Solution Brief

Reliable Secure Remote Access for SAP with Zscaler Private Access (ZPA)

With 98% of the top 100 most valued brands relying on SAP—85 of which are SAP S/4HANA customers with more business migrating workloads everyday—it's crucial to provide reliable and secure remote access to business-critical SAP applications. Additionally, as hybrid work becomes the new norm and users access SAP from anywhere, on any device, and from any location, the virtual perimeter has expanded beyond the network all the way to users, devices, and applications. Yet, organizations continue to rely on legacy, network-centric technologies such as VPNs and firewalls to control application access. These traditional approaches are ineffective in the cloud and mobile-first world, creating performance bottlenecks and increasing security risks.

Instead, your business can leverage a zero trust approach that relies on identity and behavior to verify users and machines in real-time, and restricts data and access on a least-privilege basis. In fact, Gartner states that by 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA).

Introducing Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) is the world's most deployed ZTNA platform with 150+ points of presence powered by 100% renewable energy worldwide and peered with the world's largest cloud providers, providing secure, direct connectivity to private applications. Users accessing SAP applications that run on-prem or in the public cloud are never put on the network, making applications invisible to the internet and unauthorized users or attackers. IP addresses are never exposed using inside-out connections, and applications are segmented so that users can only access a specific app, limiting lateral movement.

When remote access becomes effortless, connectivity and availability improves. For customers such as Growmark, an agriculture supply cooperative, ZPA enabled business continuity and resiliency by allowing 98% of their staff to continue to effectively carry out their work from home. Eric Fisher, Director of IT at Growmark, noted that with ZPA for SAP, "we're getting a better security footprint, better visibility and we're more compliant".

Benefits of Zscaler for SAP

- **Deliver superior SAP user experience:** Boost the productivity of your hybrid workforce and proactively resolve user experience issues with ZDX's continuous monitoring and visibility.
- **Extend zero trust across apps, workloads, and IoT:** Leverage a single global policy engine to deliver fast, direct access to private SAP apps, workloads, and OT/IIoT devices.
- **Reduce operational complexity and costs:** With no hardware or software to manage, cloud-delivered zero trust network access (ZTNA) deployments eliminate infrastructure overhead.
- **Mitigate the risk of a data breach:** Make SAP applications invisible to unauthorized users and enforce least-privileged access, minimizing application attack surface of SAP S/4HANA.

> "With ZPA for SAP, we're getting a better security footprint, better visibility and we're more compliant. We can enable our users work from anywhere – a win all around."
>
> **Eric Fisher**
> Director of IT, Growmark

