organisationsressourcen zugreifen. Sie können auch den Echtzeit-Konformitätsstatus für alle Geräte einsehen, einschließlich detaillierter Bewertungsergebnisse, die wie folgt kategorisiert sind:

- **Konform:** Geräte, die alle angegebenen Sicherheitsanforderungen und Richtlinienkriterien erfüllen.
- **Nicht konform:** Geräte, die eine oder mehrere Sicherheitsanforderungen nicht erfüllen, aber möglicherweise noch eingeschränkten Zugriff haben.
- **Zugriff verweigert:** Geräte, die erhebliche Sicherheitsrisiken darstellen und vom Zugriff auf Ressourcen blockiert sind.

Sie können die Gerätehaltungs-Protokolle und -Ereignisse im Secure Private Access-Dashboard und im Gerätehaltungs-Dashboard in der Identity and Access Management-Konsole anzeigen.

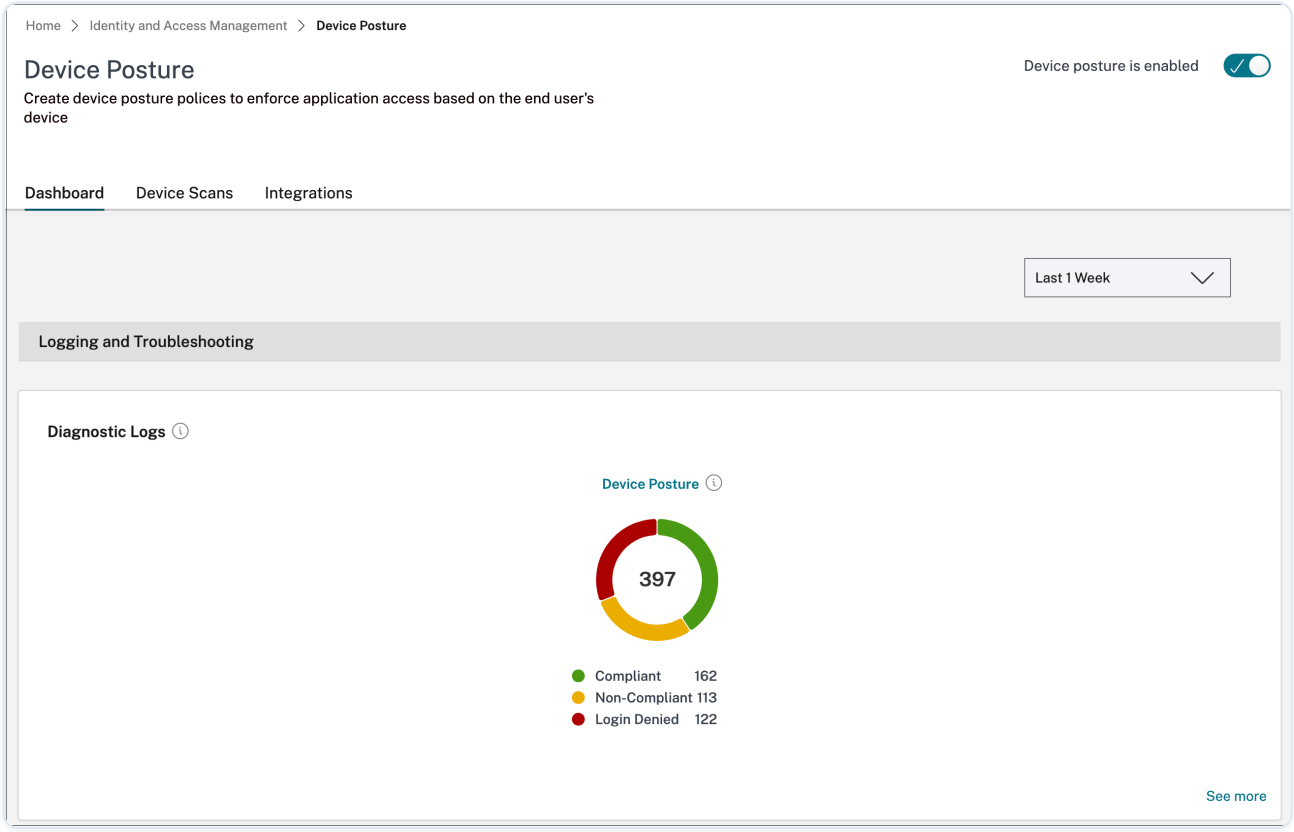
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gerätehaltungs-Dashboard in der Identity and Access Management-Konsole

Führen Sie die folgenden Schritte aus, um die Protokolle und Ereignisse für das Gerätehaltungs-Dashboard in der Identity and Access Management-Konsole anzuzeigen.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Citrix Cloud-Menü **Identity and Access Management** aus,
3. Klicken Sie auf **Device Posture > Manage** und dann auf **Dashboard.**

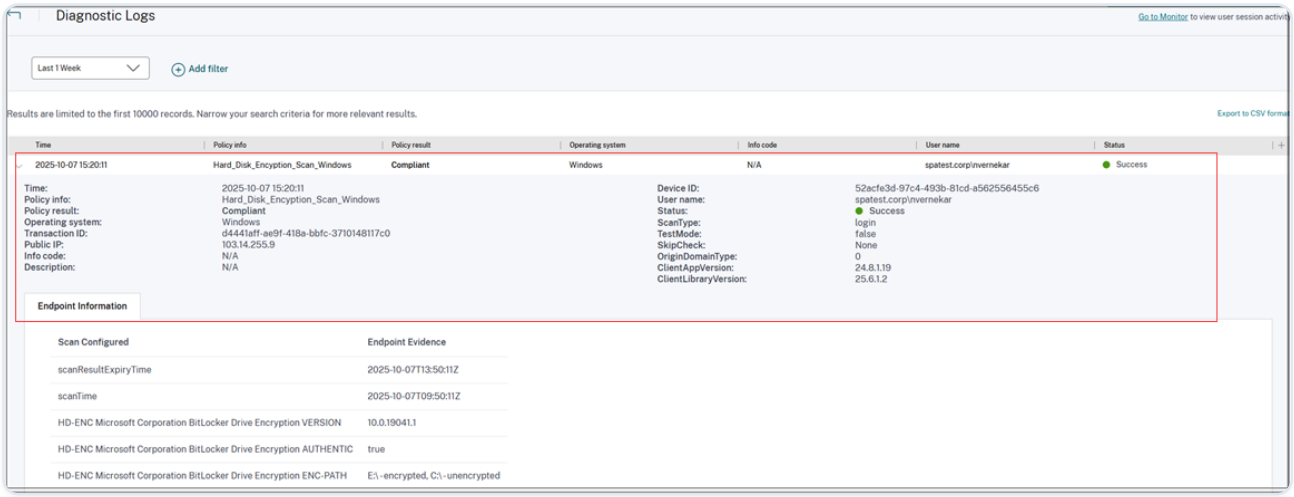
   Der Abschnitt **Logging and Troubleshooting** zeigt die Diagnoseprotokolle an, die mit dem Gerätehaltungsdienst zusammenhängen.
4. Klicken Sie auf den Link **See more**, um die Details der Protokolle anzuzeigen. Sie können Ihre Suche basierend auf den Richtlinienergebnissen (**Compliant**, **Non-Compliant** und **Login Denied**) verfeinern.



Sie können die Option **Filter hinzufügen** verwenden, um Ihre Suche basierend auf verschiedenen Kriterien wie Richtlinieninformationen, Richtlinienergebnis, Betriebssystem, Transaktions-ID, Infocode oder Geräte-ID zu verfeinern. Im Suchfeld können Sie beispielsweise auf **Geräte-ID** klicken, **~ (enthält einen Wert)** auswählen und 6273 eingeben. Alle Protokolle, die Geräte-IDs mit 6273 enthalten, werden angezeigt.

Klicken Sie auf das erweitern-Symbol neben jedem Protokolleintrag, um umfassende Details wie Scan-Typ, Client-App-Version, Client-Bibliotheksversion und Endpunktinformationen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



HINWEIS:

- Die Felder **ClientAppVersion** und **ClientLibraryVersion** zeigen die EPA-Client-Version bzw. die Bibliotheksversion an.
- Die Transaktions-ID wird dem Endbenutzer auch angezeigt, wenn der Zugriff verweigert wird.
- Wenn ein Fehler oder ein Scanfehler auftritt, zeigt der Device Posture-Dienst eine Transaktions-ID an. Diese Transaktions-ID ist im Secure Private Access-Dienst-Dashboard verfügbar. Wenn die Protokolle das Problem nicht lösen können, können Endbenutzer die Transaktions-ID mit dem Citrix Support teilen, um das Problem zu beheben.

Speicherort der Protokolle

Die Windows-Client-Protokolle finden Sie unter:

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

Die macOS-Client-Protokolle finden Sie unter:

- ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

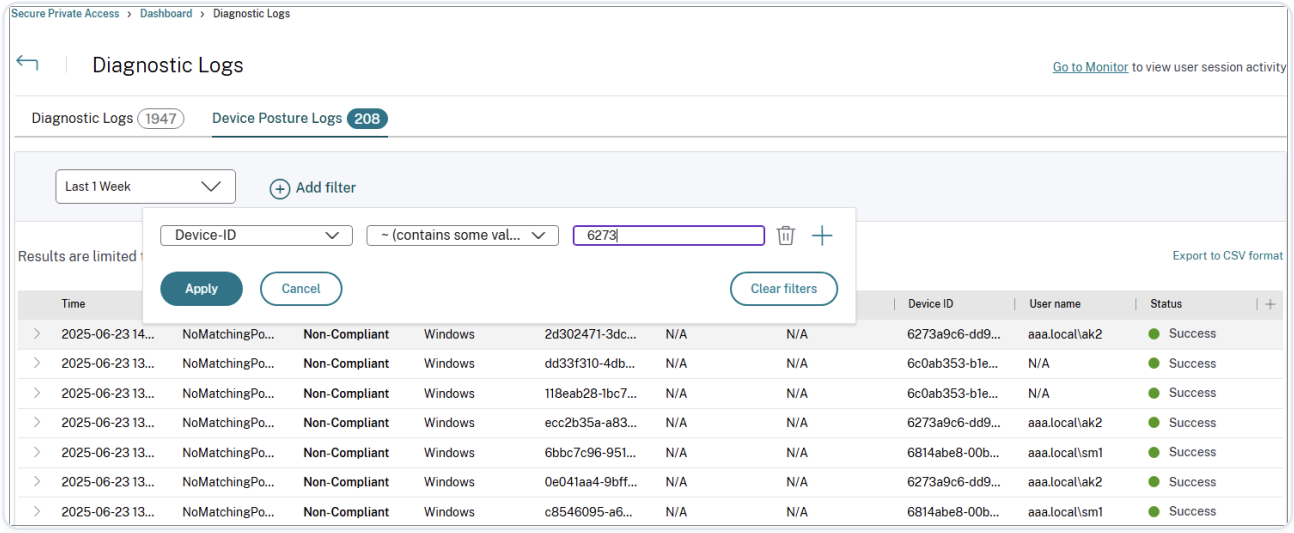
Secure Private Access-Dashboard

Führen Sie die folgenden Schritte aus, um die Protokolle und Ereignisse für den Device Posture-Dienst anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Kachel „Secure Private Access“ auf **Verwalten** und dann auf **Dashboard**.

   Der Abschnitt **Protokollierung und Fehlerbehebung** zeigt die Diagnoseprotokolle für den Device Posture-Dienst an.
3. Klicken Sie auf den Link **Mehr anzeigen**, um die Details der Protokolle anzuzeigen. Sie können Ihre Suche basierend auf den Richtlinienergebnissen (**Konform**, **Nicht konform** und **Anmeldung verweigert**) verfeinern.



Fehlerprotokolle der Gerätehaltung

Die folgenden Protokolle zum Device Posture-Dienst können im Citrix Monitor- und Secure Private Access-Dashboard angezeigt werden. Für alle diese Protokolle wird empfohlen, sich zur Lösung an den Citrix Support zu wenden.

- Fehler beim Lesen konfigurierter Richtlinien
- Fehler bei der Auswertung von Endpunktscans
- Fehler bei der Verarbeitung von Richtlinien/Ausdrücken
- Fehler beim Speichern von Endpunktdetails
- Fehler bei der Verarbeitung von Scanergebnissen von Endpunkten

Export von Gerätestatusdaten

Die Ereignisse des Device Posture-Dienstes (z. B. Gerätestatus-Ergebnisse und Ereignistypen) können an den Security Information and Event Management (SIEM)-Dienst exportiert werden. Diese Ereignisse werden generiert, wenn der Citrix Endpoint Analysis (EPA)-Client eine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Statusprüfung auf einem Gerät durchführt, das versucht, auf Citrix Virtual Apps and Desktops™- oder Citrix Secure Private Access-Ressourcen zuzugreifen.

- Informationen zum Einrichten, Konfigurieren und Exportieren Ihrer Device Posture-Dienstprotokolle nach SIEM finden Sie unter Security Information and Event Management (SIEM)-Integration.
- Um mehr darüber zu erfahren, welche Ereignisse und Protokolle Sie aus dem Device Posture-Dienst exportieren können, siehe Ereignisse des Device Posture-Dienstes.
- Um zu verstehen, wie Sie Transaktionen des Device Posture-Dienstes diagnostizieren und Fehler beheben können, siehe Transaktionen des Device Posture-Dienstes diagnostizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenexporte und Integrationen von Drittanbietern

Die folgenden Abschnitte bieten weitere Informationen zu Datenexporten und Integrationen von Drittanbietern.

Sicherheitsinformations- und Ereignismanagement-Integration

Die Integration von Secure Private Access mit dem Sicherheitsinformations- und Ereignismanagement (SIEM) ermöglicht Administratoren den Export kritischer Protokolle, Richtlinienergebnisse und Benutzeraktivitätsdaten an SIEM-Systeme von Drittanbietern mithilfe von Kafka-Push-Mechanismen. Diese Integration bietet erweiterte Transparenz, Compliance-Verfolgung und Sicherheitseinblicke für Organisationen, die Citrix Secure Private Access-Dienste nutzen.

Sie können jedes beliebige SIEM verwenden, wie z. B. Splunk, Google Chronicle, Microsoft Sentinel oder Elastic.

Eine Liste der Benutzerereignisse, die mit Secure Private Access und dem Device Posture-Dienst in Ihrem SIEM verbunden sind, finden Sie in den folgenden Themen:

- Secure Private Access-Ereignisse
- Device Posture-Dienstereignisse

Benutzerdefinierten Bericht mit OData-APIs erstellen

Die Secure Private Access Monitor OData REST-APIs ermöglichen Administratoren den Export von Sitzungsdaten und das Erstellen benutzerdefinierter Berichte. Diese Funktion ist nützlich für die Verfolgung von Rollouts, die Analyse der Benutzeraktivität und das Gewinnen von Einblicken in die Leistung und Nutzung von Secure Private Access-Diensten.

Informationen zu den Arten von Secure Private Access-Daten, die für den Export verfügbar sind, finden Sie in den folgenden Themen:

- Secure Private Access-Sitzungen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Secure Private Access-Anwendungen
- Secure Private Access-Enumerationen

Systemprotokolle exportieren

Die Funktion **Systemprotokoll** in Citrix Cloud bietet eine zeitgestempelte Aufzeichnung von Ereignissen, die innerhalb des Secure Private Access-Dienstes auftreten. Administratoren können diese Protokolle als CSV-Datei zur weiteren Analyse und Überprüfung exportieren. Weitere Informationen finden Sie unter Syslog aus Citrix Cloud.

Daten aus Kafka exportieren

Kafka ist eine quelloffene, verteilte Streaming-Plattform, die für die Echtzeit-Datenverarbeitung und -Analyse entwickelt wurde. Mit Kafka können Unternehmen Streaming-Daten in Echtzeit analysieren, um schnellere Erkenntnisse zu gewinnen, proaktive Entscheidungen zu ermöglichen und erweiterte Sicherheitsüberwachungsfunktionen zu unterstützen.

Sie können Secure Private Access-Ereignisse und Device Posture-Dienstereignisse aus Kafka exportieren, um sie in externe Security Information and Event Management (SIEM)-Systeme, Analyseplattformen und benutzerdefinierte Überwachungslösungen zu integrieren.

Secure Private Access-Ereignisse

Die Benutzerereignisse werden in Echtzeit in Citrix Analytics for Security empfangen, wenn Benutzer über Citrix Secure Private Access auf Anwendungen zugreifen, wie z. B. Citrix Workspace-App, Citrix Secure Access-Clients oder Citrix Enterprise Browser.

Weitere Informationen finden Sie unter Secure Private Access-Ereignisse.

Device Posture-Dienstereignisse

Die Benutzerereignisse werden generiert, wenn der Citrix Endpoint Analysis (EPA)-Client eine Statusprüfung auf einem Gerät durchführt, das versucht, auf Citrix Virtual Apps and Desktops- oder Citrix Secure Private Access-Ressourcen zuzugreifen.

Weitere Informationen finden Sie unter Device Posture-Dienstereignisse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audit- und Systemprotokolle exportieren

Die Funktion **Systemprotokoll** in Citrix Cloud erfasst eine vollständige, mit Zeitstempel versehene Aufzeichnung von Ereignissen, die im Secure Private Access-Dienst auftreten. Diese Audit-Protokolle sind entscheidend für die Einhaltung gesetzlicher Vorschriften, die Sicherheitsüberwachung und die Fehlerbehebung bei administrativen Vorgängen. Administratoren können Protokolldaten als CSV-Dateien für detaillierte Analysen, die Überprüfung der Compliance und die nahtlose Integration in externe Sicherheitsüberwachungssysteme exportieren.

Die folgenden Ereignisse werden im **Systemprotokoll** für den Secure Private Access-Dienst erfasst:

- Anwendungskonfigurationsänderungen, einschließlich Erstellung, Änderung und Löschung.
- Richtlinienaktualisierungen wie Zugriffsregeln, Sicherheitskonfigurationen und Einstellungen für den bedingten Zugriff.
- Benutzer- und Gruppenverwaltungsoperationen wie das Hinzufügen oder Entfernen von Benutzern und Gruppen.
- Informationen zu Anwendungsdomänen.
- Zugelassene und blockierte URL-Listen.

Secure Private Access-Ereignisse mit der SystemLog-API exportieren

Sie können die SystemLog-API verwenden, um die Secure Private Access-Ereignisse zu exportieren. Die SystemLog-API ermöglicht es Ihnen, Ereignisse abzurufen, die in Ihrem Citrix Cloud-Konto für von Ihnen angegebene Zeiträume aufgetreten sind.

- Details zur Verwendung der SystemLog-API zum Exportieren von Ereignissen finden Sie unter Citrix Cloud - SystemLog in der Citrix Developer-Dokumentation.
- Informationen zu den Ereignisdaten, die das **Systemprotokoll** für den Secure Private Access-Dienst erfasst, finden Sie unter System Log Events Reference.
- Weitere Informationen zur Monitor-Dienst-API finden Sie unter About Citrix Monitor Service API.

Sitzungsdaten mit OData exportieren

Die Secure Private Access Monitor OData REST-APIs ermöglichen Administratoren den Export von Sitzungsdaten und die Erstellung benutzerdefinierter Berichte. Diese Funktion ist besonders

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nützlich für die Verfolgung von Rollouts, die Analyse der Benutzeraktivität und die Gewinnung von Einblicken in die Leistung und Nutzung von Secure Private Access-Diensten.

- Administratoren können die OData REST-APIs nutzen, um benutzerdefinierte Berichte zu erstellen, die spezifische organisatorische Anforderungen erfüllen. Diese Flexibilität ermöglicht eine detaillierte Analyse von Sitzungsdaten, Benutzeraktivitäten und Anwendungsnutzung.
- Die APIs ermöglichen die Verfolgung von Rollouts und helfen Administratoren, die Akzeptanz und Effektivität von Secure Private Access-Konfigurationen und -Richtlinien im gesamten Unternehmen zu überwachen.
- Mithilfe von OData-APIs können Sitzungsdaten zur weiteren Analyse in externe Tools oder Systeme exportiert werden.

Details zu den Secure Private Access Monitor OData REST-APIs finden Sie in den folgenden Themen:

- Secure Private Access-Sitzungen
- Secure Private Access-Anwendungen
- Secure Private Access-Aufzählungen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rollenbasierte Zugriffssteuerung

Secure Private Access verwendet ein rollenbasiertes Zugriffssteuerungsmodell, um Benutzerberechtigungen und Zugriffsebenen zu verwalten. Dies bedeutet, dass jedem Benutzer eine bestimmte Rolle zugewiesen wird, und diese Rolle bestimmt, was er innerhalb des Systems tun und nicht tun kann. Dieses Modell trägt dazu bei, dass Benutzer über die angemessene Zugriffsebene verfügen, um ihre Aufgaben auszuführen, und verhindert gleichzeitig, dass sie auf sensible Daten oder Funktionen zugreifen, auf die sie keinen Zugriff haben dürfen.

Die folgenden vier Hauptrollen stehen für Secure Private Access-Administratoren zur Verfügung. Jede dieser Rollen verfügt über einen anderen Satz von Berechtigungen, die auf die Bedürfnisse verschiedener Benutzertypen zugeschnitten sind.

- Vollzugriffsadministrator
- Nur-Lese-Administrator
- Vollständiger Überwachungsadministrator
- Helpdesk-Administrator

HINWEIS:

Um Secure Private Access mit DaaS Monitor zu überwachen, müssen Administratoren zusätzlich zu einer der Secure Private Access-Rollen die DaaS-Rolle zugewiesen werden.

Die folgende Tabelle bietet eine kurze Beschreibung jeder Rolle:

ROLLE	BESCHREIBUNG
Vollzugriffsadministrator	Vorgesehen für Personen, die die vollständige Kontrolle über die Konfiguration, Verwaltung und den Betrieb der Secure Private Access-Umgebung benötigen. Der Vollzugriffsadministrator verfügt über die folgenden Berechtigungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ROLLE	BESCHREIBUNG
	Zugriff auf alle Secure Private Access-Funktionen.
	Berechtigungen zum Erstellen, Bearbeiten und Ändern von Apps, Richtlinien und Einstellungen innerhalb der Secure Private Access-Konsole.
Administrator mit Leseberechtigung	Vorgesehen für Personen, die die Secure Private Access-Aktivitäten und die Systemleistung überwachen und analysieren müssen. Der Administrator mit Leseberechtigung verfügt über die folgenden Berechtigungen.
	Zugriff auf das Secure Private Access-Dashboard.
	Möglichkeit, alle Secure Private Access-Anwendungskonfigurationen und -Einstellungen anzuzeigen.
	Der Administrator mit Leseberechtigung hat keine Berechtigungen für die Funktionen zum Erstellen/Aktualisieren/Löschen.
Administrator mit vollständiger Überwachungsberechtigung	Vorgesehen für Benutzer, die für die Überwachung der Secure Private Access-Aktivitäten und -Leistung in der Monitor-Konsole verantwortlich sind. Der Administrator mit vollständiger Überwachungsberechtigung verfügt über die folgenden Berechtigungen.
	Zugriff auf alle Überwachungs-Dashboards und Berichterstellungstools innerhalb von Secure Private Access.
	Möglichkeit, alle Secure Private Access-Konfigurationen und -Einstellungen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ROLLE	BESCHREIBUNG
	Der Full Monitor Administrator hat keine Berechtigungen zum Erstellen, Bearbeiten oder Ändern von Secure Private Access-Konfigurationen, -Richtlinien oder -Einstellungen.
Helpdesk-Administrator	Vorgesehen für Helpdesk-Mitarbeiter, die für die Fehlerbehebung und Priorisierung von Benutzerzugriffsproblemen zuständig sind. Der Helpdesk-Administrator verfügt über die folgenden Berechtigungen.
	Eingeschränkte Sichtbarkeit von Secure Private Access-Konfigurationen und -Einstellungen, wobei der Schwerpunkt auf Informationen liegt, die für die Fehlerbehebung in der Monitor-Konsole relevant sind.
	Zugriff auf spezifische Fehlerbehebungstools und Diagnoseprogramme innerhalb der Secure Private Access-Konsole.
	Anzeigen des Dashboards für Fehlerbehebung und Überwachung.
	Der Helpdesk-Administrator hat keine Berechtigungen zum Erstellen, Bearbeiten oder Ändern von Secure Private Access-Konfigurationen oder -Richtlinien.

Rollen und Berechtigungen

Die folgende Tabelle fasst die Rollen und Berechtigungen zusammen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	VOLLZUGRIFFS-ADMINISTRATOR	NUR-LESE-ADMINISTRATOR	VOLLSTÄNDIGER ÜBERWACHUNGSADMINISTRATOR	HELPDESK-ADMINISTRATOR
Apps erstellen/ bearbeiten/ löschen	Ja	Nein	Nein	Nein
Richtlinien erstellen/ bearbeiten/ löschen	Ja	Nein	Nein	Nein
Konfigurationen /Einstellungen bearbeiten	Ja	Nein	Nein	Nein
Konfigurationen /Einstellungen anzeigen	Ja	Ja	Ja	Eingeschränkt
Das Widget für Protokollierung und Fehlerbehebung im Secure Private Access-Dashboard anzeigen	Ja	Ja	Ja	Ja
Benutzer suchen	Ja	Ja	Ja	Nein
Konfigurierte Domänen abgerufen	Ja	Ja	Ja	Nein
Widgets für Benutzer, Anwendungen und Zugriffsrichtlinie	Ja	Ja	Ja	Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	VOLLZUGRIFFS-ADMINISTRATOR	NUR-LESE-ADMINISTRATOR	VOLLSTÄNDIGER ÜBERWACHUNGSADMINISTRATOR	HELPDESK-ADMINISTRATOR
n im Secure Private Access-Dashboard anzeigen				
Sitzungen und Anwendungen im Monitor-Dashboard anzeigen	Ja	Ja	Ja	Eingeschränkt
Auf Berichterstellungstools zugreifen	Ja	Nein	Ja	Eingeschränkt

Rollenbasierten Zugriff für Administratoren aktivieren

Führen Sie die folgenden Schritte aus, um den rollenbasierten Zugriff für Administratoren zu aktivieren:

1. Wählen Sie nach der Anmeldung bei Citrix Cloud™ im Menü die Option **Identitäts- und Zugriffsverwaltung** aus.
2. Klicken Sie auf der Seite **Identitäts- und Zugriffsverwaltung** auf **Administratoren** und dann auf **Administrator/Gruppe hinzufügen**. Die Konsole zeigt alle aktuellen Administratoren im Konto an.
3. Wählen Sie unter **Administrator oder Gruppe 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).
4. Wenn **Citrix Identity** ausgewählt ist, geben Sie die E-Mail-Adresse des Benutzers ein und klicken Sie dann auf **Weiter**.
5. Wählen Sie **Benutzerdefinierter Zugriff** aus und klicken Sie dann auf das **>** Symbol in **Secure Private Access**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

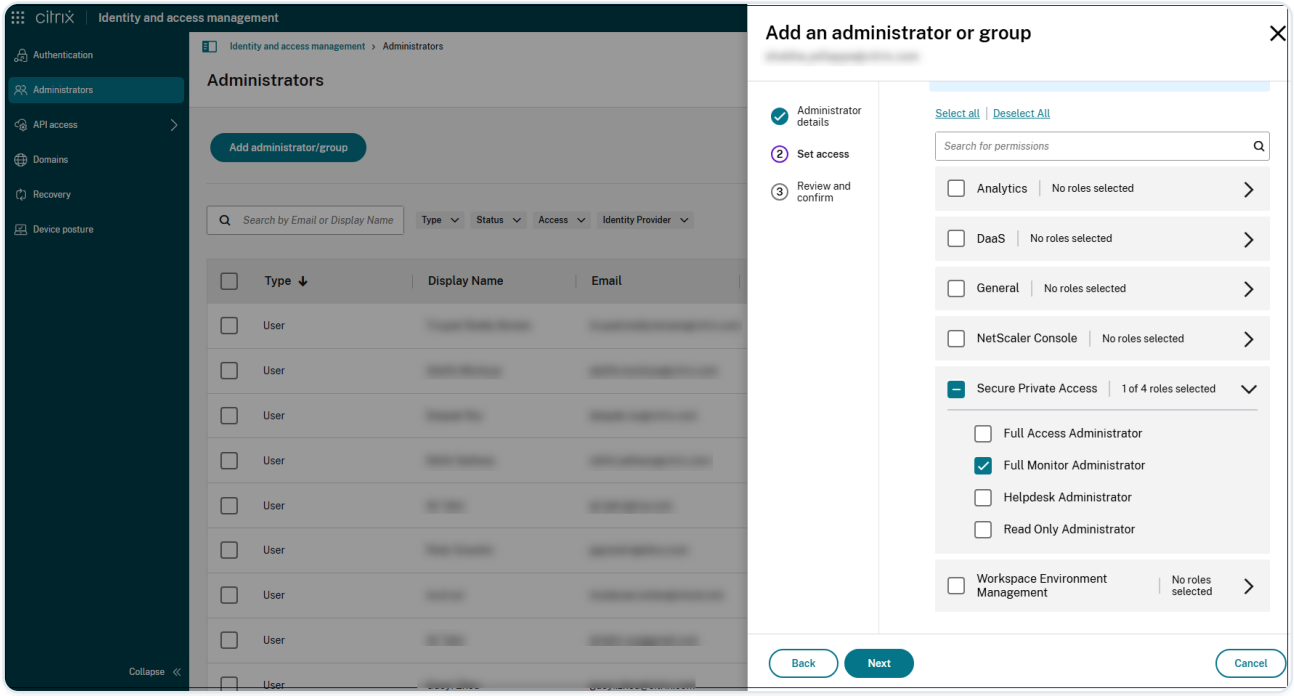
6. Wählen Sie eine der folgenden Rollen aus und klicken Sie auf Weiter.

    - Administrator mit vollem Zugriff
    - Administrator mit Lesezugriff
    - Administrator mit vollständiger Überwachung
    - Helpdesk-Administrator

7. Klicken Sie auf **Einladung senden**.

HINWEIS:

Die Dienste **Analytics** und **General** müssen für alle Secure Private Access-Rollen aktiviert sein. Der Dienst **Analytics** ist für Überwachung und Berichterstellung erforderlich, während die Dienste **General** für Authentifizierung, Domänen, Autorisierung, Datenverkehrsrouting und andere Funktionen benötigt werden.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützung für Mehrsitzungs-Virtual-Desktop-Infrastruktur

In einer Mehrsitzungs-Virtual-Desktop-Infrastruktur (VDI) teilen sich mehrere Benutzer eine virtuelle Maschine, während sie individuelle Desktop-Umgebungen beibehalten. Ab der Version 24.8.1.19 des Citrix Secure Access Clients für Windows können Sie auf Ihre Unternehmensanwendungen von Mehrsitzungs-VDIs für Secure Private Access-Bereitstellungen zugreifen, indem Sie sicherstellen, dass die Sitzung jedes Benutzers isoliert, privat und geschützt bleibt.

Mehrsitzungs-VDI-Workflow(/en-us/citrix-secure-private-access/media/vdi-process.png)

HINWEIS:

- Mehrsitzungs-VDI wird auf Windows-Betriebssystemen ab Windows 10 und ab Windows Server 2019 unterstützt.
- Mehrsitzungs-VDI funktioniert nur auf Azure-basierten VDIs.

Hauptmerkmale und Vorteile

- **Authentifizierung:** Unterstützt verschiedene Authentifizierungsmethoden, einschließlich der bedingungsbasierten Authentifizierung.
- **Kontextbezogener Zugriff:** Ermöglicht den Zugriff nur auf autorisierte Anwendungen basierend auf Secure Private Access-Richtlinien für Benutzer, die auf Faktoren wie Standort, Gerät und Gruppe basieren.
- **Geringere Kosten:** Ermöglicht mehreren Benutzern die gemeinsame Nutzung von Computern, was Unternehmen helfen kann, Hardwarekosten zu sparen. Die Citrix Secure Access™ Client für Windows App verbessert diese Kosteneinsparungen weiter, indem sie Benutzern ermöglicht, von jedem Gerät aus auf ihre virtuellen Desktops zuzugreifen, wodurch der Bedarf an dedizierten Workstations reduziert wird, ohne auf Expressrouten oder Legacy-VPN angewiesen zu sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Erhöhte Flexibilität:** Ermöglicht Endbenutzern, sich von überall aus zu verbinden, unter Einhaltung der Secure Private Access-Richtlinien, um nur autorisierten Anwendungszugriff zu ermöglichen.

Mehrsitzungs-VDI aktivieren

Um die Mehrsitzungs-VDI-Unterstützung in der Citrix Secure Access Client für Windows App zu aktivieren, müssen Administratoren sicherstellen, dass der Citrix Secure Access Client für Windows 24.8.1.19 oder höher auf der Mehrsitzungs-Betriebssystemmaschine installiert ist.

Der Administrator muss die folgenden Schritte ausführen, um Benutzern auf der Mehrsitzungs-Betriebssystemmaschine kontextbezogenen Zugriff zu ermöglichen:

1. Öffnen Sie den **Registrierungs-Editor** (**regedit.exe**).
2. Navigieren Sie zu **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**.
3. Erstellen Sie die Registrierungseinträge `EnableMultiSessionFlow` und `EnableWFP`, um die Multi-Session-VDI zu aktivieren. Weitere Informationen finden Sie unter NetScaler Gateway Windows VPN-Client-Registrierungsschlüssel.
4. Schließen Sie den **Registrierungs-Editor**.
5. Starten Sie den Computer neu, um sicherzustellen, dass die Einstellungen wirksam werden.

Für in die Domäne eingebundene Maschinen, bei denen die IP-Adresse des Domänencontrollers mit der DNS-IP-Adresse übereinstimmt, muss der Administrator die folgenden Schritte ausführen, um die Multi-Session-VDI zu aktivieren.

1. Öffnen Sie den **Registrierungs-Editor** (**regedit.exe**).
2. Navigieren Sie zu **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**.
3. Erstellen Sie die Registrierungseinträge `EnableMultiSessionFlow` und `AlwaysOnService`, um die Multi-Session-VDI zu aktivieren. Weitere Informationen finden Sie unter NetScaler Gateway Windows VPN-Client-Registrierungsschlüssel.
4. Erstellen Sie einen Registrierungseintrag `CloudAlwaysOnUrl` vom Typ **REG_SZ** und geben Sie die Verbindungs-URL an.
5. Schließen Sie den **Registrierungs-Editor**.
6. Starten Sie den Computer neu, um sicherzustellen, dass die Einstellungen wirksam werden.
7. Im Secure Private Access-Dashboard erstellen Sie eine Anwendung für den Domänencontroller und den Cloud Connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn die IP-Adresse des Domänencontrollers mit der DNS-IP-Adresse übereinstimmt, werden alle an den Domänencontroller gerichteten Aufrufe abgefangen und verworfen. Um zu vermeiden, dass Domänencontroller-Pakete verworfen werden, wird empfohlen, eine Anwendung zu erstellen und allen Benutzern den Zugriff zu ermöglichen.

8. Fügen Sie die IP-Adresse des Domänencontrollers, die der IP-Adresse des DNS-Servers entspricht, der Anwendung hinzu, wobei alle TCP/UDP-Ports zugelassen sind.
9. Legen Sie Zugriffsrichtlinien fest, um sicherzustellen, dass alle Benutzer auf den Domänencontroller zugreifen können.
10. Fügen Sie den Cloud Connector zum Datenverkehrsrouting-Typ **Extern** hinzu, um zu verhindern, dass er getunnelt wird, wenn der Hostname des Cloud Connectors mit Ihrem Suffix übereinstimmt (zum Beispiel ist der Hostname des Cloud Connectors cloudconnector.cloud.com und das Suffix ist *.cloud.com).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Private Access für Mobilgeräte

Die Citrix Secure Private Access Bereitstellungen werden für Mobilgeräte ab Secure Access Client Version 25.08.1 für iOS und Secure Access Client Version 25.11.1 für Android unterstützt. Mobile Benutzer können im Rahmen des Zero-Trust-Modells von Secure Private Access auf Unternehmensanwendungen und Webressourcen zugreifen, wobei die gleichen Sicherheitskontrollen, die gleiche Richtliniendurchsetzung und das gleiche nahtlose Erlebnis wie für Desktop-Benutzer geboten werden.

Unterstützte Versionen und Plattformen

iOS-Geräte:

- **CSA Client**: iOS 25.08.1 (Verfügbar im App Store)
- **iOS-Betriebssystemversion**: Mindestens iOS 16
- **Bereitstellungsmodelle**
  - Secure Private Access für Cloud-Bereitstellungen
  - Secure Private Access für Hybrid-Bereitstellungen

Android-Geräte:

- **CSA Client**: Android 25.11.1 (Verfügbar im Google Play Store)
- **Android-Betriebssystemversion**: Mindestens Android 12
- **Bereitstellungsmodelle**
  - Secure Private Access für Cloud-Bereitstellungen
  - Secure Private Access für Hybrid-Bereitstellungen

Unterstützte Funktionen

Bei Secure Private Access-Bereitstellungen wird der Ressourcenzugriff durch die Richtlinienkonfiguration gesteuert. Administratoren können Richtlinien definieren, die festlegen,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

welche Benutzer oder Gruppen unter bestimmten Bedingungen und von genehmigten Geräten oder Standorten auf bestimmte Anwendungen und Ressourcen zugreifen können.

- Zugriff auf Web-, SaaS- und TCP/UDP-Anwendungen gemäß Ihren Secure Private Access-Richtlinienbedingungen.
- Sitzungssicherheitsrichtlinien: Data Loss Prevention (DLP)-Kontrollen, die von Chrome Enterprise unterstützt werden.

Eine vollständige Liste der unterstützten Funktionen finden Sie unter Citrix Secure Access-Clientfunktionen, die in NetScaler Gateway unterstützt werden.

Voraussetzungen

Der Secure Private Access-Dienst muss konfiguriert und auf dem neuesten Stand sein. Weitere Informationen finden Sie in den folgenden Themen:

- Erste Schritte mit Citrix Secure Private Access
- Secure Private Access-Onboarding und -Einrichtung
- App-Konfiguration und -Verwaltung

Workflow für iOS- und Android-Benutzer mit Citrix Secure Access-Client

Die folgenden Schritte fassen den Secure Private Access-Flow für Benutzer auf iOS- und Android-Geräten mit dem Citrix Secure Access-Client zusammen.

- **Installation des Citrix Secure Access-Clients**: Der Citrix Secure Access-Client muss auf dem Mobilgerät installiert sein. Dies kann über Mobile Device Management (MDM) für Unternehmensgeräte oder manuell durch den Benutzer erfolgen, indem die Anwendung aus dem App Store des Geräts heruntergeladen wird.
- **Zugriff auf Store-/Gateway-URL**: Der Benutzer greift dann auf die vorgesehene Store- oder Gateway-URL zu. Diese URL dient als Einstiegspunkt für den Zugriff auf die Ressourcen des Unternehmens.
- Benutzerauthentifizierung: Der Benutzer wird aufgefordert, seine Identität zu authentifizieren. Dies beinhaltet typischerweise die Eingabe von Anmeldeinformationen wie Benutzername und Passwort oder die Verwendung von Multi-Faktor-Authentifizierungsmethoden (MFA).
- **Richtlinienauswertung und Zugriffsgewährung**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Richtlinie erfüllt: Wenn die Authentifizierung und der Gerätestatus des Benutzers die definierten Sicherheitsrichtlinien erfüllen, wird der Zugriff gewährt. Dies ermöglicht dem Benutzer den Zugriff auf autorisierte Web-, SaaS- und private Webanwendungen.
    - Richtlinie fehlgeschlagen: Wenn der Benutzer die Richtlinienanforderungen nicht erfüllt (z. B. veraltetes Betriebssystem, nicht genehmigtes Gerät, falsche Anmeldeinformationen), wird der Zugriff je nach Richtlinienkonfiguration entweder eingeschränkt oder vollständig verweigert.

