DATENBLATT

Zscaler™ Client Connector

Schneller, sicherer und zuverlässiger Zugriff auf alle Anwendungen von jedem Standort oder Gerät aus – mit einer einzigen Anwendung

Heute arbeiten User an wechselnden Standorten und greifen über verschiedene Geräte auf Anwendungen in der Cloud und im Rechenzentrum zu. Diese neuartigen hybriden Arbeitskonzepte setzen einen schnellen, reibungslosen und vor allem standortunabhängigen Zugriff auf Unternehmensanwendungen voraus. Flexibilität darf dabei nicht auf Kosten der Sicherheit gehen. Deswegen setzen IT-Experten auf Zscaler – und insbesondere den Zscaler Client Connector –, um sicherzustellen, dass die Mitarbeiter jederzeit und überall auf alle erforderlichen Daten zugreifen können.

Früher saß die Mehrzahl der User in Präsenzarbeit am Unternehmensstandort. Zur Sicherung ihres Zugriffs aufs Internet und Geschäftsanwendungen kamen netzwerkbasierte Kontrollen zum Einsatz. Inzwischen geht der Trend zunehmend zu dezentralen Belegschaften. Dadurch haben IT-Teams keine Kontrolle mehr über die Netzwerke, die Mitarbeiter zum Zugriff auf Unternehmensressourcen nutzen, und somit auch keine Informationen darüber, wer im Einzelnen worauf zugreift.

Hybride und dezentrale Arbeitskonzepte setzen voraus, dass User, die im Homeoffice oder auch im Café arbeiten, genauso reibungslos auf alle benötigten Ressourcen zugreifen können wie ihre Kollegen im Büro. Zugangskontrollen, die im Rechenzentrum installiert sind, stellen hier keine optimale Lösung dar. Sinnvoller ist es, sie global möglichst nahe an den jeweiligen Standorten der User bereitzustellen. Stattdessen verlassen sich viele IT-Teams weiterhin auf VPNs, die Usern Zugang zum Unternehmensnetzwerk gewähren. Das verstößt gegen das Prinzip der minimalen Rechtevergabe und erhöht das Risiko einer lateraler Verbreitung von Bedrohungen. Zudem werden durch das Backhauling von Remote-Usern zum Rechenzentrum Latenzen verursacht. Zukunftsorientierte Ansätze erfordern User-zentrische Zugangskontrollen, die Zugriff nicht anhand der IP-Adresse, sondern basierend auf der Identität des Users gewähren.

Eine weitere entscheidende Voraussetzung für den Erfolg dieser neuen Arbeitsformen ist die Bereitstellung von Zugriffsdiensten, die alle gängigen Gerätetypen und Netzwerke unterstützen. Von Laptops und Smartphones über POS-Systeme (Point-of-Sale) bis hin zu RF-Scannern nutzen User eine Vielzahl von Geräten für ihre Arbeit. Entsprechend benötigen sie überall gleichermaßen zügigen und sicheren Zugriff auf Geschäftsanwendungen.

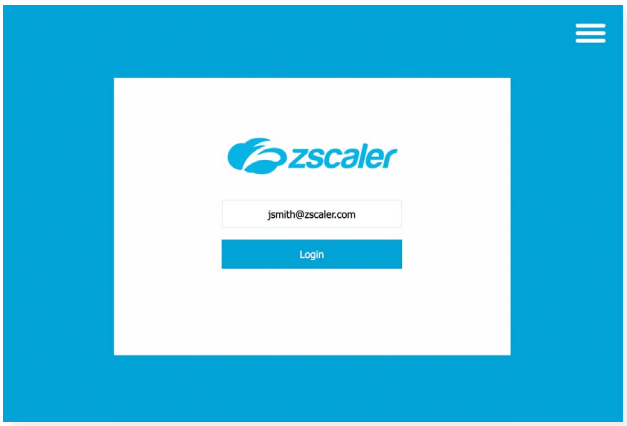
Mitarbeiter und Geschäftspartner des Unternehmens benötigen die Flexibilität, geeignete Geräte ihrer Wahl zur Erledigung ihrer Arbeit einzusetzen. Daher können IT-Teams nicht länger auf Legacy-Lösungen setzen. Zukunftsfähige Arbeitskonzepte erfordern neue Ansätze zur Vereinfachung des sicheren standort- und geräteunabhängigen Zugriffs auf Unternehmensressourcen.