How Zscaler Private Access Works

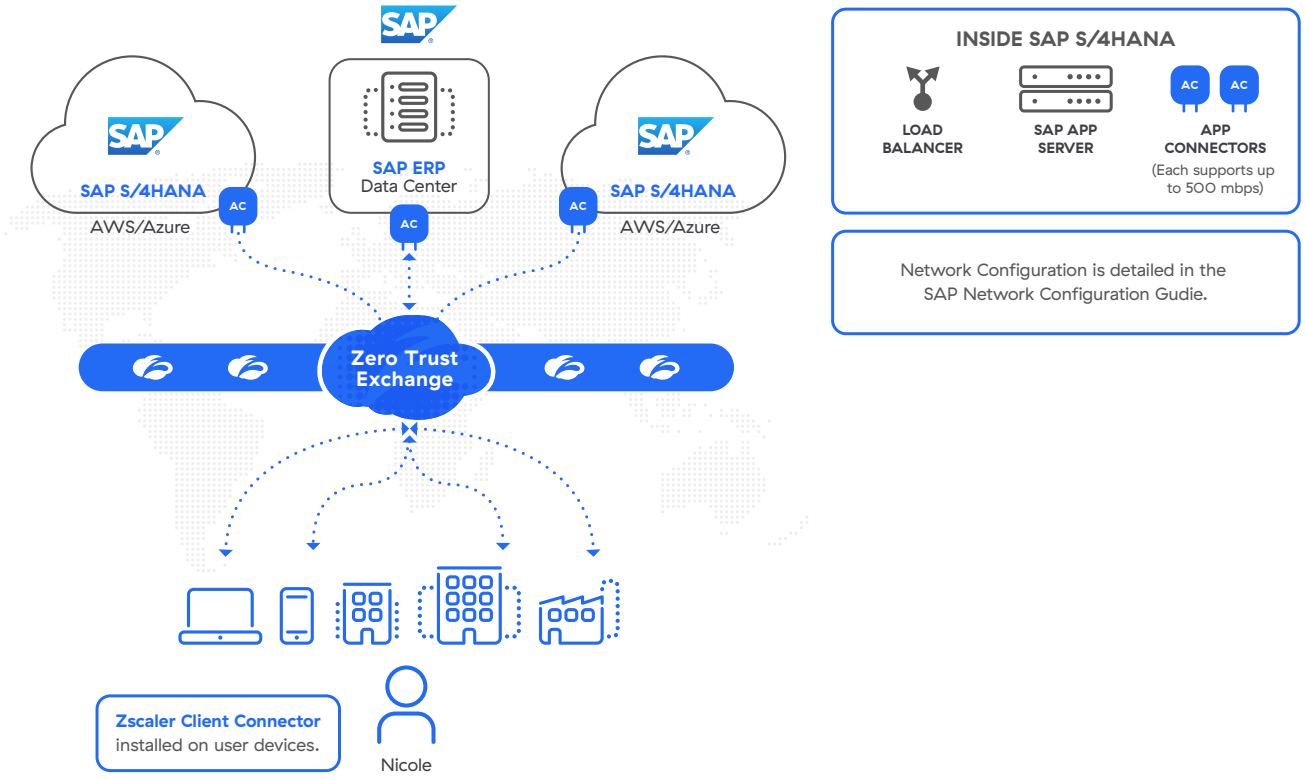


Figure 1: User reliably while securely accessing SAP applications in S/4HANA with ZPA

ZPA and SAP can be easily configured by understanding these common components, configuration steps, and following SAP best practices.

ZPA/SAP Components

- **App Connectors** provide an authenticated secure interface between organizations application servers and the ZPA cloud.
- **The Zscaler Zero Trust Exchange Platform (ZTE)** enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. The Zero Trust Exchange consists of 150 data centers worldwide, ensuring that the service is close to your users, co-located with the cloud providers and applications they are accessing, such as Microsoft 365 and AWS. It guarantees the shortest path between your users and their destinations, providing comprehensive security and an amazing user experience.
- **Zscaler Client Connector** is an application installed on your device to ensure that your internet traffic and access to your organization's internal apps are secure and in compliance with your organization's policies.
- **Applications** are a fully qualified domain name (FQDN), local domain name, or IP address that you define on a standard set of ports. Applications must be defined within an application segment.
- **App Segment** is a grouping of defined applications, based upon access type or user privileges.

- **Policies** in ZPA control how users access applications. Before a user can access an application, a policy must be defined. There are many types of policies. Please refer to our resource link for more information on policy types.
- **A Zscaler Tunnel (Z-Tunnel)**, is a TLS-encrypted, mutually authenticated point-to-point connection between Zscaler Client Connector and a ZPA Public Service Edge managed by Zscaler, or it's between an App Connector and a ZPA Private Service Edge managed by an organization. A Z-Tunnel does not contain any direct IP data. Also, the Z-Tunnel can carry within it multiple communication channels called Microtunnels.
- **A Microtunnel (M-Tunnel)** is an end-to-end communication channel created between Zscaler Client Connector and an internal application via a ZPA Public Service Edge, or ZPA Private Service Edge and an App Connector upon demand.
- **SAP App Servers** are servers that host SAP applications.