- **Erzwungene Sitzungsschutzmaßnahmen**: Sobald der Zugriff gewährt wurde, werden die von Chrome Enterprise unterstützten DLP-Kontrollen (Data Loss Prevention) durchgesetzt. Zum Beispiel:
    - Inkognito-Modus deaktivieren
    - Drucken blockieren
    - URL-Filterung
    - Downloads blockieren
    - Konfigurierte (verwaltete) Lesezeichen

Verwandte Themen

- Citrix Secure Private Access für Cloud-Bereitstellungen
- Citrix Secure Private Access für Hybrid-Bereitstellungen

Kerberos-Authentifizierung mit der iOS Kerberos-Erweiterung

Dieses Thema beschreibt die End-to-End-Konfiguration, die erforderlich ist, um Kerberos-basiertes Single Sign-On (SSO) für interne Web-Apps über die Citrix Secure Access für iOS-App zu ermöglichen.

- iOS-Clientkonfiguration
- MDM-Serverkonfiguration
- IIS-Konfiguration
- Domänencontroller-Konfiguration

iOS-Clientkonfiguration

Die folgenden Abschnitte enthalten weitere Informationen zur iOS-Clientkonfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

Stellen Sie sicher, dass das iOS-Gerät bei MDM registriert ist. Das iOS-Gerät muss in einer MDM-Lösung (z. B. Microsoft Intune) registriert sein, bevor eine SSO-Konfiguration angewendet werden kann. Die MDM-Registrierung ermöglicht das Pushen des Kerberos-SSO-Erweiterungsprofils auf das Gerät.

MDM-Registrierung auf dem iOS-Gerät überprüfen

1. Gehen Sie auf dem iOS-Gerät zu **Einstellungen > Allgemein > VPN & Geräteverwaltung**.

   Unter Geräteverwaltung muss das MDM-Profil Ihrer Organisation aufgeführt sein (z. B. Microsoft Intune oder der Name des MDM-Profils Ihres Unternehmens).
2. Tippen Sie auf das Profil, um zu bestätigen, dass es installiert ist und der Status **Verifiziert** oder **Installiert** anzeigt.
3. Um zu bestätigen, dass die Kerberos-SSO-Erweiterung von MDM gepusht wurde:

   - Gehen Sie zu **Einstellungen > Allgemein > VPN & Geräteverwaltung**.
   - Tippen Sie auf das MDM-Profil, suchen Sie unter den Profildetails nach **Single Sign-On-Erweiterungen** oder **Kerberos**.
   - Alternativ gehen Sie zu **Einstellungen > Allgemein > VPN & Geräteverwaltung > Single Sign-On** und überprüfen Sie, ob die Kerberos-Erweiterung aufgeführt ist.

   Wenn das Gerät nicht registriert ist oder das Profil fehlt, wenden Sie sich an Ihren MDM-Administrator, um das Gerät zu registrieren, bevor Sie fortfahren.

MDM-Serverkonfiguration

HINWEIS:

Die Konfiguration der MDM-SSO-Erweiterungs-Payload basiert auf der offiziellen Apple-Dokumentation.

- Einstellungen für die Single Sign-On-Geräteverwaltungs-Payload für Apple-Geräte
- Kerberos Single Sign-On-Erweiterung mit Apple-Geräten

Stellen Sie sicher, dass die folgenden Felder in der MDM-SSO-Erweiterungs-Payload konfiguriert sind:

1. **Domain:** Die URLs, die für Kerberos verwendet werden.

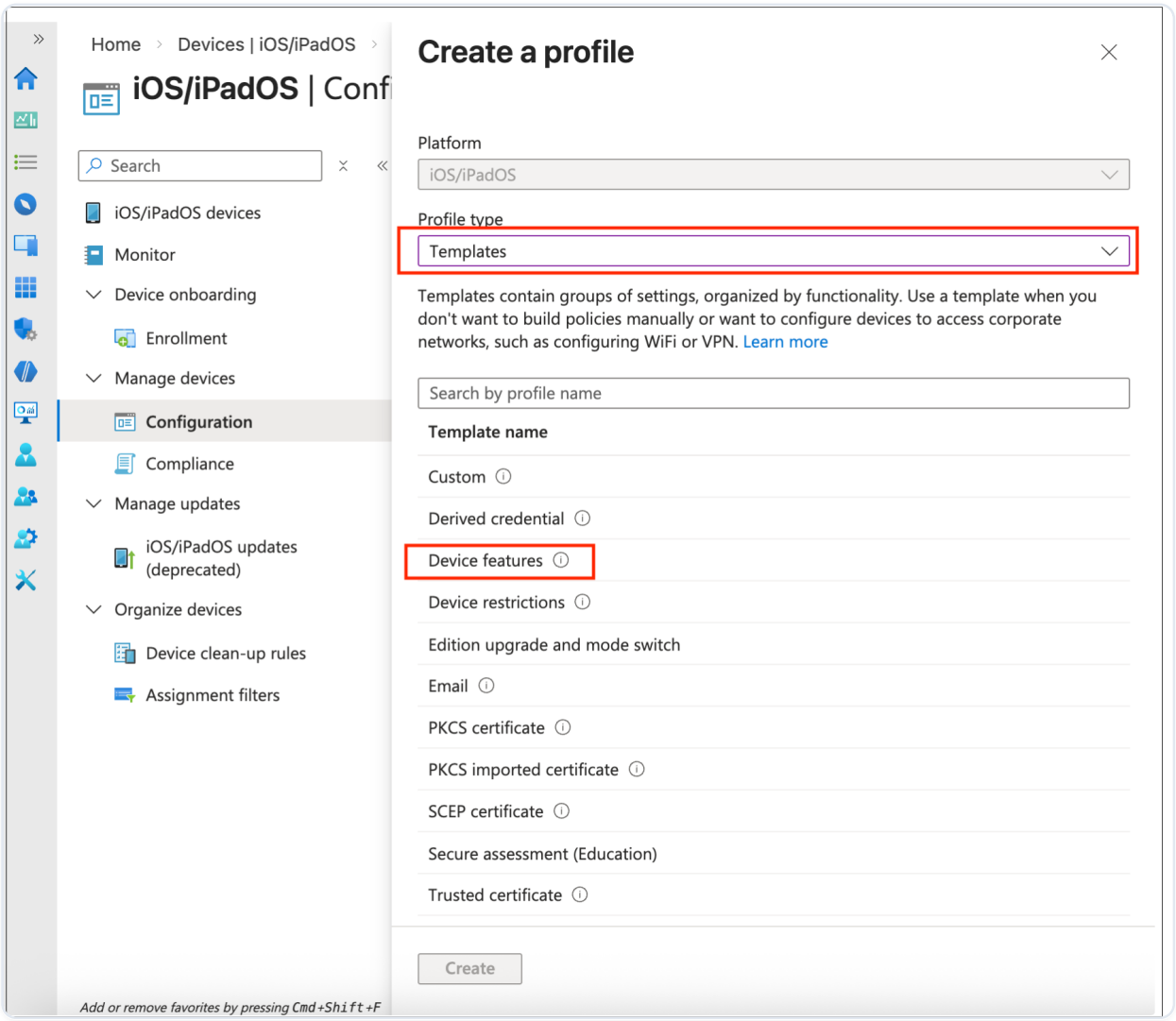
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **AppBundleIDs:** Zulassungsliste der Apps, die verwendet werden. (Zum Beispiel: Chrome: `com.google.chrome.ios`, Citrix Secure Access: `com.citrix.securehub`)
3. **Realm:** Standort Ihres Rechenzentrums.

Intune-Richtlinienkonfiguration

Voraussetzungen: Stellen Sie sicher, dass das iOS-Gerät in Intune registriert ist.

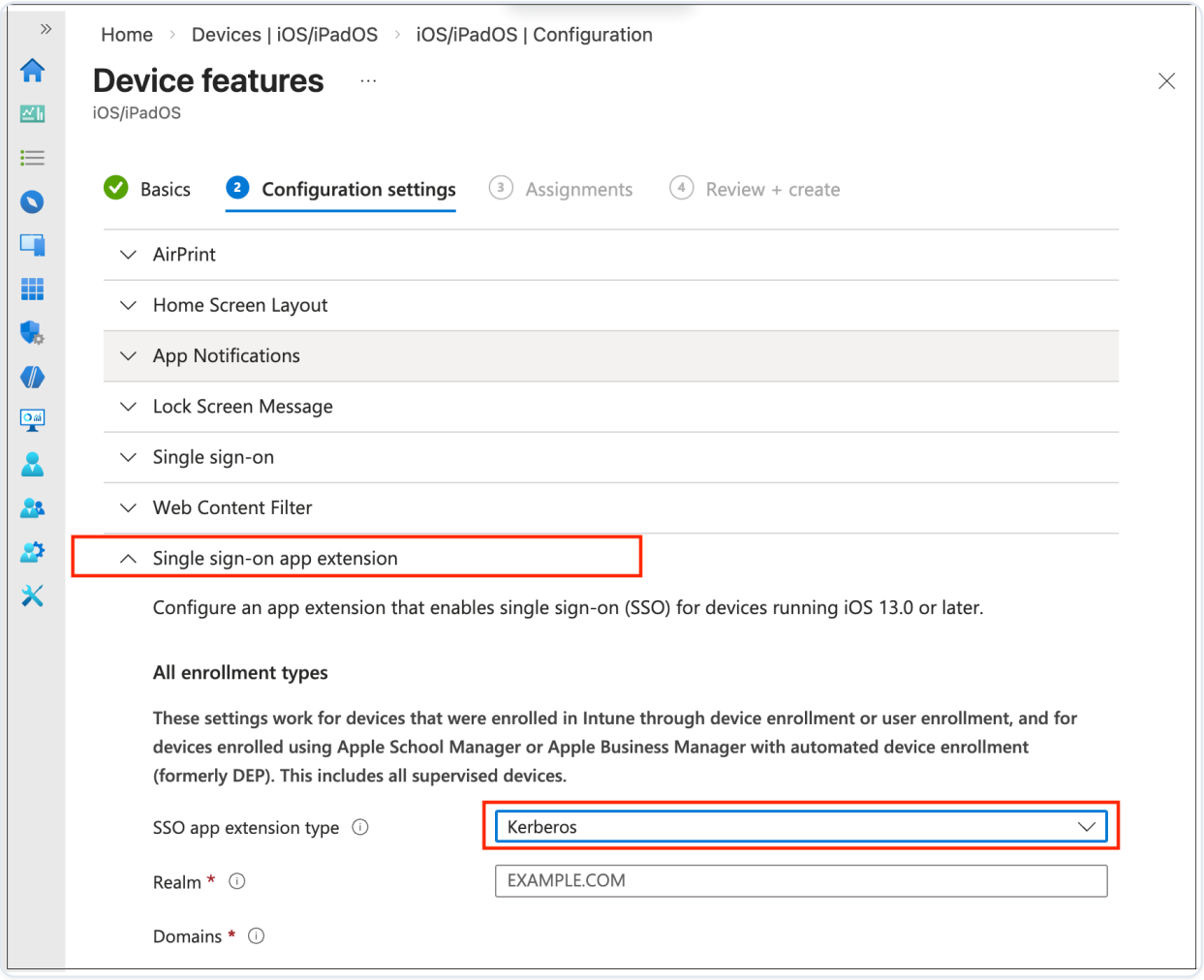
1. Navigieren Sie in der Intune-Administratorkonsole zu **Home > Geräte | iOS/iPadOS → iOS/iPadOS | Konfiguration**.
2. Erstellen Sie eine neue Richtlinie.
3. Wählen Sie unter **Profiltyp** die Option **Vorlagen** und anschließend **Gerätefunktionen** aus.



4. Klicken Sie auf **Erstellen**.
5. Geben Sie einen Namen für die Richtlinie ein und fahren Sie dann mit den **Konfigurationseinstellungen** fort.

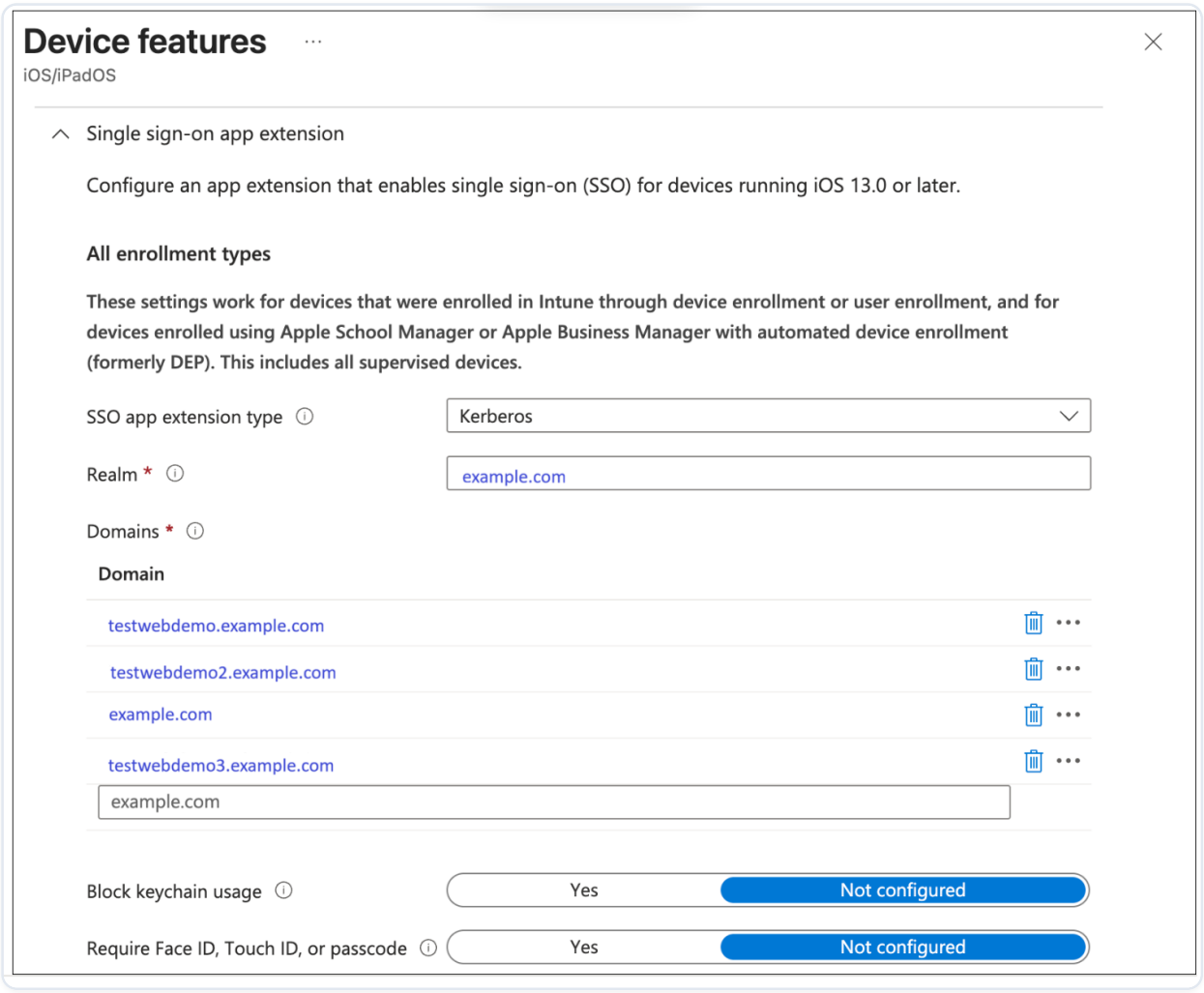
© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Wählen Sie unter **Single Sign-On-App-Erweiterung > SSO-App-Erweiterungstyp** die Option **Kerberos** aus.

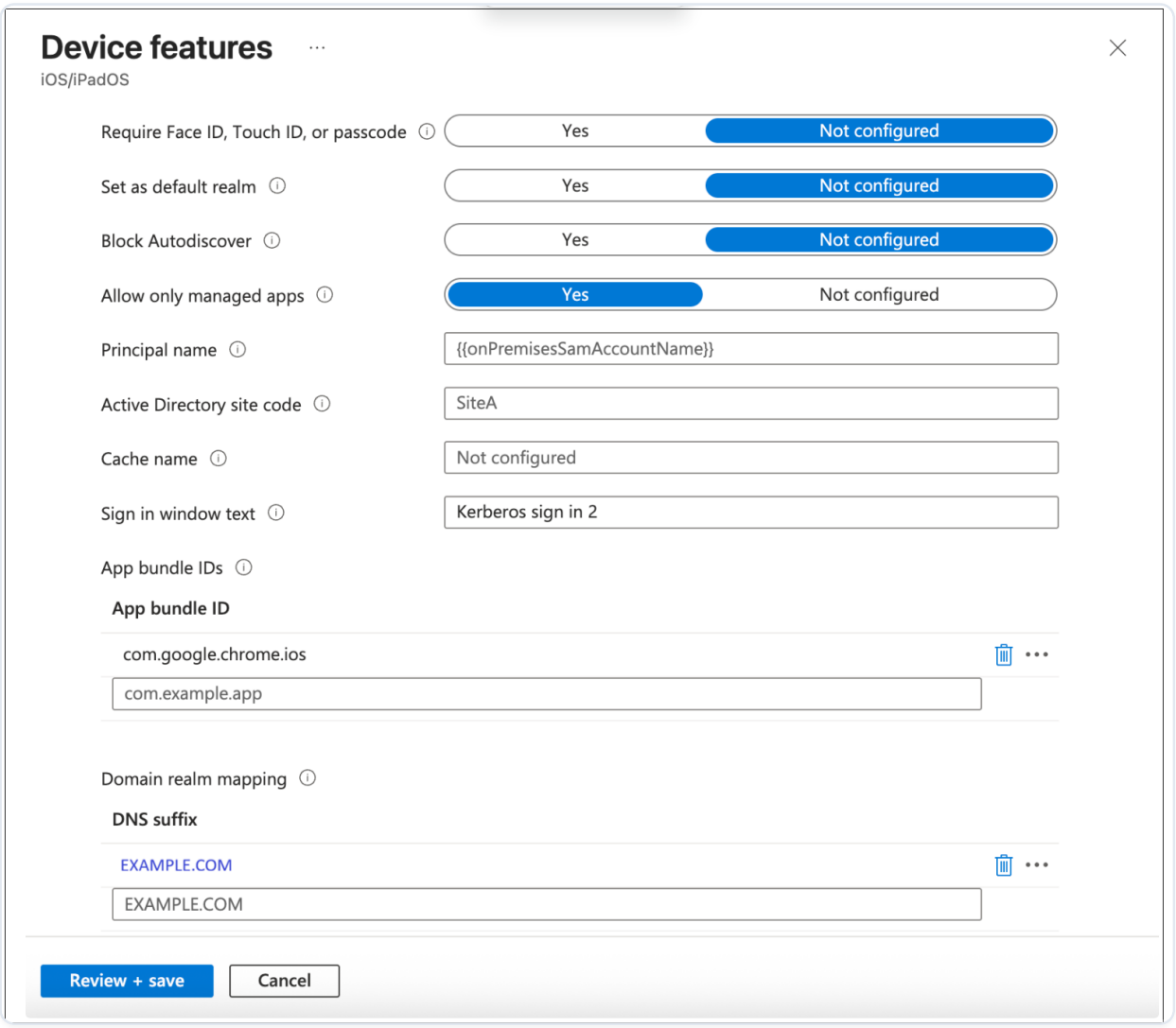


7. Füllen Sie die Informationen gemäß Ihren Einrichtungsanforderungen aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Klicken Sie auf **Überprüfen + speichern**.
9. Binden Sie die Richtlinie an Ihr Gerät:
    - Gehen Sie zu **Richtlinie bearbeiten** und klicken Sie auf die Richtlinie.
    - Bearbeiten Sie **Zuweisungen**.
    - Wählen Sie Ihre Gerätegruppe aus (erstellen Sie zuerst eine Gerätegruppe mit Ihrem Gerät, falls noch nicht geschehen).
10. Synchronisieren Sie das Gerät.

IIS-Konfiguration

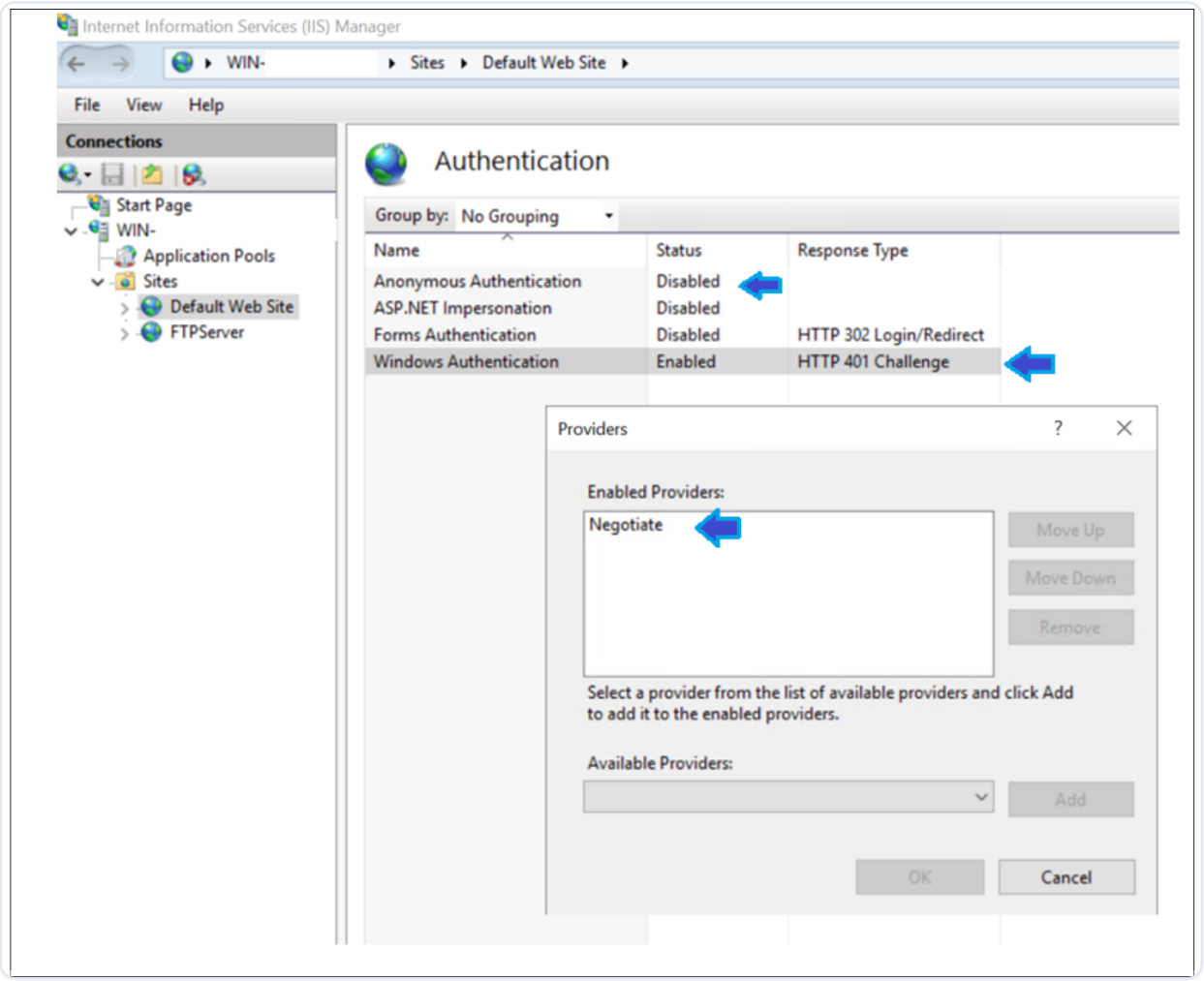
Aktivieren Sie auf dem IIS-Webserver die **Windows-Authentifizierung** mit dem Negotiate-Anbieter und deaktivieren Sie die **Anonyme Authentifizierung**, um die Kerberos-basierte Authentifizierung zu erzwingen.

Schritte zur Konfiguration der IIS-Authentifizierung:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Öffnen Sie den IIS-Manager (**inetmgr** über **Ausführen** oder **Start**).
2. Wählen Sie im Bereich **Verbindungen** die zu konfigurierende Site oder Anwendung aus.
3. Doppelklicken Sie im IIS-Abschnitt der Featureansicht auf **Authentifizierung**.
4. Deaktivieren Sie die **Anonyme Authentifizierung**.
    - Wählen Sie **Anonyme Authentifizierung** aus und klicken Sie im Bereich **Aktionen** auf **Deaktivieren**.
5. Aktivieren Sie die **Windows-Authentifizierung**.
    - Wählen Sie **Windows-Authentifizierung** aus und klicken Sie im Bereich **Aktionen** auf **Aktivieren**.
6. Legen Sie den Negotiate-Anbieter fest.
    - Wenn **Windows-Authentifizierung** ausgewählt ist, klicken Sie im Bereich **Aktionen** auf **Anbieter…**.
    - Stellen Sie sicher, dass **Negotiate** an erster Stelle steht (über NTLM). Fügen Sie es hinzu, falls es fehlt.
    - Klicken Sie auf **OK**.
7. Klicken Sie im Bereich **Aktionen** auf **Übernehmen**, um die Änderungen zu speichern.
8. Führen Sie optional `iisreset` von einer erhöhten Eingabeaufforderung aus, um die Konfiguration sofort anzuwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Konfiguration auf der Domänencontrollerseite

SPN-Registrierung für Kurznamen und FQDN: Kerberos erfordert eine exakte Übereinstimmung zwischen der vom Client verwendeten URL und einem registrierten SPN in der Domäne. Ein Client, der auf `http://testwebdemo` zugreift, verwendet einen anderen SPN als ein Client, der auf `http://testwebdemo.example.com` zugreift, daher müssen beide registriert werden.

1. Ersetzen Sie `<dc-hostname>` unten durch den Hostnamen Ihres Domänencontrollers.
2. Registrieren Sie beide Formen.

   - Kurzer Hostname (wird verwendet, wenn der Client über einen Kurznamen zugreift, z. B. `http://testwebdemo`)

     ```
     setspn -s HTTP/testwebdemo example.com\<dc-hostname>
     ```

   - FQDN (wird verwendet, wenn der Client über den vollständigen Domänennamen zugreift, z. B. `http://testwebdemo.example.com`)

     ```
     setspn -s HTTP/testwebdemo.example.com example.com\<dc-hostname>
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Überprüfen Sie, ob beide auf dem richtigen Konto registriert sind.
    - setspn -L beispiel.com\<dc-hostname>
4. Die erwartete Ausgabe muss beides enthalten:
    - HTTP/testwebdemo
    - HTTP/testwebdemo.example.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einstellung von Funktionen

Dieser Artikel informiert Sie vorab über Secure Private Access-Dienstfunktionen, die eingestellt werden, damit Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Kundennutzung und das Feedback, um zu bestimmen, wann Funktionen zurückgezogen werden. Ankündigungen können sich in nachfolgenden Releases ändern und möglicherweise nicht jede eingestellte Funktion oder Funktionalität umfassen. Details zum Produktlebenszyklus-Support finden Sie unter Product Lifecycle Support Policy.

Die folgende Tabelle listet die Secure Private Access-Dienstfunktionen auf, die eingestellt wurden oder deren Einstellung geplant ist.

ELEMENT	EINSTELLUNG ANGEKÜNDIGT IN	EINSTELLUNGSDATUM	ALTERNATIVE
Clientlose VPN-Zugriffsmethode für den Web-App-Zugriff	Januar 2023	October 17, 2023	Verwenden Sie Citrix Enterprise Browser oder Direct Access je nach Anwendungsfall. Weitere Details finden Sie unter About deprecation of clientless VPN access for Web app access.
Kategoriebasierte Webfilterung	Dezember 2022	December 31, 2022	Die Funktionalität zur Zulassung, Verweigerung oder RBI-Umleitung pro Website in Secure Private Access bleibt erhalten, um einen selektiven Zugriff auf nicht arbeitsbezogene Websites über Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ELEMENT	EINSTELLUNG ANGEKÜNDIGT IN	EINSTELLUNGSDATUM	ALTERNATIVE
			Enterprise Browser zu ermöglichen.
Sicherheitskontrolle zur Navigationseinschränkung	April 2022	15 June 2022	NA
Citrix Gateway Konnektor	Mai 2022	30 September 2022	Konnektor-Appliance. Informationen zur Migration Ihres Gateway Konnektors zur Konnektor-Appliance finden Sie unter Gateway Konnektor zu Konnektor-Appliance migrieren.

Informationen zur Einstellung des clientlosen VPN-Zugriffs für den Web-App-Zugriff

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

  Citrix Secure Private Access™ verwendet die CVPN-basierte Zugriffsmethode, wenn eine interne Web-App, die ohne erweiterte Sicherheitseinschränkungen konfiguriert ist, über ihre Store-URL in einem Webbrowser aufgerufen wird.

  HINWEIS:

  Die clientlose VPN-Zugriffsmethode wird nur verwendet, wenn eine interne App über die Store-URL in einem Webbrowser aufgerufen wird. Nur Apps, die ohne erweiterte Sicherheitseinschränkungen konfiguriert sind, werden blockiert.

- Warum stellen wir diese Funktion ein?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die clientlose VPN-Methode verwendet clientseitige URL-Umschreibungen, die bestimmte branchenweite technologische Einschränkungen aufweisen. In mehreren Fällen kann dies zu Fehlern beim App-Zugriff führen, wenn bestimmte Links innerhalb der Web-Apps umgeschrieben werden. Dies führt zu einer schlechten Benutzererfahrung. Um unseren Kunden die beste App-Zugriffserfahrung zu bieten, stellen wir diese Funktion ein und empfehlen, zu einer der unten genannten Alternativen zu wechseln.

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

  Wenn über die Store-URL von einem Webbrowser aus auf eine Web-App zugegriffen wird, die ohne erweiterte Sicherheitsbeschränkungen konfiguriert ist, wird der Zugriff auf diese Anwendung blockiert. Dies hat keine Auswirkungen auf Endbenutzer, die über die Citrix Workspace-App, Direct Access, den Remote Browser Isolation-Dienst (RBI) oder den Secure Access Agent auf Anwendungen zugreifen.

- Welche Alternativen gibt es und was sollten die Administratoren 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 Endbenutzererfahrung mit erweiterten Sicherheitseinstellungen (wie Einschränkung von Downloads, Druckbeschränkungen, Wasserzeichen, Einschränkung des Zwischenablagezugriffs) und Browserverwaltung. **Direct Access:** Wenn Sie eine clientlose Methode für den Zugriff auf Webanwendungen wünschen, verwenden Sie die Direct Access-Methode, mit der Apps direkt von jedem nativen Browser wie Chrome 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.

- Betrifft dies bestehende Anwendungen, 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 eine in einem Webbrowser geöffnete Store-URL zugegriffen wird. Diese Einstellung hat keine Auswirkungen auf Anwendungen, auf die über die Citrix Workspace-App oder Secure Access-Clients zugegriffen wird, die auf Endgeräten installiert sind. Wenn auf eine Webanwendung, die mit erweiterten Sicherheitsbeschränkungen konfiguriert ist, über einen Webbrowser zugegriffen wird, wird der Zugriff auf diese Anwendungen blockiert.

- Haben Sie weitere Fragen?

  Wenden Sie sich an den Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datengovernance

Dieses Thema enthält Informationen bezüglich der Erfassung, Speicherung und Aufbewahrung von Protokollen durch den Citrix Secure Private Access-Dienst. Alle großgeschriebenen Begriffe, die nicht in den Definitionsabschnitten definiert sind, haben die Bedeutung, die im Citrix Endbenutzer-Dienstleistungsvertrag festgelegt ist.

Datenresidenz

Citrix Secure Private Access verwendet eine Multi-Region-Architektur, die hohe Verfügbarkeit und Redundanz gewährleistet. Weitere Informationen finden Sie unter Points of Presence.

- USA (Osten)
- USA (Westen)
- Brasilien (Süden)
- Südostasien
- Nordeuropa
- Westeuropa
- Australien (Osten)
- Südindien

Im Folgenden sind die verschiedenen Ziele für die Dienstkonfigurations- und Laufzeitprotokolle aufgeführt.

- Splunk-Dienst für Systemüberwachungs- und Debug-Protokolle, nur am Standort USA.
- Citrix Analytics Service für Diagnose- und Benutzerzugriffsprotokolle, weitere Informationen finden Sie unter Citrix Analytics Service Data Governance.
- Citrix Application Delivery Management Service für die aggregierten Benutzerzugriffsprotokolle, weitere Informationen finden Sie unter Citrix ADM Data Governance.
- Citrix Cloud™ System Logs Service für Administrator-Audit-Protokolle, siehe den untenstehenden Link

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allgemeine Informationen zu Citrix Cloud Services finden Sie unter Citrix Cloud Services Customer Content and Log Handling und Geographical Considerations.

Datenerfassung

Citrix Secure Private Access ermöglicht Administratoren die Konfiguration und Verwaltung des Dienstes und der zugehörigen Connector Appliances über eine zentrale Verwaltungsoberfläche. Der Dienst verarbeitet die folgenden Arten von Kundendaten:

- Für den Secure Private Access-Dienst
  - Private und SaaS-Anwendungen des Kunden
  - FQDNs und URLs für Web-Apps oder beides
  - IP-Adressen/-Bereiche, Ports und Protokolle
  - Die zugehörigen Ressourcenstandorte
  - Single Sign-On-Parameter für Web- und SaaS-Apps
- Benutzerkennungen für App-Berechtigungen
- Bedingungen für Adaptive Access-Richtlinien
  - Benutzeridentität
  - Geo-Standort des Benutzers/Geräts
  - Benutzer-/Geräte-Netwerkstandort über die Citrix Cloud Netwerkstandort-Konfiguration. Weitere Informationen finden Sie unter Optimize connectivity to stores with Direct Workload Connection.
  - Gerätetyp
- Informationen zur Connector Appliance-Plattform finden Sie unter Connector Appliance for Cloud Services im Zusammenhang mit Secure Private Access.
  - IP-Adressen oder FQDNs
  - Benutzer-, Geräte- und Ressourcenstandort-Identifikatoren
  - Interne Proxy-Konfiguration

Für Laufzeitprotokolle, die von den Dienstkomponenten erfasst werden, bestehen die wichtigsten Informationen aus Folgendem:

- Benutzername

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Benutzerobjekt-ID
- E-Mail-Adresse des Benutzers
- Benutzer-UPN
- Benutzergruppenmitgliedschaften
- Client-IP-Adresse und Port
- Ziel-FQDN/-Adresse und Port
- Client-User-Agent
- Anwendungsname
- Anwendungs-URL-Pfad
- Anwendungszugriffszeit und -dauer
- Anforderungs-Byte-Anzahl
- Antwort-Byte-Anzahl
- Webfilter-Entscheidung für nicht genehmigte Anwendungen
- HTTP-Transaktions-ID

Eine umfassende Liste der an den Citrix Analytics Service gesendeten Daten finden Sie unter Citrix Analytics Service Data Governance.

Datenübertragung

Citrix Secure Private Access sendet Protokolle an Ziele, die durch Transport Layer Security geschützt sind.

Datenkontrolle

Der Citrix Secure Private Access-Dienst bietet dem Kunden derzeit keine Optionen, das Senden von Protokollen zu deaktivieren oder die globale Replikation von Kundeninhalten zu verhindern.

Datenaufbewahrung

Gemäß der Citrix Cloud-Datenaufbewahrungsrichtlinie werden die Kundenkonfigurationsdaten 90 Tage nach Ablauf des Abonnements aus dem Dienst gelöscht.

Die Protokollziele behalten ihre dienstspezifische Datenaufbewahrungsrichtlinie bei.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen finden Sie unter Daten-Governance bezüglich der Aufbewahrungsrichtlinie für die Analyseprotokolle.
- Für die in Citrix Application Delivery Management gespeicherten Ereignisse siehe Daten-Governance.
- Die Splunk-Protokolle werden nach 90 Tagen archiviert und schließlich entfernt.

Datenexport

Es gibt verschiedene Datenexportoptionen für verschiedene Protokolltypen.

- Die Administrator-Auditprotokolle sind über die Citrix Cloud System Log-Konsole zugänglich.
- Die Diagnoseprotokolle des Secure Private Access Service können aus dem Citrix Analytics Service als CSV-Datei exportiert werden.
- Die Splunk-Protokolle sind nicht für den Kundenverbrauch bestimmt. Diese Ereignisse können auch aus Splunk als CSV-Datei exportiert werden.

Definitionen

- Kundeninhalte bezeichnet alle Daten, die zur Speicherung auf ein Kundenkonto hochgeladen werden, oder Daten in einer Kundenumgebung, auf die Citrix zum Erbringen von Services Zugriff erhält.
- Protokoll bezeichnet eine Aufzeichnung von Ereignissen im Zusammenhang mit den Services, einschließlich Aufzeichnungen, die Leistung, Stabilität, Nutzung, Sicherheit und Support messen.
- Services bezeichnet die zuvor beschriebenen Citrix Cloud-Services für die Zwecke von Citrix Analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Produktzertifizierungen und Compliance

Citrix Secure Private Access ist eine Zero Trust Network Access (ZTNA)-Lösung, die Unternehmen dabei hilft, Benutzer sicher mit Anwendungen zu verbinden, ohne Netzwerke direkt dem Internet auszusetzen. Secure Private Access wird als Teil des breiteren Citrix Cloud- und Hybrid-Serviceportfolios bereitgestellt und unterliegt den Compliance- und Auditprogrammen für Cloud-Dienste von Citrix.

Diese Seite fasst die für Secure Private Access geltenden Zertifizierungen und Compliance-Bescheinigungen zusammen.

Zertifizierungen und Audits

- **SOC 2® Typ 2:**

  Secure Private Access ist im Rahmen des SOC 2 Typ 2-Auditprogramms von Citrix abgedeckt.

  SOC 2 Typ 2-Audits haben die Sicherheits-, Verfügbarkeits-, Vertraulichkeits-, Verarbeitungs- und Datenschutz-Kontrollen bewertet, die für Citrix Cloud-Dienste, einschließlich Secure Private Access, gelten.

- **ISO 27001 & ISO 27701:**

  Secure Private Access ist im zertifizierten Serviceportfolio von Citrix für ISO 27001 (Informationssicherheitsmanagement) und ISO 27701 (Datenschutzinformationsmanagement) enthalten.

  Diese weltweit anerkannten Zertifizierungen bestätigen, dass Sicherheits- und Datenschutzmanagementpraktiken formell etabliert, dokumentiert und kontinuierlich verbessert werden.

- **HIPAA:**

  Secure Private Access ist für den Einsatz in Umgebungen geeignet, die HIPAA-Konformität erfordern, wenn es entsprechend konfiguriert und vertraglich vereinbart ist. Die Cloud-Compliance-Dokumentation von Citrix weist auf die HIPAA-Anwendbarkeit für Secure Private Access hin.

- **PCI DSS 4.0:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access ist in den jährlichen PCI DSS-Bewertungen von Citrix für anwendbare Cloud-Dienste enthalten. Kunden, die Secure Private Access in PCI-relevanten Umgebungen bereitstellen, müssen möglicherweise zusätzliche Kontrollen implementieren, um die PCI-Anforderungen zu erfüllen. Die PCI DSS-Konformität folgt einem Modell der geteilten Verantwortung zwischen Citrix und dem Kunden.

- **FIPS / Common Criteria:**

  Secure Private Access kann als Teil einer FIPS-konformen Lösung bereitgestellt werden, wenn es mit FIPS-zertifizierten oder FIPS-fähigen NetScaler-Plattformen und dem FIPS-zertifizierten Citrix CryptoKit, das von der Citrix Workspace-App verwendet wird, kombiniert wird.

  Für Common Criteria integriert sich Secure Private Access in Common Criteria (NDcPP)-zertifizierte NetScaler-Plattformen und die Common Criteria-zertifizierte Citrix Workspace-App, wodurch Bereitstellungen ermöglicht werden, die den Common Criteria-Anforderungen auf Lösungsniveau entsprechen.

- **Australien IRAP (Information Security Registered Assessors Program):**

  Secure Private Access ist in den Cloud-Diensten von Citrix enthalten, die von akkreditierten Gutachtern der australischen Regierung IRAP-Bewertungen unterzogen werden.