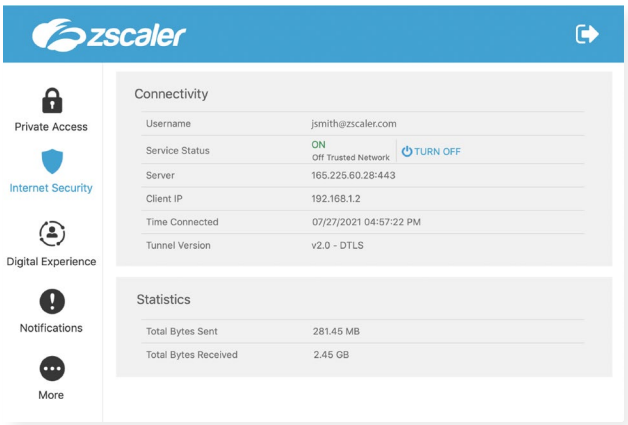
Zscaler Client Connector

Eine einzige Anwendung für Zero-Trust-Zugriff auf alle Unternehmensressourcen
Zscaler Client Connector ist im Leistungsumfang von Zscaler Internet Access™ (ZIA™) und Zscaler Private Access™ (ZPA™) inbegriffen. Client Connector läuft als ressourcenschonende Anwendung auf dem Endgerät des Users und leitet den gesamten User-Traffic automatisch zum nächstgelegenen Zscaler Service Edge weiter. Durch die Bereitstellung in über 150 Rechenzentren weltweit wird die einheitliche Durchsetzung von Sicherheits- und Zugriffsrichtlinien für alle Geräte, Standorte und Anwendungen ohne Beeinträchtigung der User Experience gewährleistet. Zscaler Client Connector erkennt automatisch, ob User auf das Internet, eine SaaS-Anwendung oder eine interne Anwendung zugreifen wollen, und leitet den Traffic entsprechend entweder an Zscaler Internet Access oder Zscaler Private Access weiter.

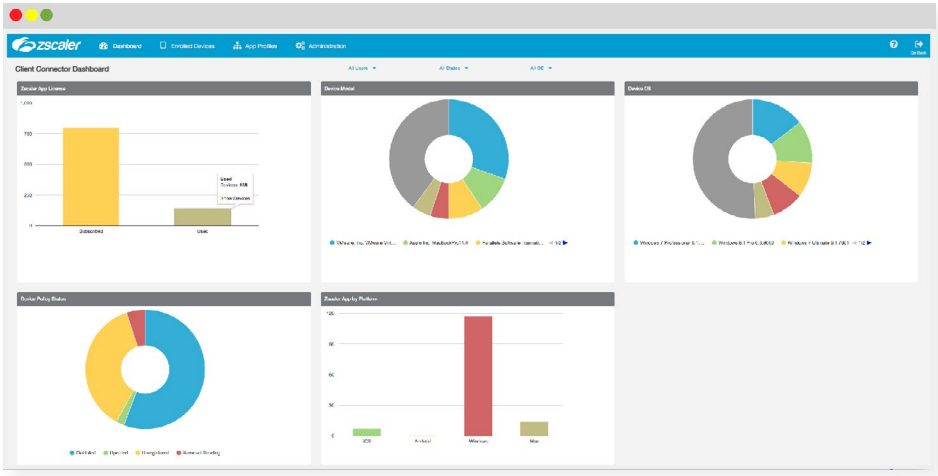
Reibungsloser Zugriff für End-User
User können von jedem beliebigen Gerät aus ohne komplizierte Anmeldeverfahren auf geschäftskritische Anwendungen zugreifen. Die Einrichtung eines VPN bei jeder Verbindung zu einem neuen Netzwerk entfällt. Als zusätzliche Vereinfachung kann der Client Connector zur Gewährleistung einer reibungslosen Authentifizierung mit Identitäts- und MFA-Anbietern integriert werden.