Securing remote access for users to SAP S/4HANA with ZPA

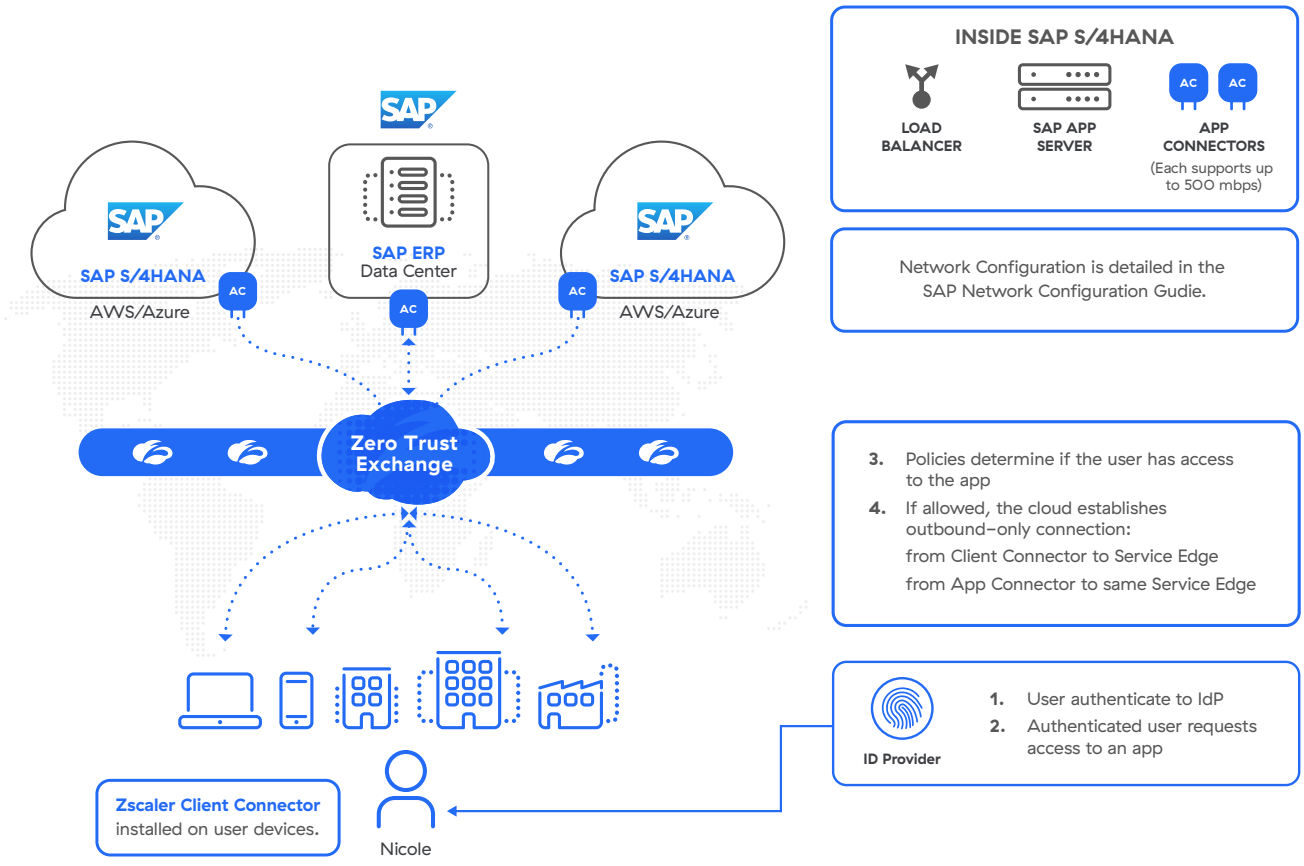
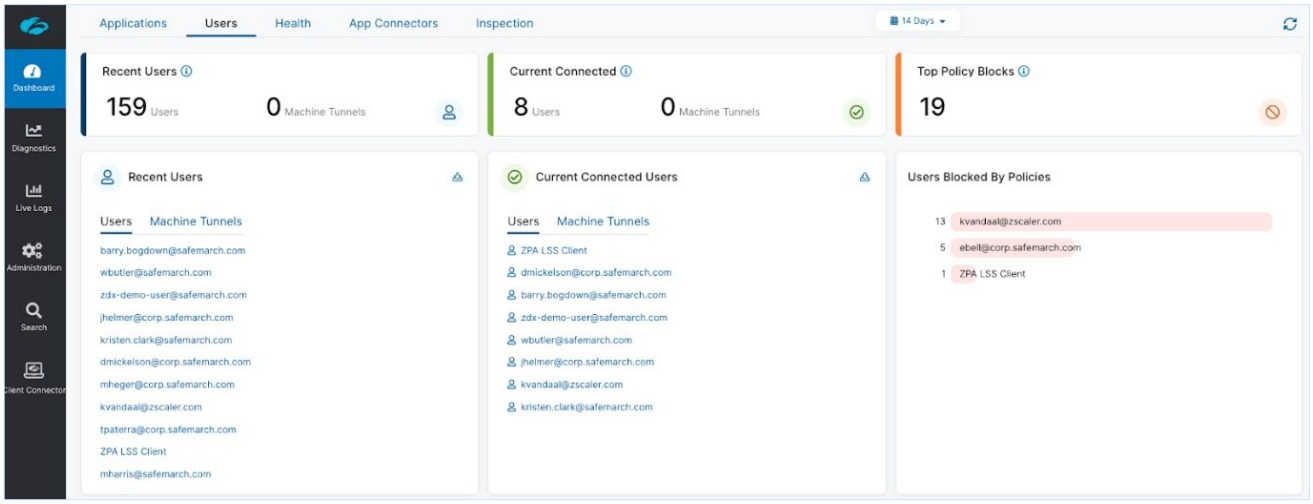