  IRAP bietet eine unabhängige Validierung, dass die Citrix Cloud-Dienste den Sicherheitskontrollen des Australian Government Information Security Manual (ISM) entsprechen.

Zertifikate und Auditberichte

Laden Sie die verfügbaren Zertifikate und Auditberichte über das Citrix Trust Center herunter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Gateway Connector zu Connector Appliance migrieren
- Routingtabellen zur Lösung von Konflikten, die aus denselben verwandten Domänen resultieren
- Einmaliges Anmelden beim Citrix Secure Access™ Client über die Citrix Workspace-App
- ADFS-Integration mit Secure Private Access
- Citrix Secure Private Access™
- DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten
- G Suite konfigurieren
- Jira konfigurieren
- O365 konfigurieren
- ERP Cloud konfigurieren
- ServiceNow konfigurieren
- Tableau konfigurieren
- Workday konfigurieren
- Zoom konfigurieren
- Richtlinienerzwingung basierend auf dem Zugriffsmodus
- Unterstützung für Server-zu-Client-Verbindungen – Vorschau

Gateway Connector zu Connector Appliance migrieren

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Übergeordnete Schritte zur Migration von Gateway Connector zu Connector Appliance

1. Installieren Sie die Connector Appliances zusätzlich zu den Gateway Connectors am selben Ressourcenstandort.
2. Fahren Sie die Gateway Connectors herunter und testen Sie die Konnektivität der vorhandenen Web-Apps. Überprüfen Sie, ob die am selben Ressourcenstandort gehostete Web-App zugänglich ist.
3. Entfernen Sie den Citrix Gateway Connector, sobald die Tests abgeschlossen sind.

So installieren Sie Connector Appliance

Führen Sie die folgenden Schritte aus, um eine Connector Appliance zu installieren.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links auf dem Bildschirm **Ressourcenstandorte** aus.
3. Klicken Sie auf das Plus-Symbol neben Connector Appliance für den Ressourcenstandort, 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 (IP-Adresse auf der Konsole des Hypervisors angegeben) an und richten Sie bei Bedarf einen Proxy ein.
7. Klicken Sie auf die Schaltfläche **Registrieren** und rufen Sie den Kurzcode ab.
8. Fügen Sie den Kurzcode in die Citrix Cloud-Benutzeroberfläche ein, die beim Herunterladen der Connector Appliance verwendet wurde (Schritt 5).

   Die Connector Appliance ist registriert.

Ausführliche Schritte finden Sie unter Connector Appliance für Cloud Services.

FAQs

- Wie lade ich die Connector Appliance herunter?

  Herunterladen der Connector Appliance.

- Wie installiere ich die Connector Appliance?

  Installieren der Connector Appliance.

- Wie registriere ich die Connector Appliance?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registrieren der Connector Appliance.

- Was sind die Konnektivitätsanforderungen für die Connector Appliance?

  Internet-Konnektivitätsanforderungen für die Connector Appliance.

- Was sind die Systemanforderungen für die Connector Appliance?

  Systemanforderungen für die Connector Appliance.

- Wie wird die Connector Appliance aktualisiert?

  Connector Appliance-Updates

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

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

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

Funktionsweise der Routingtabelle

Die Administratoren können die folgenden Routing-Typen für die Anwendungen definieren, je nachdem, wie sie den Datenverkehrsfluss definieren möchten.

- **Intern – Proxy umgehen** – Der Domänenverkehr wird über den Citrix Cloud Connector™ geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.
- **Intern über Connector** – Die Anwendungen sind extern, aber der Datenverkehr muss über die Connector Appliance zum externen Netzwerk fließen.
- **Extern** – Der Datenverkehr fließt direkt ins Internet.

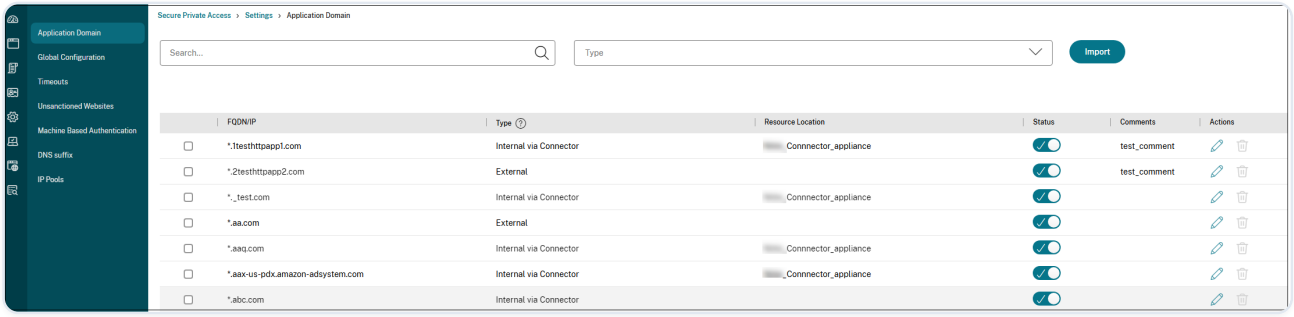
© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Routing-Einträge haben keinen Einfluss auf die Sicherheitsrichtlinien, die für die Anwendungen konfiguriert sind.
- Wenn Administratoren einen Eintrag in der Routingtabelle nicht verwenden möchten oder wenn die entsprechenden Anwendungen nicht wie beabsichtigt funktionieren, können Administratoren den Eintrag einfach deaktivieren, anstatt ihn zu löschen.
- Alle Connector Appliances für einen bestimmten Kunden erhalten, unabhängig vom Anwendungstyp, die SSO-Einstellungen. Zuvor war die SSO-Einstellung für eine bestimmte Anwendung an einen Ressourcenstandort gebunden.

Hauptroutingtabelle

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. Dies kann verwendet werden, um die folgenden Informationen für jede Domäne anzuzeigen:



Die Hauptroutentabelle kann verwendet werden, um die folgenden Informationen für jede Domäne anzuzeigen:

- **FQDN/IP:** FQDN oder die IP-Adresse, für die die Art der Datenverkehrsweiterleitung konfiguriert werden soll.
- **Typ**: App-Typ. **Intern**, **Intern – Proxy umgehen** oder **Extern**, wie beim Hinzufügen der App ausgewählt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

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

- **Ressourcenstandort:** Ressourcenstandort für die Weiterleitung vom Typ **Intern**. Wenn kein Ressourcenstandort zugewiesen ist, wird in der Spalte **Ressourcenstandort** für die jeweilige App ein dreieckiges Symbol angezeigt. Wenn Sie den Mauszeiger über das Symbol bewegen, wird die folgende Meldung angezeigt.

  Ressourcenstandort fehlt. Stellen Sie sicher, dass diesem FQDN ein Ressourcenstandort zugeordnet ist.
- **Status:** Der Umschalter in der Spalte **Status** kann verwendet werden, um die Route für einen Routeneintrag zu deaktivieren, ohne die App zu löschen. Wenn der Umschalter ausgeschaltet ist, wird der Routeneintrag nicht wirksam. Wenn FQDNs mit exakter Übereinstimmung vorhanden sind, können Administratoren auch die zu aktivierende oder deaktivierende Route auswählen.
- **Kommentare:** Zeigt Kommentare an, falls vorhanden.
- **Aktionen:** Das Bearbeitungssymbol wird verwendet, um einen Ressourcenstandort hinzuzufügen oder den Typ des Routeneintrags zu ändern. Das Löschsymbol wird verwendet, um die Route zu löschen.

Mini-Routentabelle

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

Routen zur Mini-Routentabelle hinzufügen

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 Unternehmens-Web-Apps beschrieben, mit Ausnahme der folgenden zwei Änderungen:

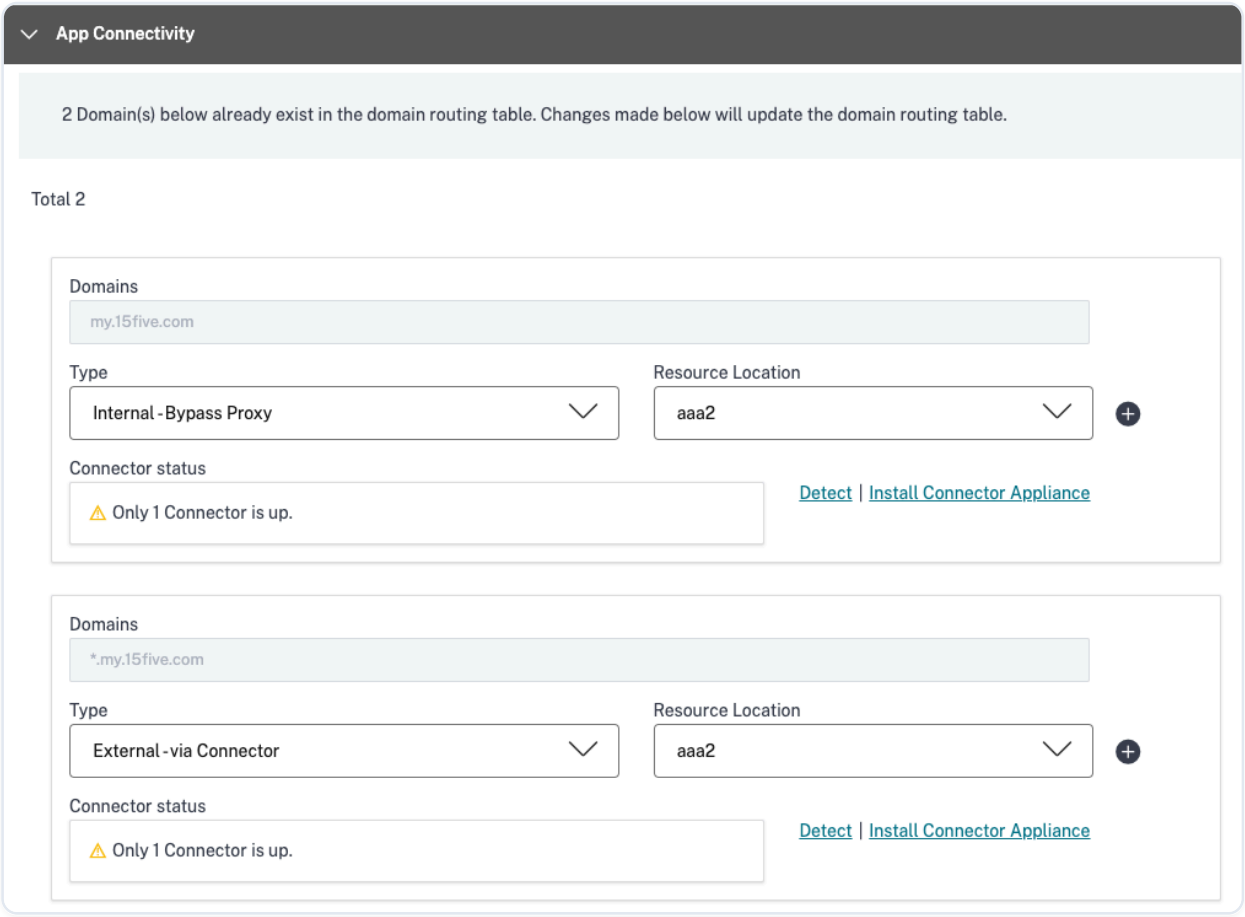
1. Führen Sie die folgenden Schritte aus:

   - Wählen Sie eine Vorlage aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Geben Sie die App-Details ein.
- Wählen Sie gegebenenfalls erweiterte Sicherheitsdetails aus.
- Wählen Sie gegebenenfalls die Single Sign-On-Methode aus.

2. Klicken Sie auf **App-Konnektivität**. – Eine Mini-Version der Tabelle „Anwendungsdomänen“ 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. Die erste Zeile zeigt die tatsächliche App-URL an, die der Administrator beim Hinzufügen der App-Details eingegeben hat. Die anderen Zeilen sind alle verwandten Domänen, die beim Hinzufügen der App-Details eingegeben werden. Wenn die App-URL und die verwandten Domänen identisch sind, werden sie in einer Zeile angezeigt.

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

- **Typ:** Wählen Sie eine der folgenden Optionen aus.
  - **Intern – Proxy umgehen** – Der Domänenverkehr wird über den Citrix Cloud™ Connector geleitet, wobei der auf der Connector Appliance konfigurierte Web-Proxy des Kunden umgangen wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Intern über Connector** – Die Apps sind extern, aber der Datenverkehr muss über die Connector Appliance 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 ihn, wenn ein anderer Ressourcenstandort gewünscht wird.
- **Status der Connector Appliance:** Wird zusammen mit dem Ressourcenstandort automatisch ausgefüllt, wenn Sie den Typ „Intern“ für eine App auswählen.

Einmaliges Anmelden beim Citrix Secure Access™ Client über die Citrix Workspace-App

Der Citrix Secure Access Client unterstützt jetzt das einmalige Anmelden für die Store-URL, wenn bereits über die Citrix Workspace-App angemeldet. Diese SSO-Funktionalität verbessert die Benutzererfahrung, indem sie mehrere Authentifizierungen vermeidet.

Voraussetzungen

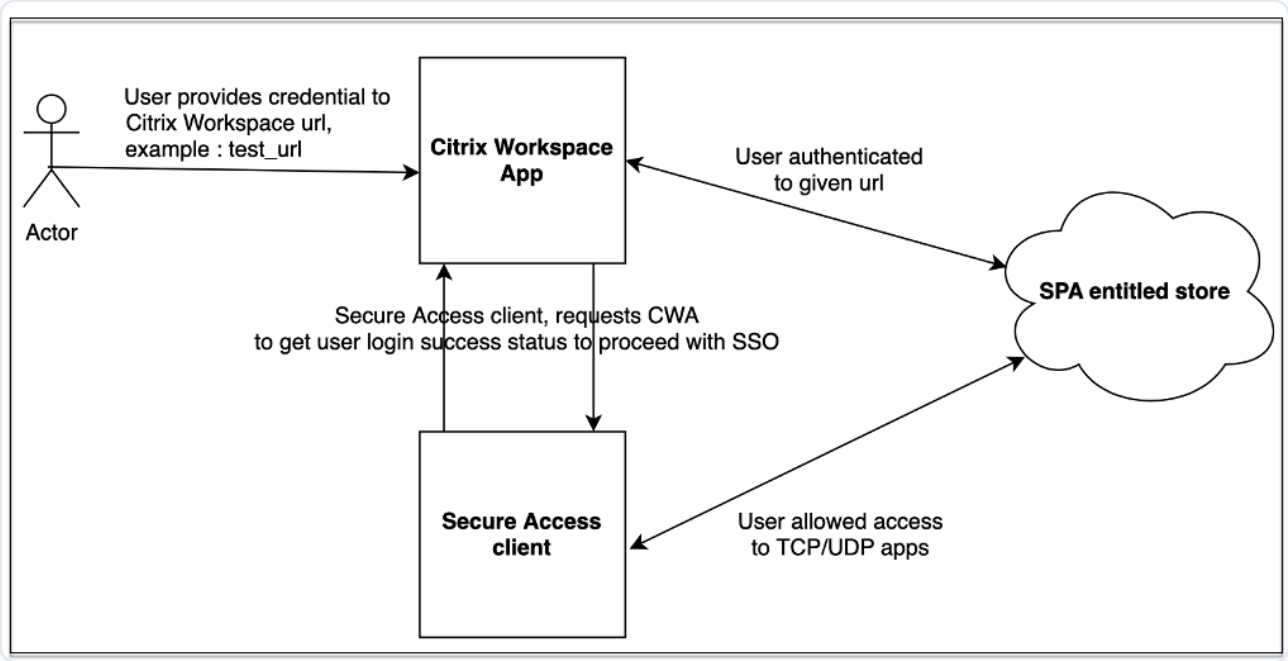
- Sowohl die Citrix Workspace-App als auch der Secure Access Client müssen auf dem Gerät installiert sein.
- Benutzer müssen sich zuerst bei der Citrix Workspace-App angemeldet haben, damit das automatische SSO im Citrix Secure Access Client erfolgt.

HINWEIS:

Die Funktion für einmaliges Anmelden wird nur für den primären Store unterstützt, der in der Citrix Workspace-App konfiguriert ist. Wenn sich der Benutzer bei einem anderen Store als dem primären Store anmeldet, erfolgt kein SSO. Der Benutzer muss sich manuell beim Citrix Secure Access Client anmelden.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Funktionsanforderungen für Windows

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

Die SSO-Funktion ist standardmäßig deaktiviert. Um diese Funktion zu aktivieren, fügen Sie den folgenden Registrierungseintrag auf dem Endbenutzergerät hinzu.

- Registrierungsname – EnableCWASSO
- Registrierungspfad – HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Registrierungstyp – REG_DWORD
- Registrierungswert – 1

WICHTIG:

Manchmal müssen die Endbenutzergeräte möglicherweise neu gestartet werden, um Single Sign-On mit der Citrix Workspace-App erfolgreich herzustellen.

ADFS-Integration mit Secure Private Access

Anspruchsregeln sind notwendig, um den Fluss von Ansprüchen durch die Anspruchspipeline zu steuern. Anspruchsregeln können auch verwendet werden, um den Anspruchsfluss während des

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ausführungsprozesses der Anspruchsregeln anzupassen. Weitere Informationen zu Ansprüchen finden Sie in der Microsoft-Dokumentation.

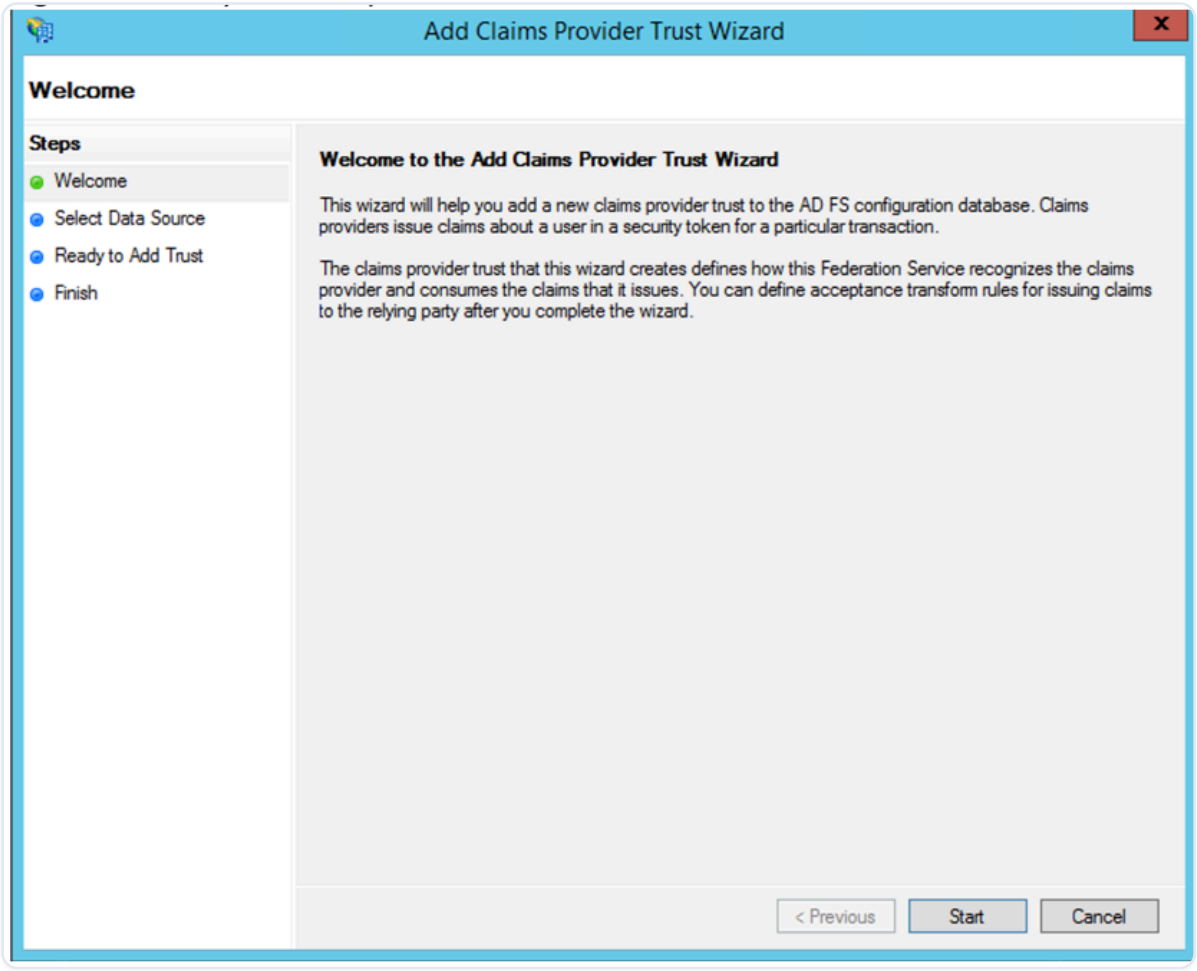
Um ADFS so einzurichten, dass es Ansprüche von Citrix Secure Private Access™ akzeptiert, müssen Sie die folgenden Schritte ausführen:

1. Anspruchsanbieter-Vertrauen in ADFS hinzufügen.
2. Schließen Sie die App-Konfiguration in Citrix Secure Private Access ab.

Anspruchsanbieter-Vertrauen in ADFS hinzufügen

1. Öffnen Sie die ADFS-Verwaltungskonsole. Gehen Sie zu **ADFS > Vertrauensstellung > Anspruchsanbieter-Vertrauen**.

   a. Klicken Sie mit der rechten Maustaste und wählen Sie **Anspruchsanbieter-Vertrauen hinzufügen**.

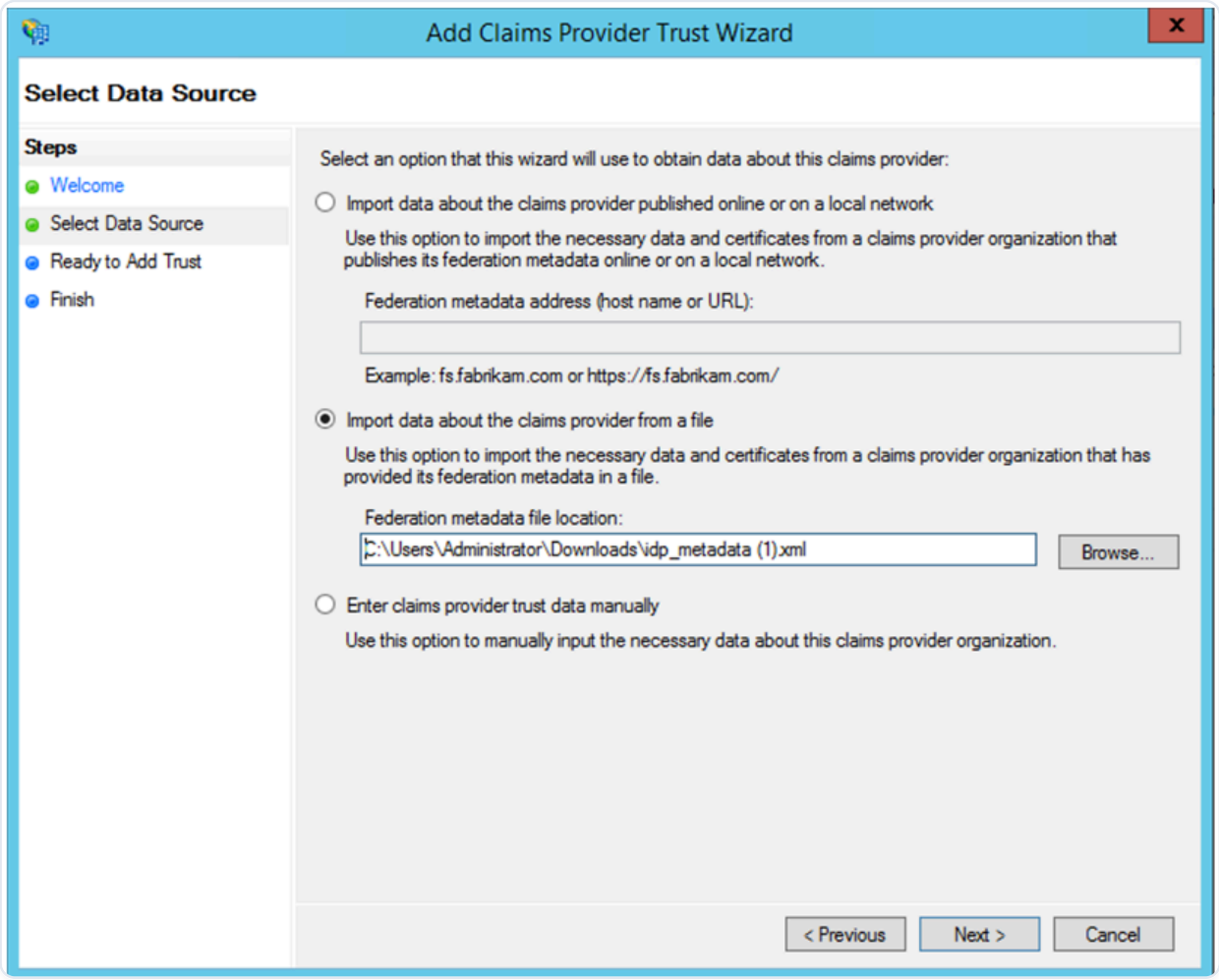


   b. Fügen Sie eine App in Secure Private Access hinzu, die zur Föderation mit ADFS verwendet wird. Details finden Sie unter App-Konfiguration in Citrix Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

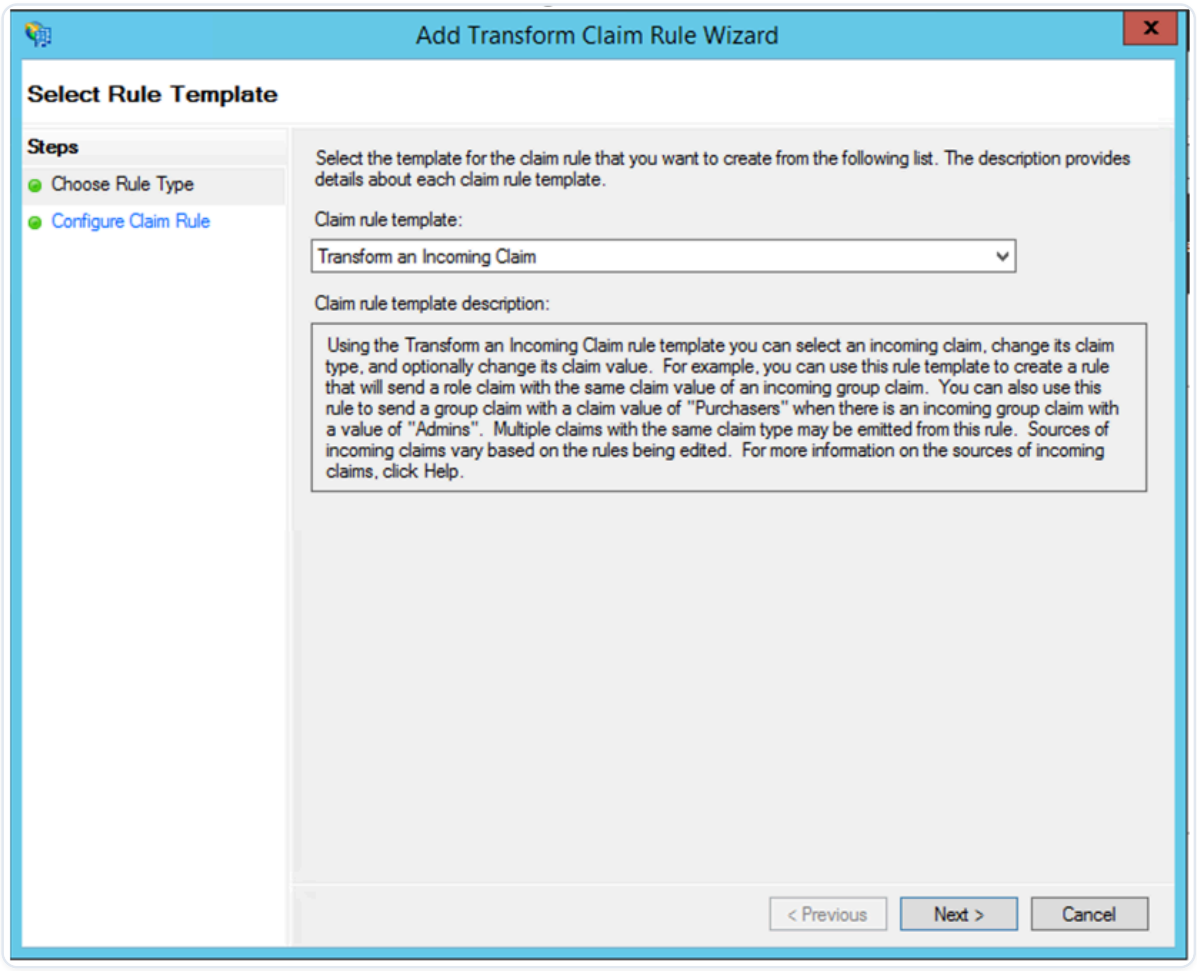
Fügen Sie zuerst die App hinzu, und aus dem SSO-Konfigurationsbereich der App können Sie die SAML-Metadatendatei herunterladen und anschließend die Metadatendatei in ADFS importieren.



a. Schließen Sie die Schritte zum Hinzufügen des Anspruchsanbieter-Vertrauens ab. Nachdem Sie das Anspruchsanbieter-Vertrauen hinzugefügt haben, wird ein Fenster zur Bearbeitung der Anspruchsregel angezeigt.

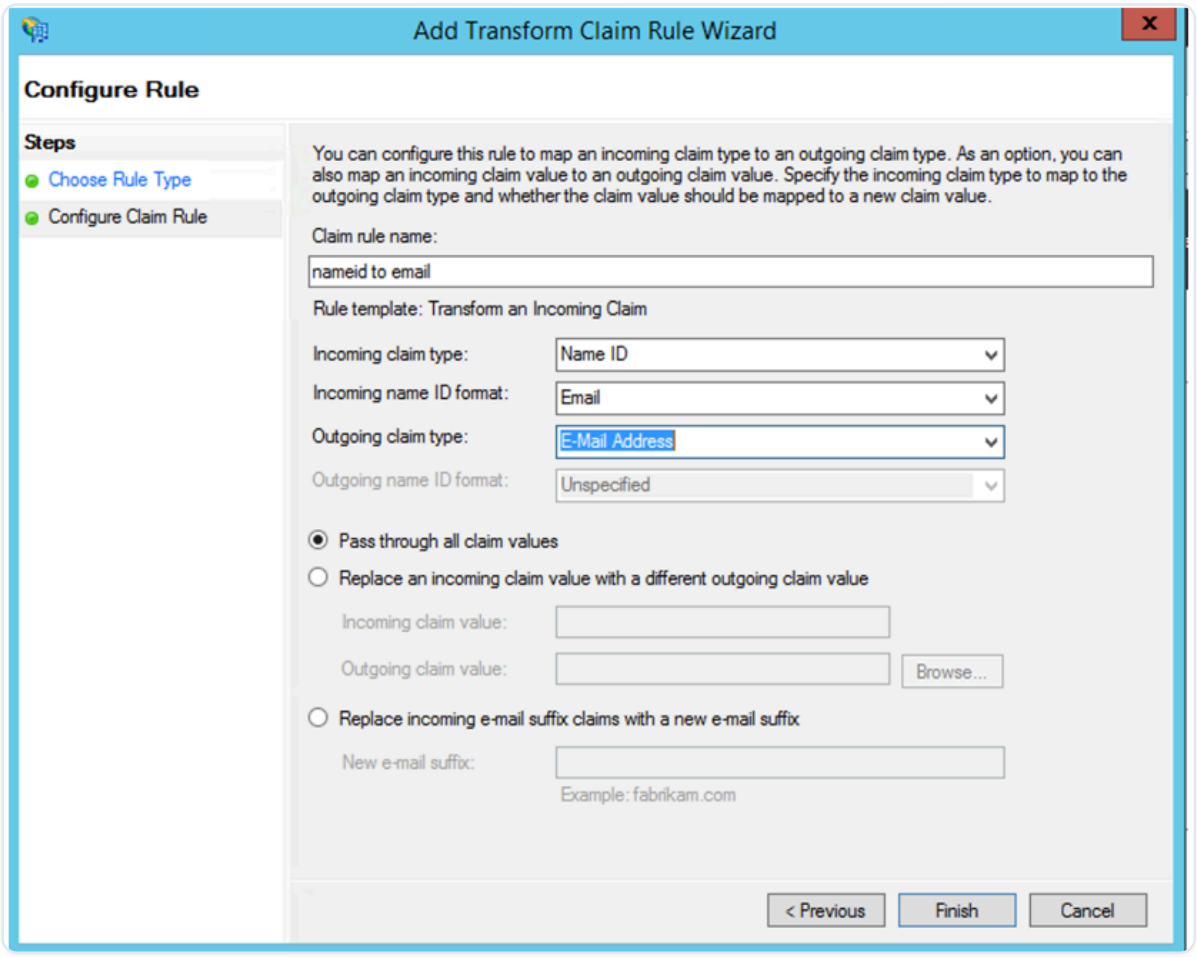
b. Fügen Sie eine Anspruchsregel mit **Eingehenden Anspruch transformieren** hinzu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. Schließen Sie die Einstellungen wie in der folgenden Abbildung gezeigt ab. Wenn Ihr ADFS andere Ansprüche akzeptiert, verwenden Sie diese Ansprüche und konfigurieren Sie SSO in Secure Private Access entsprechend.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

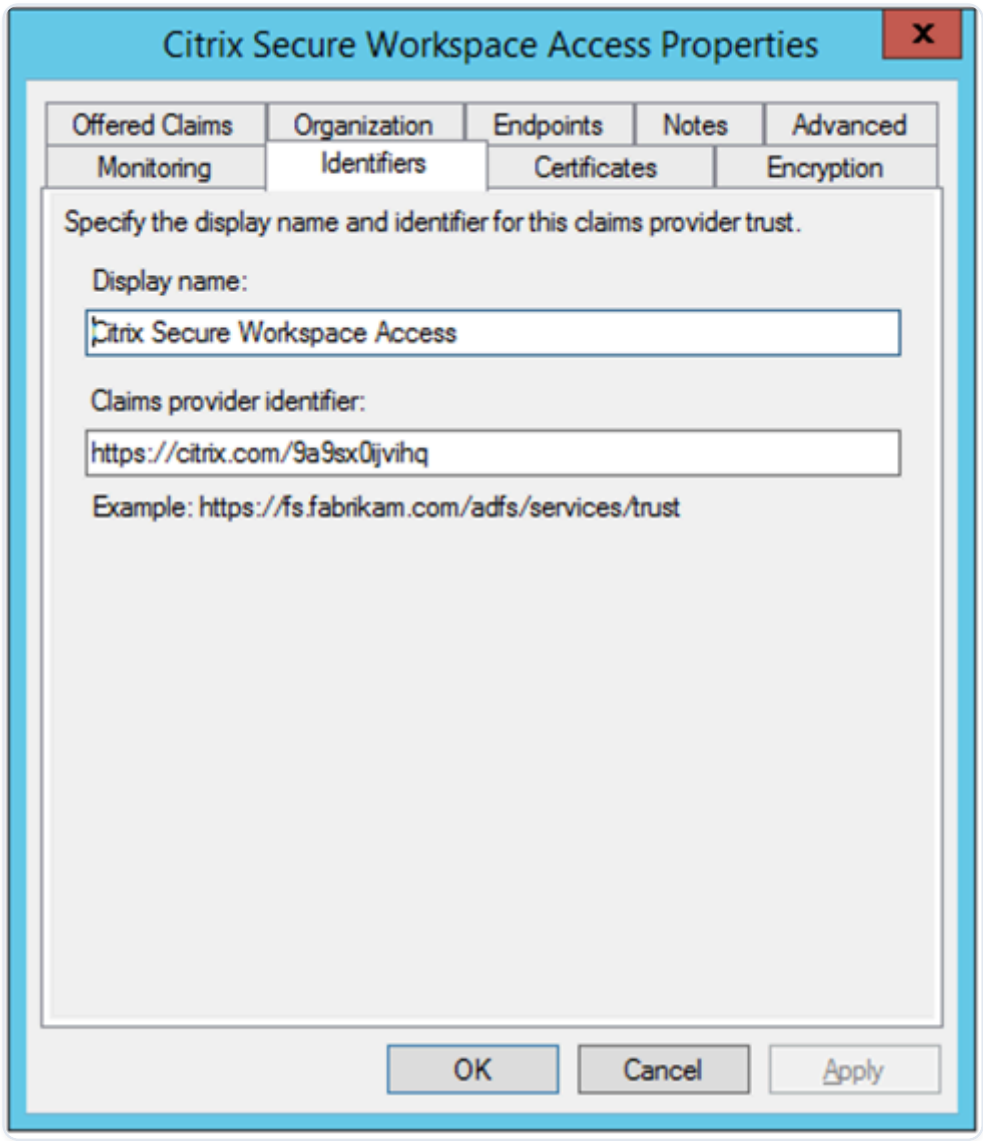


Sie haben nun die Vertrauensstellung des Anspruchsanbieters konfiguriert, die bestätigt, dass ADFS Citrix Secure Private Access für SAML vertraut.

ID der Vertrauensstellung des Anspruchsanbieters

Notieren Sie sich die ID der Vertrauensstellung des Anspruchsanbieters, die Sie hinzugefügt haben. Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.

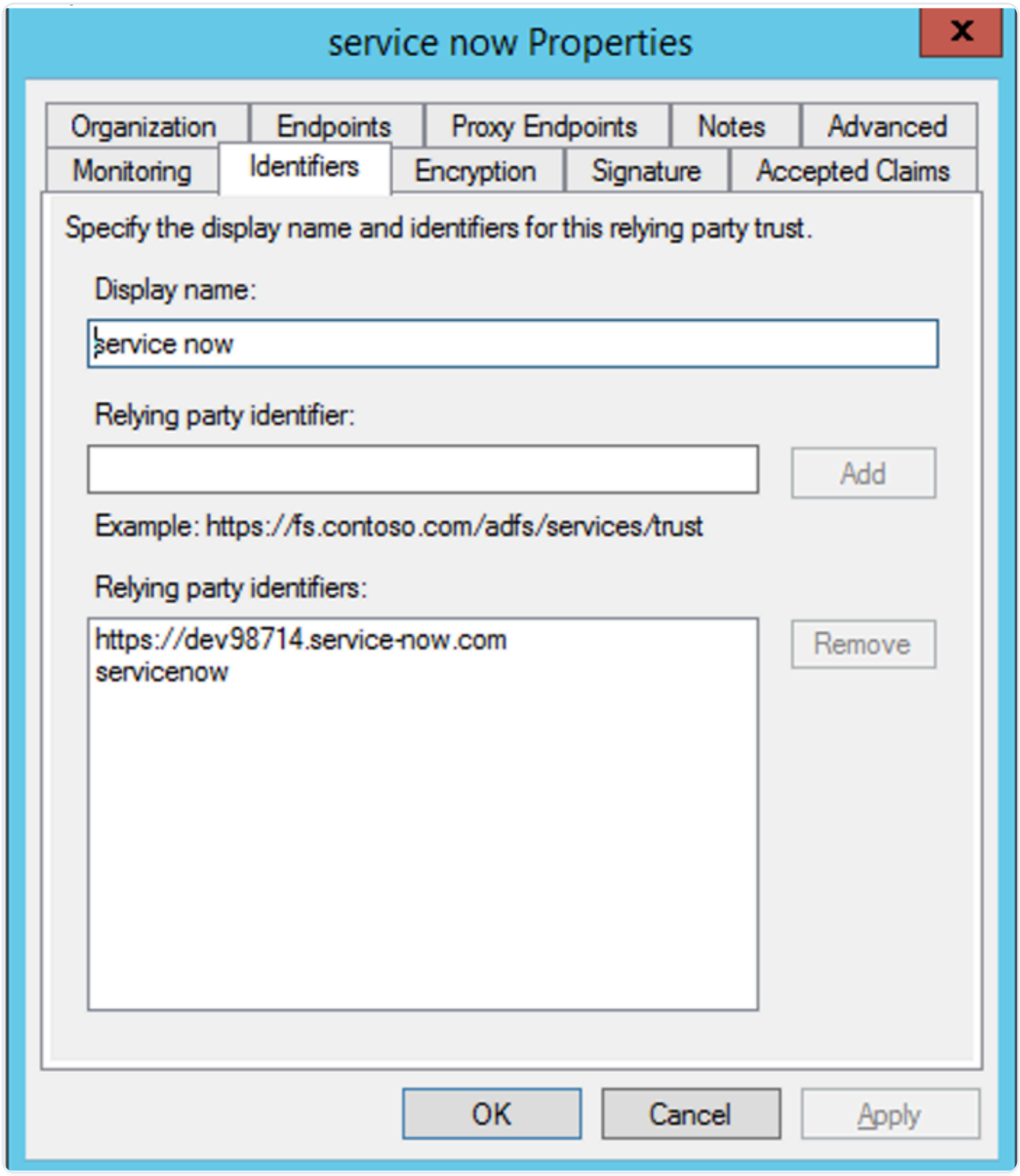
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Bezeichner der vertrauenden Seite

Wenn Ihre SaaS-App bereits mit ADFS authentifiziert ist, dann muss die Vertrauensstellung der vertrauenden Seite für diese App bereits hinzugefügt worden sein. Sie benötigen diese ID bei der Konfiguration der App in Citrix Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Relay-Status im IdP-initiierten Fluss aktivieren

RelayState ist ein Parameter des SAML-Protokolls, der verwendet wird, um die spezifische Ressource zu identifizieren, auf die Benutzer zugreifen, nachdem sie angemeldet und zum Verbundserver der vertrauenden Seite weitergeleitet wurden. Wenn RelayState in ADFS nicht aktiviert ist, sehen Benutzer nach der Authentifizierung bei den Ressourcenanbietern, die dies erfordern, einen Fehler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für ADFS 2.0 müssen Sie das Update KB2681584 (Update Rollup 2) oder KB2790338 (Update Rollup 3) installieren, um RelayState-Unterstützung bereitzustellen. ADFS 3.0 verfügt über integrierte RelayState-Unterstützung. In beiden Fällen muss RelayState noch aktiviert werden.

