Secure Mobile Access with Zscaler Client Connector

Reference Architecture

Contents

About Zscaler Reference Architecture Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler Account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the Zscaler website at Reference Architectures (https://www.zscaler.com/resources?type=reference-architectures).

You can join our user and partner community and get answers to your questions in the Zenith Community (https://community.zscaler.com/).

Terms and Acronyms Used in This Guide

Acronym	Definition
ADFS	Active Directory Federation Service
AI	Artificial Intelligence
AUP	Acceptable Use Policy
CRL	Certificate Revocation List
DC	Data Center
DTLS	Datagram Transport Layer Security
GRE	Generic Routing Encapsulation
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
OS	Operating System
PAC	Proxy Auto Configuration
POS	Point-of-Sale
SSL	Secure Socket Layer (superseded by TLS)
TLS	Transport Layer Security
URL	Uniform Resource Locator
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

Icons Used in This Guide

The following icons are used in the diagrams contained in this guide.


Administrator


Application


Branch Office


Cloud-based Application

Cloud-based SaaS


Firewall


Headquarters


Identity Provider


Laptop, User


Private Data Center


Private Data Center Application

Public Cloud Service

Public Internet


Remote or Hybrid User


Router


Laptop with Zscaler Client Connector


Smartphone with Zscaler Client Connector


ZIA Public Service Edge


ZPA Public Service Edge


Zscaler App Connector

Zscaler Zero Trust Exchange


Approve


Deny

Introduction

In the past, most users worked inside your organization's facilities, using equipment you issued and configured for them. It made sense to rely on network-based controls to allow users to access the internet and business applications. Many organizations continue to rely on VPNs for remote access. These VPNs backhaul user traffic to a central data center where it applies security through a legacy appliance stack.

This adds latency for cloud applications while at the same time placing the user on your organization's network. Being on the network increases the risk of lateral movement and over-privileged access. Instead of granting access based on an IP address, controls should be user-centric, tied to an authenticated user's identity.

With the continuing shift towards hybrid and remote work, some or all of your users might be remote and located anywhere in the world. Your IT teams no longer control the networks employees use, and possibly not the computing platforms they choose to leverage. This leads to a lack of visibility for your organization into what users are accessing and how the network is performing.

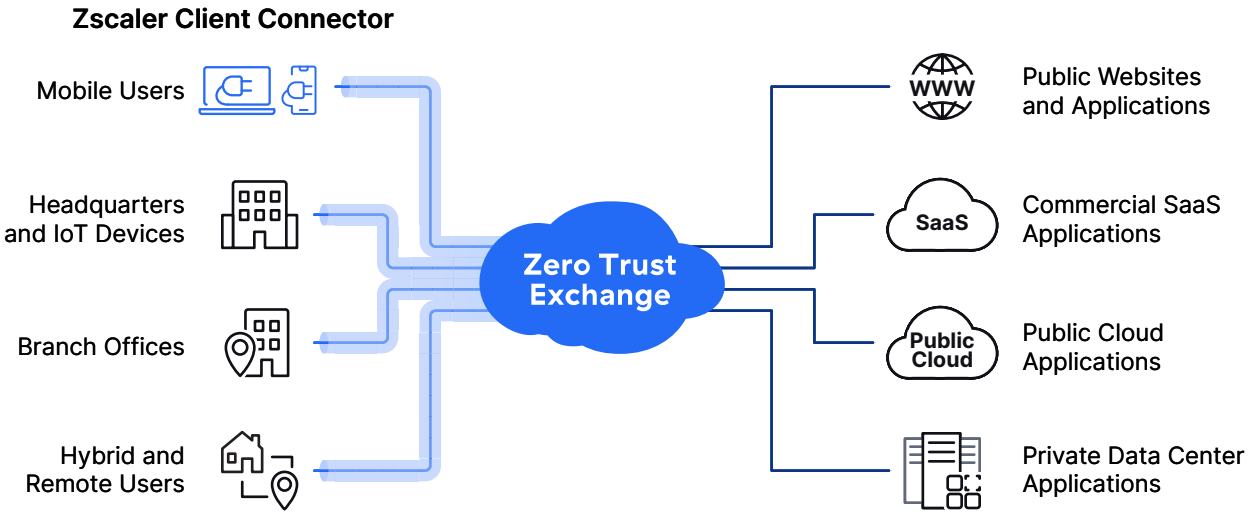

Figure 1: Zscaler Client Connector connects your organization's devices to secure internet browsing, private application access, and visibility for your IT staff

Zscaler Client Connector is a lightweight, tamper-resistant agent that connects your users and devices to the Zscaler services in the Zscaler Zero Trust Exchange (ZTE). Zscaler Client Connector supports Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX) by default, allowing your team to combine best-in-class internet security with Zero Trust access to internal applications. Zscaler Client Connector is included for all your licensed users as a part of a subscription to one of the Zscaler services.

Because Zscaler Client Connector can connect to all user-facing Zscaler services, it has quickly become one of the easiest, fastest, and most popular ways to extend our services to users working anywhere they have an internet connection. By connecting to the ZTE, Zscaler Client Connector enables secure access to the internet and your private applications anywhere in the world. Zscaler Client Connector also provides visibility into the user's network and application experience.Zscaler Client Connector is available on multiple operating systems: Windows, macOS, Linux, iOS, Android, and Android Chrome OS. Multiple installation types are available, giving you the ability to deploy Zscaler Client Connector on devices that never connect to your organization's network. Zscaler Client Connector is an application that runs natively on an endpoint, but it is entirely managed from within the Zscaler Client Connector Admin Portal in the Zscaler cloud.

This new, hybrid and remote workforce demands fast and seamless access to business applications, from any device in any location. However, that speed can't come at the risk of exposing your organization's data to risk. IT leaders have turned to Zscaler and Zscaler Client Connector to help them connect users to the data they need to get their work done.

Zscaler Client Connector connects your users to where your security policy and access controls are configured and enforced. Zscaler Client Connector connects to the geographically closest Zscaler secure data center to the user. Zscaler currently has over 150 data centers around the world to service our customers' traffic as close to the user as possible.

Work-from-anywhere also means that access services must be flexible enough to extend to every user device from any network. Laptops, smartphones, point-of-sale (POS) systems, inventory scanners, and more are used for your organization's work, and all of them require fast, secure connections to your applications.

Connection to Zscaler Services

Zscaler Client Connector provides access to three Zscaler services via a single user agent on your user's device.

Zscaler Client Connector and Zscaler Internet Access

For a user enrolled in Zscaler Internet Access, Zscaler Client Connector redirects their outbound internet traffic to the ZIA cloud. This ensures that the organization's security, content, and data protection policies are in full effect. All user activity on the public web is safe, secure, and compliant, even when a user is traveling or working from home. ZIA protects your user's internet traffic with full TLS/SSL inspection. ZIA also leverages AI-powered protection for all users, all apps, and all locations, providing a safe and secure internet access experience.

Zscaler Client Connector and Zscaler Private Access

For a user enrolled in Zscaler Private Access, Zscaler Client Connector dynamically creates secure, encrypted Microtunnels from their endpoint to the Zscaler cloud, so that the user can access private applications they've been assigned to in the Zscaler Private Access Portal. ZPA provides secure access to applications, not to networks. Working in conjunction with Zscaler App Connectors and Zscaler Cloud Connectors, you can provide secure access to authorized applications for users.

Zscaler Client Connector and Zscaler Digital Experience

For a user enrolled in Zscaler Digital Experience, Zscaler Client Connector is a powerful source of performance data gathered at the endpoint level. In a ZDX use case, Zscaler Client Connector gathers metrics that our cloud alone can't see, including details like the CPU load, Wi-Fi signal strength and throughput, or whether or not that endpoint is fully up to date with the latest operating system patches. ZDX provides visibility into the health of your applications from the user's device. This includes monitoring of the application and testing the network connection hop-by-hop from device to application, no matter where the application is hosted.

Key Features and Benefits

Auto-route traffic for a seamless user experience and easier IT.

By default, the app routes mobile traffic through the Zscaler cloud for secure access and optimal routing, with no virtual private network (VPN) to spin up. The app also integrates with identity and multi-factor authentication (MFA) providers, and it can detect trusted networks and captive portals to prioritize the user experience.

Support all the devices your business needs.

Zscaler Client Connector supports most device types, including laptops, smartphones, and tablets, and runs on iOS, macOS, Android, Windows, CentOS, and Ubuntu 20.04.

Use device posture and fingerprinting for context-aware access and security.

Through integration with endpoint security providers, the app can enforce context-aware security that ensures devices are mapped to specific users based on criteria like device model, platform, and operating system. Security remains intact even in the event of credential or device theft.

Easily enforce enrollment to stay secure.

IT can require enrollment of user devices prior to accessing apps. It can prevent users from turning off the app to ensureall mobile traffic is secure.

Gain more visibility with an intuitive dashboard.

The Zscaler Client Connector Admin Portal allows administrators to view data for remote devices with the app deployed, as well as manage policies specifically for the app.

Make deployment almost invisible to users.

Easily deploy Zscaler Client Connector on endpoints to minimize user friction with MDM, Microsoft Intune, LDAP, or ADFS. Silent deployment auto-installs client and TLS/SSL certificates onto devices during enrollment.

New to Zscaler Client Connector or the Zscaler Platform?