Figure 2: User reliably while securely accessing SAP applications in S/4HANA with ZPA (additional details)

Figure 1 and 2 depicts a ZPA deployment for a hybrid SAP environment. Nicole is an employee at ACME who needs to access an SAP application. Nicole can be located anywhere—at company headquarters, at her home, off-site at a company factory, or a coffee shop in the city.

When Nicole first requests access to an SAP application, she is prompted to authenticate with her organization's IDP. After authentication, the Zscaler Cloud evaluates Nicole's application request against existing policy. If Nicole is permitted to access the application, the Zero Trust Exchange will reach out to the App Connector nearest to the application, which will establish an inside out Z-Tunnel, an encrypted TLS connection, from the application to the Zero Trust Exchange. At the same time, the Zscaler Cloud will initiate an inside out Z-Tunnel from the Client Connector on Nicole's device back to the Zscaler Cloud. The Zscaler Cloud will then stitch the Z-Tunnels together and form an M-Tunnel inside of it, an end-to-end communication channel between Nicole and the application. Nicole now has secure access to the SAP application with the best user experience possible by leveraging the fastest connection from one of the over 150 global Zscaler points-of-presence.

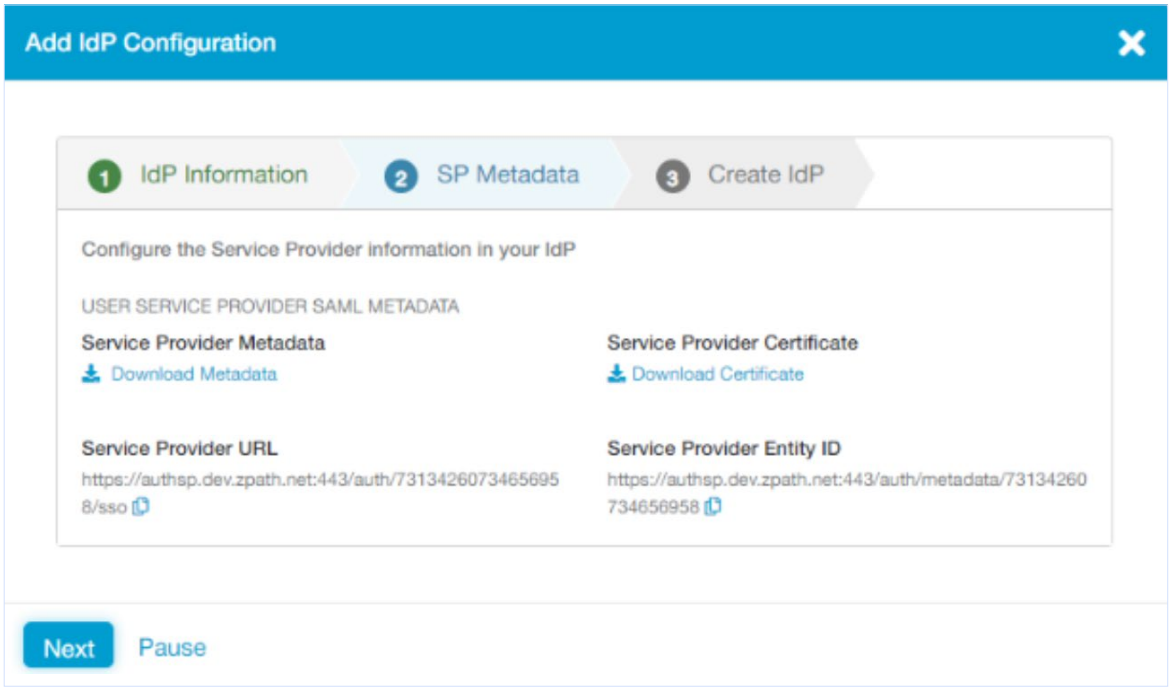


> "It's critical to provide our employees with a secure and highly available working environment by guaranteeing them secure access to applications in the cloud like SAP, and the internet at all times, while reducing our exposure."
>
> **Schmitz Cargobull**

Getting started with ZPA and SAP

For detailed steps on configuring ZPA refer to https://help.zscaler.com/zpa.

Step 1: Configure Single sign-on (SSO) Authentication and IDP

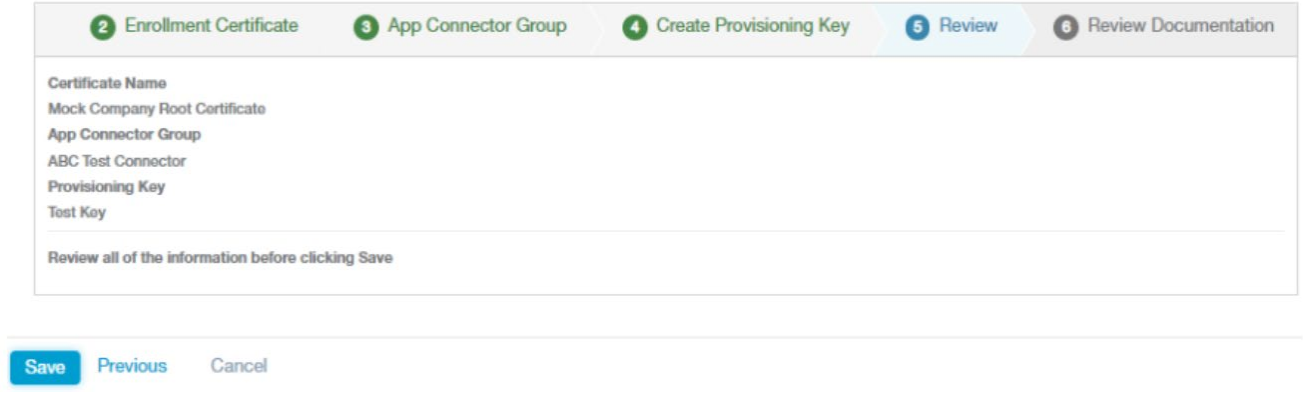


ZPA leverages user identities from an organization's existing Identity Provider (IdP), and can be configured to support one or multiple IdP solutions. ZPA supports single sign-on (SSO) via SAML so that your remote users can access enterprise applications without having to log in separately to ZPA.