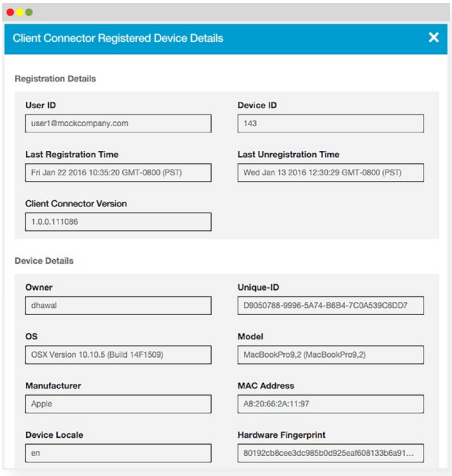
Durch die automatische Weiterleitung des Traffics zum nächstgelegenen Zscaler Service Edge wird der sichere Zugriff auf das Internet sowie SaaS- und interne Anwendungen möglichst nahe am Standort des jeweiligen Users bereitgestellt. Zur Herstellung der Verbindung sind keine PAC-Dateien, IPsec-VPNs, Authentifizierungs-Cookies oder zusätzliche Maßnahmen seitens des End-Users erforderlich.





Transparenz und Kontrolle für die IT
Das Admin-Portal des Zscaler Client Connector bietet IT-Teams neuartige Möglichkeiten zur Einblicknahme in und Verwaltung von Gerätedaten. Die optionale Integration mit Zscaler Digital Experience liefert zusätzliche Informationen über die Performance einzelner Anwendungen, Netzwerke und Geräte, die insbesondere für IT-Administratoren und Servicedesk-Mitarbeiter von hohem Interesse sind.





Vorteile des Client Connector

Hervorragende User Experience durch intelligente Weiterleitung des Traffics
Client Connector leitet den Traffic von Mobilgeräten automatisch über den optimalen Pfad zum nächstgelegenen Zscaler-Edge-Standort. Zudem werden vertrauenswürdige Netzwerke und Zugangsportale erkannt und die User Experience entsprechend priorisiert.

Verbesserte Einblicke in User-Aktivitäten und Device Posture
Im Admin-Portal des Zscaler Client Connector erhalten IT-Administratoren Informationen zu allen Usern, Geräten und Richtlinien speziell für Client Connector. Das zentrale Dashboard liefert eine ganzheitliche Übersicht über alle eingesetzten Geräte und ermöglicht die Einrichtung granularer Richtlinien für einzelne Geräte.

Einfaches Onboarding mit Bereitstellung im Hintergrund über MDM
Der Client Connector kann im Hintergrund über MDM-Lösungen, Microsoft Intune, LDAP oder ADFS bereitgestellt werden, um die Beeinträchtigung der User Experience auf den Endgeräten zu minimieren. Die Installierung, Registrierung und Überprüfung der SSL-Zertifikate erfolgt automatisch ohne erforderliche Maßnahmen seitens des Users.

Erzwungene Registrierung
Vor dem Zugriff auf Anwendungen kann die IT die Registrierung von Benutzergeräten erzwingen. Zur Absicherung des gesamten Traffics können User daran gehindert werden, den Client Connector zu deaktivieren.

Device Posture und Fingerprinting für kontextbezogene Zugriffs- und Sicherheitskontrollen
Durch die Integration mit Anbietern von Sicherheitslösungen für Endgeräte (u. a. Microsoft, CrowdStrike und VMware Carbon Black) kann Client Connector kontextbezogene Sicherheitskontrollen durchsetzen. Dazu werden variable Kriterien wie der Gerätezustand, das Betriebssystem und die Präsenz einer aktiven Sicherheitslösung überprüft. Durch die Verknüpfung von User-Zugangsdaten mit einem bestimmten Gerät kann eine zusätzliche Sicherheitsschicht eingebaut werden, um den Zugriff verdächtiger bzw. infizierter Geräte auf vertrauliche Daten zu verhindern.