So aktivieren Sie den RelayState-Parameter auf Ihren ADFS-Servern

1. Öffnen Sie die Datei.
    - Geben Sie für ADFS 2.0 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.IdentityServer.Servicehost.exe.config
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 `IISReset` aus, um IIS neu zu starten.
3. Starten Sie für beide Plattformen die Active Directory-Verbunddienste `(adfssrv) service.` neu. **Hinweis:** Wenn Sie Windows 2016 oder Windows 10 verwenden, nutzen Sie den folgenden PowerShell-Befehl, um dies zu aktivieren. `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

Link zu Befehlen – `<https://docs.microsoft.com/de-de/powershell/module/adfs/set-adfsproperties?view=win10-ps>`

App-Konfiguration in Citrix Secure Private Access

Sie können entweder den IdP-initiierten Flow oder den SP-initiierten Flow konfigurieren. Die Schritte zur Konfiguration des IdP- oder SP-initiierten Flows in Citrix Secure Private Access sind dieselben, außer dass Sie für den SP-initiierten Flow das Kontrollkästchen **App über die angegebene URL starten (SP-initiiert)** in der Benutzeroberfläche auswählen 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>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ADFS FQDN** – FQDN Ihrer ADFS-Einrichtung.
- **RP-ID** – Die RP-ID ist die ID, die Sie von Ihrem vertrauenden Drittanbieter erhalten. Sie ist identisch mit dem Bezeichner des vertrauenden Drittanbieters. Wenn es sich um eine URL handelt, erfolgt eine URL-Kodierung.
- **IDP-ID** – Die IdP-ID ist identisch mit der Anspruchsanbieter-Vertrauens-ID. Wenn es sich um eine URL handelt, erfolgt eine URL-Kodierung.

  Beispiel: `<https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq>`

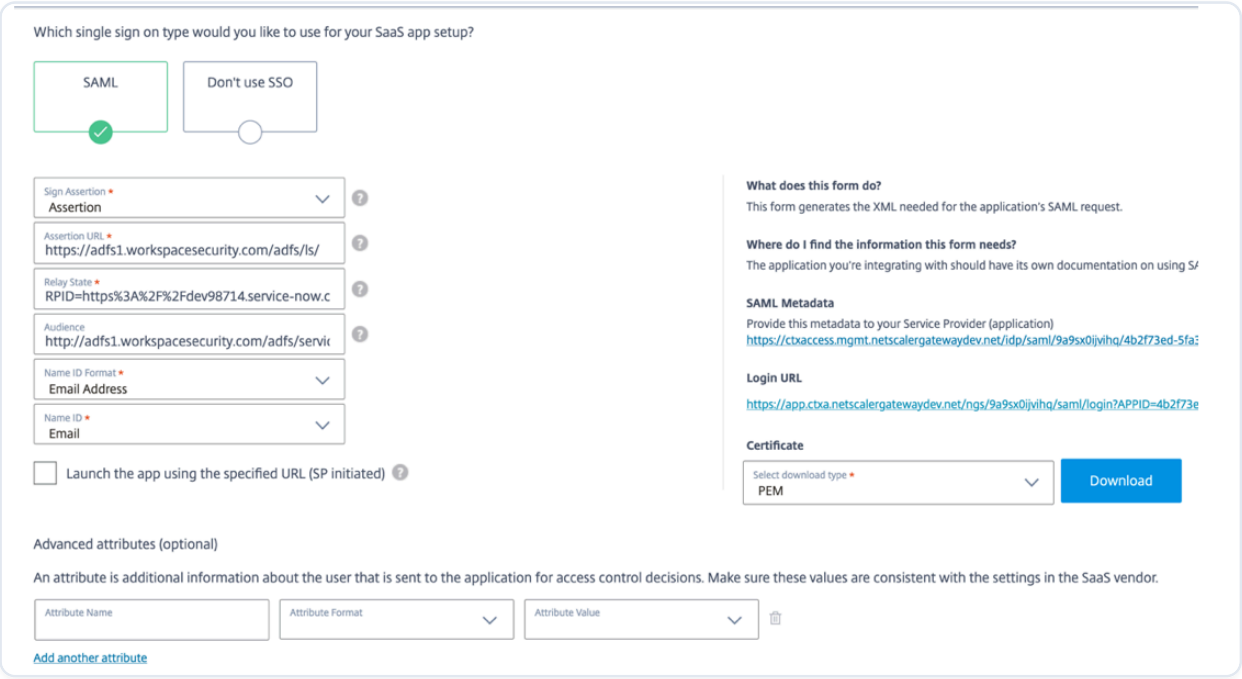
2. SAML-SSO-Konfiguration.

   Die folgenden Werte sind die Standardwerte des ADFS-Servers. Wenn einer der Werte geändert wurde, rufen Sie die korrekten Werte aus den Metadaten des ADFS-Servers ab. Die Verbundmetadaten des ADFS-Servers können von seinem Verbundmetadaten-Endpunkt heruntergeladen werden, dessen Endpunkt unter **ADFS > Dienst > Endpunkte** bekannt ist.

   - **Assertions-URL** – `https://<adfs fqdn>/adfs/ls/`
   - **Relay State** – Der Relay State ist wichtig für den IdP-initiierten Flow. Folgen Sie diesem Link, um ihn korrekt zu konstruieren – `https://docs.microsoft.com/de-de/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%2Fdev98714.service-now.com%2F
   - **Zielgruppe** – `http://<adfsfqdn>/adfs/services/trust`
   - Für die anderen SAML-SSO-Konfigurationseinstellungen siehe die folgende Abbildung. Weitere Informationen finden Sie unter Unterstützung für SaaS-Apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Speichern Sie die App und abonnieren Sie sie für den Benutzer.

SP-initiierter Flow

Konfigurieren Sie für den SP-initiierten Flow die Einstellungen wie im Abschnitt **IDP-initiierter Flow** beschrieben. Aktivieren Sie zusätzlich das Kontrollkästchen **App über die angegebene URL starten (SP-initiiert)**.

Citrix Secure Private Access™

Der Citrix Secure Private Access-Dienst ermöglicht es Administratoren, eine kohärente Erfahrung zu bieten, die Single Sign-On, Fernzugriff und Inhaltsprüfung in einer einzigen Lösung für die End-to-End-Zugriffssteuerung integriert. IT-Administratoren können den Zugriff auf genehmigte SaaS-Apps mit einer vereinfachten Single Sign-On-Erfahrung steuern. Mit dem Citrix Secure Private Access-Dienst können Administratoren auch das Netzwerk der Organisation und die Endbenutzergeräte vor Malware und Datenlecks schützen, indem sie den Zugriff auf bestimmte Websites und Website-Kategorien 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 kritischen Geschäftsanwendungen, unabhängig davon, ob sie sich im Büro, zu Hause oder auf Reisen befinden.

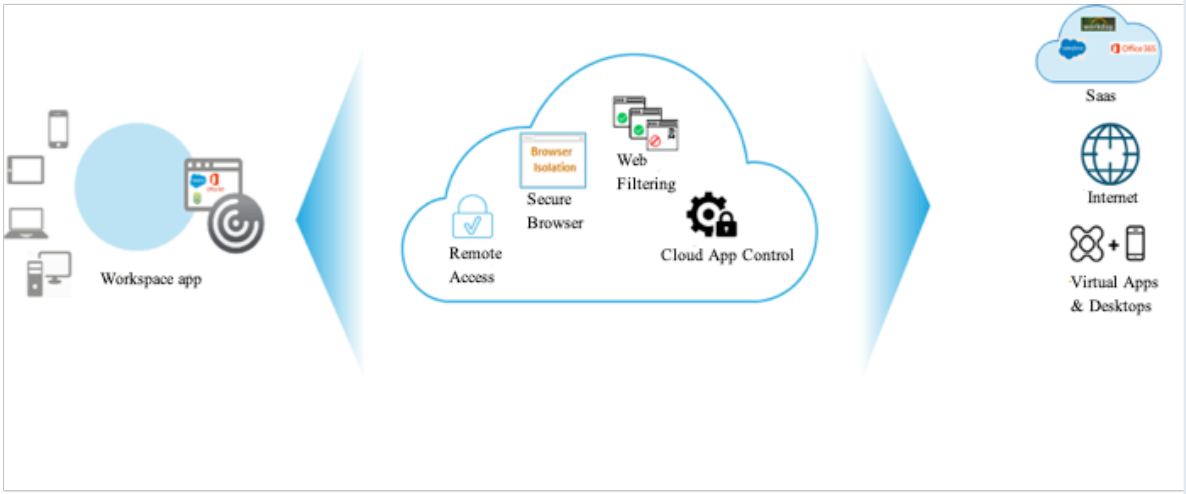
Administratoren können Benutzeraktivitäten überwachen, wie z. B. besuchte bösartige, gefährliche oder unbekannte Websites, den verbrauchten Bandbreitenverbrauch sowie riskantes Download- und Upload-Verhalten. Mithilfe der Analysen zu aufgerufenen Websites und Website-Kategorien können Administratoren Korrekturmaßnahmen ergreifen, um das Unternehmensnetzwerk zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

schützen. Gleichzeitig bietet der Dienst Endbenutzern nahtlosen und sicheren Zugriff auf alle ihre gehosteten Apps.

Administratoren können auch Aktionen einschränken, wie z. B. eingeschränktes Drucken, Downloads und den Zugriff auf die Zwischenablage (Kopieren-Einfügen).

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



Hauptfunktionen von Citrix Secure Private Access

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

- **SaaS-Apps mit Single Sign-On-Zugriff veröffentlichen** – Sobald der Benutzer mit einer primären Identität in seinem Store authentifiziert ist, werden nachfolgende Authentifizierungsanforderungen für SaaS- und Web-Apps automatisch durch die Single Sign-On-Funktion in der Citrix Cloud™ mithilfe von SAML-Assertions erfüllt.

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

- **Erweiterte Sicherheitsrichtlinien für SaaS-Apps festlegen. (Zum Beispiel Wasserzeichen, Kopier-/Einfüge-Beschränkung und Downloads verhindern.)** – Zum Schutz von Inhalten integrieren Organisationen erweiterte Sicherheitsrichtlinien in die SaaS-Anwendungen. Jede

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Richtlinie erzwingt eine Einschränkung für den Citrix Enterprise Browser™ bei Verwendung der Workspace-App für Desktops oder für den Secure Browser bei Verwendung der Workspace-App für Web oder Mobilgeräte.

  - Bevorzugter Browser: Deaktiviert die Verwendung lokaler Browser und greift auf die Citrix Enterprise Browser-Engine (Workspace-App – Desktop) oder den Secure Browser (Workspace-App – Mobil und Web) zurück.
  - Zugriff auf die Zwischenablage einschränken: Deaktiviert Ausschneide-/Kopier-/Einfüge-Vorgänge zwischen der App und der Zwischenablage des Endpunkts.
  - Drucken einschränken: Deaktiviert die Möglichkeit, aus dem App-Browser heraus zu drucken.
  - Downloads einschränken: Deaktiviert die Möglichkeit des Benutzers, aus der SaaS-App herunterzuladen.
  - Wasserzeichen anzeigen: Überlagert ein bildschirmbasiertes Wasserzeichen, das den Benutzernamen und die IP-Adresse des Endpunkts anzeigt. 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, können Inhalte in der SaaS-App tatsächlich gefährlich sein und ein Sicherheitsrisiko darstellen. Wenn ein Benutzer auf einen Hyperlink innerhalb einer SaaS-App klickt, wird der Datenverkehr über die Webfilterfunktion geleitet, die eine Risikobewertung für den Hyperlink bereitstellt. Basierend auf der Risikobewertung des Hyperlinks und der angepassten Liste der URL-Kategorien erlaubt, verweigert oder leitet die Webfilterfunktion die Hyperlink-Anfrage des Benutzers wie folgt um:
  - Genehmigt: Der Hyperlink wird als sicher eingestuft, und der Citrix Enterprise Browser greift innerhalb der Workspace-App auf den Hyperlink zu.
  - Verweigert: Der Hyperlink wird als gefährlich eingestuft und der Zugriff wird verweigert.
  - Umgeleitet: Die Hyperlink-Anfrage wird an den Remote Browser Isolation-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 eine verbesserte Sicherheit in sich tragen. Die Citrix Workspace-App, der Secure Private Access-Dienst und der Remote Browser Isolation-Dienst stellen dem Sicherheitsanalysedienst

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen über die folgenden Benutzer- und Anwendungsverhalten bereit. Diese Analysen beeinflussen den gesamten Risikowert des Benutzers:

- Startzeit der App
- Endzeit der App
- Druckaktion
- Zwischenablagezugriff
- URL-Zugriff
- Daten-Upload
- Daten-Download

Die Webfilterfunktion bewertet das Risiko jedes innerhalb der SaaS-Anwendung ausgewählten Hyperlinks. Der Zugriff auf diese Websites und die Überwachung von Änderungen im Benutzerverhalten erhöhen den gesamten Risikowert des Benutzers, da dies signalisiert, dass das Endpunktgerät kompromittiert ist und begonnen hat, Daten zu infizieren oder zu verschlüss, oder dass der Benutzer und das Gerät geistiges Eigentum stehlen.

Secure Private Access REST-APIs

Sie können die Secure Private Access REST-APIs verwenden, um mehrere Anwendungen und Richtlinien direkt zu konfigurieren. Weitere Informationen finden Sie unter Citrix Secure Private Access.

DNS-Abfragen an anwendungsspezifische Ressourcenstandorte weiterleiten

Administratoren können DNS-Abfragen für bestimmte Anwendungen direkt an deren dedizierte Ressourcenstandorte weiterleiten. Dies ermöglicht eine genauere DNS-Auflösung, intelligentes Traffic-Management und eine bessere Benutzererfahrung. Zuvor wurden alle DNS-Abfragen standardmäßig an den geografisch nächstgelegenen verfügbaren DNS-Server weitergeleitet, unabhängig davon, wo die Anwendung gehostet wird. Dies erforderte, dass DNS-Server an allen Ressourcenstandorten synchronisiert wurden, was nicht immer erreichbar ist.

Systemanforderungen

Citrix Secure Access Client:

- macOS – V25.08.1.1 und höher (Citrix Downloads), V25.08.1 und höher (App Store).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows – 25.7.1.11 oder höher.

Funktionsaktivierung

Die anwendungsspezifische DNS-Routing-Funktion ist standardmäßig deaktiviert. Um die Funktion für Ihr Unternehmen zu aktivieren, wenden Sie sich an den Citrix Support.

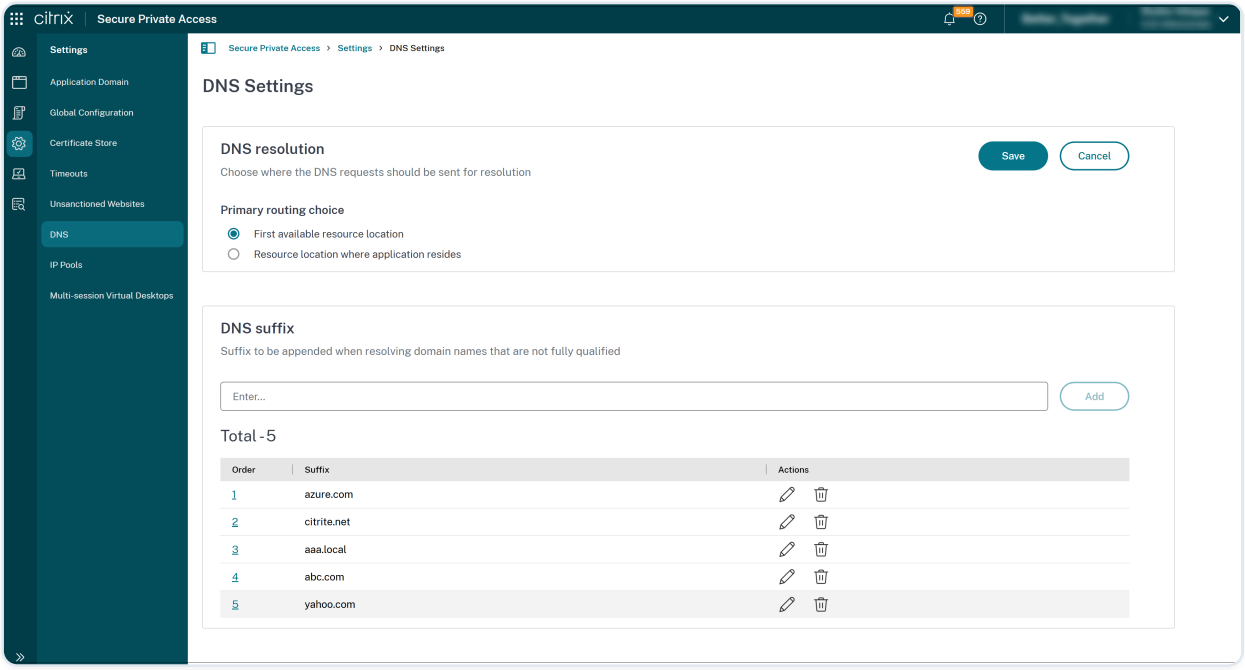
Routing für DNS-Abfragen konfigurieren

Nachdem die Funktion aktiviert wurde, können Sie DNS-Abfragen mit einer der folgenden zwei Optionen weiterleiten:

- **Erster verfügbarer Ressourcenstandort:** Behalten Sie das alte Verhalten bei, bei dem alle Abfragen an den geografisch nächstgelegenen Ressourcenstandort weitergeleitet werden. Stellen Sie sicher, dass alle DNS-Server an allen Ressourcenstandorten synchronisiert sind, wenn Sie diese Option wählen.
- **Ressourcenstandort, an dem sich die Anwendung befindet:** Leiten Sie zum anwendungsspezifischen Ressourcenstandort weiter: Sie können DNS-Abfragen basierend auf dem Hostnamen der Anwendung an den dedizierten Ressourcenstandort der Anwendung leiten.

Führen Sie die folgenden Schritte aus, um das DNS-Routing zu konfigurieren:

1. Navigieren Sie zu **Einstellungen > DNS > DNS-Auflösung**.
2. Klicken Sie auf **Hinzufügen**.



3. Wählen Sie eine der folgenden Optionen aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Erster verfügbarer Ressourcenstandort**
- **Ressourcenstandort, an dem sich die Anwendung befindet**

4. Klicken Sie auf **Speichern**.

Secure Private Access unterstützt einen robusten DNS-Routing-Fallback-Mechanismus, um die Servicekontinuität zu gewährleisten. Wenn für eine bestimmte DNS-Abfrage kein anwendungsspezifischer Ressourcenstandort identifiziert werden kann, fällt die Anforderung automatisch auf eine festgelegte Fallback-Route zurück.

HINWEIS:

Das Routing für nicht zugeordnete oder nicht veröffentlichte Domänen kann nur konfiguriert werden, wenn Sie die primäre Routing-Option als **Ressourcenstandort, an dem sich die Anwendung befindet** festgelegt haben.

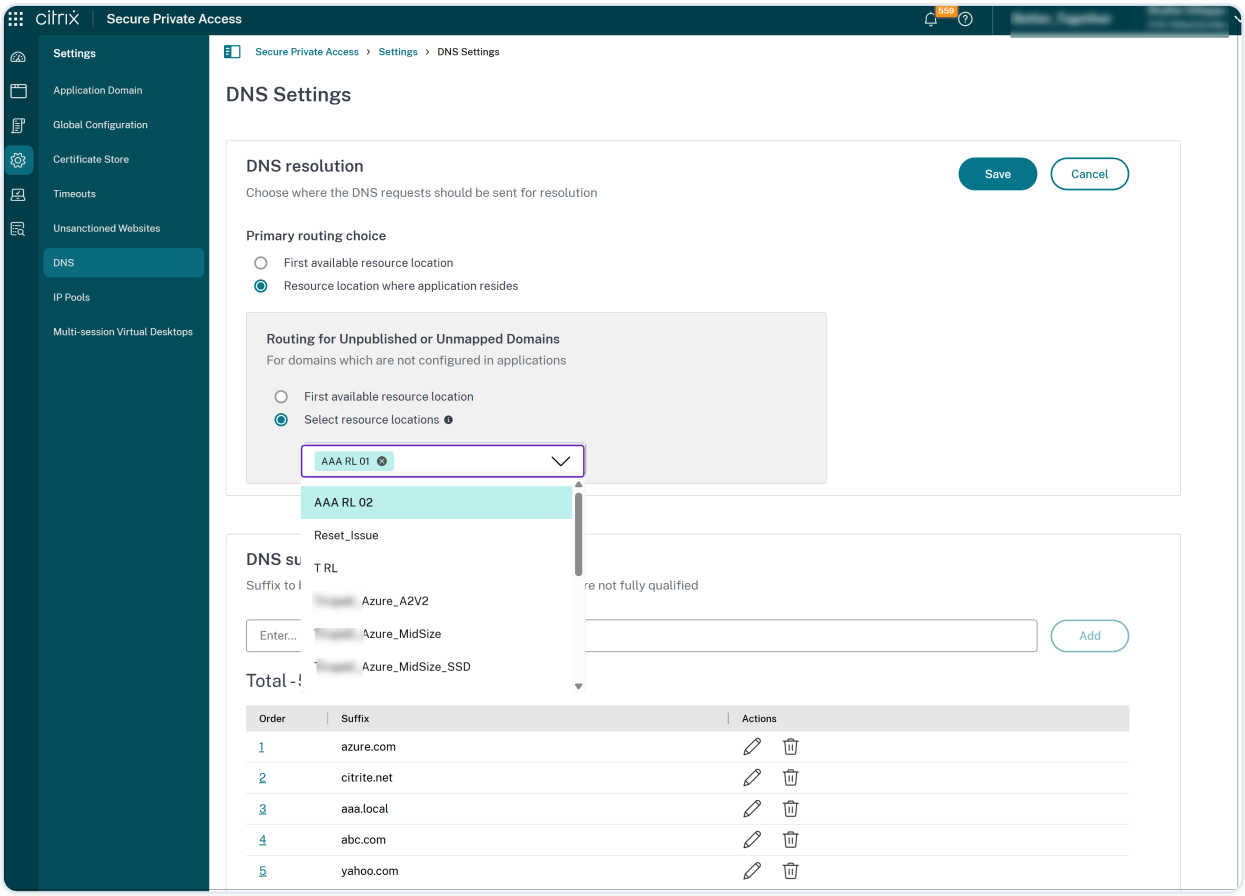
Sie können den Fallback-Mechanismus auf eine der folgenden Optionen konfigurieren:

- **Erster verfügbarer Ressourcenstandort:** Der nächstgelegene geografische Ressourcenstandort.
- **Ressourcenstandorte auswählen:** Einer der Standorte aus einer Liste konfigurierter Ressourcenstandorte, die vom Administrator definiert wurden.

Fallback-Routing für DNS-Abfragen konfigurieren:

1. Navigieren Sie zu **Einstellungen > DNS > DNS-Auflösung**.
2. Klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Wählen Sie unter **Primäre Routing-Option** die Option **Ressourcenstandort, an dem sich die Anwendung befindet**.
4. Wählen Sie unter **Routing für unveröffentlichte oder nicht zugeordnete Domänen** eine der folgenden Optionen aus:

   - **Erster verfügbarer Ressourcenstandort**
   - **Ressourcenstandorte auswählen**

   Wenn Sie die Option **Ressourcenstandorte auswählen** auswählen, wählen Sie die gewünschten Ressourcenstandorte aus der Liste aus. Sie können mehr als einen Ressourcenstandort auswählen.
5. Klicken Sie auf **Speichern**.

G Suite konfigurieren

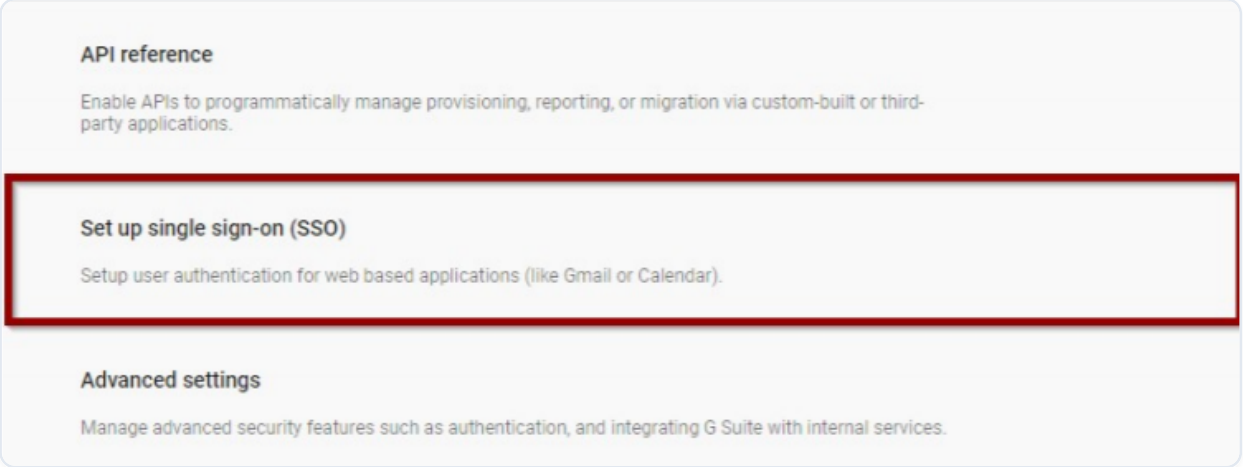
Um G Suite für das Single Sign-On über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als Administrator bei G Suite an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

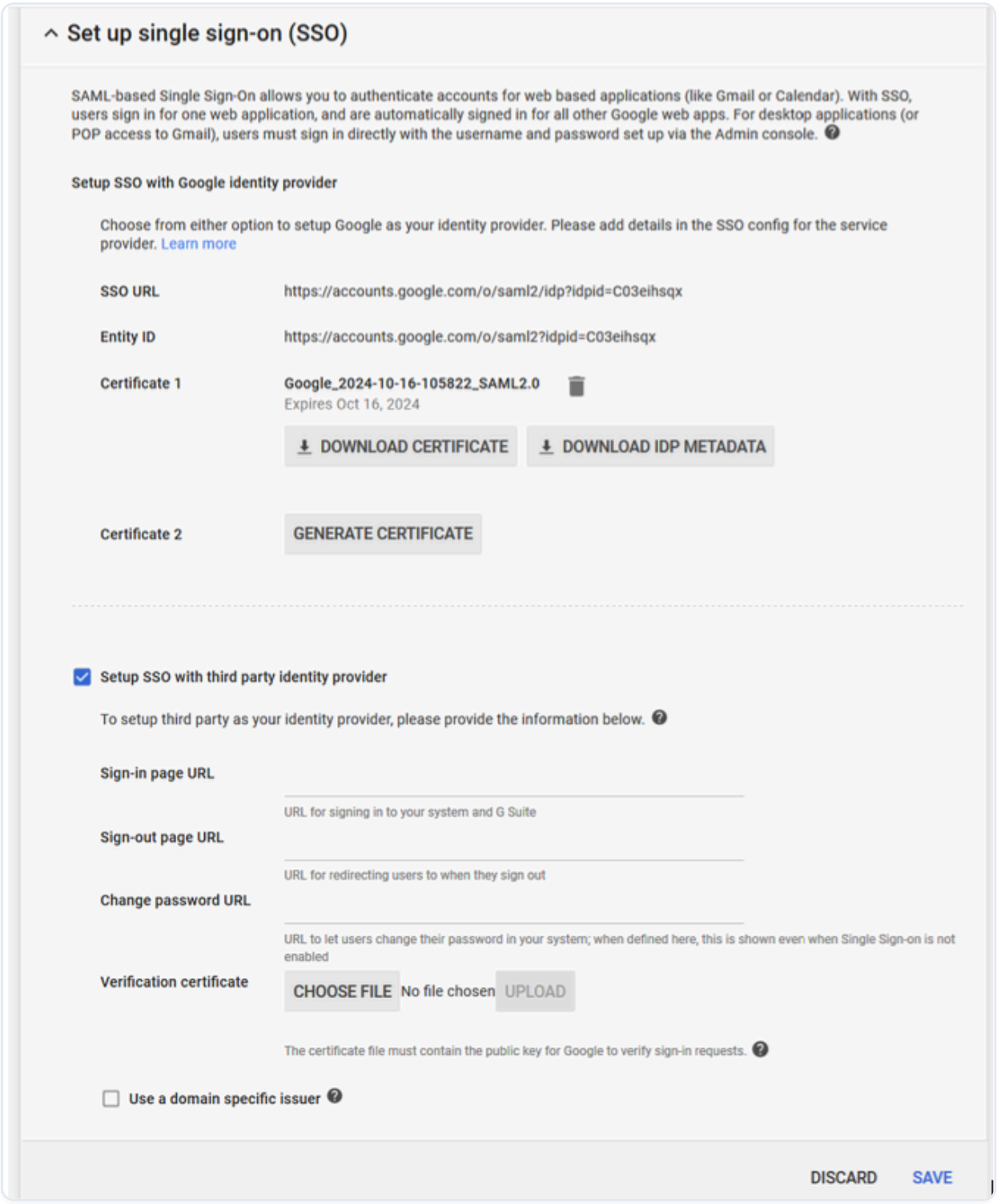


2. Klicken Sie auf **Sicherheit**.



3. Klicken Sie auf der Seite **Sicherheit** auf **Single Sign-On (SSO) einrichten**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Wählen Sie auf der Seite **Single Sign-On (SSO) einrichten** die Option **SSO mit Identitätsanbieter eines Drittanbieters einrichten** aus und geben Sie die Details ein.

   - **Anmeldeseiten-URL** – Sie können die SAML-SSO-Anmelde-URL aus dem Citrix Cloud-Assistenten kopieren (**Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > Anmelde-URL**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Überprüfungszertifikat** – Sie können das Zertifikat aus dem Citrix Cloud-Assistenten herunterladen (**Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > Zertifikat**).
- **Einen domänenspezifischen Aussteller verwenden** – Aktivieren Sie das Kontrollkästchen.

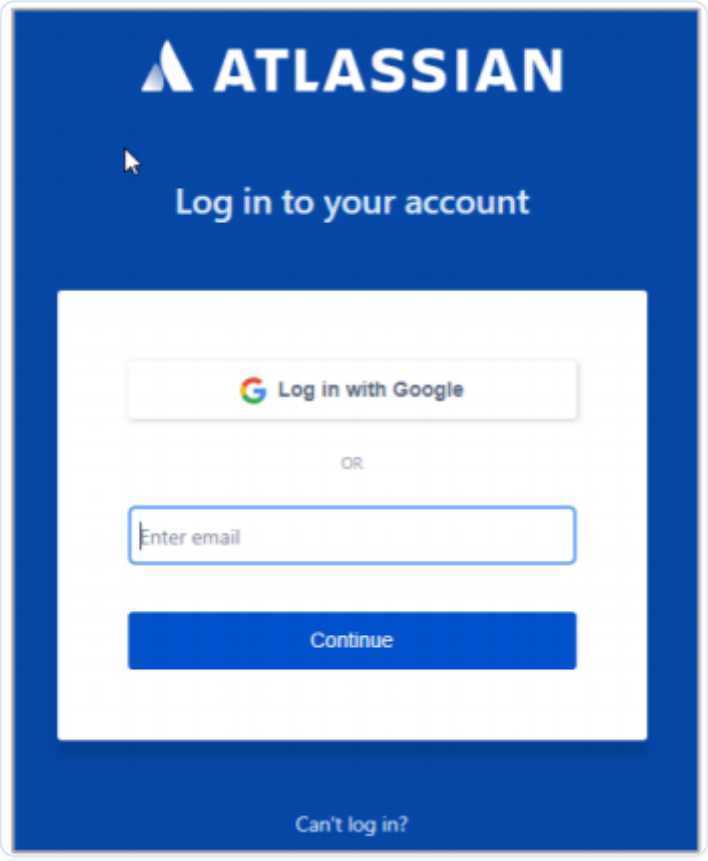
Jira konfigurieren

Die folgenden Abschnitte enthalten weitere Informationen zur Konfiguration von Jira.

Citrix Gateway SaaS-Anwendung

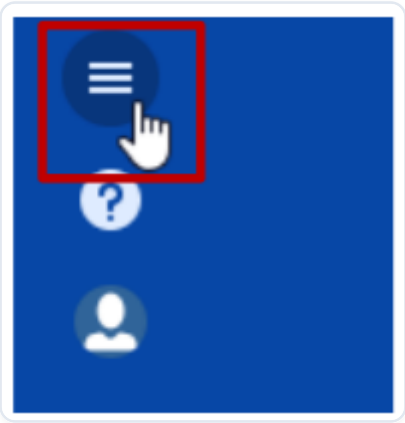
Durch die Konfiguration von Jira für SSO können Administratoren ihre Benutzer mit NetScaler verwalten. Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei Jira anmelden. Um Jira für SSO über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Geben Sie in einem Browser die Atlassian Cloud-URL Ihrer Organisation ein und drücken Sie die EINGABETASTE.
2. Melden Sie sich bei Ihrem Atlassian-Konto an.

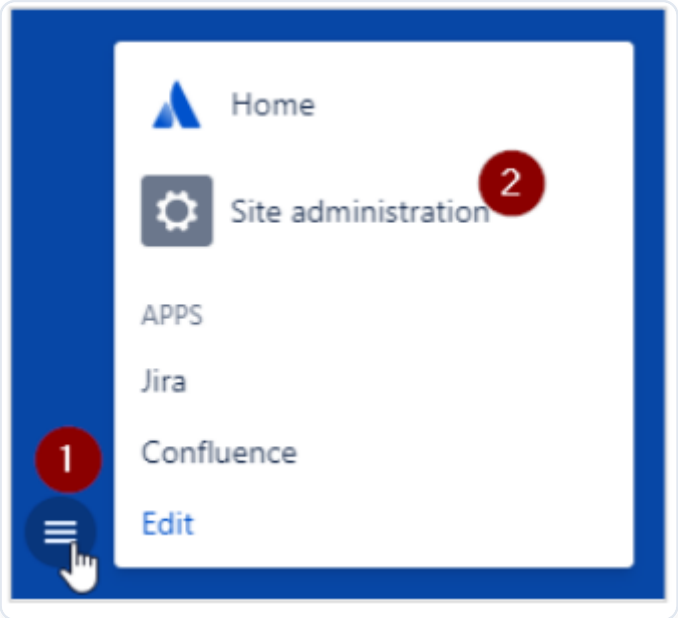


3. Klicken Sie auf der Startseite unten links auf das Ellipsensymbol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

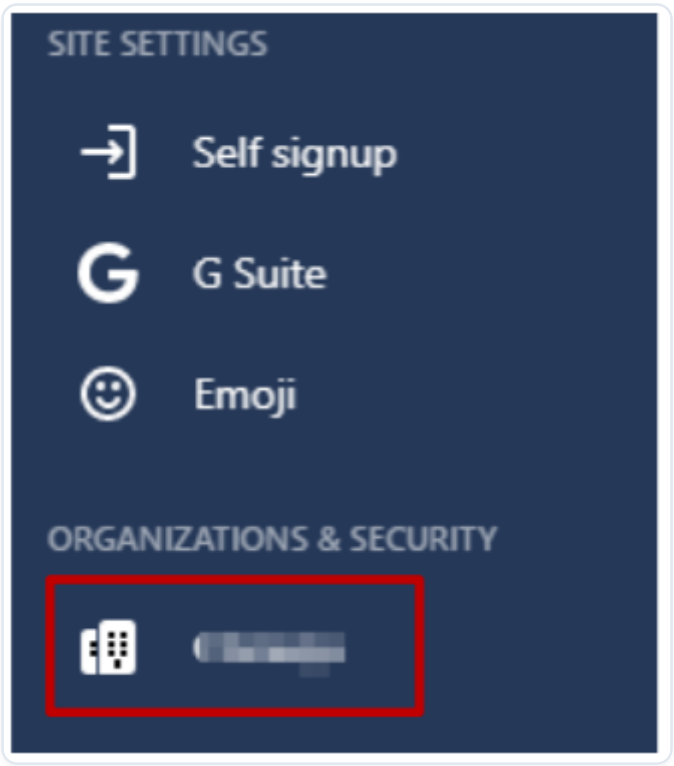


4. Klicken Sie auf **Site-Administration**.



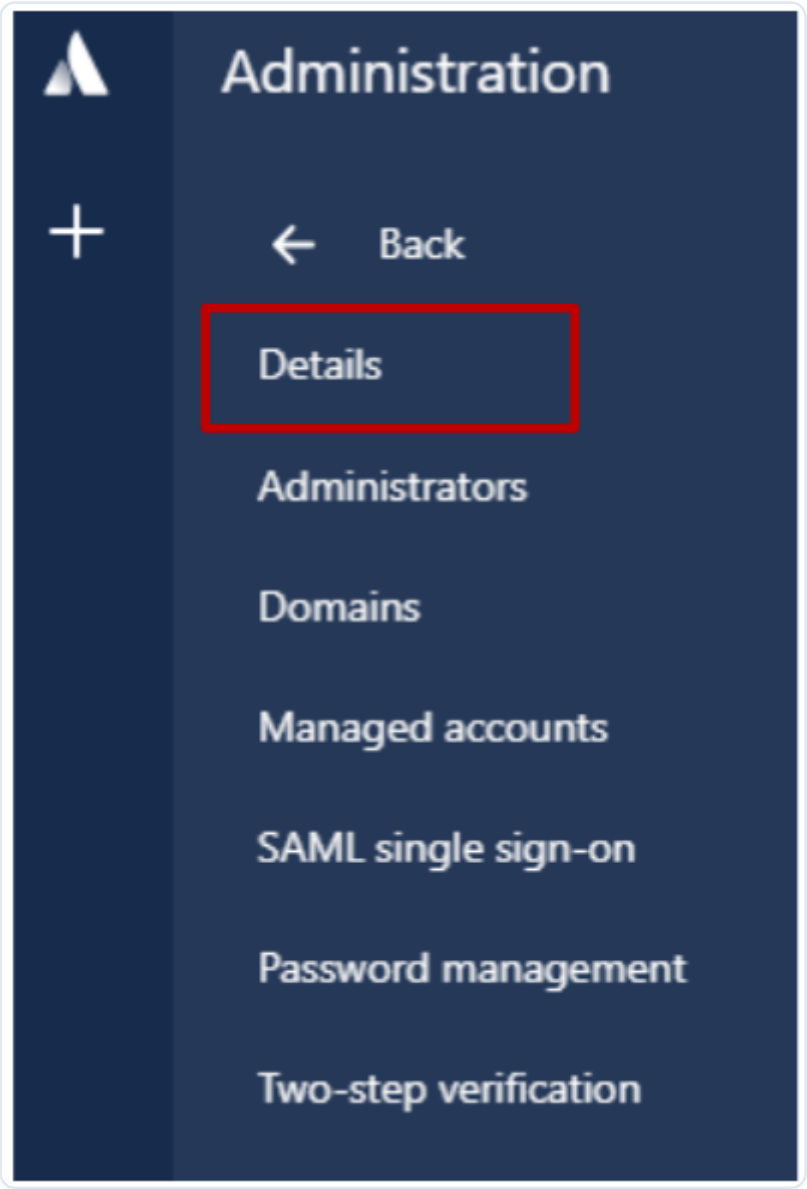
5. Klicken Sie auf der Administrationsseite im Abschnitt ORGANISATION & SICHERHEIT auf den Namen der Organisation, für die Sie die SAML-Authentifizierung konfigurieren möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



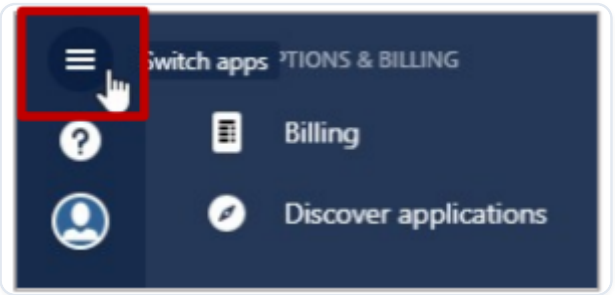
6. Klicken Sie auf **Details** und überprüfen Sie die Domäne.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



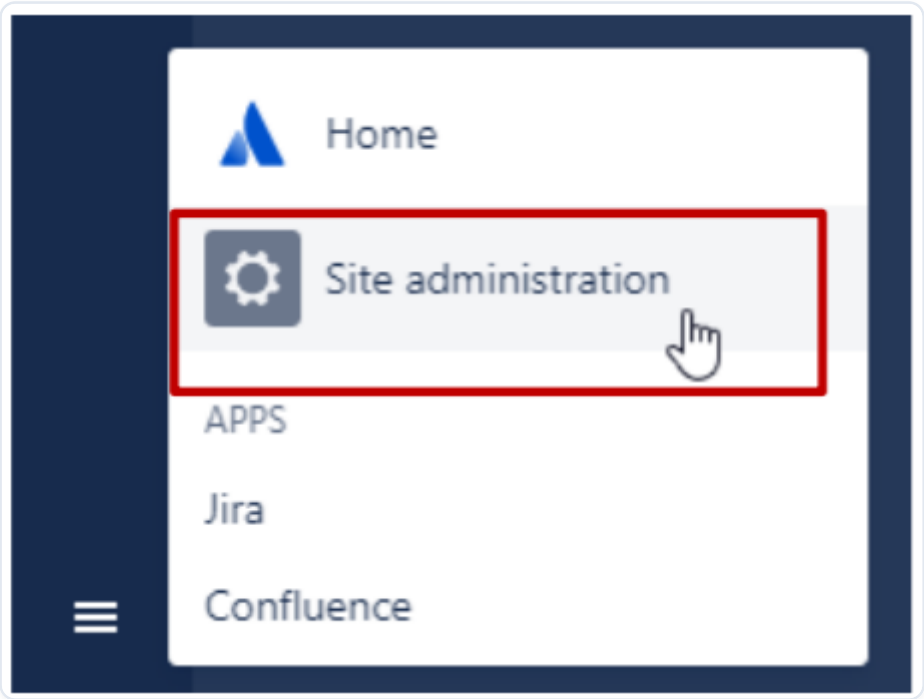
Gehen Sie wie folgt vor, um die Domäne zu überprüfen:

a. Klicken Sie auf das Symbol **Apps wechseln** in der unteren linken Ecke.



a. Klicken Sie auf **Site-Administration**.

