FICHE TECHNIQUE

Zscaler™ Client Connector

Accès rapide, sécurisé et fiable à toutes les applications, quel que soit l'emplacement ou l'appareil, à partir d'une seule application

De nos jours, les utilisateurs sont partout et accèdent à toutes leurs applications — dans le cloud et le data center — en utilisant tous leurs appareils. Cette main-d'œuvre nouvelle et hybride a besoin d'un accès rapide et transparent aux applications professionnelles, mais cette rapidité ne doit pas être obtenue au risque de mettre en péril les données de l'entreprise. Les leaders informatiques se sont tournés vers Zscaler et Zscaler Client Connector, pour les aider à connecter les utilisateurs aux données dont ils ont besoin pour faire leur travail.

Dans le passé, la majorité des utilisateurs travaillaient au bureau, et il était donc logique de s'appuyer sur des contrôles basés sur le réseau pour permettre aux utilisateurs d'accéder à Internet et aux applications professionnelles. Mais aujourd'hui, le personnel peut se trouver n'importe où, et les équipes informatiques n'ont plus la maîtrise des réseaux utilisés par les employés, de sorte qu'elles manquent de visibilité sur ce à quoi les utilisateurs accèdent.

Comme les utilisateurs ont besoin de la même expérience d'accès depuis leur domicile ou un café que lorsqu'ils sont au bureau, les contrôles d'accès ne devraient plus être ancrés dans le data center. Ils devraient être répartis partout dans le monde et aussi proches que possible de l'utilisateur. Pourtant, de nombreuses équipes continuent de compter sur les VPN, qui font transiter les utilisateurs par un data center, les plaçant sur le réseau d'entreprise, ce qui augmente le risque de mouvement latéral et d'accès trop privilégié. Au lieu d'accorder l'accès sur la base d'une adresse IP, les contrôles devraient être centrés sur l'utilisateur, liés à l'identité d'un utilisateur authentifié.

Le télétravail implique également que les services d'accès doivent être suffisamment souples pour s'étendre à tous les appareils des utilisateurs, quel que soit le réseau. Ordinateurs portables, smartphones, systèmes de points de vente (POS), scanners RF : tous ces appareils sont utilisés à des fins professionnelles et nécessitent tous des connexions rapides et sécurisées aux applications métier.

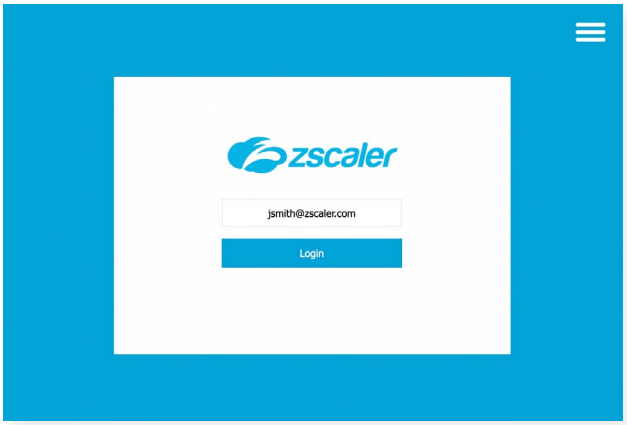
Pour aider les employés et les partenaires à se servir d'un large éventail d'appareils pour accomplir leur tâche, le service informatique doit abandonner les anciennes solutions et chercher à simplifier l'accès grâce à une nouvelle approche de la connectivité.

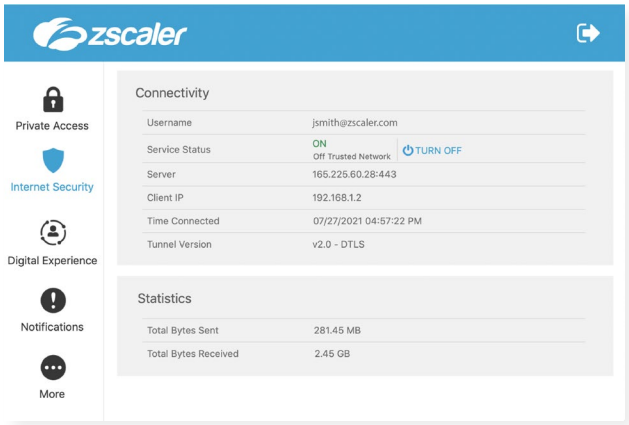
Zscaler Client Connector

Une application pour un accès Zero Trust à toutes les applications métier.
Zscaler Client Connector fait partie des services Zscaler Internet Access™ (ZIA™) et Zscaler Private Access™ (ZPA™). Client Connector est une application légère qui s'exécute sur le terminal d'un utilisateur. Client Connector transfère automatiquement tout le trafic utilisateur vers le data center de service Zscaler le plus proche — plus de 150 sont disponibles dans le monde — ce qui garantit que les politiques de sécurité et d'accès sont appliquées sur tous les appareils, emplacements et applications. Zscaler Client Connector détermine automatiquement si un utilisateur cherche à accéder au Web, à une application SaaS ou à une application interne, puis achemine le trafic vers le service Zscaler approprié.