- Read the Zscaler Client Connector data sheet (https://www.zscaler.com/resources/data-sheets/zscaler-mobile-app.pdf).
- If you are an end user of Zscaler Client Connector, view the End User Guide (https://help.zscaler.com/zscaler-client-connector/end-user-guide).
- Learn more about Zscaler Internet Access (ZIA) (https://www.zscaler.com/products-and-solutions/zscaler-internet-access).
- Learn more about Zscaler Private Access (ZPA) (https://www.zscaler.com/products-and-solutions/zscaler-private-access).
- Learn more about Zscaler Digital Experience (ZDX) (https://www.zscaler.com/products-and-solutions/zscaler-digital-experience-zdx).
- Learn more about Zscaler Deception (https://www.zscaler.com/products-and-solutions/deception-technology).

Understanding Zscaler Client Connector Operations

Overview of Zscaler Client Connector

Zscaler Client Connector is a software agent that runs on your user and IoT devices to connect them to Zscaler services. This low-impact agent runs in the background, inspecting traffic and directing it toward the appropriate Zscaler service based on your policy and Zscaler subscriptions. If you are a subscriber to ZDX, Zscaler Client Connector is also responsible for sending network and application probes.

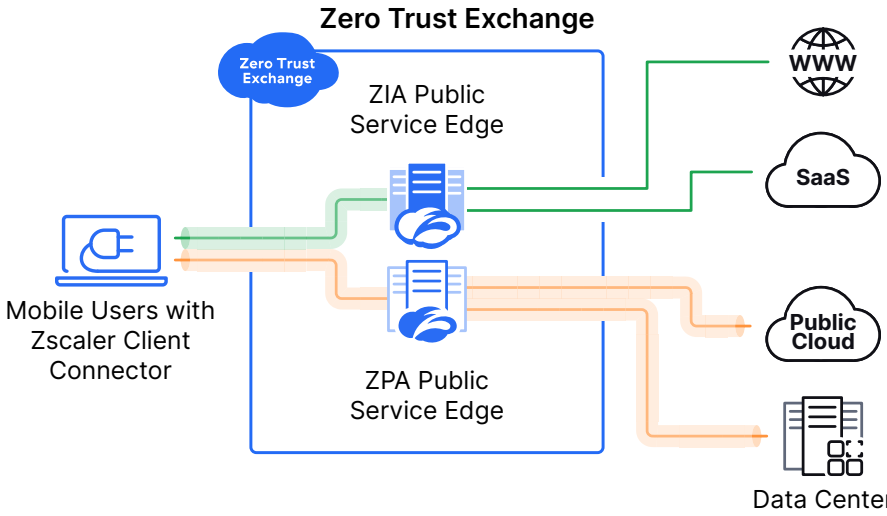

Figure 2: Zscaler Client Connector connects to a ZIA Public Service Edge and a ZPA Public Service Edge geographically closest to the user

When your device starts up, it connects via transport layer security (TLS) to services in the Zscaler Zero Trust Exchange (ZTE). Depending on your subscriptions, this will be a ZIA Public Service Edge, a ZPA Public Service Edge, or both. If you subscribe to ZDX or Deception, these will also connect to a ZIA Public Service Edge.

Your users authenticate to the services using your existing identity provider (IdP) via the security association markup language (SAML) protocol. No matter what ZIA Public Service Edge or ZPA Public Service Edge your device connects to, your organization's policy for that user is applied, and your logs are still routed to your location of choice.

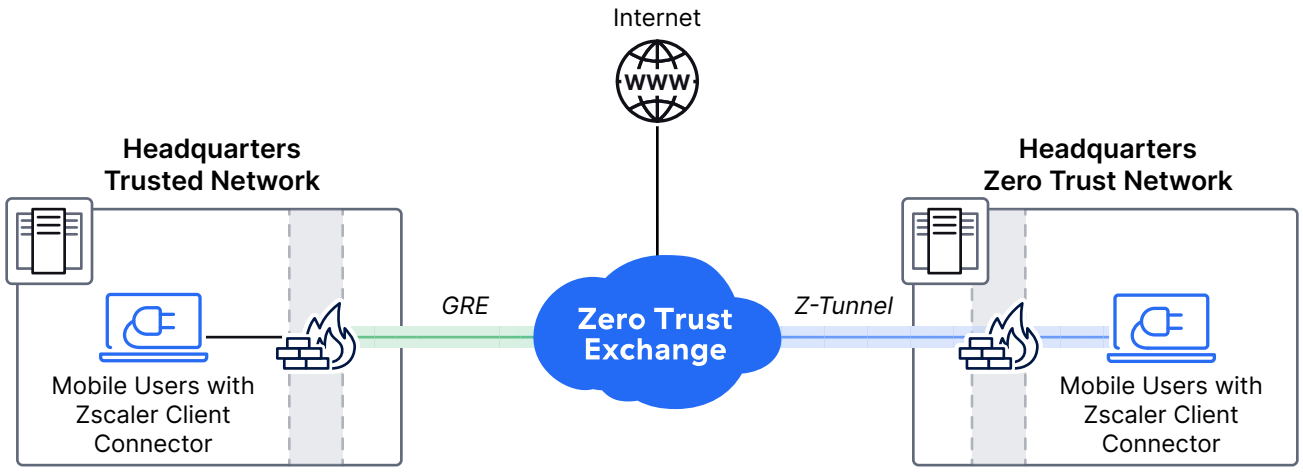

Figure 3: You can choose to run Zscaler Client Connector at your organization's location, or have it turn off when it discovers it is on a trusted network

Zscaler Client Connector can be set to automatically start with the device, ensuring that users are always protected. There are no scaling limits with Zscaler services, which makes it possible to run Zscaler Client Connector on devices even when they at your organization's sites. If you also leverage ZPA, you can place your corporate data center behind Zscaler App Connectors.

By always using Zscaler Client Connector in conjunction with ZIA and ZPA, you can achieve true Zero Trust Network Access. This allows you to simplify your network, treating all network connections like you would your home internet connection, and requiring Zscaler Client Connector to reach your corporate applications and the internet.

If you have an existing generic routed encapsulation (GRE) or internet protocol security (IPSec) tunnel to Zscaler, Zscaler Client Connector can detect that your users are on a trusted network and will not establish their tunnels. However, ZPA and ZDX continue to operate to provide application access and network-level diagnostics.

Zscaler makes enrolling your devices a simple task for your help desk by providing clients you preconfigure for your users. This allows you to deploy a fully configured Zscaler Client Connector with your standard operating system images, or make it available for users to download from your intranet portal. If you use industry-standard software management platforms such as Microsoft Intune, you can also push Zscaler Client Connector as a software update to your managed devices. Zscaler Client Connector is included with your Zscaler subscriptions and can be installed on up to 16 devices per licensed user.

Operating System Support

Zscaler Client Connector supports a wide variety of the most common operating systems, including Windows, macOS, CentOS, Ubuntu (20.04+), iOS, and Android. Zscaler Client Connector can be deployed via direct download or Mobile Device Management (MDM) for silent installs.

The desktop versions of Zscaler Client Connector provide administrators the ability to preconfigure the client. This eliminates user error and help desk calls; administrators only need the ability to install software. You can host the software on your intranet, a publicly available location, or through MDM push. When installed, your users are required to log in to the client to access resources. After authentication successfully completes, the client device is available for inspection in the Zscaler Client Connector Admin Portal.

You can prevent users from disabling Zscaler Client Connector or uninstalling the software by using an admin-provided password. This ensures that your users are always protected when accessing internet resources.

Learn more about Choosing Provisioning and Authentication Methods (https://help.zscaler.com/zia/choosing-provisioning-authentication-methods).

To see which features are available by operating system, see the Zscaler Client Connector data sheet (https://www.zscaler.com/resources/data-sheets/zscaler-mobile-app.pdf).

The Zscaler Client Connector Admin Portal

The Zscaler Client Connector agent provides device access to all Zscaler for Users services. To manage the client from any service, Zscaler Client Connector has a dedicated portal for agent monitoring and configuration. The Zscaler Client Connector Admin Portal is reachable from the dedicated portals for ZIA, ZPA, and ZDX, and serves multiple functions.