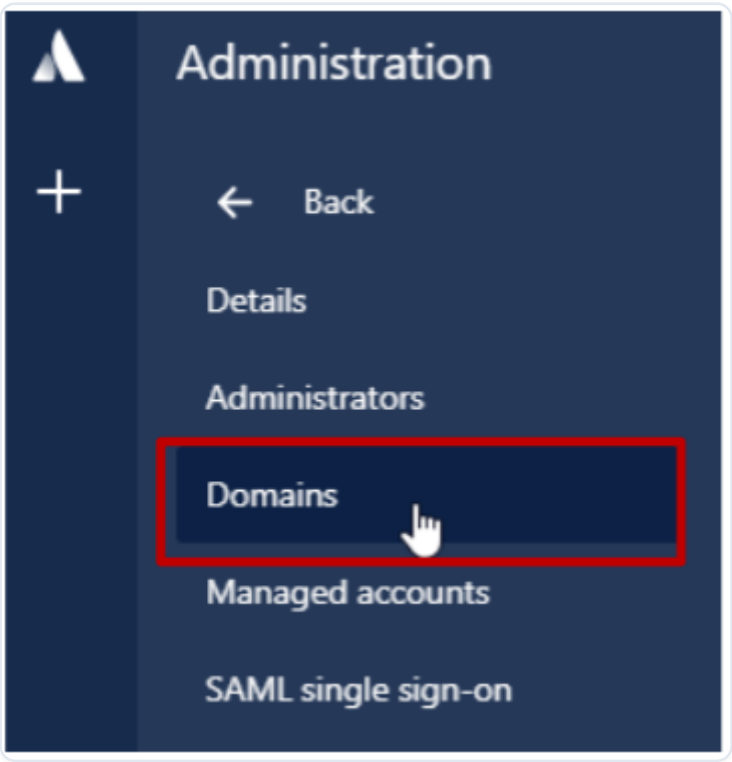
© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Klicken Sie auf den Organisationsnamen.

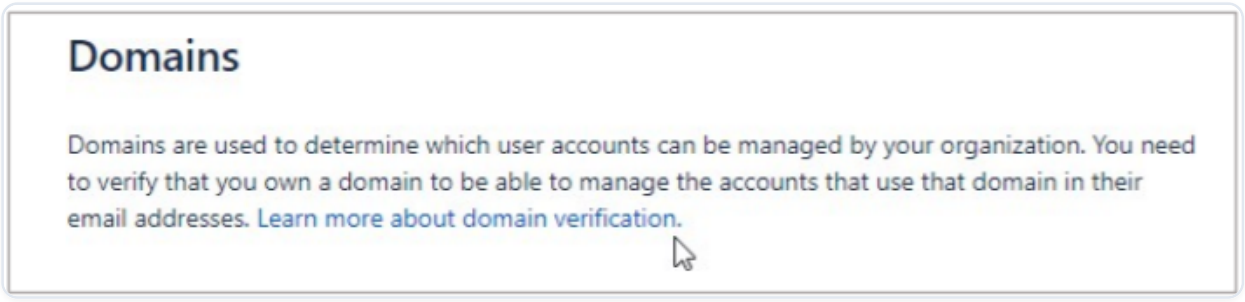


a. Klicken Sie auf **Domänen**.

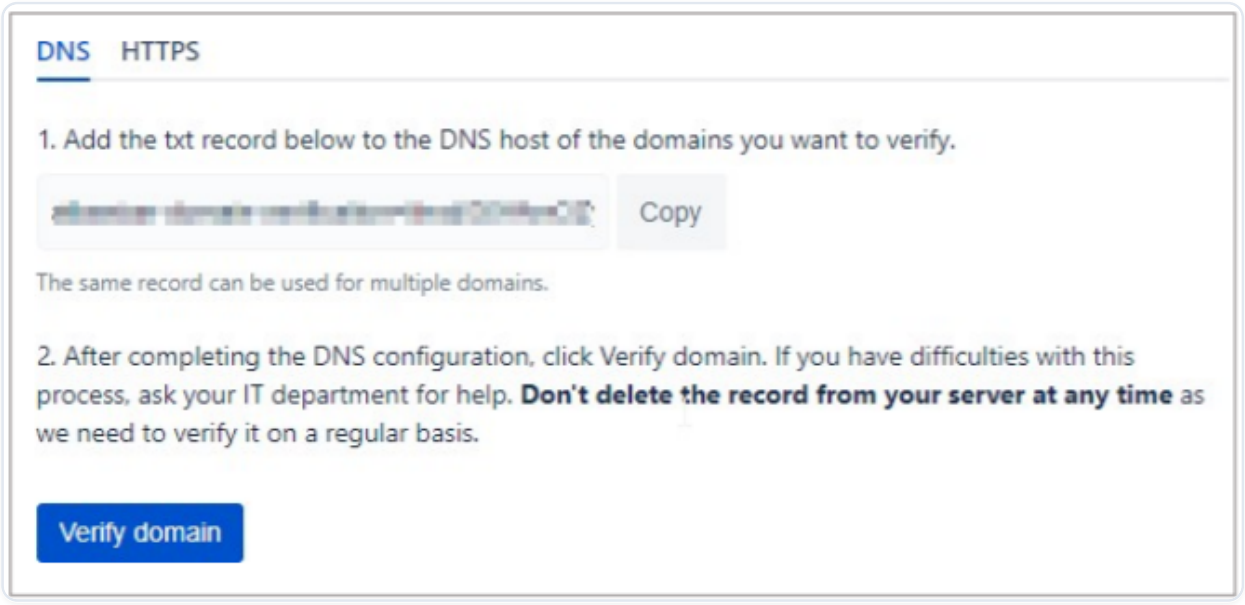


© 1997–2026 Citrix Systems, Inc. All rights reserved.

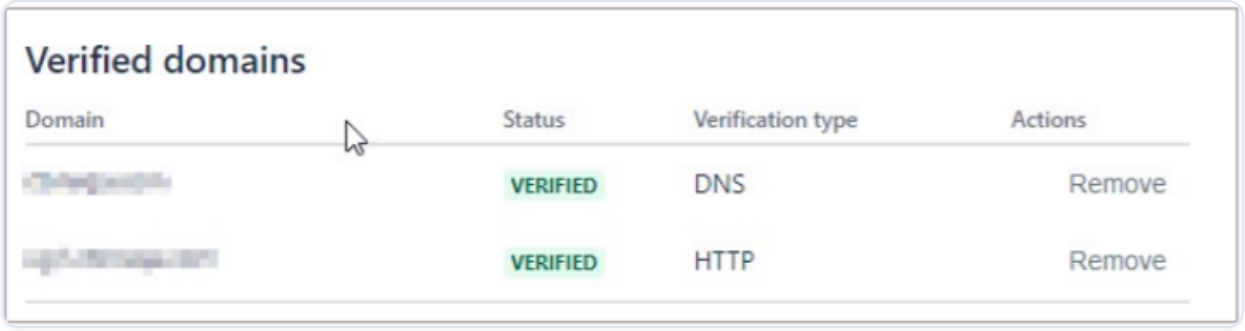
a. Sie können eine Domäne mithilfe von DNS oder HTTPS überprüfen. Weitere Informationen zu den Schritten zur Überprüfung einer Domäne finden Sie im rechten Bereich unter dem Abschnitt „Domänen“. Klicken Sie dort auf den Link „Weitere Informationen zur Domänenüberprüfung“.



a. Nachdem Sie die Schritte abgeschlossen haben, klicken Sie auf **Domäne überprüfen**.

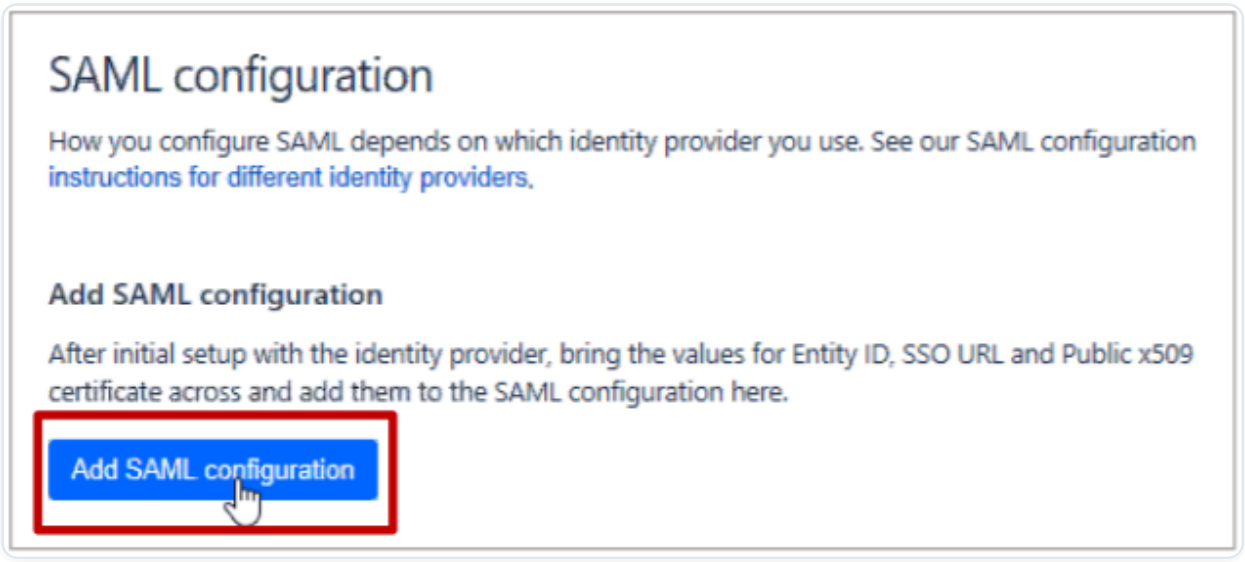


a. Die Spalte „Status“ im Abschnitt „Verifizierte Domänen“ zeigt **VERIFIZIERT** an.



7. Klicken Sie auf **SAML-Single Sign-On**.
8. Klicken Sie im rechten Bereich unter SAML-Konfiguration auf **SAML-Konfiguration hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

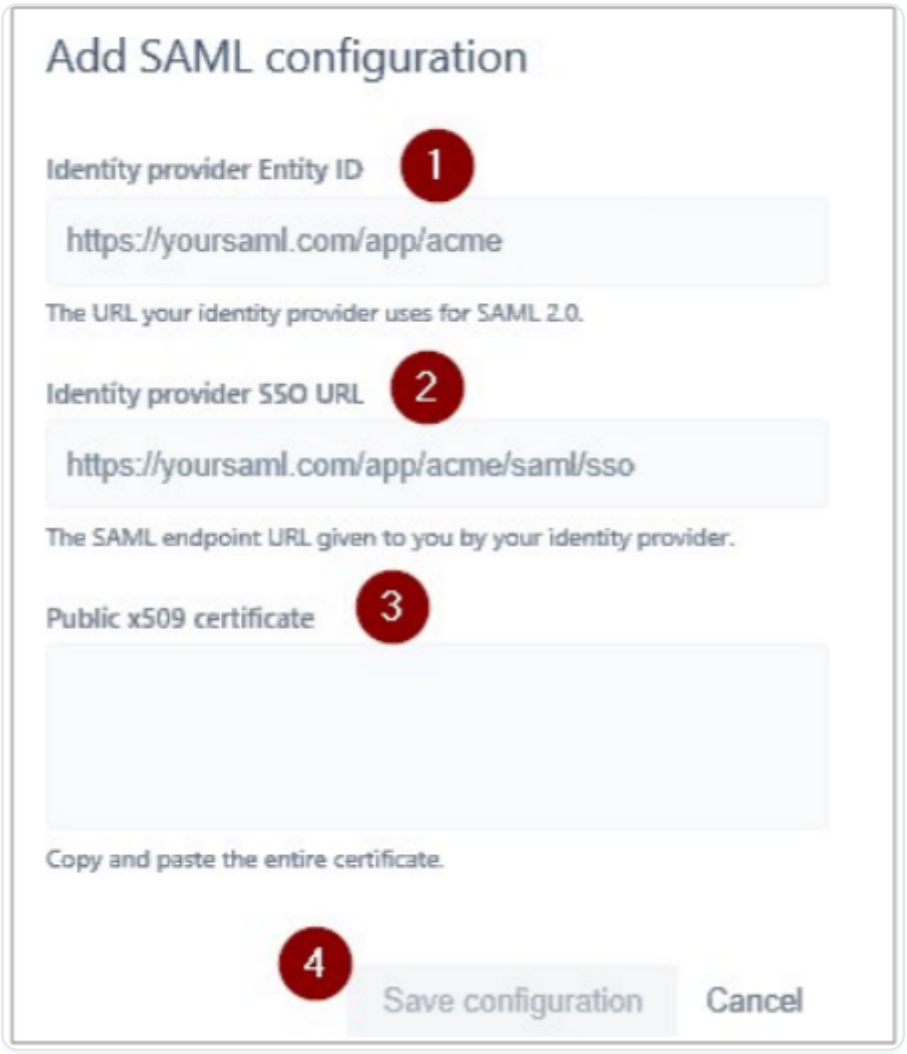


9. Geben Sie im Bereich **SAML-Konfiguration hinzufügen** die folgenden Informationen an:

   - Identitätsanbieter-Entitäts-ID – Geben Sie eine eindeutige Aussteller-ID ein. Zum Beispiel: `yourcompany_NS_Jira`
   - Identitätsanbieter-SSO-URL – Geben Sie die IdP-URL ein.

     Hinweis: Sie können die URL aus dem Citrix Cloud-Assistenten kopieren (**Citrix Gateway Service > Eine Web-/SaaS-App hinzufügen > Single Sign-On > Anmelde-URL**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Öffentliches x509-Zertifikat – Kopieren Sie das SAML-IdP-Signaturzertifikat und fügen Sie es ein.

  a. Laden Sie das Zertifikat aus dem Citrix Cloud-Assistenten herunter (**Citrix Gateway Service > Eine Web-/SaaS-App hinzufügen > Single Sign-On > Zertifikat**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

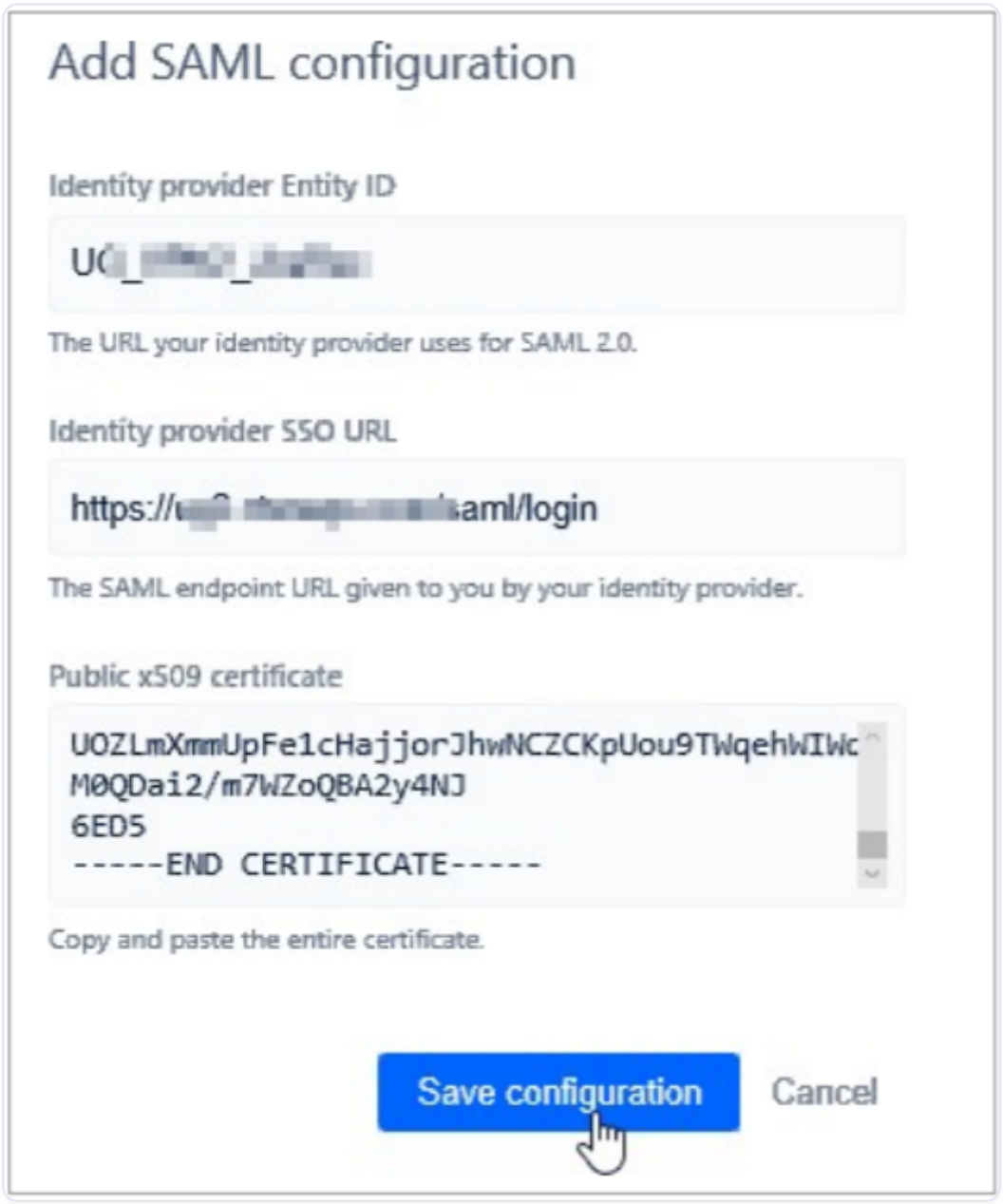


b. Kopieren Sie den Text zwischen -----BEGIN CERTIFICATE----- und -----END CERTIFICATE-----

c. Fügen Sie den Text in einen Texteditor ein und speichern Sie die Datei in einem geeigneten Format, z. B. `your company name`.pem.

10. Klicken Sie auf **Konfiguration speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



O365 konfigurieren

Die folgenden Abschnitte enthalten weitere Informationen zur Konfiguration von O365.

Voraussetzungen

Um O365-Apps in der Citrix Workspace-App zu konfigurieren, stellen Sie sicher, dass Sie Folgendes abgeschlossen haben:

- **Wenn Sie eine primäre Domäne in Microsoft Entra ID haben, die nicht mit anderen Diensten verbunden ist**, können Sie diese Domäne verwenden, um eine Föderation mit Citrix Secure Private Access herzustellen. Stellen Sie sicher, dass diese Domäne, entweder die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

übergeordnete oder die untergeordnete Domäne davon, noch nicht föderiert ist und die übergeordnete Domäne davon noch nicht in Microsoft Entra ID hinzugefügt wurde.

Wenn sich Ihr Benutzer beispielsweise mit `user1@demo.citrix.com` anmeldet, ist demo.citrix.com die primäre Domäne, citrix.com die übergeordnete Domäne und us.demo.citrix.com die untergeordnete Domäne.

- **Wenn Sie die primäre Domäne nicht föderieren können**, fügen Sie eine neue Domäne zu Microsoft Entra ID hinzu und föderieren Sie sie mit Citrix Secure Private Access. Erstellen Sie die Domäne und schließen Sie die Überprüfung ab. Weitere Informationen finden Sie unter `<https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/add-custom-domain>`.

  ODER

  Sie können eine Unterdomäne zu Microsoft Entra ID hinzufügen, die für die Föderation mit Citrix Secure Private Access für SSO genutzt werden kann. Dazu müssen Sie die Unterdomäne hinzufügen und zu einer Stammdomäne hochstufen. Weitere Informationen finden Sie unter `<https://docs.microsoft.com/de-de/azure/active-directory/enterprise-users/domains-verify-custom-subdomain>`.

  Hinweis: Möglicherweise müssen Sie Microsoft Entra ID Graph Explorer anstelle von Microsoft Graph Explorer für die POST-Anfrage verwenden, um eine Unterdomäne in eine Stammdomäne zu ändern.

  Details dazu, warum Sie eine föderierte Domäne benötigen, finden Sie unter Wie die Domänenföderation funktioniert.

- **Bestätigen Sie, dass die neue Domäne oder die von Ihnen hinzugefügte Unterdomäne in Microsoft Entra ID den Status „Verifiziert“ hat.**
- **Richten Sie eine Vertrauensstellung zwischen Ihrem SAML-Identitätsanbieter und Microsoft Entra ID ein.** Um eine Vertrauensstellung einzurichten, müssen Sie eine Domäne haben, die in Microsoft Entra ID verifiziert ist. Wenn eine Föderation in Microsoft Entra ID unter Verwendung einer Domäne konfiguriert wird, vertraut Microsoft Entra ID dem SAML-Anbieter für die Benutzerauthentifizierung bei Microsoft Entra ID, selbst wenn der Benutzer aus einer anderen Domäne als der föderierten Domäne stammt. Im SP-initiierten Fluss, wenn Microsoft Entra ID identifizieren muss, welcher IdP für die Authentifizierung verwendet werden soll (Benutzer zum föderierten IdP beschleunigen), wird dies anhand des `whr query param` oder `domain_hint` identifiziert, das an die URL `<https://docs.microsoft.com/de-de/azure/`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`active-directory/manage-apps/configure-authentication-for-federated-users-portal>` übergeben wird.

Das Hinzufügen einer Föderation für eine neue Domäne hat keine Auswirkungen auf eine bestehende Föderation, die Sie in Ihrer Einrichtung haben. Wenn Sie ADFS bereits mit einer Domäne föderiert haben, ist dies nicht betroffen, da Sie eine Föderation auf einer anderen Domäne einrichten, die weder eine Unterdomäne noch eine übergeordnete Domäne einer bereits föderierten Domäne ist.

SSO kann die folgenden zwei Abläufe haben:

IDP-initiierter Flow: Wird typischerweise verwendet, wenn Sie sich beim Microsoft Entra ID-Portal anmelden möchten. Der Citrix Secure Private Access-Dienst sendet die SAML-Assertion an Microsoft Entra ID. Microsoft Entra ID validiert diese basierend auf der zuvor vorgenommenen Föderationseinstellung. Wenn die Validierung erfolgreich ist, wird das `nameid`-Attribut von SAML extrahiert. Das `nameid`-Attribut muss mit `immutableId` des Benutzers übereinstimmen, der in Microsoft Entra ID vorhanden ist.

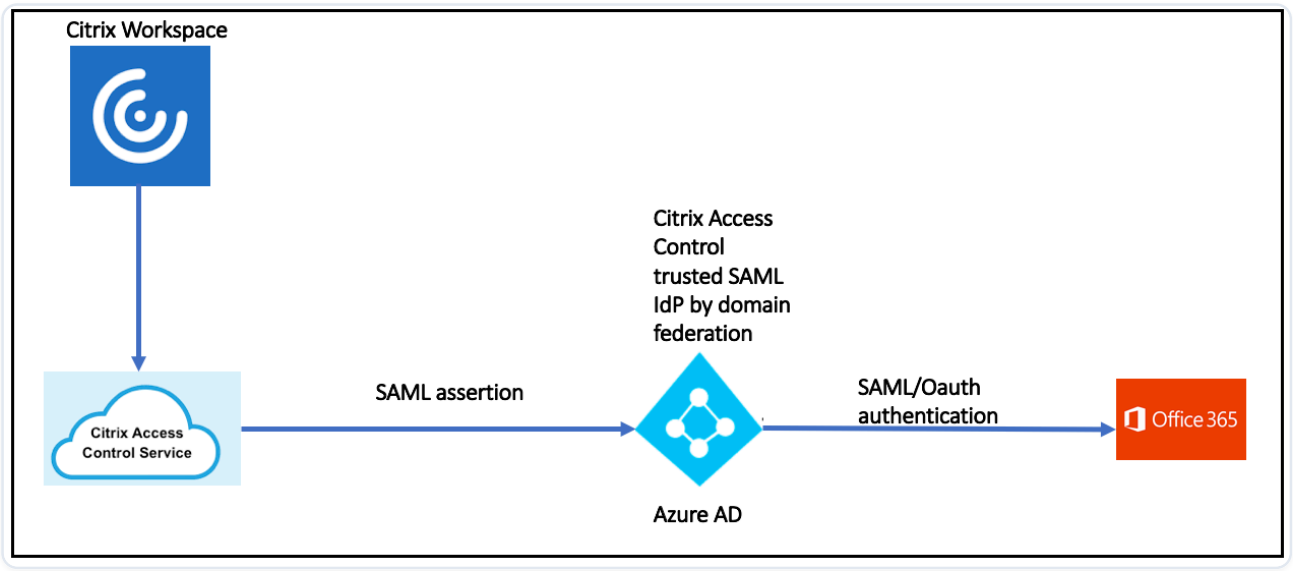
SP-initiierter Flow: Wird typischerweise verwendet, wenn Sie direkt zur App gelangen möchten, anstatt zum Microsoft Entra ID-Portal. In diesem Flow lädt der Citrix Secure Private Access-Dienst die in den App-Einstellungen konfigurierte URL. Die URL geht an Microsoft Entra ID, und da die URL einen Hinweis auf die föderierte Domäne enthält, wird der Benutzer mit einer SAML-Anfrage und einem Relay-Status an den Citrix Secure Private Access-Dienst umgeleitet. Der Citrix Secure Private Access-Dienst sendet die SAML-Assertion mit demselben Relay-Status, der in der Anfrage enthalten war, an Microsoft Entra ID. Sobald SAML validiert ist, leitet Microsoft Entra ID einen Benutzer zum Kontext im Relay-Status um, und somit gelangt der Benutzer direkt zur App.

- **Konfigurieren Sie die O365-App im Citrix Secure Private Access-Dienst**. Weitere Informationen finden Sie unter Support für Software-as-a-Service-Apps.

So funktioniert die Domänenföderation

Die folgende Abbildung veranschaulicht einen typischen Ablauf nach Abschluss einer Domänenföderation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Angenommen, Sie möchten die Office 365-App zu Citrix Workspace hinzufügen und Wasserzeichen aktivieren sowie Downloads einschränken. Der typische Ablauf ist wie folgt:

1. Sie starten die Office 365-App in Citrix Workspace.
2. Die Anfrage geht an den Citrix Secure Private Access-Dienst.
3. Der Citrix Secure Private Access-Dienst erstellt die SAML-Assertion und leitet sie an Microsoft Entra ID weiter.
4. Da die Anfrage von einem vertrauenswürdigen SAML-IdP kommt, identifiziert Microsoft Entra ID sie über die erstellte Domänenföderation und übergibt die SAML-Assertion an die Office 365-App.

   Die Office 365-App wird gestartet.

Unterstützte Authentifizierungsmethoden für die Office 365-App

Standardmäßig verwendet Citrix Cloud™ den Citrix Identitätsanbieter, um die Identitätsinformationen für alle Benutzer in Ihrem Citrix Cloud-Konto zu verwalten.

Citrix Workspace unterstützt die folgenden Authentifizierungsmethoden für Office 365. Okta und Google IdP werden derzeit nicht unterstützt.

- Lokales Active Directory
- Active Directory und Token
- Microsoft Entra ID

  Hinweis: Wenn Microsoft Entra ID zur Authentifizierung am Workspace verwendet wird, können Sie die primäre Domäne (Anmeldedomäne des Benutzers) nicht föderieren, da dies eine Schleife erzeugt. In solchen Fällen müssen Sie eine neue Domäne föderieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Private Access
- Active Directory und RADIUS

Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung.

Konfigurieren der O365-App im Secure Private Access-Dienst

Im Folgenden sind die übergeordneten Schritte zur Konfiguration der O365-App im Secure Private Access-Dienst aufgeführt. Weitere Informationen finden Sie unter Unterstützung für Software-as-a-Service-Apps.

1. Navigieren Sie zum Secure Private Access-Dienst in Citrix Cloud.
2. Suchen Sie nach Office 365 und wählen Sie die Vorlage **Office365** aus. Details zur Konfiguration einer App mithilfe der Vorlage finden Sie unter Unterstützung für Software-as-a-Service-Apps.

   HINWEIS:

   Sobald Sie die Vorlage **Office365** auswählen, werden die folgenden zugehörigen Domänen im Abschnitt **App-Details** automatisch ausgefüllt.

   - *.office.com
   - *.office365.com
   - *.sharepoint.com
   - *.live.com
   - *.onenote.com
   - *.microsoft.com
   - *.powerbi.com
   - *.dynamics.com
   - *.microsoftstream.com
   - *.powerapps.com
   - *.yammer.com
   - *.windowsazure.com
   - *.msauth.net
   - *.msauthimages.net

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- *.msocdn.com
- *.microsoftonline.com
- *.windows.net
- *.microsoftonline-p.com
- *.akamaihd.net
- *.sharepointonline.com
- *.officescriptsservice.com
- *.live.net
- *.office.net
- *.msftauth.net

3. Aktivieren Sie bei Bedarf erweiterte Sicherheitskontrollen.
4. SSO konfigurieren.

   Hinweis: Die einzige Änderung, die Sie vornehmen müssen, ist sicherzustellen, dass „Name ID“ die Active Directory GUID ist.

5. Stellen Sie sicher, dass erweiterte Attribute auch `IDPEmail` senden.

   - Attributname: `IDPEmail`
   - Attributformat: Nicht angegeben
   - Attributwert: E-Mail

6. Klicken Sie auf SAML-Metadaten, um sie in einem neuen Tab zu öffnen.

   - Kopieren Sie „entityID“
   - Kopieren Sie „Login-URL“
   - Laden Sie das Zertifikat im CRT-Format herunter

Konfigurieren der Domänenföderation von Microsoft Entra ID zu Citrix Workspace

Voraussetzungen:

- Aktivieren Sie PowerShell in Microsoft Entra ID
- Installieren Sie das Microsoft MSOnline-Modul

Im Folgenden sind die PowerShell-Befehle zum Installieren der erforderlichen Module aufgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
`PS> Install-Module AzureAD -Force`


`PS> Import-Module AzureAD -Force`


`PS> Install-Module MSOnline -Force`


`PS> Import-module MSOnline -Force`
```

Wenn die Module bereits installiert sind, führen Sie den folgenden Befehl aus.

```
PS> connect-msolservice
```

Hinweis: Ein Microsoft-Cloud-Konto ist erforderlich, um eine Verbindung mit `msolservice` herzustellen. Zum Beispiel `admin.user@onmicrosoft.com`.

Schritte zum Konfigurieren der Domänenföderation von Microsoft Entra ID zu Citrix Workspace

1. **Führen Sie die folgenden Befehle in PowerShell aus, um die Föderation zu konfigurieren:**

   - `PS> $dom = "ad-domain.com"`

   Hinweis: ad-domain.com ist die neue Domäne, die zu Microsoft Entra ID hinzugefügt wurde.

   - `PS> $IssuerUri = "https://citrix.com/[customerID]"`

   Hinweis: Die Kunden-ID finden Sie an den folgenden Speicherorten:

   - **Citrix Cloud > Identitäts- und Zugriffsverwaltung > API-Zugriff**
   - **Citrix Cloud > Citrix Secure Private Access.** Die Kunden-ID finden Sie in den App-Konfigurationsdetails (**Einmaliges Anmelden > SAML-Metadatendatei > entityID**).
   - `PS> $fedBrandName = “CitrixWorkspace”`
   - `PS> $logoffuri = "https://app.netscalergateway.net/cgi/logout"`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `PS> $uri = "https://app.netscalergateway.net/ngs/[customerID]/saml/login?APPID=[AppID]”`

Hinweis: $uri kann von **Citrix Secure Private Access Service > Web-/SaaS-App hinzufügen > Einmaliges Anmelden > Anmelde-URL** oder von **SAML-Metadaten > Speicherort** kopiert werden.

- `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2(“<location of certificate downloaded from Citrix Secure Private Access service/filename.crt>”)`

  Zum Beispiel: `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`

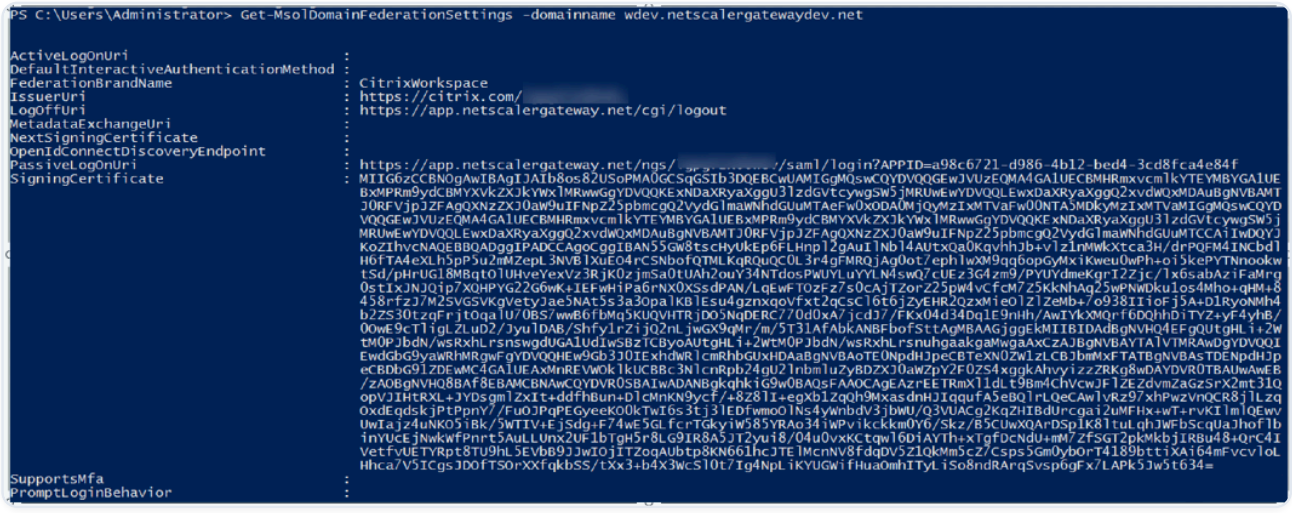
`PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

2. **Führen Sie die PS-Zeichenfolge aus, um die Föderation mit Citrix Secure Private Access abzuschließen:**

   `PS> Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri -SigningCertificate $certData -IssuerUri $IssuerUri -PreferredAuthenticationProtocol SAMLP`

3. **Überprüfen Sie die Einstellungen für die Domänenföderation, indem Sie den folgenden Befehl ausführen:**

   `Get-MsolDomainFederationSettings -DomainName <domain name>`



Automatisierte Domänenföderation von Microsoft Entra ID zu Citrix Workspace

Bei der manuellen Domänenföderation von Microsoft Entra ID zu Citrix Workspace müssen Benutzer zwischen Cloud-Portal und PowerShell wechseln, um Daten zu kopieren und die Skripte auszuführen. Zum Beispiel:

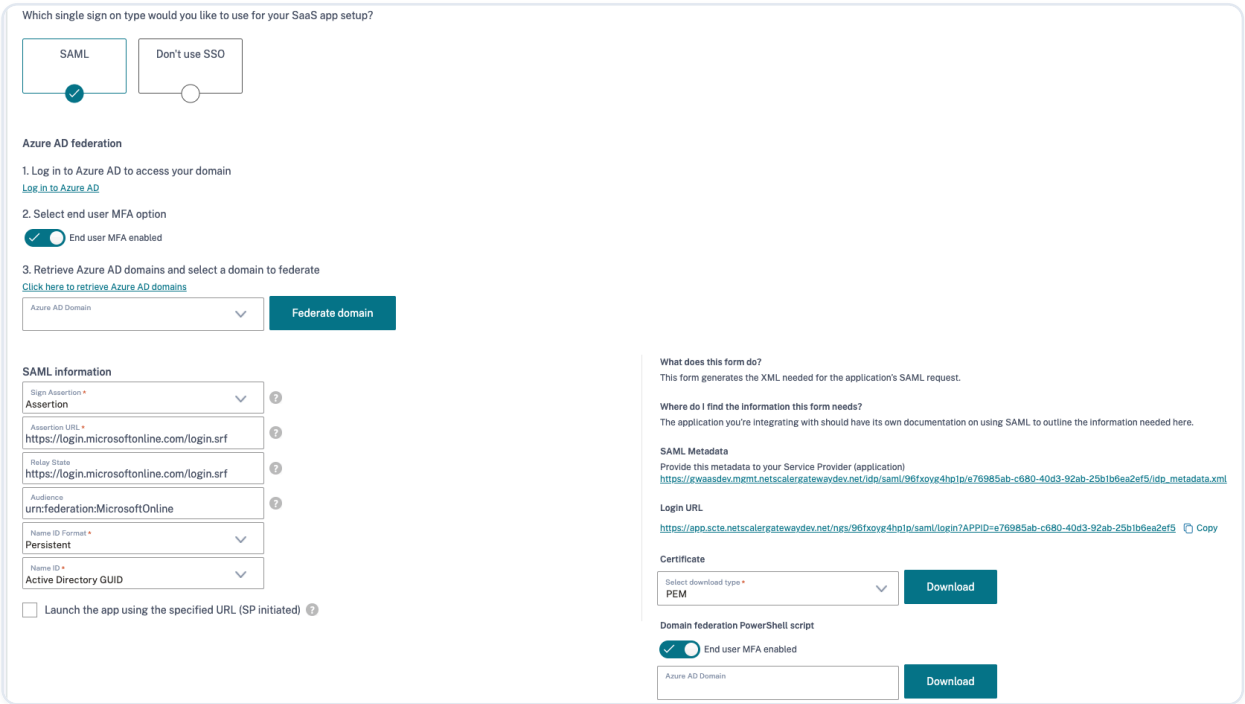
- Daten wie Kunden-ID und App-ID aus dem Cloud-Portal kopieren.
- Das Zertifikat aus dem Cloud-Portal herunterladen.
- Die PowerShell-Skripte ausführen.

Diese manuelle Kopier- und Einfügeaktion kann zu Fehlern führen, wodurch die Föderation möglicherweise nicht erfolgreich ist.

Die Schritte zur Föderation einer Domäne sind jetzt in die Benutzeroberfläche des Citrix Secure Private Service integriert, wodurch der Föderationsprozess automatisiert wird. Die PowerShell-Skripte werden im Backend ausgeführt, wenn Benutzer die entsprechenden Links in der Benutzeroberfläche anklicken. Benutzer müssen nicht zwischen Cloud-Portal und PowerShell wechseln.

Schritte zur automatischen Föderation einer Domäne

1. Konfigurieren Sie die O365-App. Einzelheiten finden Sie unter Konfigurieren der O365-App im Secure Private Access Service.
2. Wählen Sie unter Single Sign-On **SAML** aus.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Melden Sie sich mit Ihren Anmeldeinformationen bei Microsoft Entra ID an. Wenn Sie auf **Bei Entra ID anmelden** klicken, werden Sie zur Authentifizierung zum Microsoft Entra ID Anmeldeportal weitergeleitet.
    - Das OAuth-Protokoll wird zur Authentifizierung verwendet. Nach erfolgreicher Authentifizierung müssen Sie der Föderation der Domäne zustimmen.
    - **Endbenutzer-MFA-Option auswählen** ist standardmäßig aktiviert.
4. Klicken Sie auf **Hier klicken, um Entra ID-Domänen abzurufen**, um die Liste aller Domänen anzuzeigen.
5. Wählen Sie die Domäne aus, die Sie verknüpfen möchten, und klicken Sie auf **Domäne verknüpfen**.

HINWEIS:

- Wenn Sie auf **Domäne verknüpfen** klicken, werden die PowerShell-Skripte im Backend ausgeführt und die Domäne wird verknüpft.
- Sie können die PowerShell-Skripte bei Bedarf auch über die Benutzeroberfläche herunterladen. Klicken Sie unter **PowerShell-Skript zur Domänenverknüpfung** auf **Herunterladen**.

Multifaktor-Authentifizierung (MFA) unterdrücken

Eine Option wird zu den erweiterten Attributen von O365-Apps hinzugefügt, die die MFA unterdrückt, wenn der Benutzer die MFA bereits während der Benutzerauthentifizierung bei Citrix Workspace eingegeben hat.

- **Attributname:** „`http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod`“,
- **Attributwert:** „`http://schemas.microsoft.com/claims/multipleauthn`“

Damit die Microsoft Entra ID diesen Anspruch akzeptiert, verknüpfen Sie sie mit dem folgenden PowerShell-Befehl:

```
Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`-SigningCertificate $certData -IssuerUri $IssuerUri -PreferredAuthenticationProtocol SAMLP -SupportsMfa $true`

HINWEIS:

Der IdP-initiierte Ablauf berücksichtigt den Relay-Status nicht. Verwenden Sie den SP-initiierten Ablauf, um direkt zur App zu gelangen.