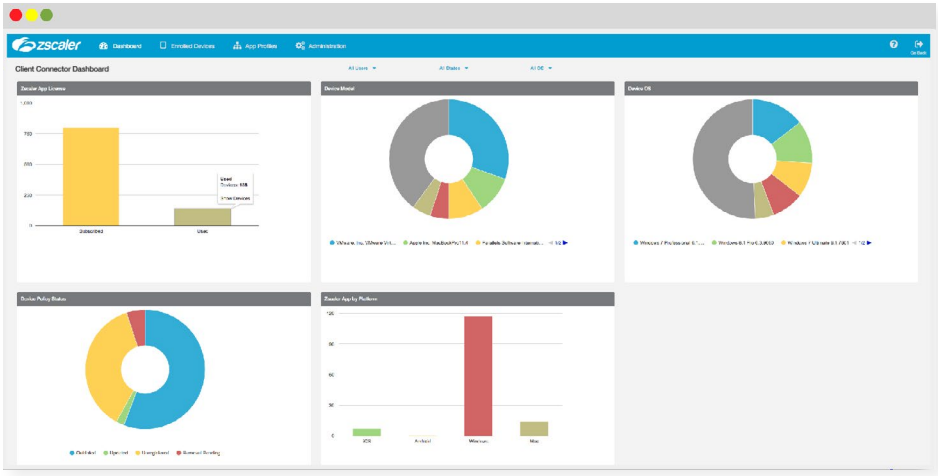
Une expérience d'accès transparente pour les utilisateurs finaux.
Les utilisateurs peuvent accéder aux applications critiques de l'entreprise depuis n'importe quel appareil, sans avoir à réfléchir à la méthode d'accès requise. Il n'y a pas de VPN à lancer à chaque fois que l'utilisateur se connecte à un nouveau réseau, et le connecteur s'intègre aux fournisseurs d'identité et d'authentification multi-facteur (MFA) pour une expérience fluide.

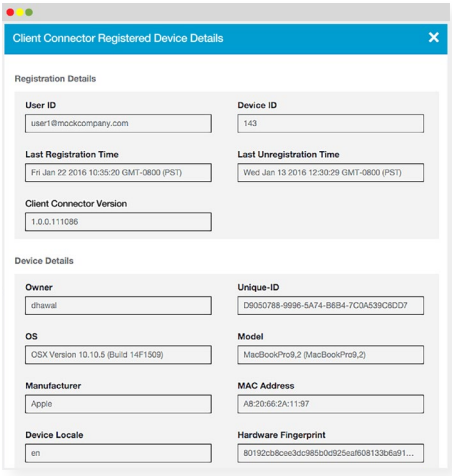
Zscaler Client Connector achemine automatiquement le trafic vers l'emplacement de la périphérie du service Zscaler au plus proche de l'utilisateur que possible, ce qui permet un accès rapide et sécurisé à Internet, aux SaaS et aux applications internes. Avec Client Connector, il n'y a pas besoin de fichiers PAC, de VPN IPsec, de cookies d'authentification, ni d'autres étapes supplémentaires pour l'utilisateur final.





Visibilité et contrôle pour les équipes informatiques.
Pour la première fois, les équipes informatiques bénéficient d'une visibilité et d'une gestion améliorées des données des appareils via le portail d'administration Zscaler Client Connector. Elles reçoivent une des informations supplémentaires sur les performances des applications métier, les performances réseau et les performances des appareils avec Zscaler Digital Experience (qui s'intègre à Client Connector). Cette intégration met à la disposition des administrateurs informatiques et des professionnels du centre de services qui en ont besoin de nombreux et précieux paramètres.





Avantages de Client Connector

Le trafic est acheminé de manière intelligente pour une expérience utilisateur optimale.
Client Connector achemine automatiquement le trafic mobile sur le chemin optimal vers la périphérie Zscaler la plus proche. Par ailleurs, Client Connector détecte les réseaux de confiance et les portails captifs pour prioriser l'expérience utilisateur.

Une visibilité accrue sur l'activité des utilisateurs et la posture des appareils.
Le portail Zscaler Client Connector offre aux administrateurs informatiques une visibilité complète sur les utilisateurs, les appareils et les politiques spécifiques à Client Connector. En plus de fournir une vue globale des appareils déployés, le tableau de bord centralisé de Client Connector permet pour des appareils individuels l'utilisation de politiques définies de manière granulaire.

Intégration facile avec déploiement silencieux via MDM.
Client Connector peut être déployé de manière silencieuse via des solutions MDM, Microsoft Intune, LDAP ou ADFS pour minimiser les frictions sur les terminaux. Aucune action n'est requise de la part de l'utilisateur puisque le déploiement silencieux installe automatiquement, inscrit l'appareil et vérifie les certificats SSL.