Dashboard

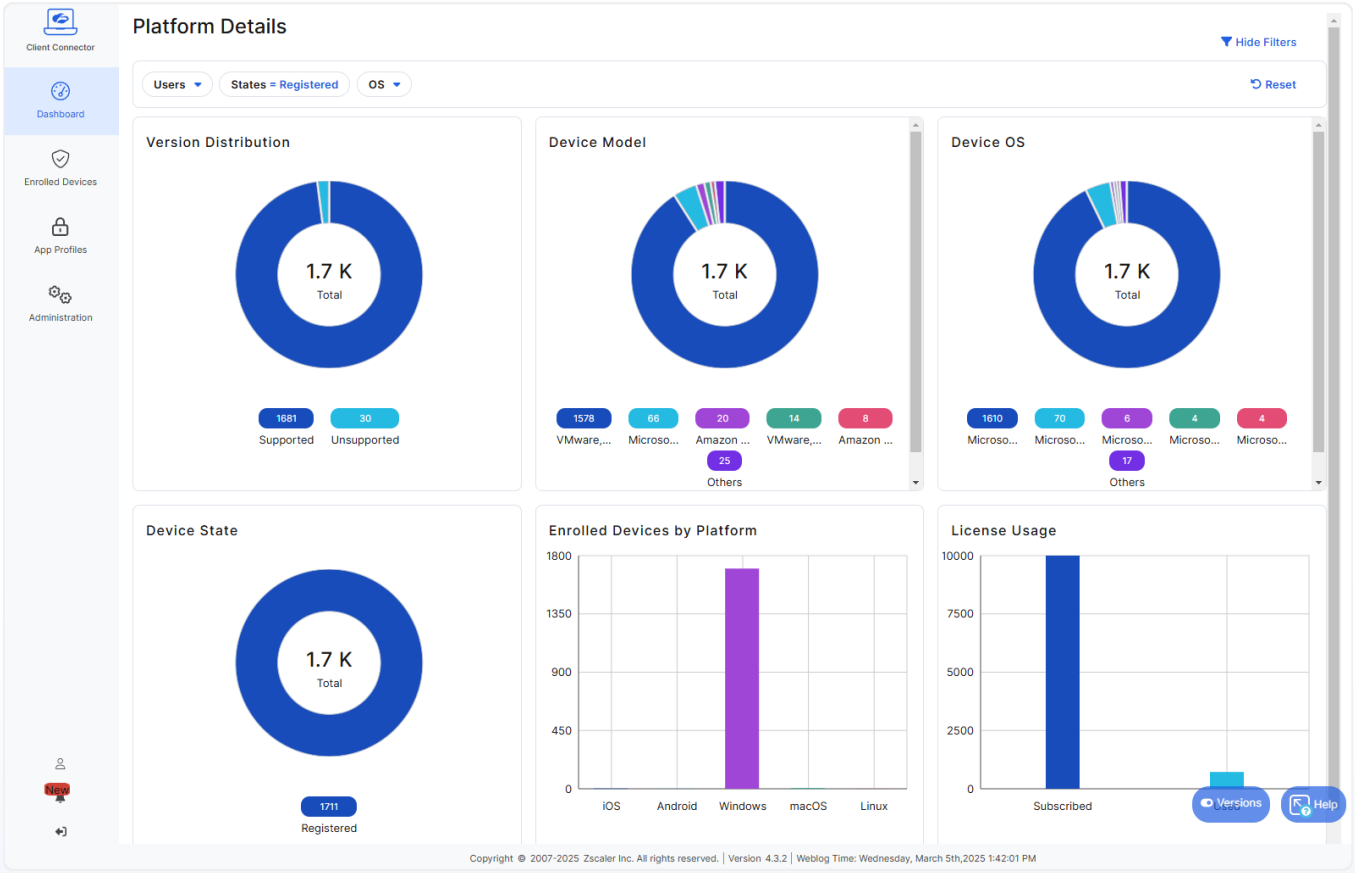

Figure 4: The Zscaler Client Connector Dashboard gives you a visual summary of your organization's devices

In the Dashboard view, details of your organization's enrolled devices are displayed as graphical charts. Widgets display the following information:

- **Version Distribution** – This widget displays how many devices are running supported and unsupported versions of Zscaler Client Connector. Unsupported versions should be investigated, and the devices should be updated if possible.
- **Device Model** – This widget displays information on devices in your organization by device type. The top 5 devices are shown, with an Other category containing the rest of your devices. You can hover over a section for details on model name, number of devices, and percentage of devices.
- **Device OS** – This widget displays information on your top 5 device operating systems in your organization, with an Other category containing all other operating systems. You can hover over a section for details on OS name, number of devices, and percentage of devices.
- **Device State** – This is the state of the device from a Zscaler Client Connector fleet management view. There are 5 states: Registered, Unregistered, Removal Pending, Removed, and Quarantined. You can learn more about each of these states at Device States for Enrolled Devices (https://help.zscaler.com/zscaler-client-connector/device-states-enrolled-devices).
- **Enrolled Devices by Platform** – This widget displays the number of devices on each of the 5 supported operating systems. All versions of a particular operating system are counted in this single metric.
- **License Usage** – This widget displays information about your license as a bar graph, including the total number of subscriptions and the number currently in use.

Enrolled Devices

The Enrolled Devices view gives you a tabular look at the status of machines that have installed Zscaler Client Connector and completed enrollment. Multiple filters exist to narrow the device view including last seen, device state, and operating system. You can also search for specific users or machines to find out a device's current state. The dashboard allows you to examine the device details and current state.

Learn more at About Enrolled Devices (https://help.zscaler.com/zscaler-client-connector/about-enrolled-devices).

Zscaler Client Connector Agent Configuration

The Zscaler Client Connector agent is configured by combining policy rules on the app profiles page. Here, you can make all configurations and customizations to your deployment, as well as configure all aspects of Zscaler Client Connector operation. You can build profiles that are applied to your users, either all sharing the same profile, or with specific profiles for different users and groups. You can also configure which versions of Zscaler Client Connector to make available to your users.

To learn more, visit About Zscaler Client Connector Profiles (https://help.zscaler.com/zscaler-client-connector/about-zscaler-client-connector-app-profiles).

Zscaler Client Connector Software Maintenance

Like any piece of software, Zscaler Client Connector must be updated on a regular basis. As a centrally managed agent, you can control when the software should be updated, or just let the agent always update to the latest version.

Updating Zscaler Client Connector

Zscaler Client Connector can be set to update itself at intervals you control. You can choose to have different options selected for macOS and Windows. Devices running iOS and Android are updated when a new version is pushed to the respective app store. Your options for updating are:

- **Always update to the latest version** – Always update to the latest version, which mirrors how the mobile app stores operate.
- **Specific versions** – Update to a version you select, typically used for you to test and certify versions before deployment.
- **Group based** – Apply a specific version to specific groups of people, including all users or specific groups with different requirements.
- **Disable** – Updates are not applied automatically.

Often customers use group based, specifying that their IT teams are upgraded before the general user population. This gives you time to ensure that any changes that need to be made are noticed by your staff prior to impacting the end users. When testing is complete, the rest of the organization can be upgraded to the newer version.

Zscaler Client Connector checks every two hours for a newer version available for Windows, macOS, and Linux. If your organization leverages MDM or other client management tools, you have the option of disabling automatic updates in favor of push deployment from your MDM.

Understanding Zscaler Client Connector Tunnel Connections

Zscaler Client Connector connects to multiple Zscaler services based on your subscriptions. When Zscaler Client Connector senses a network connection change, it attempts to reach out to the nearest ZIA Private Service Edge and/or ZPA Private Service Edge. Each of these services has its own connection setup and methods of operations.

Determining the Nearest ZIA Service Edge or ZPA Service Edge

Both the ZIA Service Edge and ZPA Service Edge use the user's location to determine where to direct Zscaler Client Connector to connect. This occurs during startup, when Zscaler Client Connector checks in for its configuration. The IP address that the Zscaler Client Connector request comes from is used to geolocate the user.

Figure 5: Zscaler has over 150 data centers around the globe for quick access to Zscaler services, no matter where your users are located

Zscaler Client Connector resolves *any.broker.prod.zpath.net* to initially connect to a ZIA Public Service Edge and ZPA Public Service Edge. Any traffic destined to **.prod.zpath.net* from Zscaler Client Connector must be bypassed from ZIA or other proxies and go directly to the internet.

Zscaler Client Connector Tunnels to ZPA Service Edge

ZPA protects your applications by only allowing authorized users to connect directly to the application itself, not the network. When an application is protected by ZPA, users must be connected via Zscaler Client Connector and authorized by policy to see the application. For any unauthorized users, it will appear as if the application doesn't exist on the internet.

Figure 6: ZPA ensures only authorized users of your organization can discover and connect to your application

With ZPA, your users establish a TLS tunnel to the nearest ZPA Service Edge from a returned list of nearby data centers, including any ZPA Private Service Edge devices. The Zscaler Client Connector agent connects to the nearest tunnel. When the user attempts to connect to a ZPA-protected application, the user's request is compared to the forwarding policy.

If the user is allowed to connect to an application, the ZPA Service Edge contacts the Zscaler App Connector nearest the application. Both the App Connector and Zscaler Client Connector establish a per-application Microtunnel TLS tunnel that allows the user to connect to the application using a private IP address. This encrypted tunnel is used only for a single application by a single user.

Zscaler Client Connector Tunnels to ZIA Service Edge

The ZIA service proxies your user's traffic to the internet and SaaS applications, inspecting and enforcing your policies. To do that, Zscaler Client Connector creates a tunnel from the endpoint to the nearest ZIA Service Edge to the user's location. Unlike VPNs, there is no need to backhaul traffic to your data center first. Users go straight to the cloud by connecting though a ZIA Service Edge.

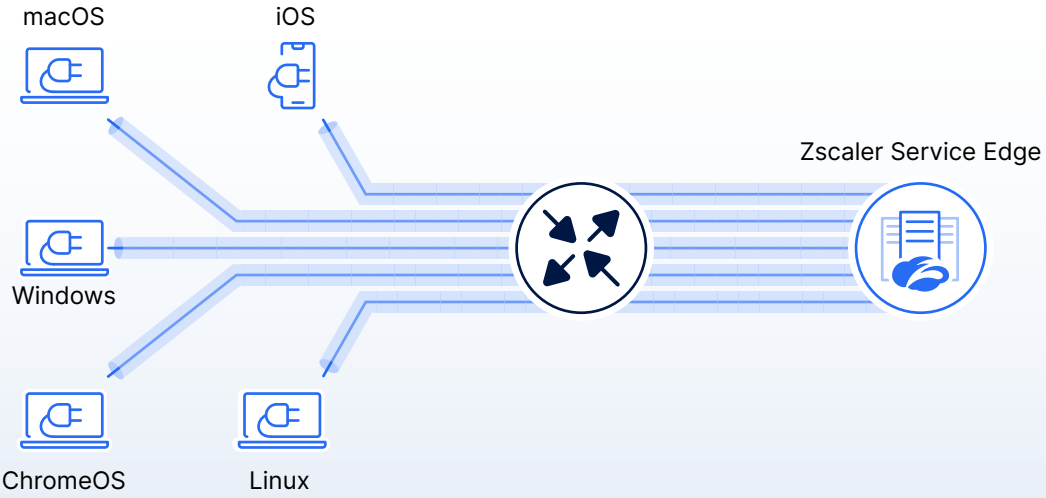

Figure 7: Zscaler Client Connector works with many operating systems and devices

When installed on a user's device, Zscaler Client Connector creates a virtual network adapter. For the ZIA use case, by default your user traffic is tunneled directly to the nearest ZIA Service Edge for inspection.