Konfigurieren einzelner Office-Suite-Anwendungen in Citrix Workspace

Führen Sie die folgenden Schritte aus, um einzelne Office-Suite-Anwendungen zu konfigurieren:

1. Schließen Sie die Domänenverknüpfung wie in den vorherigen Abschnitten beschrieben ab.
2. Wählen Sie die O365-Vorlage.
3. Ändern Sie den Namen der App, zum Beispiel in MS Word.
4. Ändern Sie die App-URL entsprechend.

Word: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FWord%3domain>`

Powerpoint: `<https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2Fpowerpdomain>`

Excel: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FExcel%domain>`

CRM/Dynamics Online: `https://<tenant>.crm.dynamics.com/?whr=<federated domain>`

OneDrive für Unternehmen: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>-my.sharepoint.com%2F&whr=<federated domain>`

Outlook Kalender: `https://outlook.office.com/owa/?realm=<federated domain>&path=/calendar/view/Month`

Outlook Web Access zu Exchange Online: `https://outlook.com/owa/<federated domain>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SharePoint Online: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>.sharepoint.com%2F&whr=<domain>`

Teams: `https://login.microsoftonline.com/common/oauth2/authorize?client_id=cc15fd57-2c6c-4117-a88c-83b1d56b4bbe&response_mode=form_post&response_type=code+id_token&scope=openid+profile&<domain>`

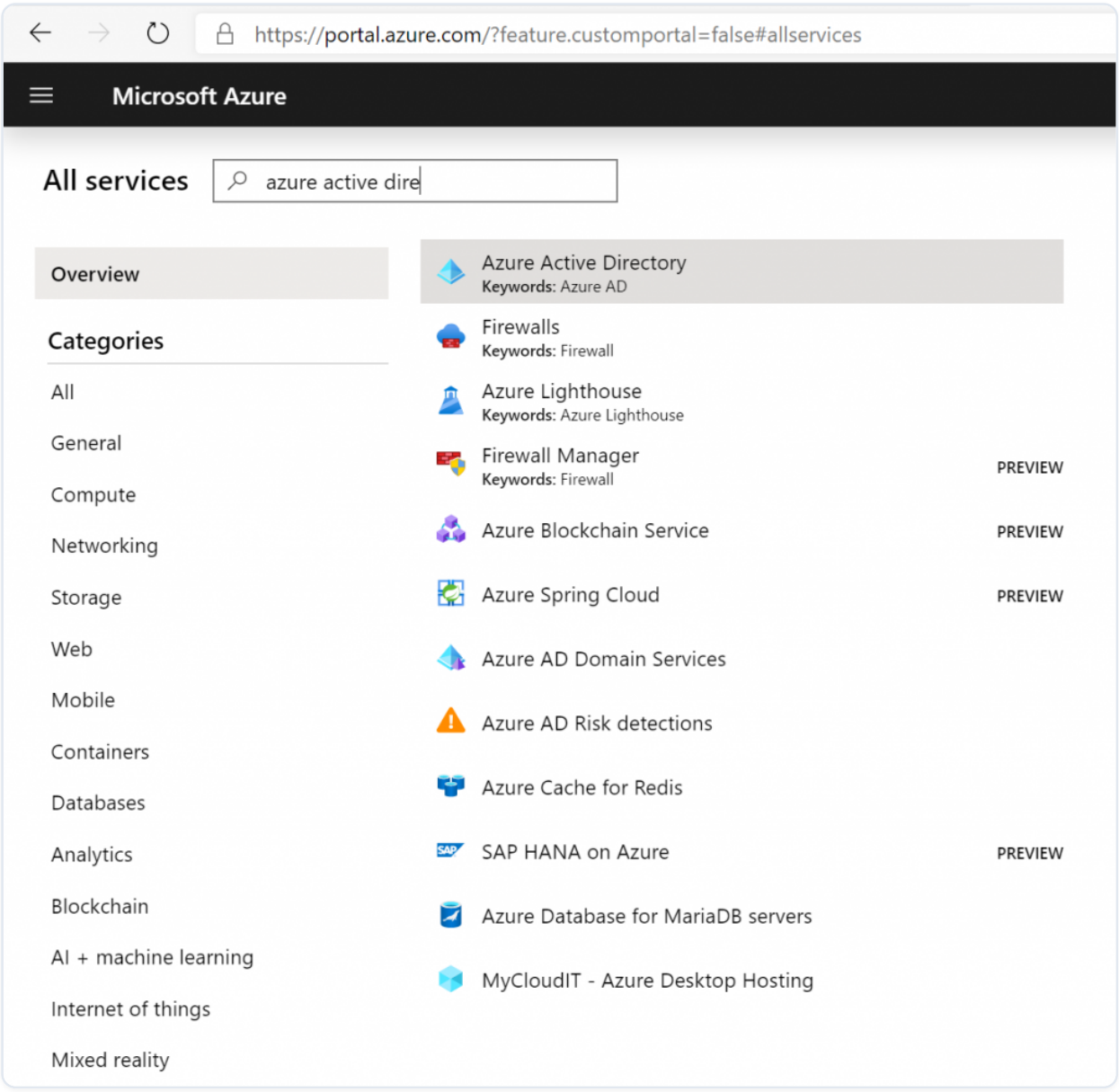
Drittanbieter-Apps, die in Microsoft Entra ID integriert sind

Wenn Sie Drittanbieteranwendungen wie Box, Salesforce, ServiceNow, Workday integriert haben, können Sie die Smart Links für diese Apps aus der Microsoft Entra ID abrufen.

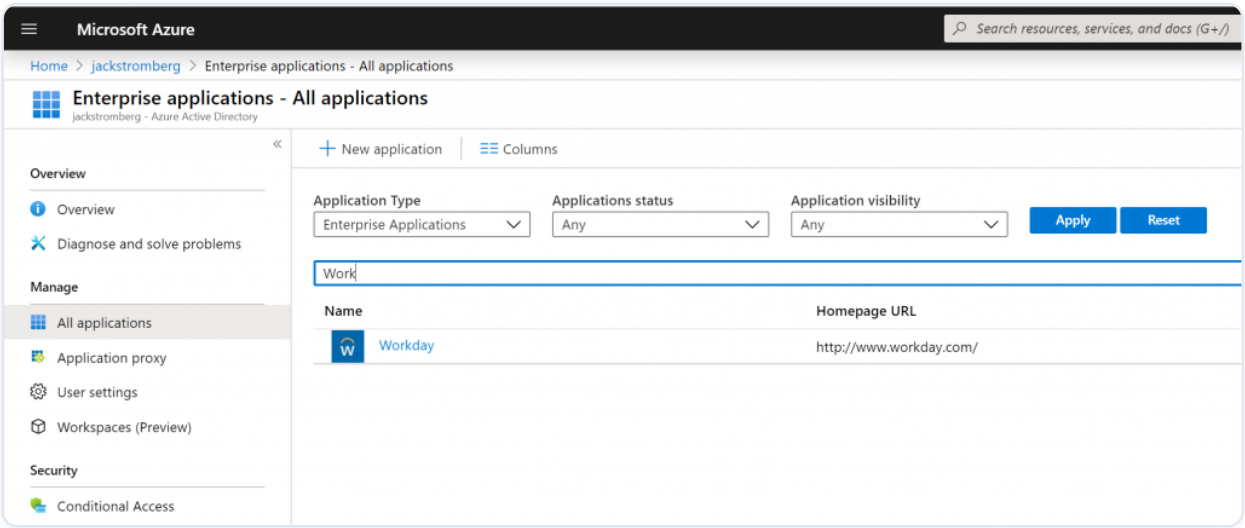
Führen Sie die folgenden Schritte aus.

1. Melden Sie sich bei Ihrem Microsoft Entra ID Portal `<https://portal.azure.com>` an.
2. Wählen Sie **Alle Dienste > Azure Active Directory** aus, und wählen Sie Ihr Verzeichnis aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

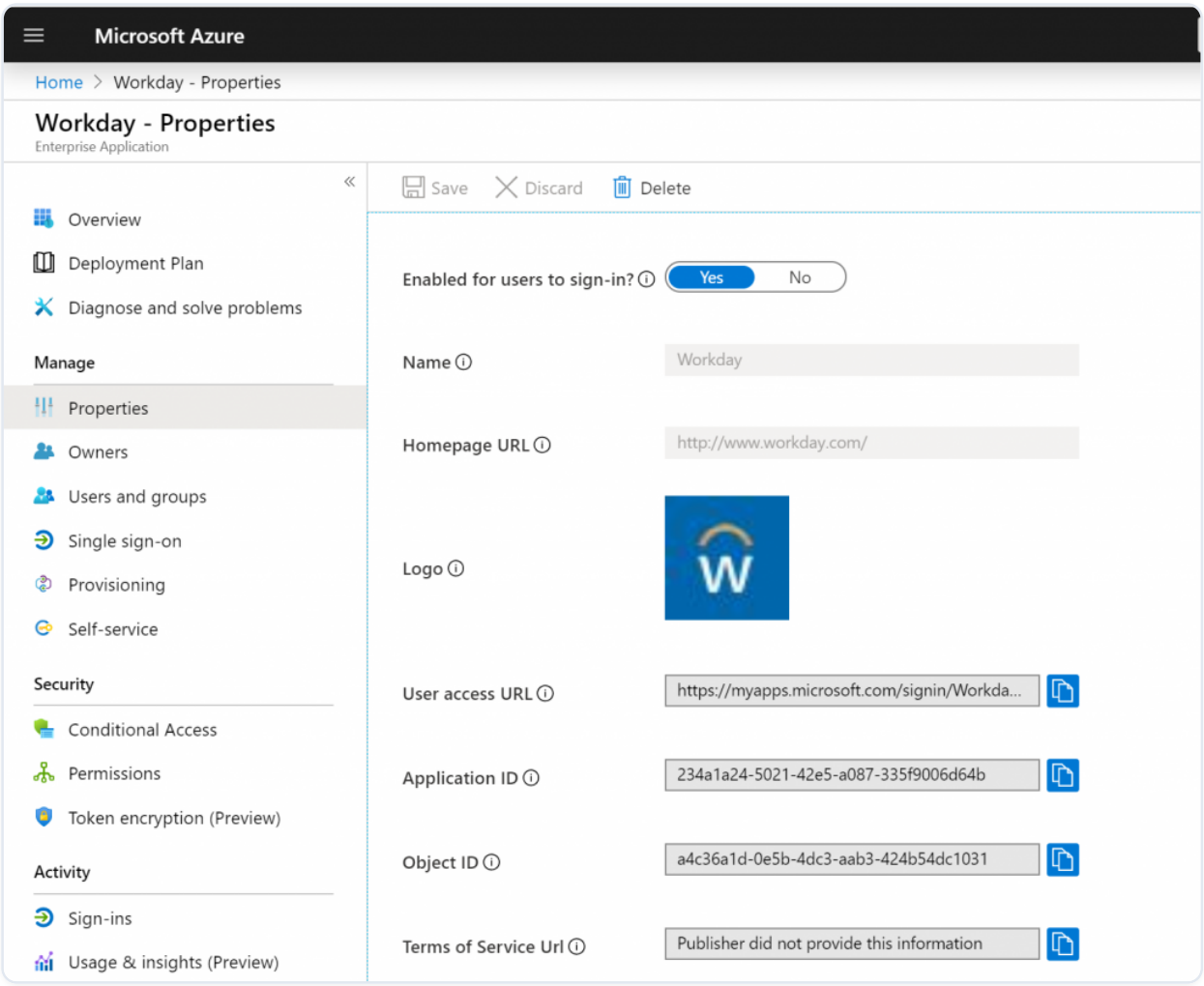


3. Wählen Sie **Unternehmensanwendungen** aus und wählen Sie dann die Anwendung, für die Sie einen Smart Link generieren möchten.



4. Wählen Sie **Eigenschaften** aus und kopieren Sie die Benutzerzugriffs-URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Nachdem Sie `whr` an die URL angehängt haben, werden die `whr` Parameter wie in der Beispiel-URL gezeigt angezeigt.

   Beispiel-URL: `https://myapps.microsoft.com/signin/Workday/12345678912345678912345678896d64b&whr=ctxnsqa.net`

   Hinweis: Hängen Sie `whr` an die URL an, damit Microsoft Entra ID weiß, welchen IdP es zur Authentifizierung eines Benutzers basierend auf der Verbundkonfiguration verwenden und automatisch zu diesem IdP umleiten soll.

6. Erweiterte Sicherheitskontrollen festlegen.
7. SSO konfigurieren.

   - Name-ID = AD GUID
   - Kontrollkästchen für SP-initiierte Anmeldung aktivieren
   - Assertions-URL = Anmelde-URL

     Wenn Sie einen IdP-initiierten Flow durchführen, werden Benutzer zur Portalseite von Microsoft Entra ID weitergeleitet. Wenn Sie direkt auf der App-Seite landen möchten, ist ein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

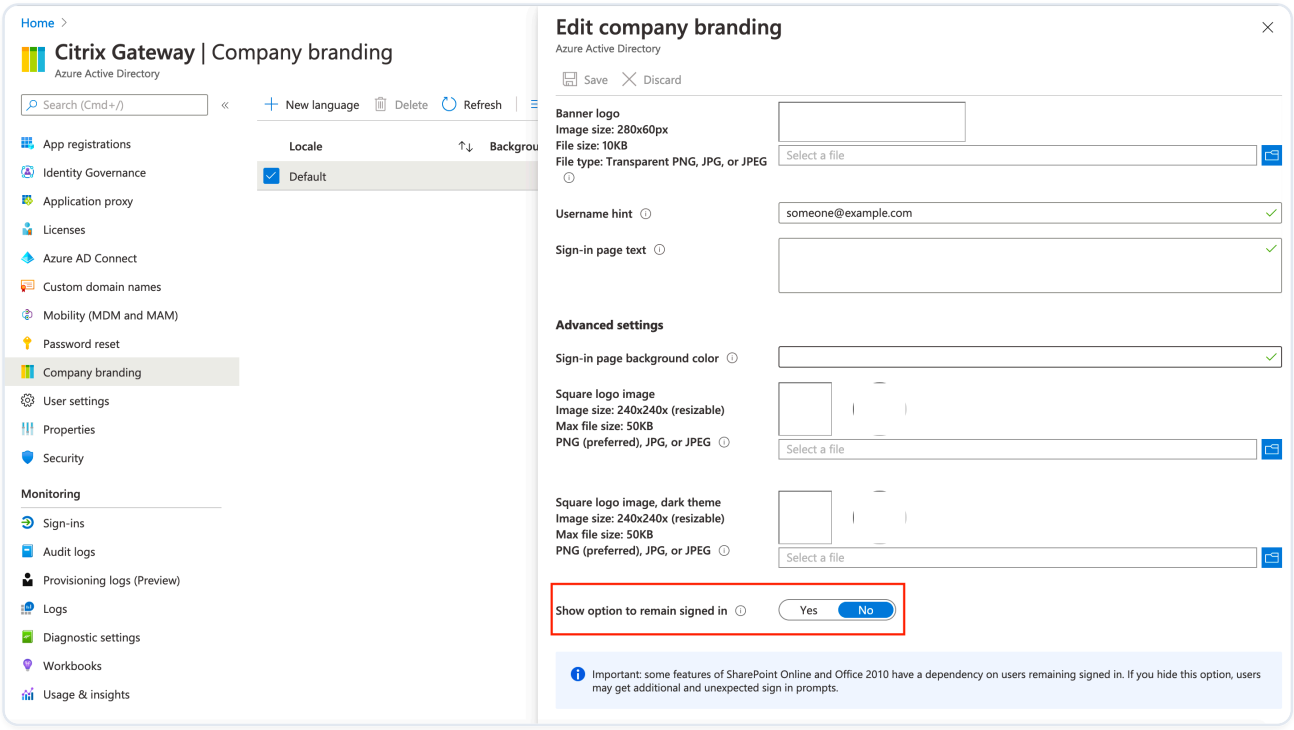
SP-initiierter Flow erforderlich, da dieser den korrekten Relay-Status in der SAML-Assertion sendet.

HINWEIS:

- Wenn die Föderation der primären Domäne aktiviert ist, werden alle Microsoft Entra ID-Benutzer bei der Authentifizierung bei Office 365-Anwendungen zu Citrix Workspace umgeleitet. Dies könnte bei Kunden zu einem Ausfall/Vorfall führen, wenn dies ohne Verständnis der Auswirkungen geschieht.
- Wenn Benutzer sich mit Microsoft Entra ID bei Citrix Workspace anmelden, darf die primäre Domäne der Benutzer, die für die Anmeldung verwendet wird, nicht mit dem Citrix Gateway-Dienst föderiert werden. Dies führt zu einer Schleife. Verwenden Sie in solchen Fällen eine andere Domäne als die Domänen der Benutzer, die sich bei Microsoft Entra ID anmelden, um sie mit dem Citrix Secure Private Access-Dienst zu föderieren.
- Wenn die primäre Domäne mit dem Citrix Secure Private Access-Dienst föderiert ist, werden alle Benutzeranmeldungen in dieser Domäne in Microsoft Entra ID an den Citrix Secure Private Access-Dienst umgeleitet. Für einen POC können Sie bei Bedarf eine Testdomäne föderieren, bevor Sie die primäre Domäne föderieren.
- Wenn Microsoft Entra ID die Standortrichtlinie aktiviert hat, müssen Benutzer nur aus der Liste der zulässigen IP-Adressen eines Unternehmensnetzwerks stammen. In solchen Fällen können Sie die O365-App als Web-App veröffentlichen und ihren Datenverkehr über die Connector Appliance leiten.
- Wenn Sie sich bei Microsoft Entra ID anmelden und die Aufforderung **Angemeldet bleiben?** vermeiden möchten, können Sie diese Einstellung über Microsoft Entra ID ändern. Beachten Sie die wichtige Meldung, die beim Ändern der Einstellung angezeigt wird, und machen Sie die Änderung bei Bedarf rückgängig.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Referenzlinks

Azure PowerShell-Modulreferenz

Bereitstellen der Office 365-Verzeichnissynchronisierung in Microsoft Azure

ERP Cloud konfigurieren

Die folgenden Abschnitte enthalten weitere Informationen zur Konfiguration von ERP Cloud.

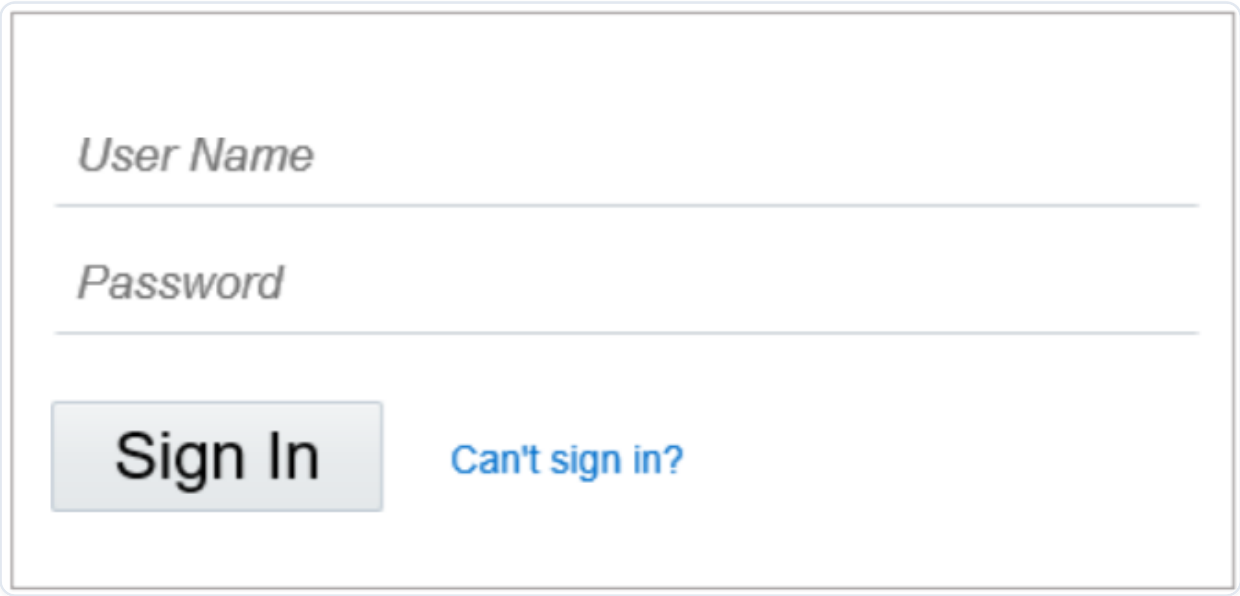
Citrix Gateway SaaS-Anwendung

Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei ERP Cloud anmelden.

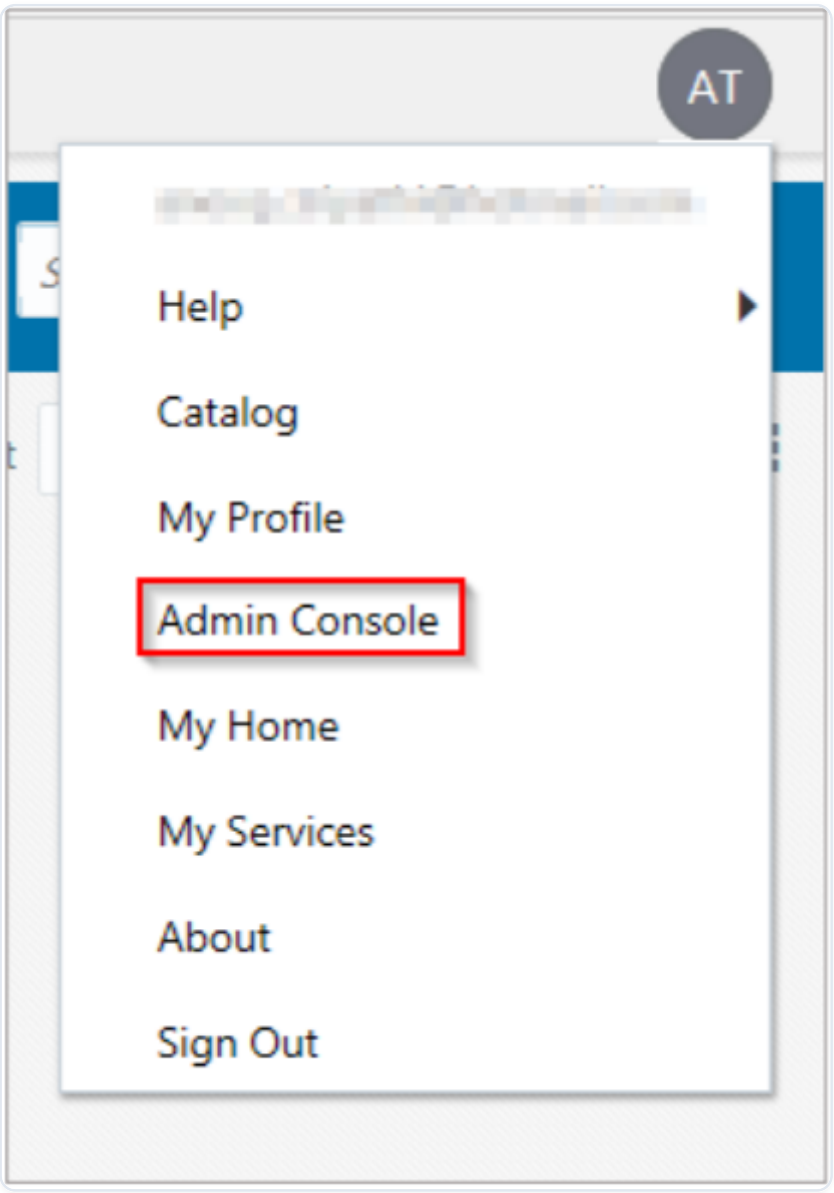
Um ERP Cloud für SSO über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Geben Sie in einem Browser `https://<organizationid>.identity.oraclecloud.com/ui/v1/adminconsole/?root=security&security=external-idp` ein und drücken Sie die Eingabetaste.
2. Melden Sie sich bei Ihrem ERP Cloud-Konto an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



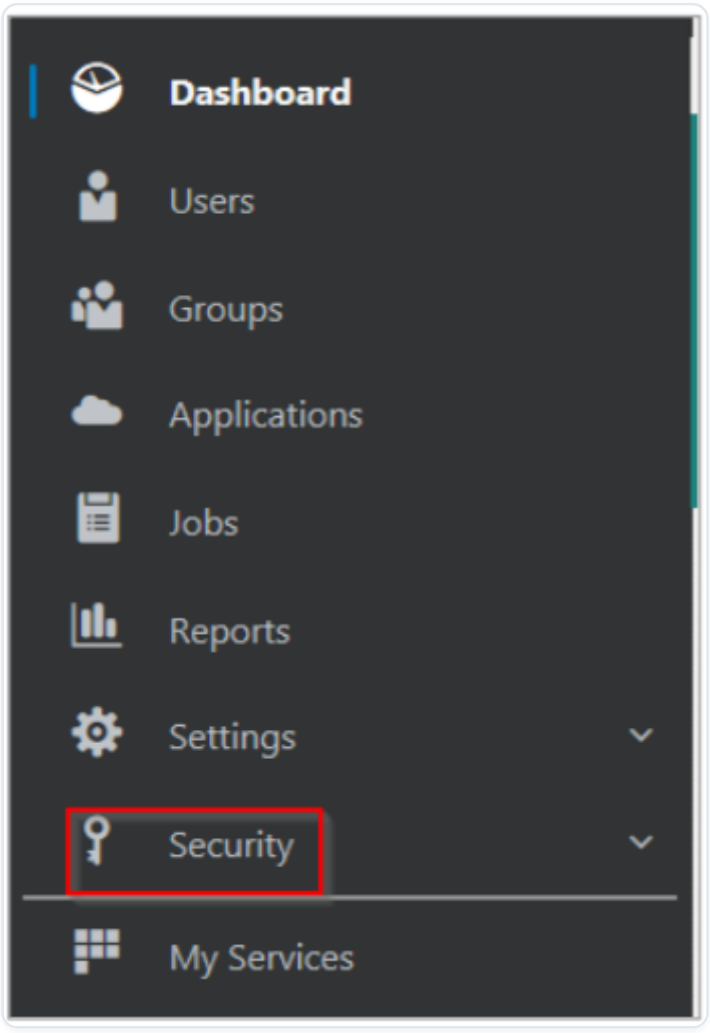
3. Klicken Sie auf der Startseite oben rechts auf Ihre Profilinitialen und dann auf Admin Console.



4. Klicken Sie oben links auf die Auslassungspunkte.

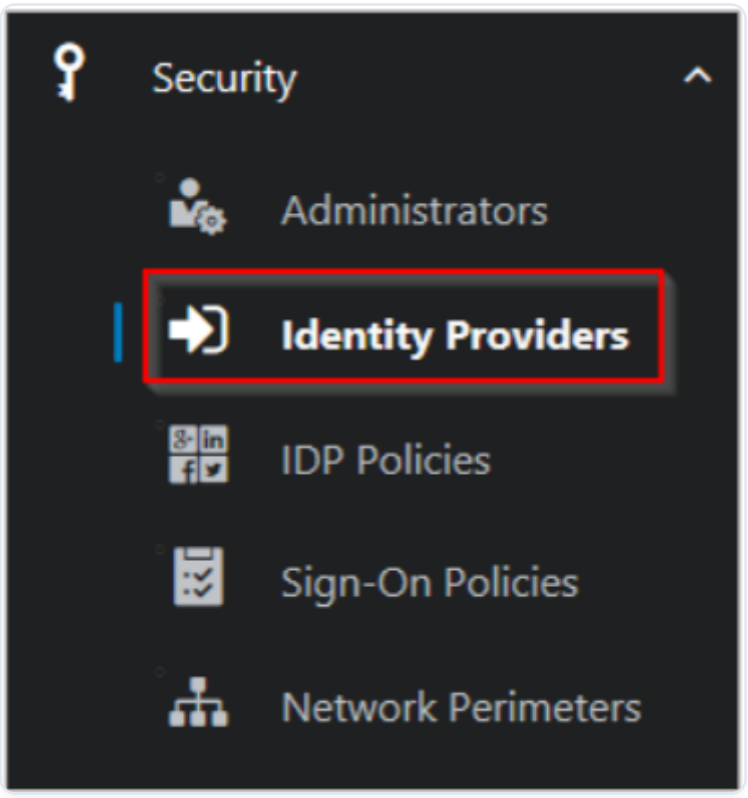
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Klicken Sie auf Sicherheit.

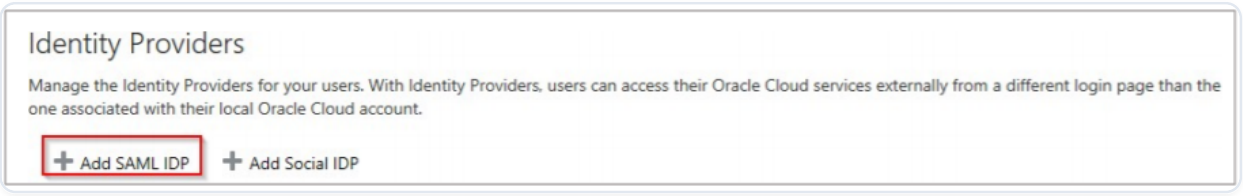


6. Klicken Sie auf Identitätsanbieter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

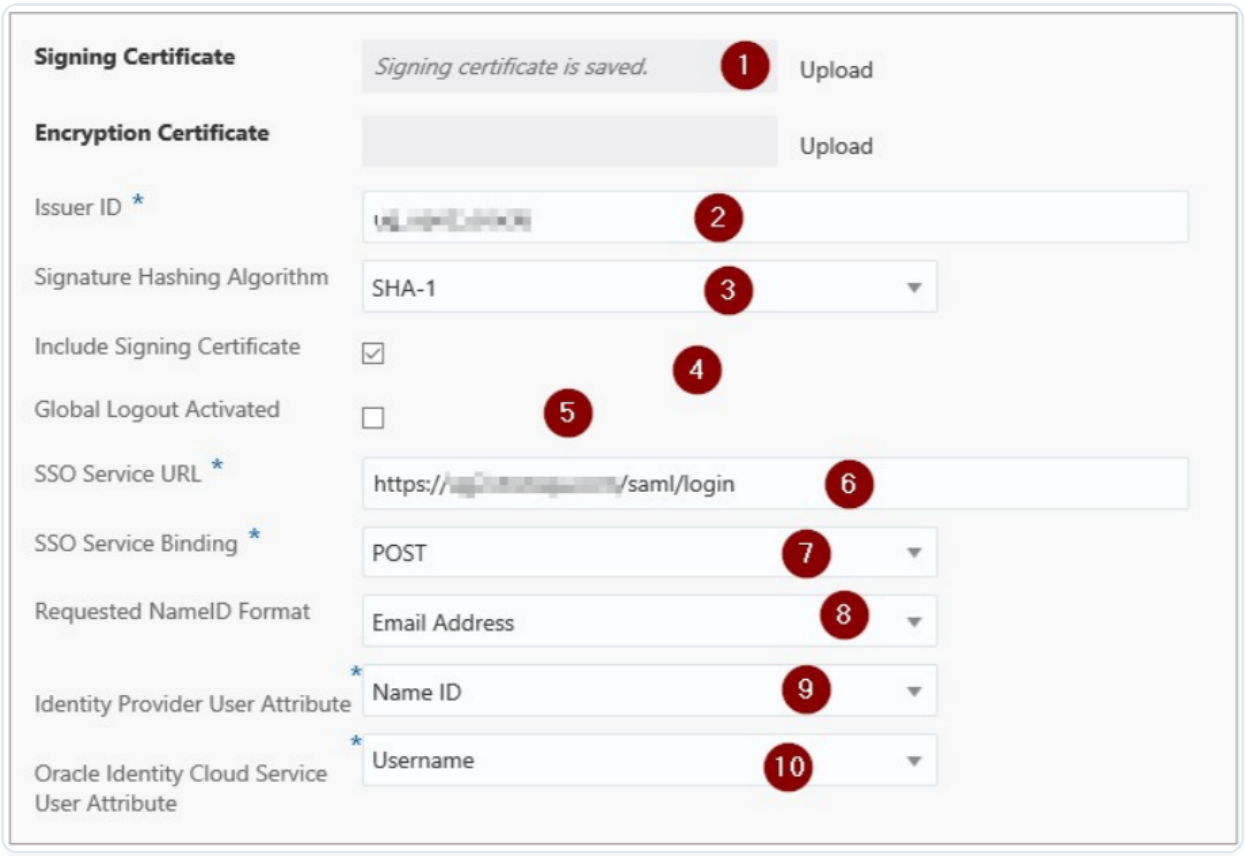


7. Klicken Sie auf der Seite Identitätsanbieter auf SAML-IdP hinzufügen.



8. Geben Sie auf der Seite Identitätsanbieter die folgenden Informationen an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. Signaturzertifikat – fügen Sie das PEM-Zertifikat ein.

   Um Ihr IdP-Zertifikat zu erhalten, führen Sie Folgendes aus:

   - Greifen Sie remote auf Ihre NetScaler®-Instanz mit PuTTY zu.
   - Navigieren Sie zum Ordner /nsconfig/ssl (mit dem Shell-Befehl `cd` /nsconfig/ssl) und drücken Sie die Eingabetaste.
   - Geben Sie cat `<certificate-name>` ein und drücken Sie die Eingabetaste.
   - Kopieren Sie den Text von -----BEGIN CERTIFICATE----- bis -----ENDCERTIFICATE-----
   - Fügen Sie den Text in einen Texteditor ein und speichern Sie die Datei in einem geeigneten Format wie `your organization name`.pem

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. Aussteller-ID – geben Sie einen eindeutigen Namen ein.

c. Signatur-Hashing-Algorithmus – wählen Sie den Hashing-Algorithmus aus, der zum Signieren von SAML-Nachrichten verwendet wird.

d. Signaturzertifikat einschließen – aktivieren Sie das Kontrollkästchen, wenn Sie das Signaturzertifikat einschließen möchten, um die Signatur der Nachrichten für den IdP zu überprüfen.

e. Globaler Logout aktiviert – aktivieren Sie das Kontrollkästchen, wenn Sie SAML-Global-Logouts aktivieren möchten.

f. SSO-Dienst-URL – Geben Sie die IdP-URL gefolgt von /saml/ login ein. Zum Beispiel: `https://<netscalerinstance>.com/saml/ login`

g. SSO-Dienstbindung – klicken Sie auf die entsprechende Option, um eine Authentifizierungsanfrage zu senden.

h. Format der angeforderten NameID – klicken Sie auf das entsprechende Format, um den Attributwert des Benutzers im IdP dem entsprechenden Attribut in Oracle Identity CloudService zuzuordnen.

i. Benutzerattribut des Identitätsanbieters – klicken Sie auf den entsprechenden Attributwert, der vom IdP empfangen wurde, um den Benutzer eindeutig zu identifizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

j. Benutzerattribut von Oracle Identity Cloud Service – klicken Sie auf das entsprechende Attribut, das Sie verwenden, um das vom IdP empfangene Attribut zuzuordnen.