Unterstützung gängiger Gerätetypen und Betriebssysteme
Zscaler Client Connector unterstützt die meisten Gerätetypen, einschließlich Laptops, Smartphones, Tablets, POS-Systeme und RF-Scanner (mobile Computer) auf gängigen Plattformen wie iOS, Android, Windows, MacOS, CentOS und Ubuntu 20.04.

Zscaler Client Connector (ehemals Zscaler App oder Z App) ist eine ressourcenschonende Anwendung, die auf dem Endgerät des Users installiert wird und den gesamten Traffic automatisch durch die Zscaler Zero Trust Exchange™ leitet, um Richtlinien und Zugriffskontrollen durchzusetzen und gleichzeitig die Leistung zu verbessern.

GESCHÄFTSNUTZEN

- Zero-Trust-Richtlinien werden konsequent durchgesetzt – unabhängig vom Gerät und Standort des Users und von der jeweiligen Anwendung
- Die User Experience wird verbessert und der Anwendungszugriff optimiert
- Richtlinienänderungen werden durch zentrale Verwaltung umgehend global durchgesetzt
- Die IT kann die Aktivitäten von Usern und Geräten verfolgen und überwachen
- Unterstützt die meisten gängigen Betriebssysteme und Gerätetypen (Laptops, Smartphones, Tablets usw.)

UNTERSTÜTZTE SYSTEME

- iOS 9 oder höher
- Android 5 oder höher
- Windows 7 oder höher
- Mac OSX 10.10 oder höher
- CentOS 8
- Ubuntu 20.04

Erste Schritte

Der einstufige Registrierungsvorgang vereinfacht das Deployment von Client Connector. Für die Bereitstellung auf Laptops ist die IT zuständig. Die App für Mobiltelefone und Tablets kann im Apple- und Google-Play-Store heruntergeladen und von den Usern selbst installiert werden. Durch sofortige Multi-Faktor-Authentifizierung bei Anmeldung über Single Sign-On (SSO) wird die Sicherheit durch eine zusätzliche Schicht verstärkt. Unsere Schritt-für-Schritt-Anleitung enthält alle erforderlichen Informationen zur Bereitstellung und Konfiguration Zscaler Client Connector.

Client Connector installieren

Client Connector für Laptops

Windows/macOS/Linux

Für Windows/macOS/Linux zuständigen Administrator kontaktieren

Client Connector für Smartphones und Tablets

iOS | Jetzt herunterladen

Android | Jetzt herunterladen

CLIENT CONNECTOR	LAPTOP			MOBILTELEFONE/TABLETS	
Betriebssystem	Win	Mac	Linux	Android	iOS
ZDX	✓	✓			
TWLP	✓	✓	✓		
Tunnel 1.0	✓	✓	✓	✓	✓
Tunnel 2.0	✓	✓	✓		
Paketfilter-Modus	✓				
Routenbasierter Modus	✓	✓	✓	✓	✓
Device Posture	✓	✓	✓ *In begrenztem Umfang	✓	✓
CLI-basierter Client					
FIPS	✓	✓	✓		
ZPA mit Drittanbieter-VPN	✓	✓	✓ *Validiert für Pulse; Validierung für AnyConnect steht noch aus		✓
Remote-Abruf von Protokollen	✓	✓		✓	
Integrierte Paketerfassung	✓	✓	✓		
DTLS für ZIA	✓	✓	✓		
DTLS für ZPA	*Demnächst verfügbar	*Demnächst verfügbar	*Demnächst verfügbar	*Demnächst verfügbar	*Demnächst verfügbar
Client Connector kann SSL-Zertifikat für die SSL-Überprüfung installieren	✓	*Apple hat die Sicherheitsrichtlinien geändert	✓		
Integrated Windows Authentication (IWA)	✓	✓	✓	✓	✓
Client Connector kann automatisch einen erneuten Anmeldeversuch für SSO durchführen	✓	✓			
CRWD-Posture-Überprüfung	✓	✓			
Konsequente Durchsetzung	✓	✓	✓		

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408 533 0288
www.zscaler.com