When your users attempt to use the internet, this virtual adapter captures that traffic flow. Zscaler Client Connector then uses geolocation to determine the closest ZIA Service Edge node, and builds a lightweight tunnel called a Z-Tunnel to that node. The user traffic is then placed inside the tunnel and forwarded to the ZIA Service Edge for inspection and policy enforcement.

Zscaler Client Connector can also be set to disable itself temporarily when it detects that it is on a trusted network, or if a captive portal is blocking access to the internet.

View a list of Zscaler's leading authentication provider partners (https://www.zscaler.com/partners/technology/identity).

Trusted Network Detection

Anyone who has supported traditional user access VPNs knows the difficulties associated with users not understanding when to launch their VPN client. Users at home might forget to log in, generating help desk calls about access. Other users log in while on the organization's network, slowing their connection and using up licenses that remote users need to connect.

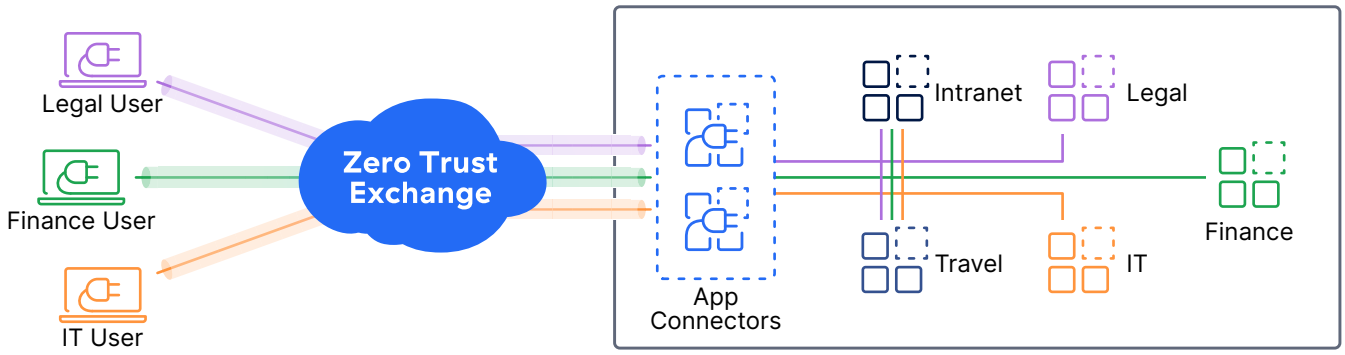

Figure 8: Trusted network connection builds a Zscaler Client Connector tunnel only when on an untrusted network

Zscaler Client Connector contains a feature called trusted network detection. You can configure the agent to understand when it is on one of your organization's network segments and disable itself. This allows your traffic to be tunneled by your internet gateway using GRE or IPSec, without the need for an additional DTLS or TLS tunnel from Zscaler Client Connector.

Zscaler Client Connector uses the following options to determine if a client is on a trusted network. This is typically a location where you are tunneling traffic to ZIA via GRE or IPSec tunnels. Except for Pre-Defined Trusted Networks, you can specify a match on ANY or ALL configured criteria for a more robust detection:

- **DNS Server (Recommended)** – Configure a list of IP addresses which are your internal corporate DNS servers. Zscaler Client Connector verifies at least one DNS server can be reached.
- **DNS Search Domains (Recommended)** – Enter a list of search domains. Zscaler Client Connector compares this list to the search domain of the active network adapter.
- **Hostname and IP** – A hostname and the IP addresses where the hostname resolves when users are on the corporate network.
- **Network Range** – A range of IP addresses. Zscaler Client Connector verifies that the current network the user is connected to is within this range.

- **Default Gateway** – Configure an IP address. Zscaler Client Connector checks if the device's current default gateway matches this.
- **DHCP Server** – Configure a list of IP addresses that are your internal DHCP servers. Zscaler Client Connector checks if its current DHCP server matches this list.
- **Egress IP** – Configure a list of IP addresses that your corporate networks will egress traffic from. Zscaler Client Connector checks if the current egress IP matches an entry in this list.
- **Pre-Defined Trusted Networks** – Configure all your trusted networks, then add them to your configuration. This detection option cannot be combined with any of the other three options in the policy, and is the only criteria used if configured.

After your criteria is defined, Zscaler Client Connector automatically disables itself when it determines it is on a trusted network. When the agent detects a network state change, it checks again to see if it is on a trusted network segment. When Zscaler Client Connector discovers it is not connected to a trusted network segment, it automatically tries to connect to the nearest ZIA Service Edge.

Zscaler recommends using DNS Server and/or DNS Search Domains for detecting trusted networks. These are the most static entities on a network and combining them gives you the most assurance of being on a trusted network.

Forwarding Profiles and Z-Tunnels

Zscaler Client Connector uses forwarding profiles to determine how to forward user traffic to the nearest ZIA Service Edge. Traffic from Zscaler Client Connector is forwarded over a virtual tunnel called a Z-Tunnel. The Z-Tunnel can use datagram transport layer security (DTLS) or transport layer security (TLS) or act as an HTTP proxy to forward traffic. When the traffic reaches the ZIA Service Edge, the tunnel headers are removed. The ZIA Service Edge then inspects the underlying traffic and applies your organization's policy to the user traffic.

There are two versions of Z-Tunnel: version 1.0 and version 2.0. These tunnels are used to transmit both user traffic if you are subscribed to ZIA, and diagnostic traffic if you are subscribed to ZDX.

Version 1.0 of Z-Tunnel is a proxy-based tunnel that uses a lightweight HTTP tunnel to forward TCP-based web traffic. Because Zscaler Client Connector acts as a web proxy, it limits Z-Tunnel 1.0 to web-based traffic using port 80 or 443. The traffic and headers are not encrypted by the Z-Tunnel, with encryption handled by the web application.

With version 2.0 of Z-Tunnel, Zscaler has adopted two new tunnel encapsulation types to send packets to the ZIA Service Edge: DTLS and TLS tunnels. Because the traffic is inside an encrypted channel, Zscaler Client Connector can forward all ports and protocols to the ZIA Service Edge. This includes the user's IP address for more granular load balancing.

If your location uses multiple bonded internet connections, ensure that each user egresses using the same IP address for all their sessions. Having a user's IP address change with each session can cause the user's traffic to land on different ZIA Public Service Edge devices, and cause the service to fail back to Z-Tunnel 1.0.

Zscaler recommends using Z-Tunnel version 2.0 for all traffic wherever possible. Learn more at About Z-Tunnel 1.0 & Z-Tunnel 2.0 (https://help.zscaler.com/zscaler-client-connector/about-z-tunnel-1.0-z-tunnel-2.0).

Zscaler Client Connector Forwarding Profiles

Forwarding profiles determine how traffic is sent to the ZTE cloud and Zscaler services based on a user's location and connection to the internet. You can have multiple profiles for different teams, and profiles for both ZIA and ZPA access. With each service, you determine what Zscaler Client Connector should do when the user is on a trusted network, on a VPN connection, or off a trusted network. Each of these can be set separately for each service.

You can name and configure multiple profiles to apply to different groups of users or situations. Zscaler recommends matching your profile name to the use case you are solving for, such as IT admins or general users. Under each profile, you can specify your trusted network criteria discussed earlier.

For Windows devices, you need to select the tunnel driver type you want to forward your traffic. Two options are supported: Route Based forwarding and Microsoft's Packet Filter Based forwarding. Zscaler recommends the Packet Filter Based forwarding for maximum compatibility.

Forwarding Profile Action for ZIA

ZIA has a series of decisions for you to make, depending on the network the user is connected to and the tunnel type you want to use. There are 3 network states and 4 forwarding options for each state. The network states are.

- On Trusted Network
- On VPN
- Off Trusted Network

The forwarding options for each state are:

- **Tunnel** – All traffic is tunneled to the ZIA Service Edge. This is the recommended option for most deployments.
- **Tunnel with Local Proxy** – When enabled, Zscaler Client Connector configures the device proxy settings so that proxy-aware traffic is sent to Zscaler.
- **Enforce Proxy** – A legacy setting that enforces the pre-existing device proxy settings on the device.
- **None** – Disables forwarding to ZIA.

Finally, you must select the type of tunnel you are going to use: Z-Tunnel 2.0 or 1.0. For most deployments, Z-Tunnel 2.0 is the recommended option so that all your traffic, regardless of ports or protocols, are forwarded to the ZIA Service Edge for inspection. Should Z-Tunnel 2.0 fail to establish a connection due to the network or firewall interference, it will attempt to establish a Z-Tunnel 1.0 connection.

In some instances, you might encounter issues with web application performance. This occurs when an ISP, carrier, or nation state disrupts or throttles UDP connections. In this case, you can choose to split your traffic across both tunnel types. In this hybrid operating mode, web applications use Z-Tunnel 1.0, while your remaining applications use Z-Tunnel 2.0. This feature is enabled via the Redirect Web Traffic to Zscaler Client Connector Listening Proxy setting in the Z-tunnel 2.0 profile.

Setting	Recommendation
On	Trusted Network None
On	VPN Tunnel with Local Proxy
Off	Trusted Network Tunnel
Tunnel Type	Z-Tunnel 2.0
Redirect Web Traffic to Zscaler Client Connector Listening Proxy	Only when needed

Table 1: Summary of ZIA forwarding recommendations

Learn more at Configuring Forwarding Profiles for Zscaler Client Connector (https://help.zscaler.com/zscaler-client-connector/configuring-forwarding-profiles-zscaler-client-connector).