9. Klicken Sie auf Änderungen speichern.

ServiceNow konfigurieren

Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei ServiceNow anmelden.

Um ServiceNow für SSO über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Geben Sie in einem Browser `https://<your-organization>.service-now.com/` ein und drücken Sie die **Eingabetaste**.

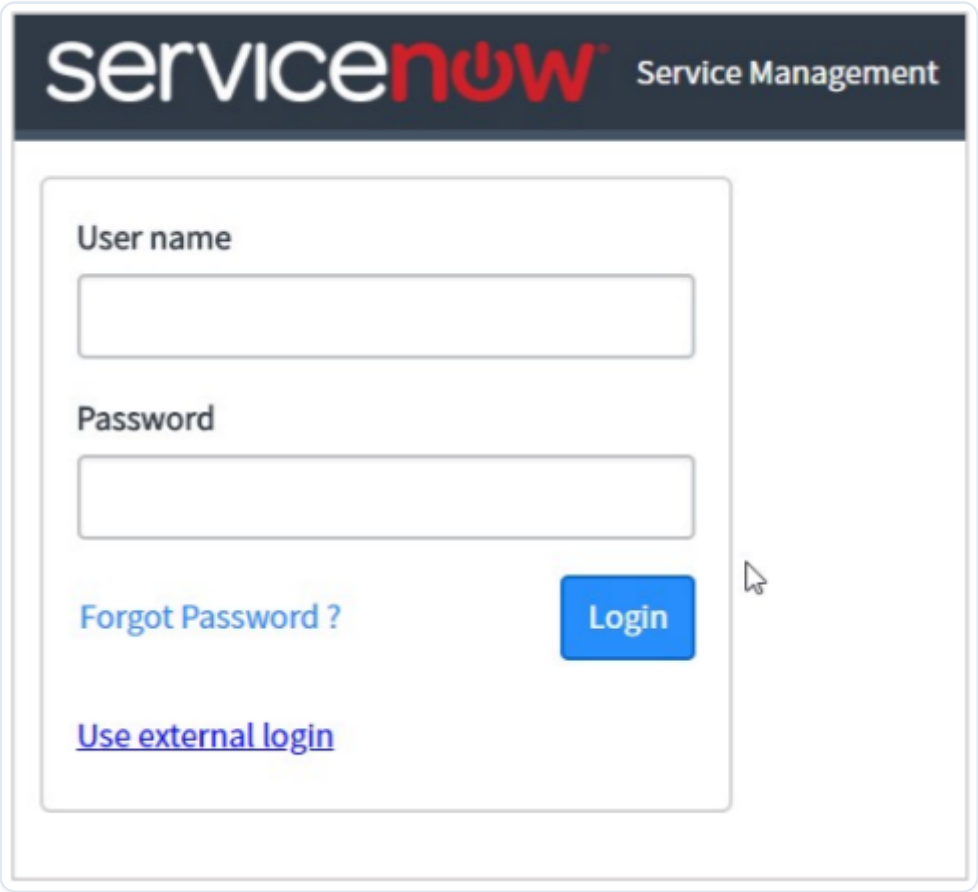
   Wenn die URL, die Sie für den Zugriff auf ServiceNow verwenden, beispielsweise `https://myserver.servicenow.com` lautet, müssen Sie `<your-organization>` durch `myserver` ersetzen.

   HINWEIS:

   - Stellen Sie sicher, dass die folgenden Details in der Benutzeroberfläche des Citrix Gateway-Dienstes angegeben werden, wenn Sie die ServiceNow-App hinzufügen.
     - Assertions-URL: `https://<your-organizaton>.service-now.com/navpage.do`
     - Relay-Status: `https://<your-organizaton>.service-now.com/`
     - Zielgruppe: `https://<your-organizaton>.service-now.com/`
     - Name-ID-Format: Wählen Sie „E-Mail-Adresse“
     - Name-ID: Wählen Sie „Benutzerprinzipalname (UPN)“
   - Das Name-ID-Format und die Name-ID-Attribute hängen von der für ServiceNow gewählten Authentifizierungsmethode ab.

2. Melden Sie sich als Administrator bei Ihrem ServiceNow-Konto an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

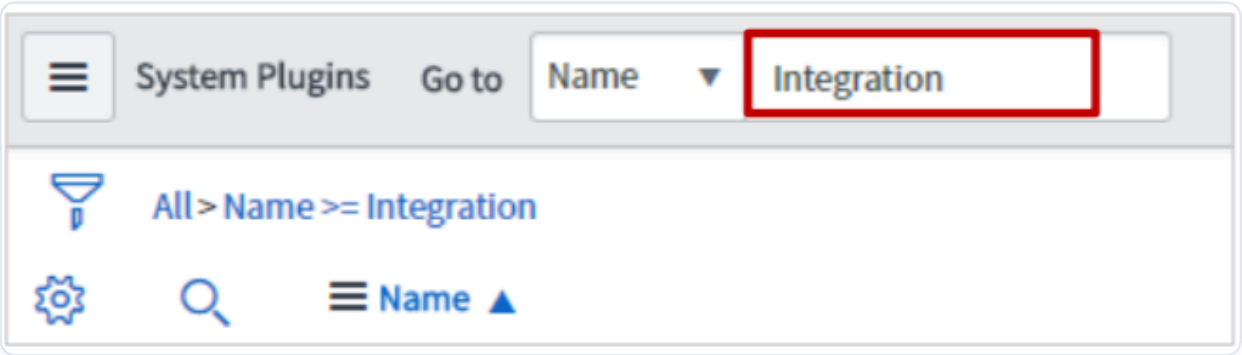


3. Suchen Sie in der oberen linken Ecke mit dem Filter-Navigator nach Plug-ins und klicken Sie in den Suchergebnissen auf **Plugins**.

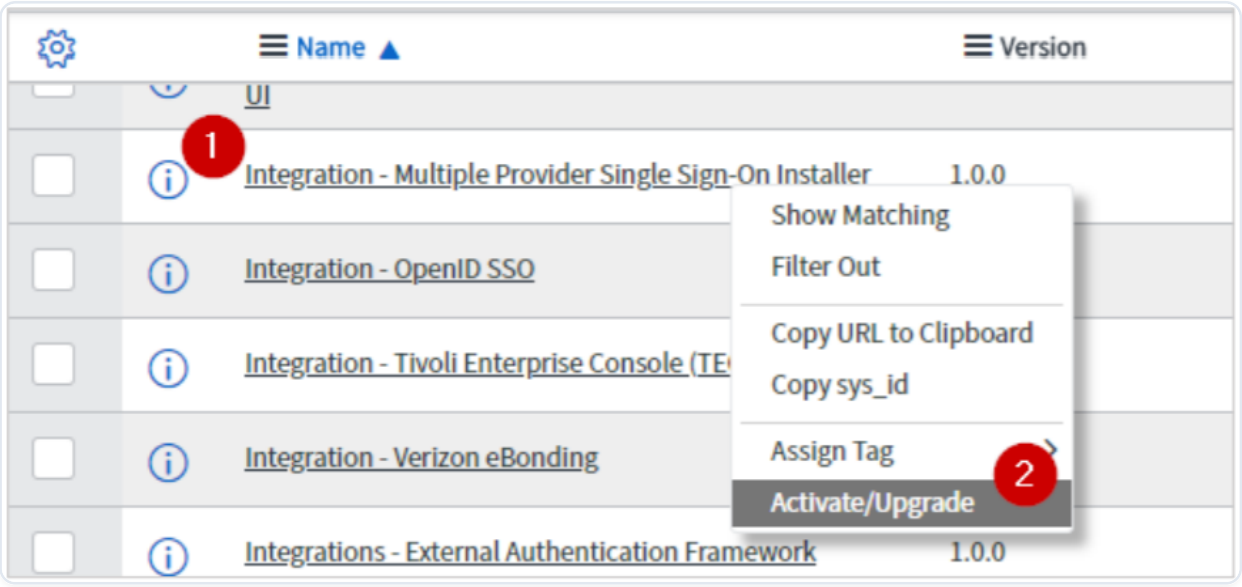


4. Suchen Sie im rechten Bereich, im Abschnitt **System Plugins**, nach Integration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf **Integration - Multiple Provider Single Sign-OnInstaller** und klicken Sie auf **Activate/Upgrade**.

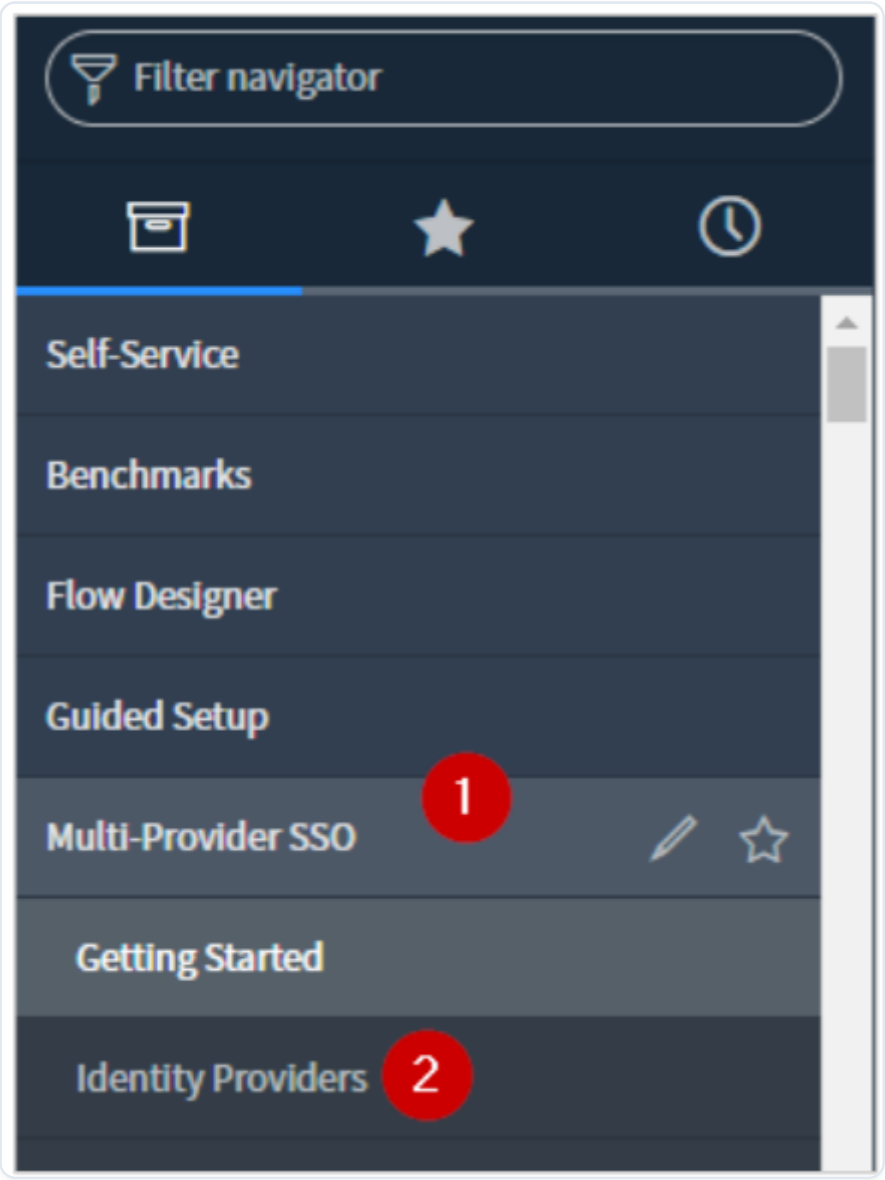


6. Klicken Sie auf **Activate**.

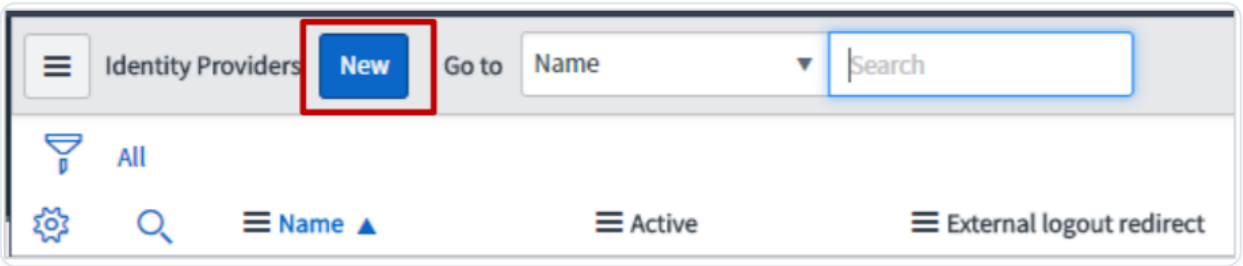
   Eine Fortschrittsanzeige zeigt den Abschluss des Aktivierungsprozesses an.

7. Scrollen Sie im linken Bereich zum Abschnitt Multi-Provider SSO und klicken Sie auf **Multi-ProviderSSO > Identity Providers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

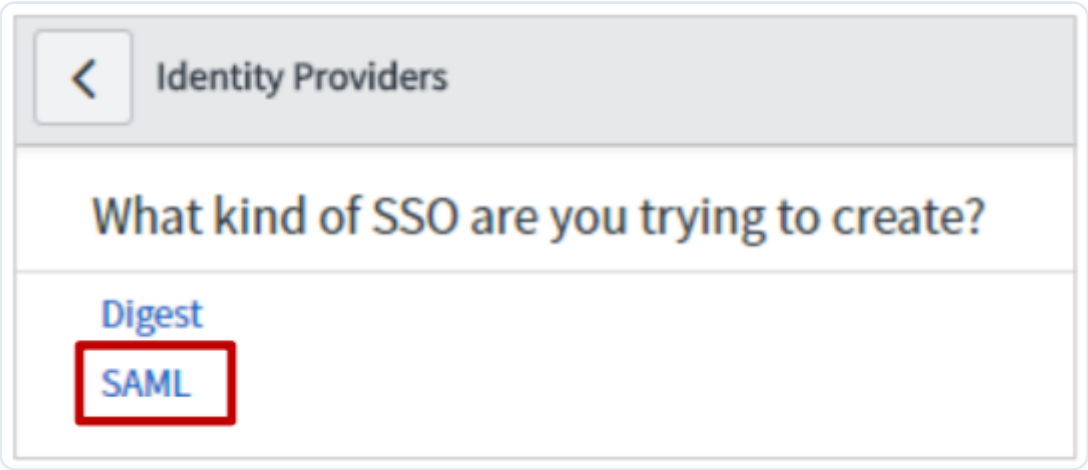


8. Klicken Sie im rechten Bereich auf **New**.



9. Klicken Sie auf **SAML**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

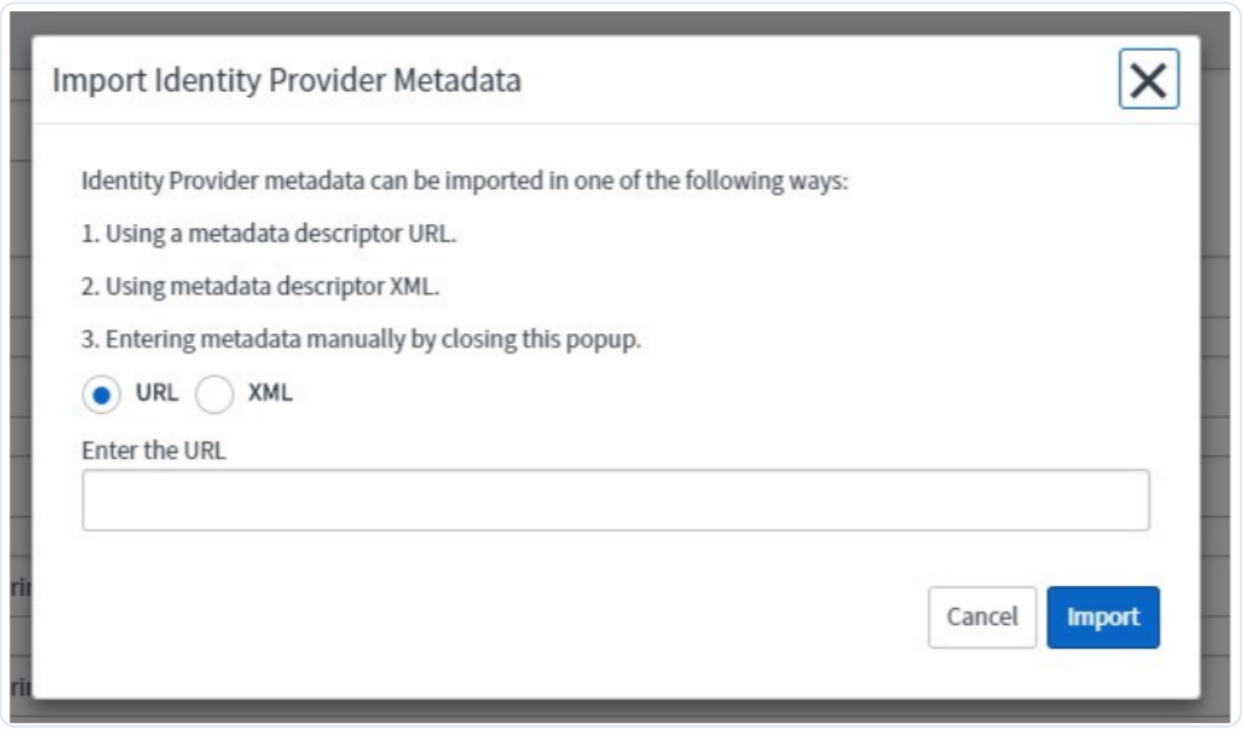


10. Wenn Sie die Metadaten-URL haben, klicken Sie im Abschnitt **Identity Provider New Record** im Pop-up-Fenster **Import Identity Provider Metadata** auf **URL**, geben Sie die Metadaten-URL ein und klicken Sie auf **Import**.

    Die Werte für die Felder des Identitätsanbieter-Datensatzes werden automatisch ausgefüllt.

    Wenn Sie die Metadaten-XML-Datei haben, klicken Sie auf XML. Kopieren Sie die XML-Daten der Identitätsanbieter-Metadaten und fügen Sie sie in das Feld ein. Klicken Sie auf **Importieren**.

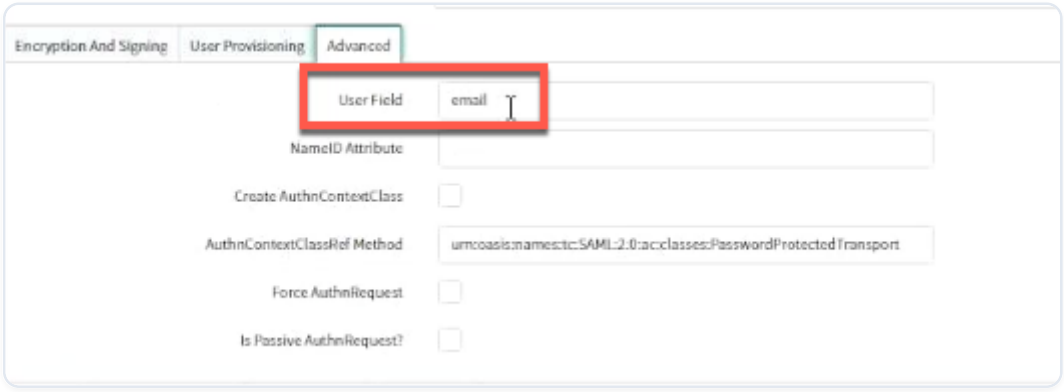
    Die Werte für die Felder des Identitätsanbieter-Datensatzes werden automatisch ausgefüllt. Sie können die Werte bei Bedarf aktualisieren.



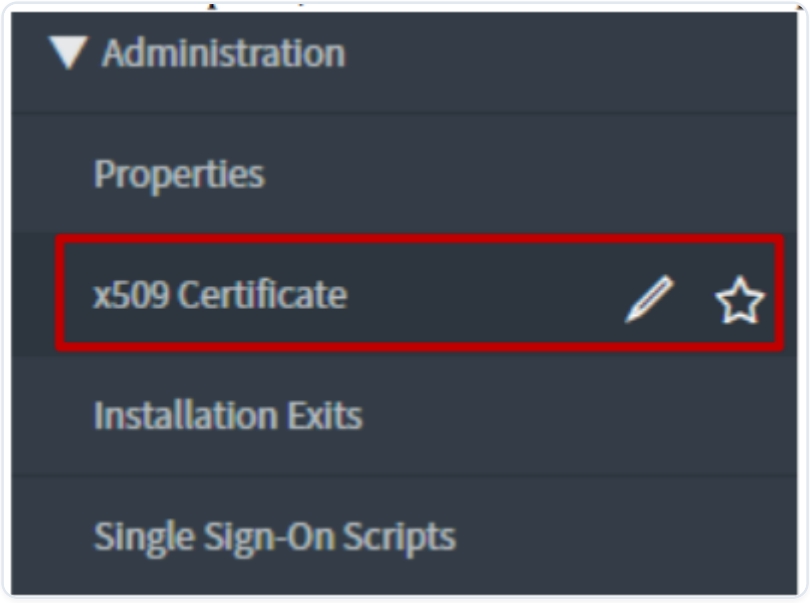
© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

- Citrix empfiehlt, die Metadaten-XML-Datei zu importieren, anstatt sie manuell zu konfigurieren. Sie können die Metadaten-XML-Datei über den Citrix Cloud-Assistenten importieren (**Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > SAML-Metadaten**).
- Stellen Sie beim Konfigurieren der Parameter auf der Registerkarte **Erweitert** sicher, dass der Wert des **Benutzerfelds** mit dem Wert übereinstimmt, der für das Feld **Name ID** in der Benutzeroberfläche des Citrix Gateway-Dienstes konfiguriert ist.

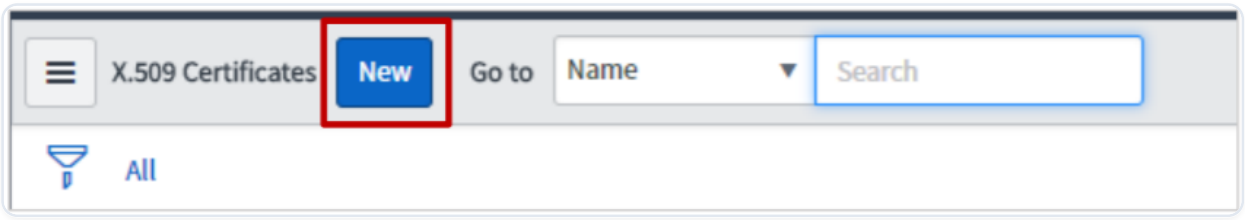


11. Klicken Sie auf **Senden**.
12. Klicken Sie im linken Bereich auf x509-Zertifikat, um das x509-Zertifikat hochzuladen.

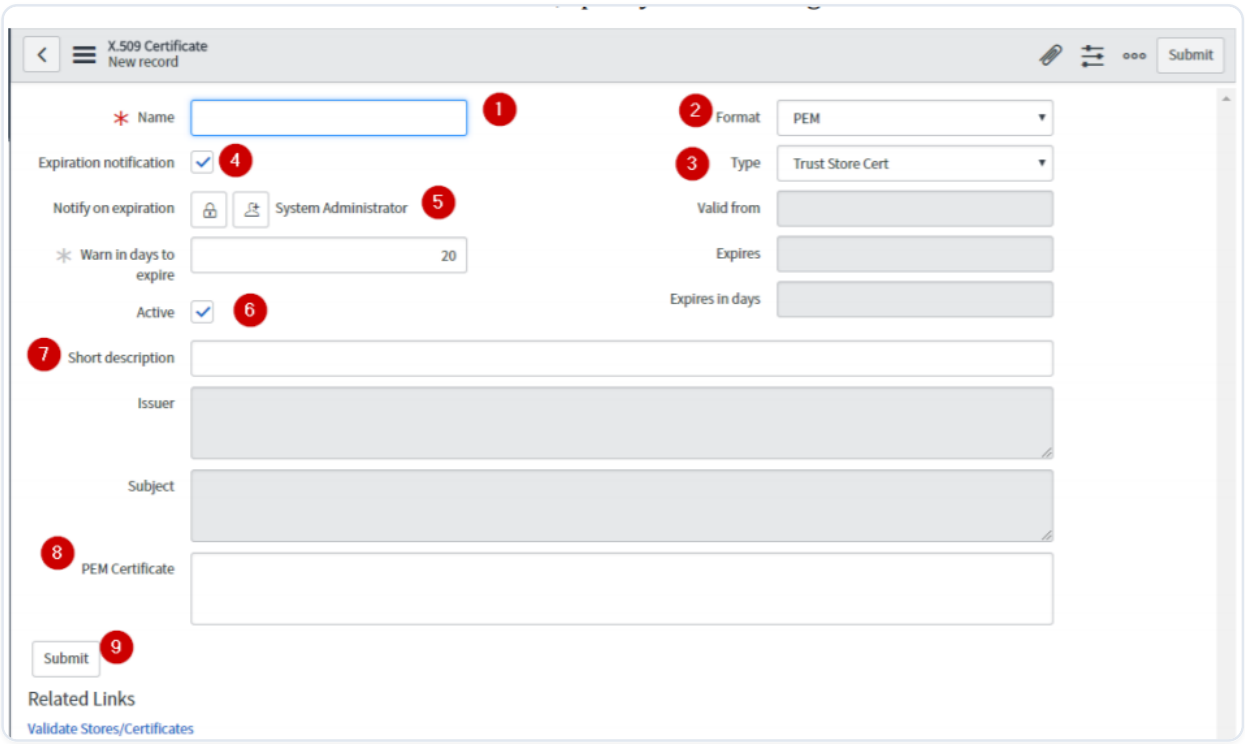


13. Klicken Sie im rechten Bereich auf **Neu**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



14. Geben Sie im Abschnitt „Neuer X.509-Zertifikat-Datensatz“ die folgenden Informationen an:



Name – Geben Sie einen Zertifikatsnamen ein.

- Format – Klicken Sie auf das entsprechende Format: zum Beispiel PEM.
- Ablaufbenachrichtigung – Aktivieren Sie das Kontrollkästchen.
- Typ – Klicken Sie auf den entsprechenden Typ.
- Bei Ablauf benachrichtigen – Klicken Sie auf das Symbol „Mich hinzufügen“, um benachrichtigt zu werden. Klicken Sie auf „Benachrichtigung bei Ablauf entsperren“, um weitere Benutzer hinzuzufügen.
- Aktiv – Aktivieren Sie das Kontrollkästchen.
- Kurzbeschreibung – Geben Sie eine Beschreibung für das Zertifikat ein.
- PEM-Zertifikat – Fügen Sie das PEM-Zertifikat ein.
    - Laden Sie das Zertifikat vom **Citrix Cloud-Assistenten (Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > Zertifikat)** herunter.
    - Kopieren Sie den Text von ——BEGIN CERTIFICATE—— bis ——END CERTIFICATE——

© 1997–2026 Citrix Systems, Inc. All rights reserved.

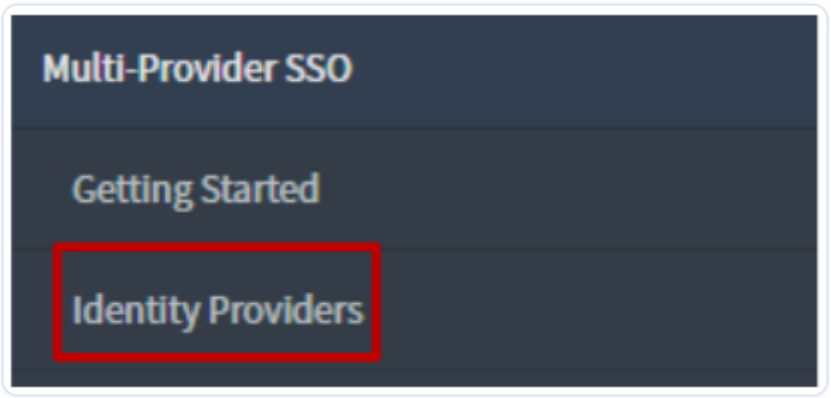
- Fügen Sie den Text in einen Texteditor ein und speichern Sie die Datei in einem geeigneten Format wie `<your organization name>.`.

Hinweis: Wenn Sie eine XML-Datei zur Konfiguration des IdP verwendet haben, müssen Sie das Zertifikat nicht konfigurieren.



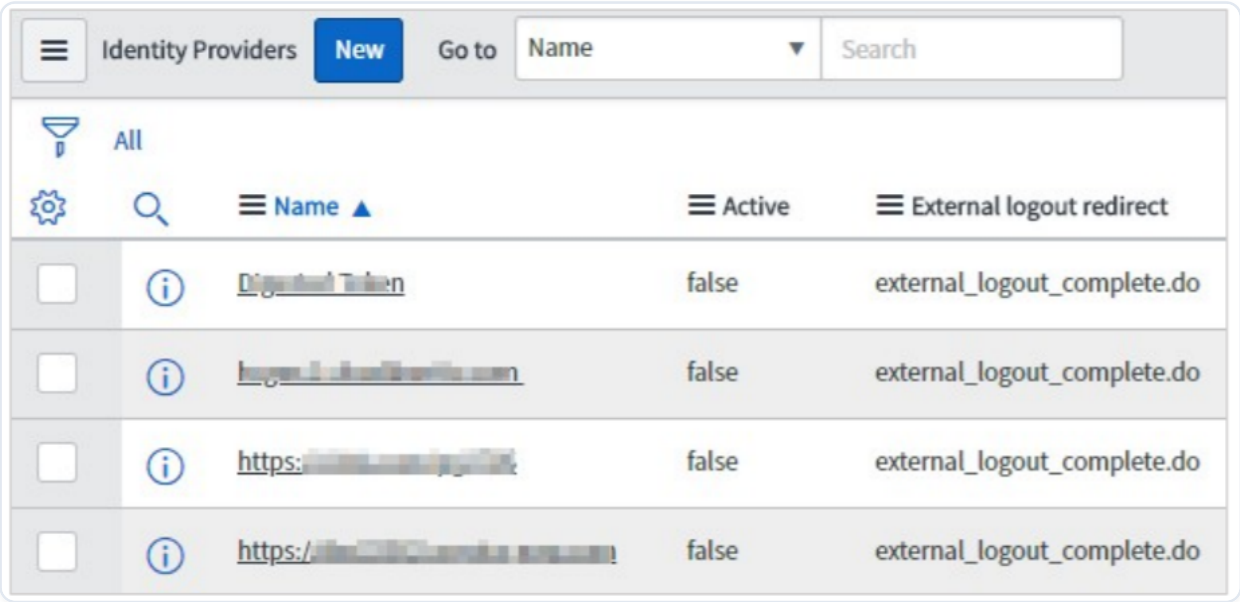
Klicken Sie auf **Senden**.

15. Klicken Sie im linken Bereich auf **Identitätsanbieter**.

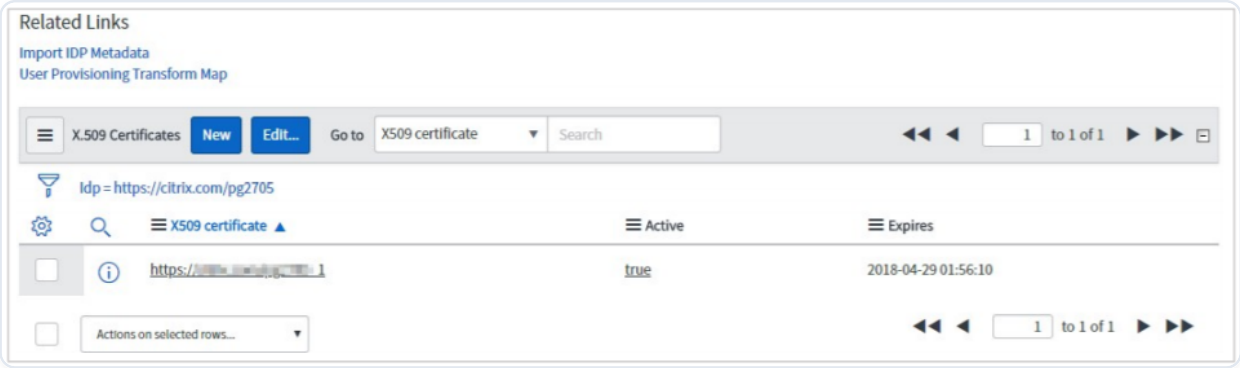


16. Klicken Sie auf den Identitätsanbieter, den Sie hinzugefügt haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

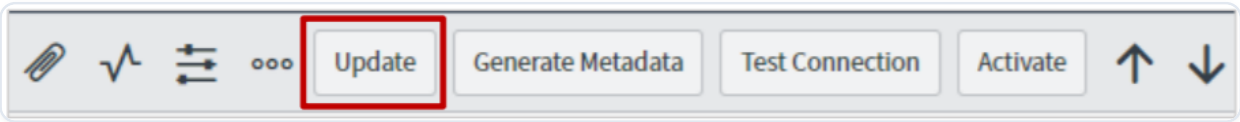


17. Auf der Detailseite des Identitätsanbieters scrollen Sie zum Abschnitt „Verwandte Links“. Suchen Sie in der Zeile „X.509-Zertifikat“ nach dem X.509-Zertifikat und fügen Sie das entsprechende Zertifikat für den Identitätsanbieter hinzu, indem Sie auf **Bearbeiten** klicken.



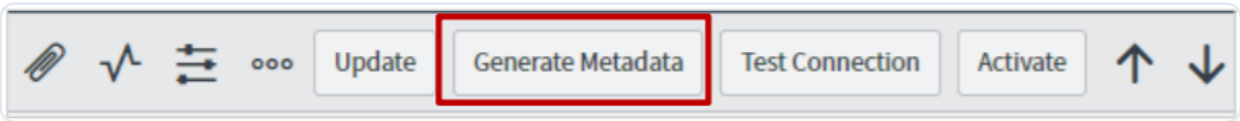
Um ein neues X.509-Zertifikat hinzuzufügen, klicken Sie auf **Neu**, und um die Zertifikate hinzuzufügen oder zu entfernen, klicken Sie auf **Bearbeiten**.

18. Klicken Sie auf der Detailseite des Identitätsanbieters auf **Aktualisieren**, um die Änderungen zu speichern.



19. Um Metadaten abzurufen, die für die IdP-Konfiguration verwendet werden sollen, klicken Sie auf **Metadaten generieren**.

    Hinweis: Sie müssen auf **Metadaten generieren** klicken, um die Aktualisierungen abzuschließen.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Metadaten des Dienstanbieters werden in einem neuen Fenster angezeigt. Sie können die Metadaten verwenden, um die Entitäten sowohl für SP als auch für IdP zu validieren.

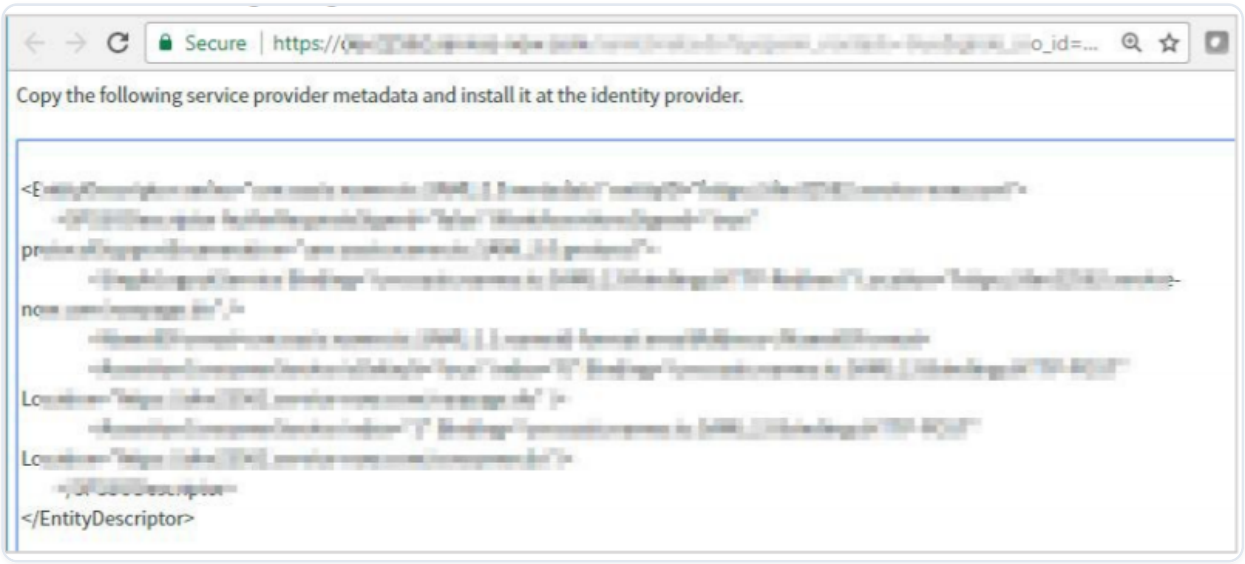
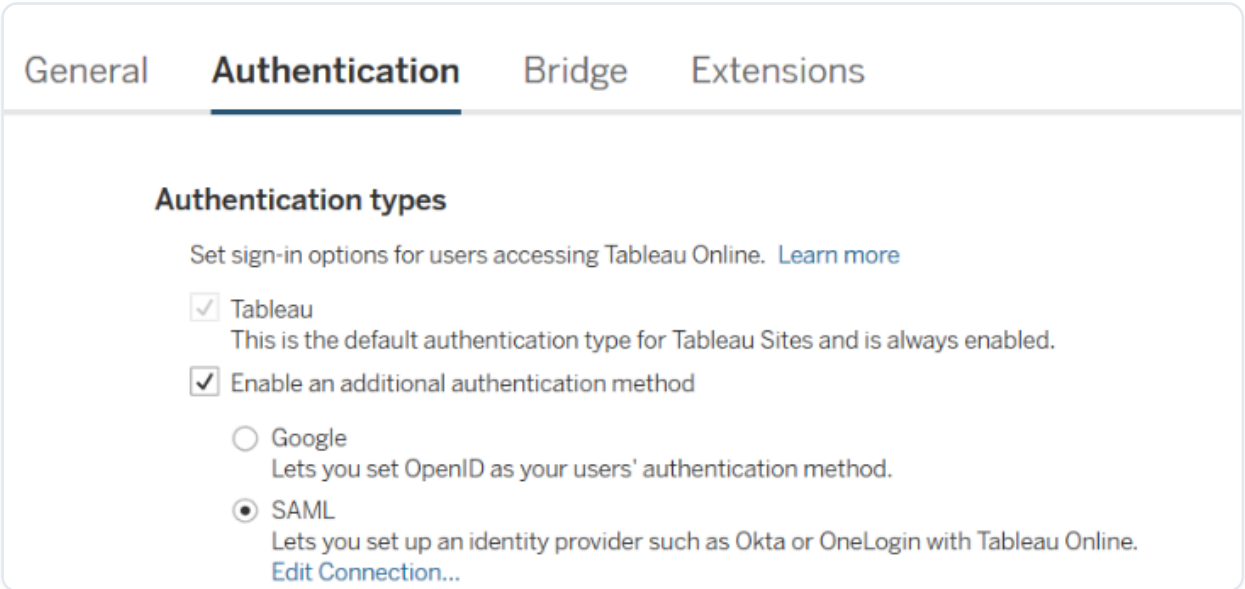


Tableau konfigurieren

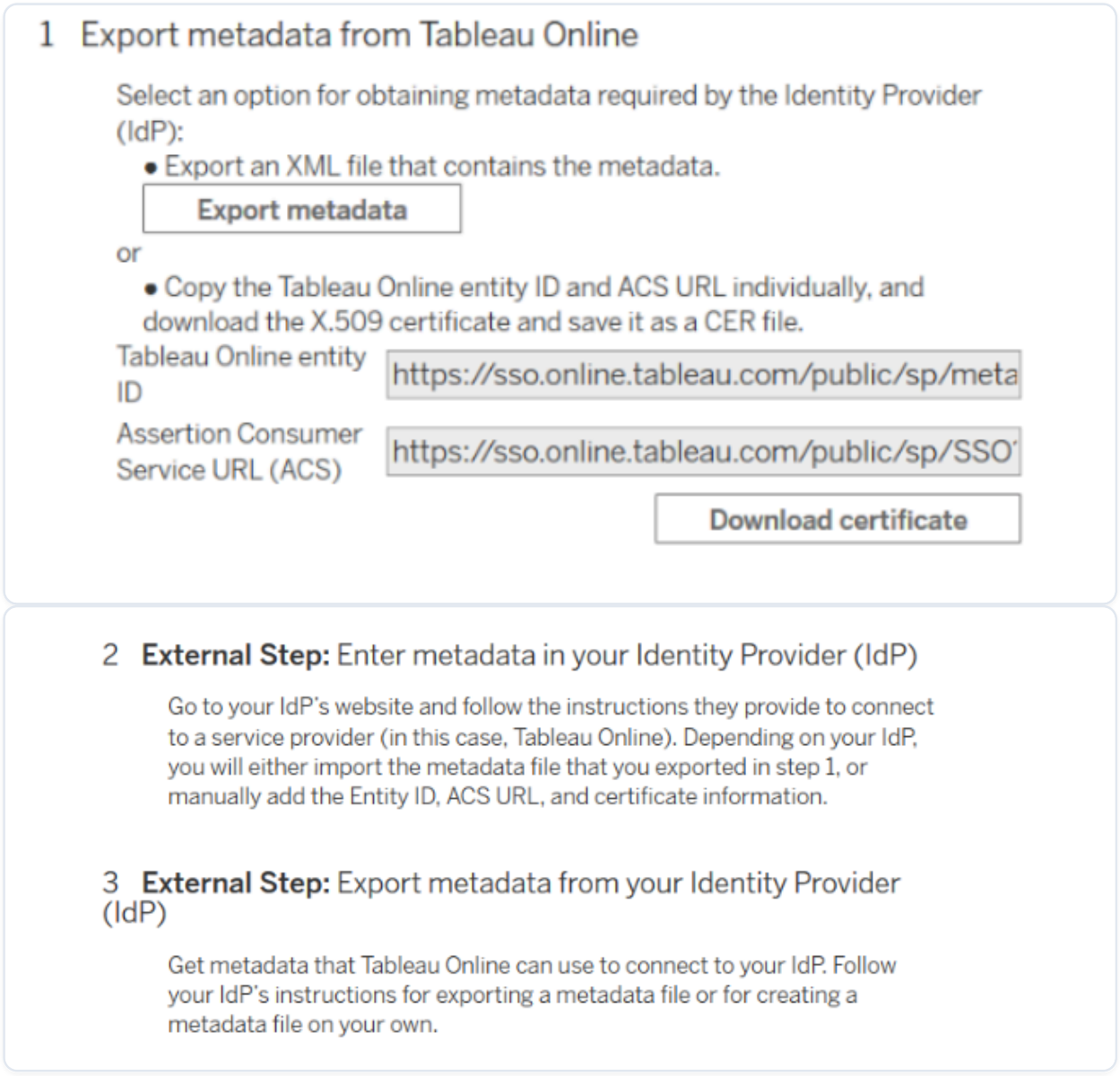
Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei Tableau anmelden.