Appliquer l'inscription de Client Connector avant l'accès.
Le service informatique peut exiger l'inscription des appareils des utilisateurs avant l'accès aux applications. Le service informatique a également la possibilité d'empêcher les utilisateurs de désactiver Client Connector, afin de s'assurer que tout le trafic est correctement sécurisé.

Empreintes digitales et posture de l'appareil pour une sécurité et un accès contextuels.
Grâce aux intégrations avec les fournisseurs de sécurité des terminaux, tels que Microsoft, CrowdStrike et VMware Carbon Black, Client Connector peut appliquer une sécurité contextuelle en identifiant des critères variables, notamment l'intégrité de l'appareil, le système d'exploitation et si une solution de terminal est en cours d'exécution ou non. En associant les informations d'identification de l'utilisateur à un appareil spécifique, le service informatique peut renforcer la sécurité et empêcher les appareils compromis d'accéder à des données sensibles.

Large prise en charge des appareils et systèmes d'exploitation utilisés pour le travail
Zscaler Client Connector prend en charge la plupart des types d'appareils, notamment les ordinateurs portables, les smartphones, les tablettes, les systèmes de point de vente et les scanners RF (ordinateurs mobiles) sur des plateformes telles que iOS, Android, Windows, macOS, CentOS 8 et Ubuntu 20.04.

Zscaler Client Connector (anciennement Zscaler App ou Z App) est une application légère déployée sur l'appareil de l'utilisateur final qui transmet automatiquement tout le trafic utilisateur via Zscaler Zero Trust Exchange™ pour appliquer les politiques et les contrôles d'accès tout en améliorant les performances.

AVANTAGES

- Les politiques Zero Trust suivent les utilisateurs, quels que soient l'appareil, l'emplacement ou l'application utilisés
- L'expérience utilisateur est améliorée et l'accès aux applications est rationalisé
- Un contrôle centralisé permet d'appliquer les changements de politique immédiatement et dans le monde entier
- Le service informatique peut suivre et surveiller les activités des utilisateurs et des appareils
- Prend en charge la plupart des systèmes d'exploitation et types d'appareils (ordinateurs portables, smartphones, tablettes, etc.)

SYSTÈMES PRIS EN CHARGE

- iOS 9 ou versions ultérieures
- Android 5 ou versions ultérieures
- Windows 7 et versions ultérieures
- Mac OSX 10.10 et versions ultérieures
- CentOS 8
- Ubuntu 20.04

Par où commence?

Le processus d'inscription en une étape de Client Connector facilite le déploiement, le service informatique supervisant le déploiement des ordinateurs portables et les utilisateurs pouvant télécharger l'application pour leurs téléphones et tablettes sur Apple et Google Play Store. Une couche supplémentaire de sécurité est ajoutée grâce à l'authentification multi-facteur instantanée pour ceux qui utilisent l'authentification unique (SSO). Notre guide étape par étape aborde tout ce que vous devez savoir sur le déploiement et la configuration de Zscaler Client Connector.

Obtenir Client Connector

Client Connector pour les ordinateurs portables

Windows/macOS/Linux

Pour Windows/macOS/Linux, contactez votre administrateur

Connecteur client pour téléphones et tablettes

iOS | Télécharger maintenant

Android | Télécharger maintenant

CLIENT CONNECTOR	ORDINATEUR PORTABLE			TÉLÉPHONES/TABLETTES	
Fonctionnalité du système d'exploitation	Win	Mac	Linux	Android	iOS
ZDX	✓	✓			
TWLP	✓	✓	✓		
Tunnel 1.0	✓	✓	✓	✓	✓
Tunnel 2.0	✓	✓	✓		
Mode de filtrage de paquets	✓				
Mode basé sur l'itinéraire	✓	✓	✓	✓	✓
Posture de l'appareil	✓	✓	✓ *Limité	✓	✓
Client basé sur l'interface CLI					
FIPS	✓	✓	✓		
ZPA avec VPN tiers	✓	✓	✓ *Validé avec Pulse ; AnyConnect pour être validé		✓
Récupérer les journaux à distance	✓	✓		✓	
Capture de paquets intégrée	✓	✓	✓		
DTLS pour ZIA	✓	✓	✓		
DTLS pour ZPA	*Prochainement	*Prochainement	*Prochainement	*Prochainement	*Prochainement
Client Connector peut installer le certificat SSL pour l'inspection SSL	✓	*Apple a modifié la politique de sécurité	✓		
Integrated Windows Authentication (IWA)	✓	✓	✓	✓	✓
Client Connector peut automatiquement réessayer l'authentification pour le SSO	✓	✓			
Vérification de la posture CRWD	✓	✓			
Application stricte	✓	✓	✓		

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com