Forwarding Profile Action for ZPA

Like the ZIA profile, ZPA uses the same three network states, but only has two options for forwarding: Tunnel or None. Tunnel enables the Microtunnel to the ZPA Service Edge for application access. Policy is enforced to determine which applications the user is allowed to access.

None disables ZPA access to applications. This is appropriate when a user should not have access to applications given the forwarding profile applied. If a user can access your organization's private applications when on a trusted network or VPN, you might choose None as well.

Zscaler recommends tunneling where possible, even if the applications are in a local data center. By protecting all your applications with ZPA, you add an extra layer of security by making the applications invisible and inaccessible to users without Zscaler Client Connector.

For more information on building a complete Zero Trust Network Access model in your organization, see Universal ZTNA with Zscaler Private Access Private Service Edge (https://www.zscaler.com/resources/reference-architectures/universal-ztna-zpa-private-service-edge.pdf).

For more information on configuring forwarding profiles, see Configuring Forwarding Profiles for Zscaler Client Connector (https://help.zscaler.com/zscaler-client-connector/configuring-forwarding-profiles-zscaler-client-connector).

Configuring Zscaler Client Connector with Application Profiles

Application profiles are designed to configure the Zscaler Client Connector agent itself, as well as how it should function as an application. Which profile a particular endpoint receives is based on its operating system, and any users or groups you choose to associate with that application profile. You can have multiple application profiles, or one shared by all your organization's users.

Because each endpoint OS supports different feature sets, each OS has its own application profile associated with it. You need at least one application profile for each endpoint OS you support.

General Configuration Options for Application Profiles

All application profiles support a set of common options for all endpoints. These are your selectors to apply rules to the correct users and endpoints.

- **Name** – All application profiles are named, and the name should reflect the use case or user groups that will use the application profile.
- **Enable** – An application policy must be explicitly enabled before it can be applied to endpoints.
- **Rule Order** – When multiple application profiles are available, the profiles are each examined until a match is found for the endpoint. The rule order determines the ordering of the application profiles. See Multiple Profiles and Rule Order for more information.
- **Groups** – Allows you to apply the application profile to groups. The options are None (don't match based on group), All, or Selected groups to apply this configuration.
- **Users** – Allows you to apply the application profile to specific users, or None to disable this match. This setting should be used only when no other group match is possible.
- **Logout Password** – If set, requires a user to enter a password to log out of Zscaler Client Connector. This disassociates their username from that instance of Zscaler Client Connector.
- **Disable Password** – If set, allows a user to disable Zscaler Client Connector from connecting to Zscaler services.
- **Custom PAC URL** – You can create custom proxy auto-configuration files hosted on the Zscaler cloud to bypass certain hosts from inspection. You'll enter the URL for the PAC file associated with the forwarding profile here. See Leveraging Custom PAC Files to Bypass Zscaler Inspection for more information.
- **Forwarding Profile** – Select the forwarding profile that is associated with the application profile. For more information, see Forwarding Profiles.
- **Hostname or IP Address Bypass for VPN Gateway** – If you have an existing split-tunnel VPN, enter the hostnames or IP addresses associated with it to bypass ZIA inspection. You can also use this field as a bypass for other internet hosts without the need for a PAC file, however a PAC file is more efficient and less subject to user error.

Multiple Profiles and Rule Order

You need at least one application profile for each OS you support. All organizations should create an application profile that has Groups and Users set to "All." This is an "all organization users" rule that is applied to everyone who authenticates as a member of your organization and doesn't have a better match.

If you don't require multiple application profiles for different users and groups, this is the only application profile you need. The configuration contained in this profile will be applied to all authenticated endpoints.

If you have more than one application profile for a given OS, you need to leverage the Rule Order to ensure users are matched correctly. Zscaler's best practice is to order your rules from most specific to least specific. Specific users first, specific groups second, and the final rule should be used for the "all organization users." This allows users with different profiles to be matched earlier, and the final configuration match is for users that don't need more specific configurations.

Logout and Disable Password Use

Logging out of or disabling Zscaler Client Connector should be used only when absolutely necessary. When the user is logged out or disabled, they lose the protection of ZIA for internet website and applications. With Zscaler Client Connector disabled, they also lose access to internal applications protected by ZPA.

Each setting can be protected by a password that prevents a user from logging out or disabling Zscaler Client Connector on their own. This password should be shared with users only when required.

If you allow users to disable the service, you can choose to have Zscaler Client Connector re-enable the service. This is determined by choosing a number of minutes after which the agent automatically tries to establish a new connection to Zscaler. Zscaler recommends setting a re-enable timer at the lowest value possible in accordance with your security policy.

Leveraging Custom PAC Files to Bypass Zscaler Inspection

Proxy auto-configuration files are small JavaScript files that you create and were originally designed to tell a web browser where the proxy service for a network was located. Zscaler leverages this technology to allow you to specify a list of hosts on the public internet for which ZIA forwarding should not occur. Typically, these are applications that were not written to support proxying of user traffic.

After you have configured and tested your PAC file, you upload it to the ZIA portal. The portal provides a randomized URL string for your PAC file, and you use that URL in the application profile.

Zscaler recommends bypassing ZIA inspection only when a critical application must be allowed to function and cannot be proxied successfully.

Learn more at Understanding PAC Files (https://help.zscaler.com/zia/understanding-pac-file).

OS-Specific Settings in Application Profiles

Not all settings are available on all operating systems. Sometimes it's the way a particular OS handles drivers, or if the system allows software to install root certificates for TLS/SSL inspection. The following list of features are commonly used but not available for every operating system:

- Automatically Install the Zscaler Root Certificate for TLS/SSL Inspection
- Z-Tunnel 2.0 Configuration Settings

Automatically Install the Zscaler Root Certificate for TLS/SSL Inspection

ZIA relies on the ability to look inside encrypted traffic that flows through a ZIA Service Edge. Zscaler performs this by proxying traffic on the user's behalf when they access the public internet. For TLS/SSL protected websites and applications, Zscaler issues a short-lived certificate acting as the destination service the user is accessing but is signed by the Zscaler Central Authority.

By issuing certificates for public services, the endpoint must trust the Zscaler Central Authority the same way it does other major certificate issuers. This requires that the Zscaler root certificate is installed in the endpoint's security store.

Certificate installation for ZIA can be handled automatically with Zscaler Client Connector on macOS and Windows operating systems. The root certificate for ZIA is added to your client's trust store. This enables the endpoint to trust the short-term certificates issued by a ZIA Service Edge. If Firefox is installed, its certificate store is also updated. For Linux and mobile devices, you need to manually add the root certificate to your device and enable inspection for mobile traffic in your policy.

Zscaler recommends inspecting 100% of your organization's traffic for threats, and recommends enabling the Install Zscaler SSL Certificate on all application profiles where possible.

- Learn more about TLS/SSL Inspection with Zscaler Internet Access (https://help.zscaler.com/zia/tls-ssl-inspection-zscaler-internet-access).
- For more information on TLS/SSL inspection and configuration, see TLS/SSL Inspection with Zscaler Internet Access (https://www.zscaler.com/resources/reference-architectures/tls-ssl-inspection-zscaler-internet-access.pdf).

Z-Tunnel 2.0 Configuration Settings

If your forwarding profile uses Z-Tunnel 2.0, you have additional configuration options. These allow you to bypass the need to create PAC files for your macOS, Windows, and Linux deployments. The supported inclusion and bypass settings are:

- **Application Bypass** – Allows you to bypass defined applications from ZIA inspection. This setting can be enabled or disabled.
- **Destination Exclusions** – Allows you to bypass IP addresses, IP address ranges, or IP subnets. You can use this setting to allow access to local home networks, such as 192.168.0.0/16 and/or 172.16.0.0/12.
- **Domain Exclusions** – Allows you to specify specific DNS domains that should be bypassed from ZIA.
- **Domain Inclusions** – Forwards traffic from specific IP addresses, IP address ranges, or IP subnets to ZIA.

- **Domain Inclusions for DNS Requests** – Allows you to specify specific DNS hostnames that Zscaler Client Connector should forward to ZIA.

Bypassing ZIA When Zscaler Client Connector Cannot Connect

There are times where you might choose to have Zscaler Client Connector fail-open. The supported options are:

- **Captive portal detected** – A captive portal is blocking access to the internet.
- **ZIA Service Edge is not reachable** – Something on the network is preventing the client from connecting to the nearest ZIA Service Edge.
- **Z-Tunnel setup issues** – Zscaler Client Connector is unable to establish a Z-Tunnel, the lightweight tunnel established from the client to the ZIA Service Edge used to forward traffic.

The use of captive portals is widespread in hospitality Wi-Fi networks, such as those found in airports and hotels. Captive portal detection allows the client to disable itself for a short time while the user authenticates to the portal, and then re-enable itself after the timer expires. You can set a value from 1 to 60 minutes. Zscaler recommends enabling captive portal detection. The disable time setting should be set as low as you feel is reasonable for users to interact and pass a captive portal registration system.

The unreachable ZIA Service Edge use case occurs when the client is unable to establish a connection due to network configuration. This could be a completely isolated network, such as in a lab setting. In this case, you can choose to either fail-open, sending traffic directly to the internet or local network, or fail-close and disable internet access. The use of this feature should be governed by your organization's policy, and how you want to treat user traffic when it cannot be secured on the internet. Zscaler Client Connector continues trying to establish a connection in the background and re-enables when connected.