Um Tableau für SSO über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als Administrator bei Tableau an.
2. Klicken Sie in der Menüleiste auf **Einstellungen**.
3. Klicken Sie auf **Authentifizierung**.
4. Wählen Sie unter Authentifizierungstypen **SAML** aus und klicken Sie auf **Verbindung bearbeiten**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Laden Sie die Metadatendatei vom Citrix Cloud-Assistenten herunter (**Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > SAML-Metadaten**).

HINWEIS:

- Citrix® empfiehlt, die Metadaten-XML-Datei zu importieren, anstatt sie manuell zu konfigurieren.
- Sie können das Zertifikat vom Citrix Cloud-Assistenten herunterladen (**Citrix Gateway Service > Web-/SaaS-App hinzufügen > Single Sign-On > Zertifikat**).

6. Importieren Sie die IdP-Metadatendatei in **Tableau Online**.

Metadaten importieren(/en-us/citrix-secure-private-access/media/tableau-saml-3.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Geben Sie die IdP-Entitäts-ID im Format `https://citrix.com/<customerID>` ein.
8. Klicken Sie auf **Verbindung testen**.
9. Ordnen Sie Ihre IdP-Attribute den Tableau-Attributen zu und klicken Sie dann auf **Anwenden**.

   Attribute zuordnen(/en-us/citrix-secure-private-access/media/tableau-saml-4.png)
10. Scrollen Sie nach unten und wählen Sie **SAML** als Standardauthentifizierungstyp für eine eingebettete Ansicht aus.

    Benutzer hinzufügen/auswählen(/en-us/citrix-secure-private-access/media/tableau-saml-5.png)
11. Fügen Sie Benutzer für SSO hinzu oder wählen Sie sie nach Bedarf aus.

    - Um neue Benutzer hinzuzufügen, klicken Sie auf **Benutzer hinzufügen** und geben Sie die E-Mail-Adresse ein.
    - Für bestehende Benutzer klicken Sie auf **Benutzer auswählen** und nehmen Sie die erforderlichen Änderungen vor.

Workday konfigurieren

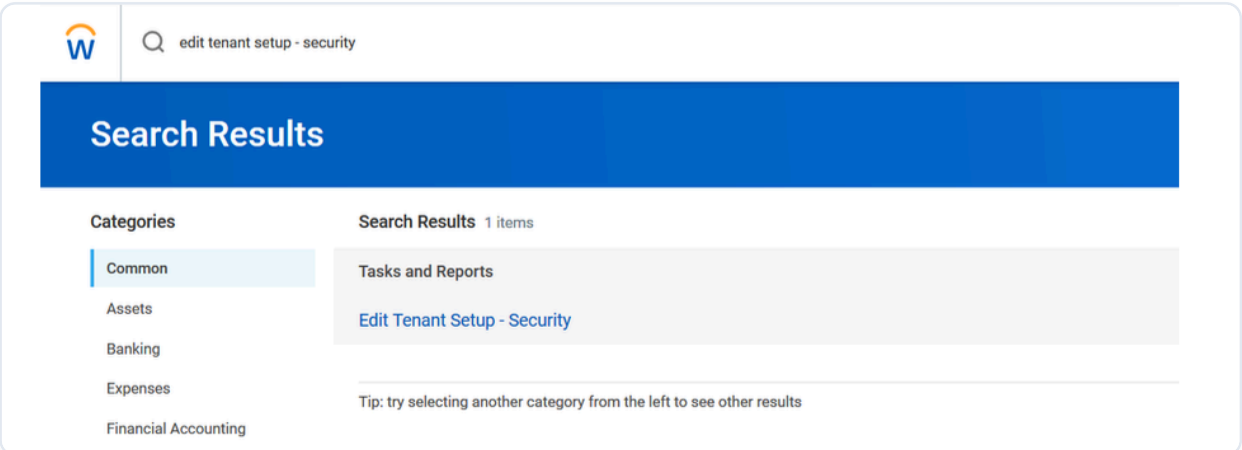
Die folgenden Abschnitte enthalten weitere Informationen zur Konfiguration von Workday.

Citrix Gateway SaaS-Anwendung

Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei Workday anmelden.

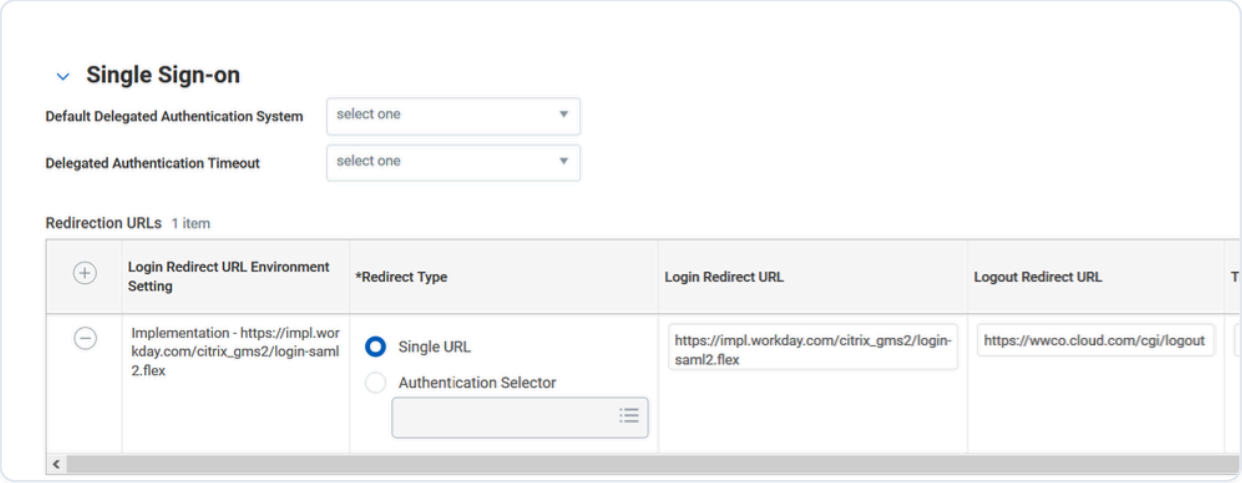
Um Workday für SSO über SAML zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als Administrator bei Workday an.
2. Navigieren Sie zu **Edit Tenant Setup - Security** und klicken Sie dann auf **Edit Tenant Setup**.

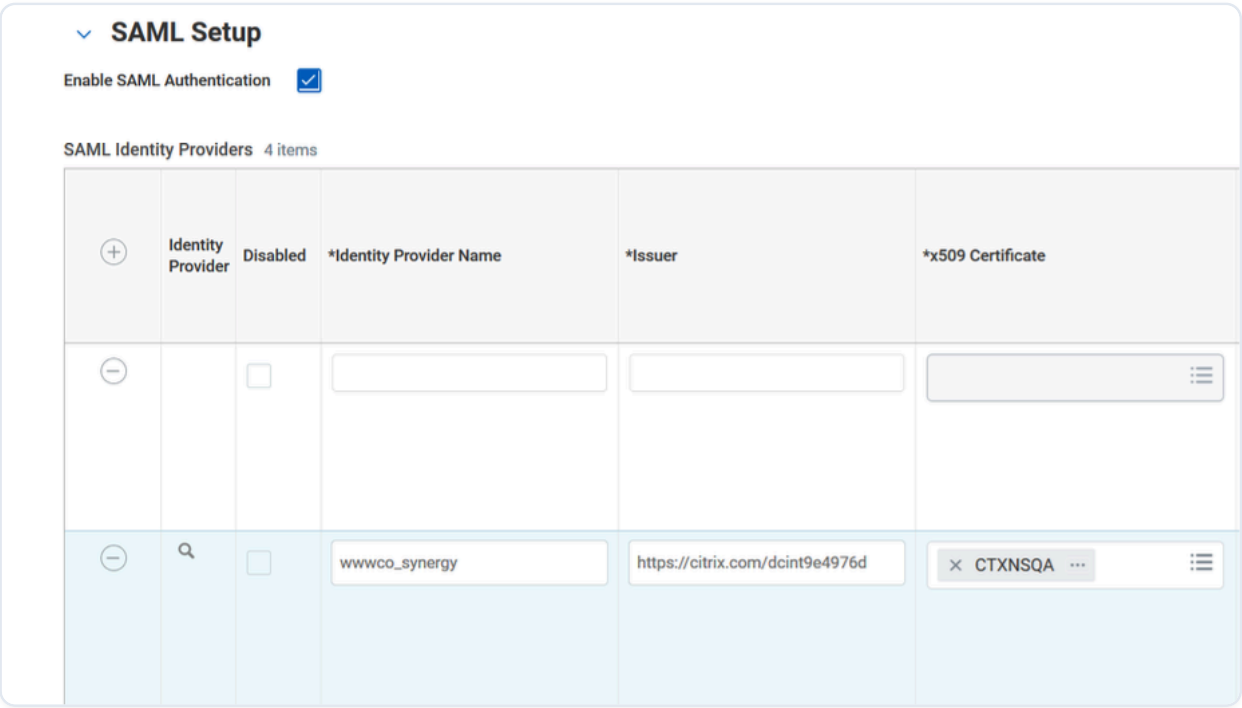


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf **Single Sign-on**.



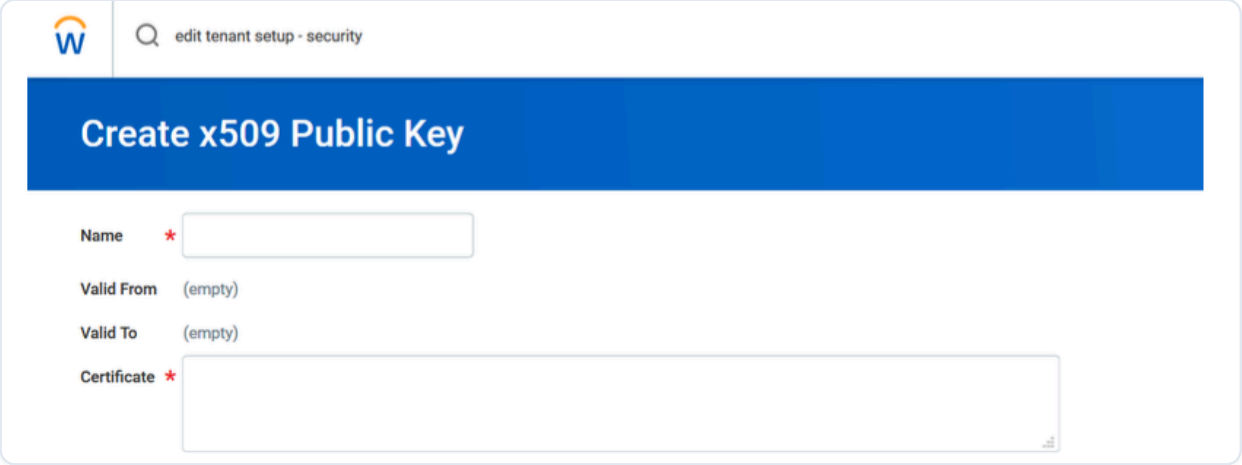
4. Klicken Sie auf das Plus-Symbol in der Tabelle „Redirection URLs“.
5. Geben Sie unter **Login Redirect URL** die URL im Format `https://impl.workday.com/<customer>/login-saml2.flex` ein.
6. Klicken Sie auf **Enable SAML Authentication**.



7. Klicken Sie unter „SAML Identity Providers“ auf das Pluszeichen (+), um eine Zeile hinzuzufügen, und geben Sie die folgenden Informationen an:
   a. **Identitätsanbietername** – geben Sie Citrix Gateway ein.
   b. **Aussteller** – geben Sie einen eindeutigen Ausstellernamen ein.
8. Klicken Sie unter **x509-Zertifikat** auf das X509-Zertifikatssymbol und dann auf **x509-öffentlichen Schlüssel erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Laden Sie das Zertifikat aus dem Citrix Cloud-Assistenten herunter (**Citrix Gateway-Dienst > Web-/SaaS-App hinzufügen > Einmaliges Anmelden > Zertifikat**).



10. Kopieren Sie den Text im Zertifikat von ——BEGIN CERTIFICATE—— bis ——END CERTIFICATE und fügen Sie das Zertifikat in das Feld „Zertifikat“ ein.
11. Klicken Sie auf **OK**.

Zoom konfigurieren

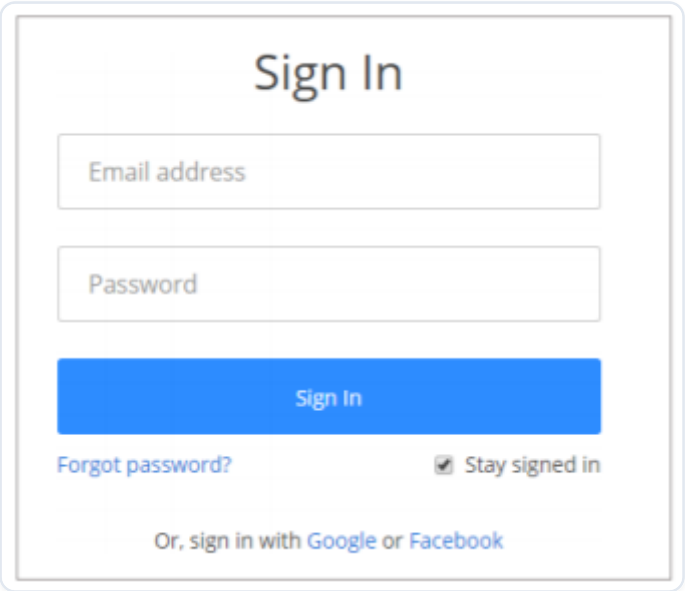
Die folgenden Abschnitte enthalten weitere Informationen zur Konfiguration von Zoom.

Citrix Gateway SaaS-Anwendung

Die Konfiguration von Zoom für SSO ermöglicht Administratoren, ihre Benutzer mit NetScaler zu verwalten. Benutzer können sich mit ihren Unternehmensanmeldeinformationen sicher bei Zoom anmelden.

1. Geben Sie in einem Browser `https://zoom.us/signin` ein und drücken Sie die Eingabetaste.
2. Melden Sie sich bei Ihrem Zoom-Konto an

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Klicken Sie auf der Seite **Mein Profil** im linken Bereich unter dem Abschnitt **Erweitert** auf **Single Sign-On**.



4. Kopieren Sie auf der Registerkarte SAML die URL, die im Feld Vanity-URL angezeigt wird. Diese URL ist für NetScaler-Konfigurationen erforderlich.
5. Geben Sie im Feld Anmeldeseiten-URL die IdP-URL Ihrer NetScaler-App ein: `https://<NetscalerGateway FQDN>/saml/login`
6. Geben Sie im Feld Abmeldeseiten-URL https:< NetScaler Gateway FQDN >.com/cgi/tmlogout ein.
7. Im Feld Identitätsanbieterzertifikat müssen Sie das Identitätsanbieterzertifikat einfügen.
8. Führen Sie die folgenden Schritte aus, um Ihr IdP-Zertifikat hochzuladen:

    - Greifen Sie remote mit PuTTY auf Ihre NetScaler-Instanz zu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Navigieren Sie zum Ordner /nsconfig/ssl (cd/nsconfig/ssl) und drücken Sie die Eingabetaste.
- Geben Sie cat certifcate-name.pem ein und drücken Sie die Eingabetaste.

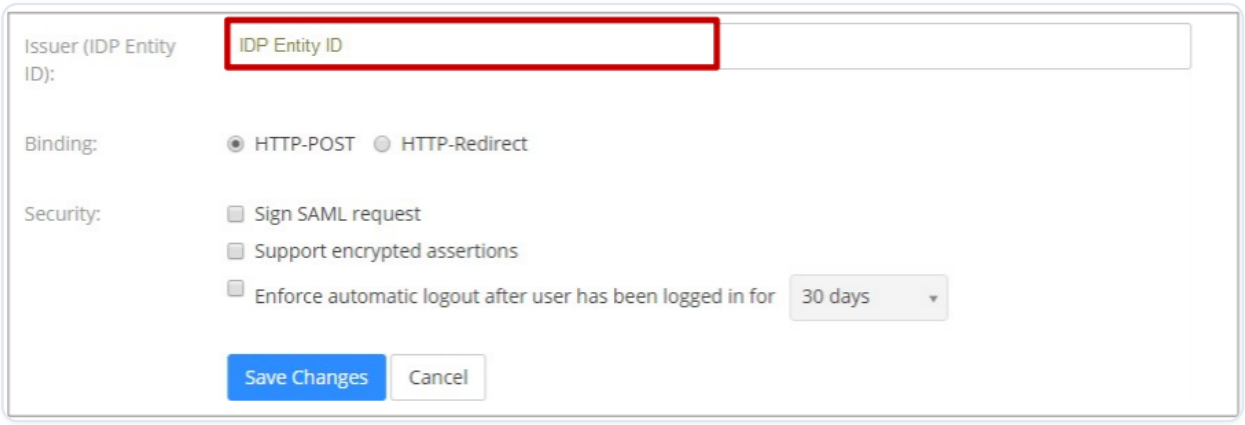
  Hinweis: Dies ist Ihr SAML IdP-Signaturzertifikat.
- Kopieren Sie den Text zwischen -----BEGIN CERTIFICATE----- und -----ENDCERTIFICATE-----



9. Kopieren Sie die URL, die im Feld Service Provider (SP) Entity ID angezeigt wird.



10. Geben Sie im Feld Issuer (IdP Entity ID) eine eindeutige Aussteller-ID ein und klicken Sie auf SaveChanges.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Richtlinienerzwingung basierend auf dem Zugriffsmodus

Die richtlinienbasierte Zugriffsmodus-Erzwingung ermöglicht es Administratoren, einzuschränken, wie ein Benutzer eine Verbindung zu einer Anwendung herstellt. Die Verbindung kann über einen browserbasierten Client oder den Citrix Secure Access Client erfolgen. Zuvor hatte Secure Private Access keine Möglichkeit, den Zugriff basierend darauf einzuschränken, welcher Client die Sitzung initiiert. Der Zugriffsmodus fügt diese Funktion hinzu.

Administratoren können beispielsweise konfigurieren, dass SSH- und RDP-Anwendungen nur über einen Browser, wie Chrome Enterprise Premium, erreichbar sind und nicht über den Citrix Secure Access Client getunnelt werden. Dies stellt sicher, dass browserbasierte Sicherheitskontrollen immer angewendet werden.

HINWEIS:

Der Zugriffsmodus ist nur eine einschränkende Bedingung. Er kann den Zugriff einschränken, aber nicht eigenständig gewähren. Alle anderen Bedingungen in der Richtlinie werden weiterhin ausgewertet.

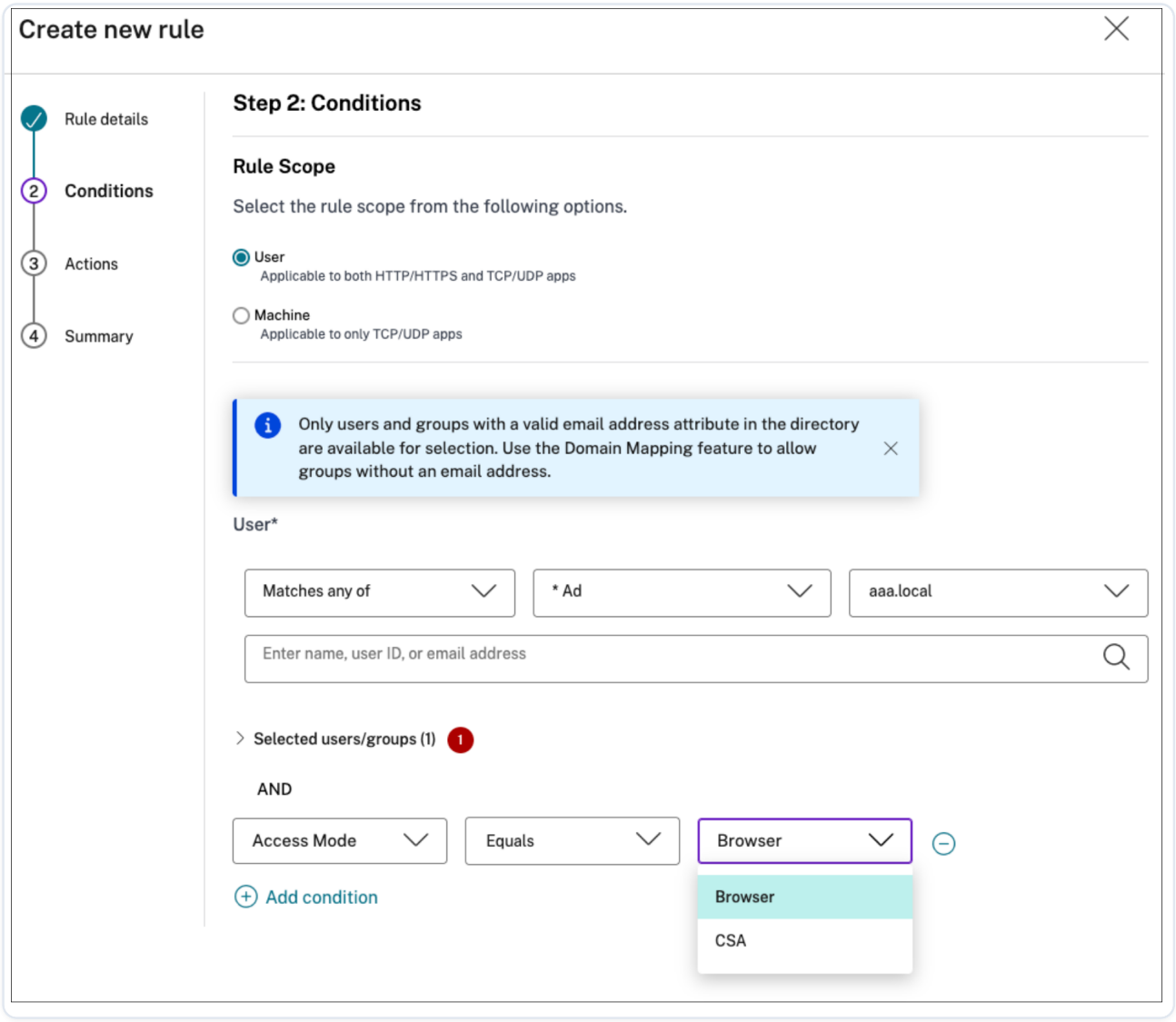
Funktionsweise

Der Zugriffsmodus wird in der Secure Private Access Admin-Konsole konfiguriert und kann einer Regel in jedem der drei Richtlinientypen hinzugefügt werden.

- Adaptive Zugriffsrichtlinie
- Sitzungsrichtlinie
- Browserrichtlinie

Die folgende Abbildung zeigt eine Beispielbedingung für eine Zugriffsrichtlinienregel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Endbenutzererfahrung

Basierend auf dem Zugriffsmodus ist die Anwendungsaufzählung und der Start entweder erlaubt oder eingeschränkt.

- **Passender Client** — Die Anwendung wird aufgelistet und startet normal.
- **Nicht übereinstimmender Client** — Die Anwendung wird während der Enumeration nicht in der App-Liste angezeigt, und ein Startversuch wird blockiert. Der Benutzer wird zur Standardseite für Zugriffsverweigerung weitergeleitet. Es wird keine neue Ablehnungsmeldung eingeführt.
- **Nicht bestimmbare Sitzung** — Wenn der Zugriffsmodus nicht bestimmt werden kann (zum Beispiel einige mobile Secure Access-Sitzungen), wird die Zugriffsmodusbedingung übersprungen und die Sitzung bleibt unbeeinflusst. Alle anderen Bedingungen gelten weiterhin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

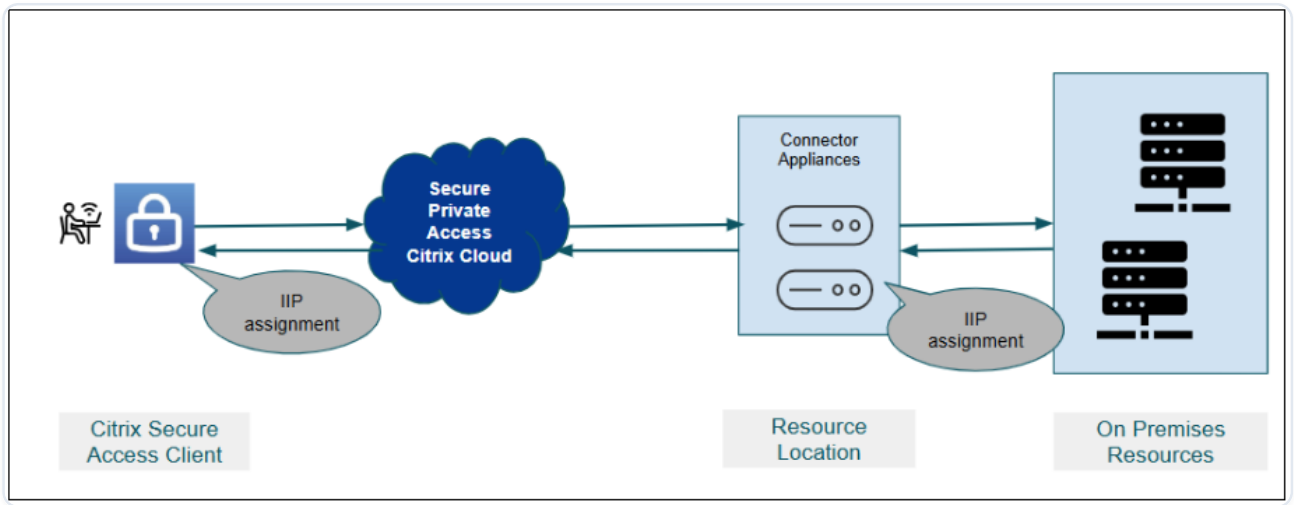
Unterstützung für Server-zu-Client-Verbindungen – Vorschau

In einer traditionellen Client-Server-Einrichtung können die Remote-Benutzer über HTTP-, TCP- und UDP-Verbindungen auf Ressourcen an Kundenressourcenstandorten zugreifen. Es gibt jedoch Szenarien, in denen der Server oder das Back-End-System eine Verbindung mit den Remote-Client-Geräten (z. B. Laptops, Smartphones, Tablets) initiieren muss, für Aufgaben wie Push-Konfigurationen, Remote-Unterstützung, Anwendungszugriff oder App-Installation, unter Wahrung des Benutzerdatenschutzes und der Sicherheit. Secure Private Access unterstützt Server-zu-Client-Verbindungen, wobei die Server am Ressourcenstandort des Kunden eine TCP/UDP-Verbindung mit dem Remote-Client herstellen können.

- Um die Server-zu-Client-Verbindung zu ermöglichen, führt Secure Private Access die Server-zu-Client-App ein. Diese App kann mit den Client-Details (Port, Protokoll) und dem IP-CIDR-Bereich des Back-End-Servers konfiguriert werden.
- Nachdem der Server-zu-Client-App-Typ erstellt wurde, müssen dann entsprechende Zugriffsrichtlinien für diese Anwendungen konfiguriert werden, um Server-zu-Client-Verbindungen zu ermöglichen.

So funktioniert die Server-zu-Client-Verbindung

Das folgende Diagramm zeigt eine Beispielarchitektur für Server-zu-Client-Verbindungen.



Die folgenden Schritte veranschaulichen den Workflow der Server-zu-Client-Verbindung:

1. Wenn sich ein Benutzer beim Citrix Secure Access™ Client anmeldet, wird dem Benutzer eine interne IP-Adresse aus dem zugewiesenen internen IP-Adresspool des Clients zugewiesen. Diese Zuweisung basiert auf dem konfigurierten Ressourcenstandort, IP-CIDR und Benutzerkontext in der IP-Adresspool-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Diese zugewiesene IP-Adresse wird dann mit einer bestimmten Connector Appliance innerhalb des konfigurierten Ressourcenstandorts und IP-Pools verknüpft. Diese Connector Appliance besitzt und verwaltet Verbindungen im Zusammenhang mit dieser IP-Adresse für den Back-End-Kundenressourcenstandort.
3. Der Back-End-Server initiiert eine TCP/UDP-Verbindung zum Remote-Client unter Verwendung der zugewiesenen internen Client-IP-Adresse über den Port der Client-Anwendung, der in der Server-zu-Client-Anwendungskonfiguration angegeben ist.
4. Der Connector kommuniziert mit Secure Private Access, um eine Verbindung mit dem Client herzustellen.
5. Secure Private Access überprüft, ob der Back-End-Server in der Server-zu-Client-Anwendung konfiguriert ist, und bewertet dann die relevante Zugriffsrichtlinie, um zu bestimmen, ob der Zugriff auf den Client-Computer zugelassen oder blockiert werden soll.
6. Wenn die Richtlinie den Zugriff zulässt, verbindet sich Secure Private Access mit dem Remote-Client-Computer. Wenn der Client-Computer einer Domäne beigetreten ist, wird der FQDN dieses Computers bei der IIP-Adresse registriert. Der Computer kann entweder über den FQDN oder die interne IP-Adresse aufgerufen werden.
7. Wenn sich ein Benutzer abmeldet, wird die zugewiesene interne IP-Adresse sowohl von der Connector Appliance als auch von der aktiven Sitzung freigegeben. Wenn sich derselbe Benutzer innerhalb von 15 Tagen erneut anmeldet, erhält der Benutzer dieselbe IP-Adresse, andernfalls wird sie für die Nutzung durch andere Benutzer freigegeben.

Eine Server-zu-Client-App erstellen

Die folgenden Abschnitte enthalten Details zur Erstellung einer Server-zu-Client-App.

Voraussetzungen

- Der interne IP-Adresspool des Clients wird erstellt. Der IP-Adresspool ist unerlässlich, um einem Benutzer und dem zugehörigen Gerät eine eindeutige IP-Adresse zuzuweisen. Weitere Informationen finden Sie unter Interne Client-IP-Adresspools.
- Der Administrator des Kunden muss ein freies Intranet-IP-CIDR-Subnetz für das Ressourcenstandortnetzwerk zuweisen. Dieses IP-CIDR darf nicht mit anderen Ressourcen-IP-Adressen in Konflikt stehen.
- Der Administrator des Kunden muss festlegen, welcher Gruppe/welchem Kontext Benutzern die Intranet-IP-Adresse von welchem Ressourcenstandort zugewiesen wird. Es wird empfohlen, ein Benutzer-zu-IP-Adress-Verhältnis von 1:3 beizubehalten. Das heißt, wenn sich 1000 Benutzer anmelden, wird empfohlen, 3000 IP-Adressen im Client-IP-Pool zuzuweisen.

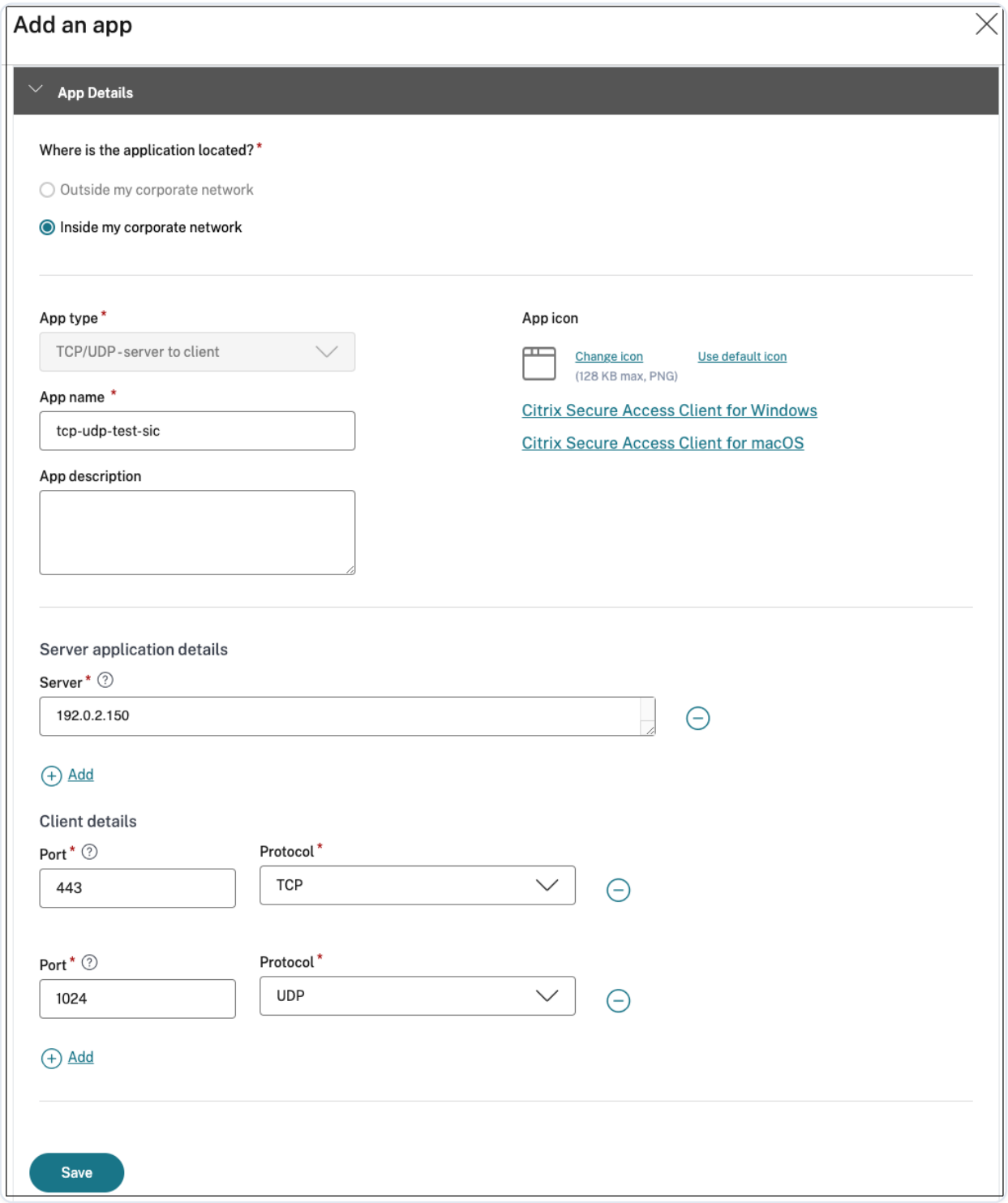
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Das freie IIP-Subnetz und die primäre IP-Adresse des Connectors müssen zum selben Netzwerk und Subnetz gehören.
- Zwischen den Ressourcenstandorten müssen Verbindungen aufrechterhalten werden, damit Server an anderen Standorten (die nicht im IP-Pool konfiguriert sind) eine Verbindung zum Client herstellen können.
- Stellen Sie sicher, dass Sie die Citrix Secure Access Client-Versionen verwenden, die Server-zu-Client-Apps unterstützen.
  - Windows 24.11.1.17 und höher
  - macOS 25.01.1 und höher
  - Linux 25.2.2 und höher

Führen Sie die folgenden Schritte aus, um Server-zu-Client-TCP/UDP-Apps zu konfigurieren

1. Melden Sie sich bei Citrix Cloud an und wählen Sie **Secure Private Access**.
2. Klicken Sie auf **Anwendungen > App-Konfiguration** und dann auf **App hinzufügen**.
3. Klicken Sie im Abschnitt **Vorlage auswählen** auf **Überspringen**. Vorlagen sind nur für SaaS-Apps verfügbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Wählen Sie den Speicherort **Innerhalb meines Unternehmensnetzwerks**.
5. Geben Sie die folgenden Details ein:

   - **App-Typ** – Wählen Sie **TCP/UDP - Server zu Client**.
   - **App-Name** – Name der Anwendung.
   - **App-Beschreibung** – Beschreibung der App, die Sie hinzufügen. Dieses Feld ist optional.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Server** – IP-Adressbereich des Back-End-Servers, der eine Verbindung mit dem Client-Computer herstellen kann. Dadurch wird sichergestellt, dass nur die Server mit IP-Adressen innerhalb dieses Bereichs auf die Ports des Clients zugreifen können.
- **Port** – Die Portnummer des Client-Computers, zu der der Back-End-Server eine Verbindung initiieren kann.
- **Protokoll** – TCP oder UDP.

6. Klicken Sie auf **Hinzufügen**, um weitere Server und Ports hinzuzufügen.
7. Klicken Sie auf **Speichern**. Die App wird der Seite **App-Konfiguration** hinzugefügt.

Sie können eine App auf der Seite „Anwendungen“ bearbeiten oder löschen, nachdem Sie die Anwendung konfiguriert haben. Klicken Sie dazu auf die Schaltfläche mit den Auslassungspunkten in der Zeile der App und wählen Sie die entsprechenden Aktionen aus.

Nachdem Sie die Server-zu-Client-App erstellt haben, erstellen Sie Zugriffsrichtlinien gemäß den Anforderungen.

HINWEIS:

Alle bestehenden Zugriffsrichtlinien werden für Server-zu-Client-Anwendungen unterstützt. Der Server-zu-Client-Zugriff ist Benutzern gestattet, deren Kontext für die konfigurierte Zugriffsrichtlinie als „Zulassen“ bewertet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.