The Z-Tunnel setup issue occurs when Zscaler Client Connector can locate a ZIA Service Edge but cannot establish a tunnel. This could be a case where the ZIA Service Edge resolves with DNS, but the tunnel setup is blocked by a network firewall. In this case, you can choose to either fail-open, sending traffic directly to the internet or local network, or fail-close and disable internet access. The use of this feature should be governed by your organization's policy, and how you want to treat user traffic when it cannot be secured on the internet. Zscaler Client Connector continues trying to establish a connection in the background and re-enables when connected.

Learn more about Configuring Fail-Open Settings for Zscaler Client Connector (https://help.zscaler.com/zscaler-client-connector/configuring-fail-open-settings-zscaler-client-connector).

Commonly Configured Settings

In addition to forwarding and application profiles, Zscaler Client Connector provides additional settings that allow you to deal with connection issues before they occur.

Captive Portals, Connection Issues, and Fail-Open Settings

When Zscaler Client Connector starts up, it attempts to reach a ZIA Public Service Edge. If it is blocked, the user is also prevented from reaching web applications and sites. Zscaler Client Connector provides mechanisms that allow you to decide how to handle connectivity issues before your users encounter them.

There are three conditions that can prevent Zscaler Client Connector from being able to connect to the ZTE cloud:

- A captive portal is blocking access to the internet.
- Zscaler Client Connector is unable to reach a Public Service Edge.
- Z-Tunnel setup is failing.

When configuring Zscaler Client Connector, you can set different responses to each of these conditions. Each setting allows one of the following actions:

- Allow direct access to the internet until a tunnel can be established (fail-open).
- Block all access until a ZIA Public Service Edge can be reached and tunnels established (fail-close).

A Captive Portal Is Blocking Access to the Internet

It is common on open Wi-Fi networks to be presented with a captive portal prior to being allowed access to the internet. This can either be to acknowledge a terms of service (TOS) agreement, or to pay for access for a duration of time. Zscaler Client Connector attempts to detect that a portal exists. If a portal is detected, you can choose to allow direct internet access for a specific number of minutes or disable detection entirely.

When you set a time value from 1 to 60 minutes, the ZIA service is disabled for that amount of time, and the user is permitted to access the internet. When the timer expires, Zscaler Client Connector attempts to establish a connection to the nearest ZIA Public Service Edge.

Zscaler recommends enabling captive portal detection. Without the ability to interact with the portal, the user cannot connect to the internet at that location. The length of time to disable ZIA should be set as low as you are comfortable setting it. While it is important to give users enough time to successfully interact with the portal, you must balance that against them having unprotected access to the internet.

Zscaler Client Connector Is Unable to Reach a Public Service Edge

There can be cases where the user is able to access the internet, but Zscaler Client Connector is unable to establish a connection to a ZIA Public Service Edge. This could be due to a routing issue with the user's ISP, a broken backbone connection, or action by a nation state. In these cases, you can choose to have Zscaler Client Connector send traffic directly to the internet, or disable all internet access until a ZIA Public Service Edge can be reached.

Your organization's policy should be used to dictate your organization's choice of allowing or disabling access. As an alternative to failing open, you can leverage ZIA disaster recovery to limit which URLs users are allowed to be accessed and when. More detail is provided in ZIA Disaster Recovery and Approved Applications.

Z–Tunnel Setup Is Failing

In some instances, network issues can cause Zscaler Client Connector to be unable to establish a Z-Tunnel to a ZIA Public Service Edge. This case differs in that the ZIA Public Service Edge is visible, but unable to establish a tunnel. These cases can be caused by some network address translation (NAT) devices, firewalls, and networks with multiple load-balanced internet connections.

In these cases, you can choose to have Zscaler Client Connector send traffic directly to the internet, or disable all internet access until a ZIA Public Service Edge can be reached. Your organization's policy should be used to dictate your organization's choice of allowing or disabling access.

Learn more about Configuring Fail-Open Settings for Zscaler Client Connector (https://help.zscaler.com/zscaler-client-connector/configuring-fail-open-settings-zscaler-client-connector).

ZIA Disaster Recovery and Approved Applications

To preserve your organization's ability to operate should Zscaler have a full worldwide outage, ZIA has a disaster recovery forwarding mode. When you configure this profile, you can choose how Zscaler Client Connector reacts if Zscaler becomes completely unreachable. A ZIA forwarding profile can be configured to allow your users to have limited access to preselected domains, full direct access to the internet, or no access at all.

If you choose limited access to certain domains, you need to also select the domains that are approved. Zscaler provides a list of preconfigured destinations that you can use. You can also create a custom destination URL list in the form of a proxy auto-configuration (PAC) file. You can choose to use both the Zscaler-provided list and a custom destination list at the same time, with the custom destination list taking precedence if there are conflicting statement definitions.

Zscaler recommends enabling ZIA disaster recovery with the URLs you are comfortable allowing users to access in an emergency.

- Learn more at Configuring Disaster Recovery (https://help.zscaler.com/zia/configuring-disaster-recovery).
- View the list of Zscaler preselected destinations (https://help.zscaler.com/zia/configuring-disaster-recovery).
- Learn more at Understanding PAC Files (https://help.zscaler.com/zia/understanding-pac-file).

Deploying Zscaler Client Connector

Authenticating Users to Zscaler Services

Zscaler services such as ZIA and ZPA require that a user authenticate to the service. By authenticating the user, the correct policy can be downloaded and applied. Zscaler Client Connector authenticates using SAML, leveraging your existing IdP data, and uses the system for cross-domain identity management (SCIM) so that user accounts remain synchronized.

Authentication Options

Zscaler Client Connector supports several authentication options. Except for Kerberos, all authentication methods supported by ZIA are also supported by Zscaler Client Connector.

While ZIA supports many other options, not all of these are suitable for large scale deployments. The complete list of supported authentication options includes Identity Federation using SAML, directory server, Zscaler Authentication Bridge, one-time link, one-time token, and passwords.

Zscaler recommends the use of SAML where possible, a modern, flexible, and robust authentication system used widely by application vendors. SAML and Zscaler Client Connector support two-factor authentication as well for added security.

Authenticating Users with SAML

When you use SAML for authentication, there are two ways a user can authenticate to the service: service provider-initiated SAML and IdP-initiated SAML. In both cases, the user is authenticated to ZIA, but the difference is where the user starts. Both authentication methods can be used at the same time to allow maximum flexibility for the end user.

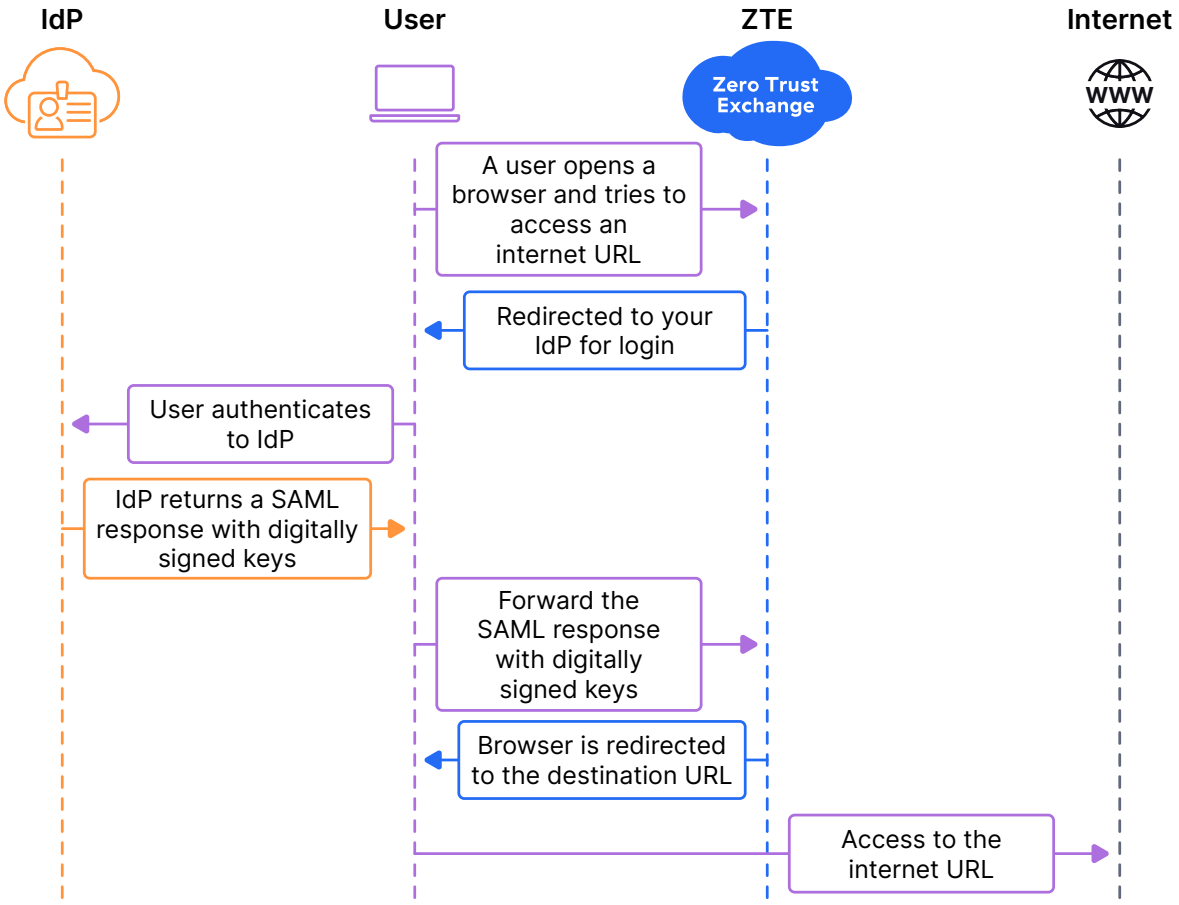

Figure 9: In service provider SAML, the user tries to use the internet and is challenged to first authenticate

In the service provider-initiated SAML authentication use case, the user attempts to go to any URL or web application, and the ZIA Service Edge first checks to see if the user is authenticated. Because the user in this case is not authenticated, the service begins the authentication process with your IdP. This is a very common model for users because it requires no additional step to trigger authentication.

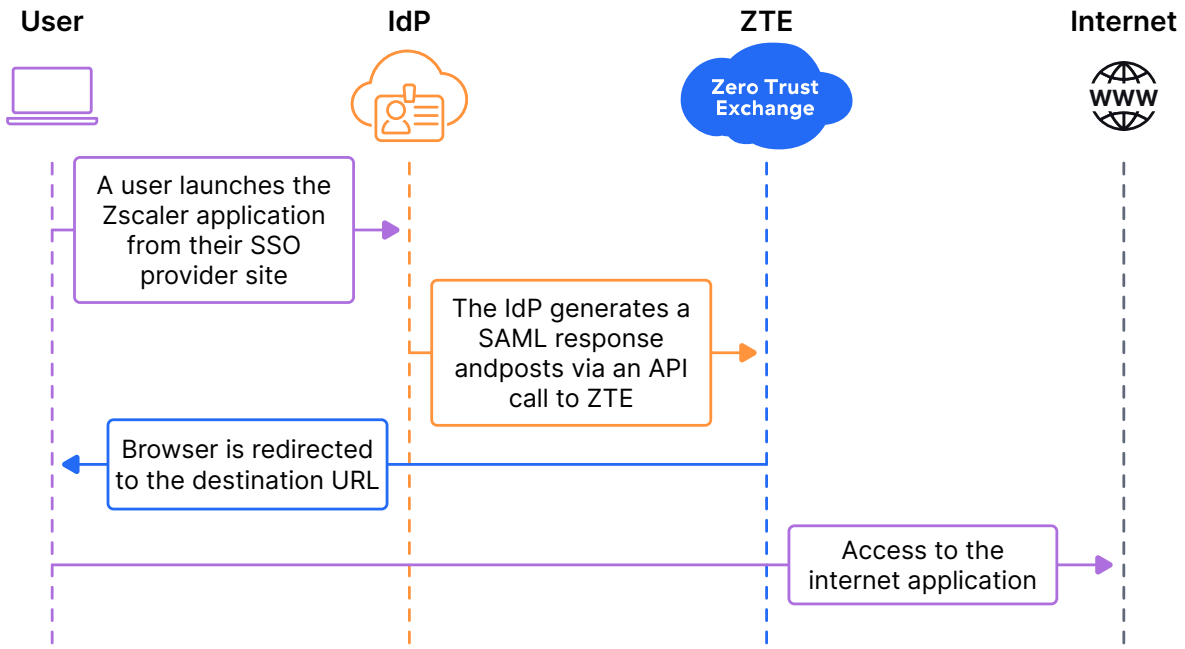

Figure 10: In IdP-initiated SAML, the user clicks on a tile to launch a website or application, and the IdP initiates authentication to the ZIA Private Service Edge.

In the IdP-initiated SAML authentication use case, the user first logs into their IdP via their SSO portal. These portals have tiles for applications that the user is authorized to access. Zscaler appears as an application tile that can be clicked to launch the application. When the user clicks the tile, they are authenticated to ZIA in the background.

Zscaler supports SAML responses up to 4 MB in size.

- For an in-depth discussion of Zscaler authentication, see User Provisioning and Authentication to Zscaler Services (https://www.zscaler.com/resources/reference-architectures/user-provisioning-authentication-zscaler-services.pdf).
- For a complete list of authentication methods, see Choosing and Provisioning Authentication Methods (https://help.zscaler.com/zia/choosing-provisioning-authentication-methods).
- Learn more about the SAML protocol at Understanding SAML (https://help.zscaler.com/zia/understanding-saml).
- Learn more at Understanding SCIM (https://help.zscaler.com/zia/understanding-scim).

SAML and SCIM (Recommended)

The use of SAML in enterprise deployments and tools has grown quickly in recent years. By filling the gap in authentication across security domains, SAML is often the tool of choice for SSO authentication. While SAML can handle provisioning on its own (see SAML Auto-Provisioning), SCIM updates are much faster than auto-provisioning

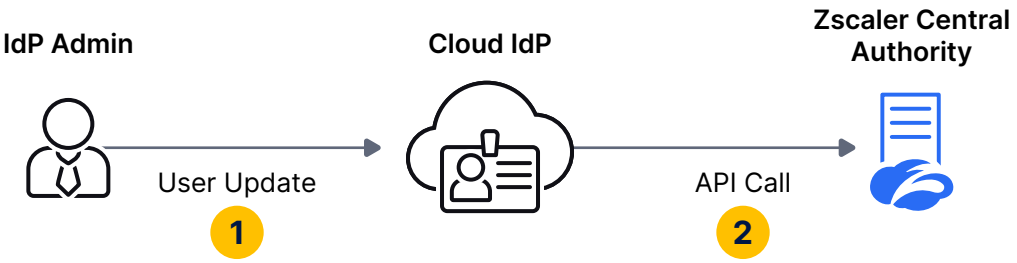

Figure 11: SCIM pushes updates via API calls to ZIA

When you enable SCIM updates, the ZTE cloud is updated in near-real time. SCIM leverages web API calls to ZTE, requesting that it update the local identity information to match the IdP data store.

1. An administrator makes a change to the user store at your IdP, in this example a cloud IdP vendor (recommended).
2. The cloud IdP in turn makes an API call to the Zscaler Central Authority (ZCA), updating the user identity information.

This includes provisioning of new users, updating as changes occur, and deprovisioning users. SCIM also has the advantage of not needing an inbound connection to your IdP, as the API call is outbound only.

To leverage SCIM, you must have a SCIM client connected to your IdP to push changes to the ZTE cloud via the API. Most major providers have SCIM clients integrated into their products, including Microsoft Azure AD, Okta, and PingFederate.

Zscaler recommends combining SAML and SCIM to be used together to provision and maintain your identity information in ZIA.

Zscaler supports only SCIM version 2.0, and it must be used with SAML for authentication. No other authentication types are supported.

SAML Auto-Provisioning

If your organization is using SAML, but your IdP does not support SCIM updates, SAML auto-provisioning is the next best alternative. With SAML auto-provisioning, identity information is retrieved from the IdP when a user attempts authentication.

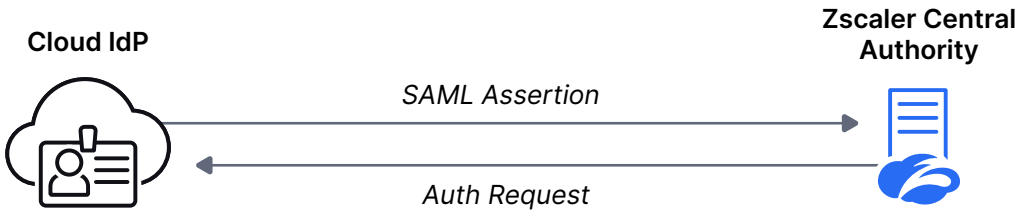

Figure 12: SAML auto-provisioning updates user information based on the information returned in the user's assertion

If successful, the user identity information is added to the database, including username, groups, and department information. The following actions are taken by auto-provisioning:

- New users who previously did not exist are added to the ZIA database with their identity information from the SAML response.
- If a user exists, but the SAML response has updated identity information, that information is updated in the ZIA database. This change can include removing information, including the user if they are no longer active in the IdP database.

While SAML auto-provisioning and SCIM result in effectively the same action, SCIM is a proactive change when the IdP is updated. Auto-provisioning is a reactive update, only changing database information when a user attempts to authenticate.

Leveraging Device Posture During Authentication

Device posture evaluation allows you to compare a set of criteria against the actual state of the endpoint. Based on the criteria you set, such as OS version or installed antivirus software, the authenticated user is given a more open or restrictive policy based on the endpoint posture.

To leverage device posture, you must build individual posture profiles. Each posture profile looks at a single posture type. The following list of posture checks are available (note that not all checks are supported by all operating systems):

- **Certificate Trust** – The endpoint must trust your organization's internal certificate authority.
- **File Path** – Specify a path to a file that must exist on the endpoint.
- **Registry Key** – A specific Windows registry key must exist.
- **Client Certificate** – An internal CA or intermediate certificate for your organization must match one on the endpoint device and can perform a certificate revocation list (CRL) check.
- **Firewall** – At least one firewall profile is active from the public, private, and domain profiles.
- **Full Disk Encryption** – Full disk encryption must be enabled.
- **Domain Joined** – The device's domain or workgroup must match the configured option.
- **Process Check** – A particular process must be running on the endpoint. It requires a path to the process and the signature thumbprint for the process signer certificate.

- **Detect Carbon Black** – The endpoint must have Carbon Black running to pass the posture validation check.
- **Detect CrowdStrike** – The endpoint must have CrowdStrike running to pass the posture validation check.
- **CrowdStrike ZTA Score** – Allows you to specify a CrowdStrike ZTA score that the endpoint must meet or exceed. Values range from 1 to 100, and the higher the required value, the more secure the endpoint.
- **Detect SentinelOne** – The endpoint must have SentinelOne running to pass the posture validation check.
- **Ownership Variable** – Enter a variable using an alphanumeric value no greater than 32 characters that must also appear on the endpoint. Use your device management solution to push the variable to the device during installation.
- **Unauthorized Modification** – Checks for unauthorized modifications on the device, such as jailbreaking or rooting.
- **Detect Microsoft Defender** – The endpoint must have Microsoft Defender running to pass the posture validation check.
- **Detect Antivirus** – Check that antivirus software is installed and running on the endpoint. Optionally, you can specify the name of an antivirus product and check that its antivirus signature dictionary is up to date.
- **OS Version** – Check that one or more editions (versions) of an operating system are installed on the endpoint.

These posture profiles are leveraged by ZIA access policies when determining which policy to apply to a user and endpoint. Each of these profiles can work alone or in conjunction with other profiles in access policy. Up to 10 posture profiles can be applied to each access policy, giving you a robust framework for device compliance.

All devices check whenever the device boots, wakes up, or connects to a new network, or when the Zscaler service restarts. In addition, macOS and Windows based endpoints check the device's posture every 15 minutes. If a device fails a posture check, that access policy is not applied to that endpoint.

Leveraging this system, an endpoint and user can be granted access to the organization's banking only if they match 10 different device posture checks and are authorized by the IdP to take such actions. If they fail the posture checks, they are given a more restrictive set of policies that do not allow access to financial services.

You can also use posture checks to assign policies that allow users to self-remediate. If a device fails an operating system edition check, users are provided access to the software update for their operating system. If a user fails an antivirus signature check, the user is allowed to access the vendor's sites to update their client. By leveraging checks, you can help your users become more self-reliant.

To view the details of each control, see About Device Posture Profiles (https://help.zscaler.com/zscaler-client-connector/about-device-posture-profiles).

Customizing Authentication Suffixes

The Zscaler Client Connector agent can be customized to include a domain suffix for the user's identity credentials. This allows them to input only their username and not the entire domain. The suffix assigned can also be different based on the domain the user is connected to.

Learn more at Customizing the Zscaler Client Connector User Agent (https://help.zscaler.com/unified/customizing-zscaler-client-connector-user-agent).

End User Notifications

Zscaler Client Connector notifies end users when an interaction with the agent needs to occur. This includes items such as when the user needs to accept the organization's network acceptable use policy (AUP). A separate set of controls is available to notify users that they need to reauthenticate to the ZPA service. Each of these notifications is discussed in the following sections.

Zscaler recommends enabling notifications for all users. For Windows users, Zscaler recommends using the Zscaler Notification Framework instead of the native Windows notification system, where a user can disable Zscaler Client Connector notifications.

Learn more at About Zscaler Client Connector Notifications (https://help.zscaler.com/zscaler-client-connector/about-zscaler-client-connector-notifications).

Acceptable Use Policy Acceptance

You can create an AUP that your users must accept before they can connect to the internet or access your organization's internal resources from devices protected by Zscaler Client Connector. Most organizations have an AUP that has already been developed and can be leveraged for this purpose.

Zscaler Client Connector supports an AUP notification that allows you to log when a user accepts the policy. You can also set the frequency for prompting for acceptance again. This can range from never after the first acceptance, to having to accept the AUP every session. The frequency should be based on your organization's policy, regulatory, and governance requirements. Consult with your legal team on the frequency and triggers for displaying the AUP acceptance notification.

To learn more about the acceptable use policy, see TLS/SSL Inspection with Zscaler Internet Access (https://www.zscaler.com/resources/reference-architectures/tls-ssl-inspection-zscaler-internet-access.pdf).

To learn more about displaying the AUP acceptance and logging for users, see Configuring the Acceptable Use Policy (https://help.zscaler.com/zia/configuring-acceptable-use-policy).

ZPA Reauthentication Notification

Reauthentication to the ZPA service is required at intervals determined by your timeout policy. The timeout policy allows you to build granular rules around reauthentication if needed. The default rule is for all users to reauthenticate to the service every 7 days.

When the user's application access expires, they won't be immediately prompted to reauthenticate. The next time that the user tries to access a ZPA protected application, they are prompted to authenticate to ZPA. If notification is enabled, you can also specify in minutes how often to notify users again.

Learn more at About Timeout Policy (https://help.zscaler.com/zpa/about-timeout-policy).

Application Data Collection and User Privacy

Because the Zscaler Client Connector agent resides locally, it has access to many pieces of data on the end user machine, and you can control which pieces of information are collected. This section also contains the ability to enable features, including local packet capture and automatic crash reporting.

The features available for configuration are:

- **Configure Zscaler Client Connector to collect device owner information** – Collects the device owner name from supported devices, making them available in dashboards and logs.
- **Configure Zscaler Client Connector to collect machine hostname information** – Collects the device hostname from supported devices, making them available in dashboards and logs.
- **Enable the Start Packet Capture option for Zscaler Client Connector** – Provides access to local packet captures by the end user for support purposes.
- **Configure automatic crash reporting for Zscaler Client Connector** – Sends crash information automatically to Zscaler Support. Zscaler recommends that you enable this feature as crash reports provide crucial information for resolving unexpected issues.
- **Configure Zscaler Client Connector to collect ZDX geolocation information** – If your organization subscribes to ZDX, Zscaler Client Connector can send geolocation information to ZDX as an additional datapoint for the user.
- **Allow end user to override Z-Tunnel 2.0 or ZPA protocol settings** – Users can change the default parameters for Z-Tunnel 2.0 or ZPA protocol settings.

Learn more at About User Privacy (https://help.zscaler.com/zscaler-client-connector/about-user-privacy).

Zscaler Client Connector Store in the Admin Interface

When deploying Zscaler Client Connector to your users, you can download customized install packages for desktop and Android operating systems. These can be posted on an internal site and pushed by a device manager, or they can be included with your standard images. For iOS, your users need to download the application from the App Store or device management platform.

As you enable new versions of Zscaler Client Connector for use, agents automatically check every two hours for a new update. When you enable a new update for use, you can specify which groups get the update, update everyone at once, or simply set the system to always update to the latest version.

The interface shows a list of available Zscaler Client Connector versions by operating system, ordered by version with the latest version first. You can also see a list of new versions and download them directly.

Learn more at About the Zscaler Client Connector App Store (https://help.zscaler.com/zscaler-client-connector/about-zscaler-client-connector-app-store).

To learn more about downloading and deployment options, Zscaler has developed an extensive guide of help articles. These cover both direct installs and our technology partners in the device management realm. To view a full list of articles, see Downloading & Deployment (https://help.zscaler.com/zscaler-client-connector/downloading-deployment).

Viewing Enrolled Devices and Removing Devices

You can view and search through all devices enrolled in your organization from the Enrolled Devices page in the Zscaler Client Connector Admin Portal. When a user authenticates a device using Zscaler Client Connector for the first time, the details of the device are recorded and it is assigned a unique ID in the system. This table of devices ties together key pieces of information to help you view devices, status, and ownership. The table provides the following tabular data:

- **User ID** – The enrolled user for the device.
- **OS Type** – The device operating system.
- **Device Model** – The device model.
- **Zscaler Client Connector Version** – The Zscaler Client Connector version installed on the device.
- **Device State** – The status of the device. To learn more, see Device States for Enrolled Devices (https://help.zscaler.com/zscaler-client-connector/device-states-enrolled-devices).

When searching for a specific user or device, you can begin by filtering the table data. You can filter by active date, allowing you to narrow your search based on the last time the user or device was known to connect. You can further filter by device OS and/or device model if you are looking for a single device. You can filter by a user ID if you are trying to find all devices linked to a single user.

Exact data match searching also exists. This search can operate on additional fields, such as the Zscaler Client Connector version installed on the device, device ID, device fingerprint, or app profile name.

When you've found your devices, you can either export the device list as a CSV file or take action to remove the device. Device removal has a few options, depending on how quickly you need a user to be logged out of the system.

Soft Removal

Soft removal logs the user out at the next update and takes approximately one hour. When a device is selected, the device shows as pending removal on the enrolled device list. The Zscaler Client Connector agent remains installed. The end user can speed up the process by manually updating the policy after removal is set using the Zscaler Client Connector interface.

Force Removal

A force removal immediately logs the user out of Zscaler Client Connector. The Zscaler Client Connector agent remains installed.

Learn more about soft removing devices at Soft Removing a Device from the Admin Portal (https://help.zscaler.com/unified/soft-removing-device-admin-portal) and force removing devices at Force Removing a Device from the Admin Portal (https://help.zscaler.com/unified/force-removing-device-admin-portal).

After a user's device is removed, the Zscaler Client Connector agent software can be uninstalled. Learn more at Uninstalling Zscaler Client Connector (https://help.zscaler.com/zscaler-client-connector/uninstalling-zscaler-client-connector).

User Guide for Zscaler Client Connector End Users

Zscaler provides a user guide to help your end users navigate their local instances of Zscaler Client Connector. This publicly available documentation should be shared with your users to enable them to answer their own questions without a helpdesk ticket. To learn more, see the Zscaler Client Connector End User Guide (https://help.zscaler.com/zscaler-client-connector/end-user-guide).

Summary

Zscaler Client Connector is a lightweight, tamper-resistant agent that connects your users and devices to Zscaler security services. Zscaler Client Connector tunnels your user and device traffic back to Zscaler's Zero Trust Exchange (ZTE), where it is inspected and your policies are applied.

Zscaler Client Connector supports ZIA, ZPA, and ZDX services. It is included with your subscription and is available on multiple operating systems: Windows, macOS, Linux, iOS, Android, and Android Chrome OS. With a flexible deployment model and always-on security, Zscaler Client Connector simplifies security and access for your organization. This provides a consistent experience for the end user at your location, at home, or while traveling.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.