In order for users to access your applications via ZPA, they must first authenticate into Zscaler Client Connector using any SAML 2.0-compliant identity provider (IdP) using the service provider-initiated (SP-initiated) model. ZPA user SSO is SP-initiated, but ZPA admin SSO can be SP-initiated or IdP-initiated.

1. Set up your IdP and specify ZPA as the SP. Before you can add an IdP configuration using the ZPA Admin Portal, you must have the IdP in place for your organization.
2. Add an IDP configuration via the ZPA Admin Portal.

Step 2. Deploy App Connectors



App Connectors provide the secure authenticated interface between SAP applications and the ZPA cloud. App Connectors are generally deployed in pairs for high-availability, and typically deployed adjacent to the SAP application server. App Connectors can be deployed in several forms. Zscaler distributes a standard virtual machine (VM) image for deployment in enterprise data centers, local private cloud environments, such as VMware, or public cloud environments such as Amazon Web Services (AWS) EC2. Additionally, Zscaler provides packages that can be installed on supported Linux distributions.

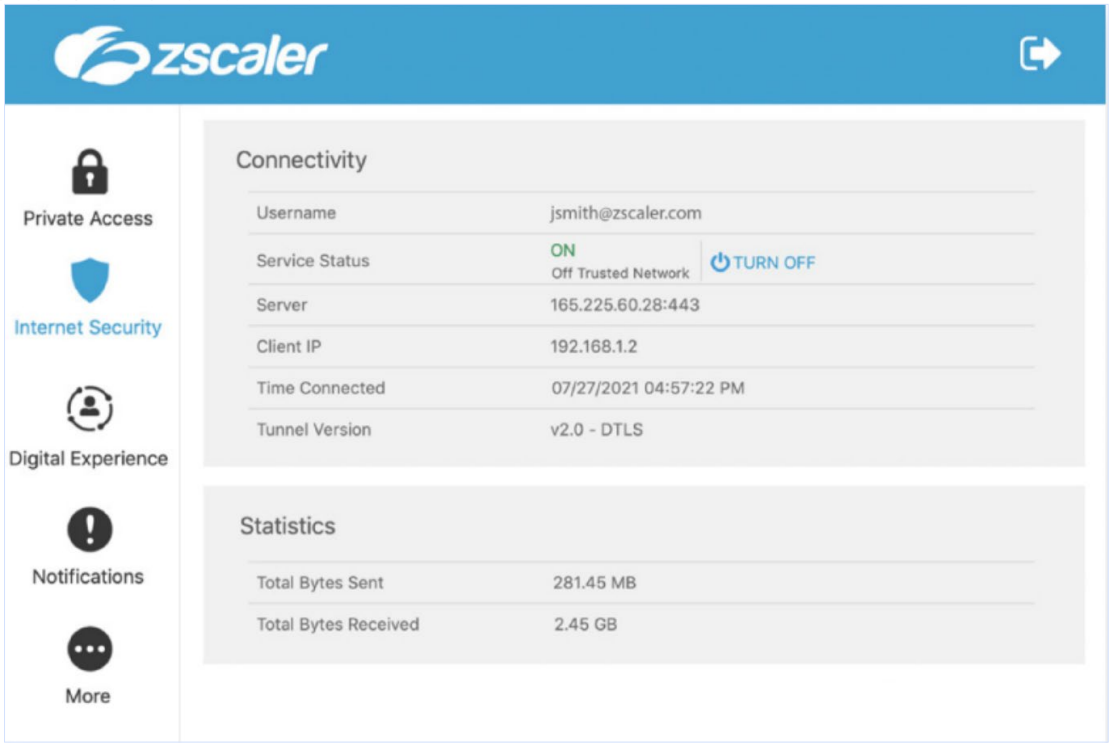
Standard App Connector configuration consists of two main steps:

1. Add an App Connector via the ZPA Admin Portal.
2. Deploy App Connectors on the supported platform of your choice.

However, configuring App Connectors for SAP HEC/PCE requires special steps:

1. SAP customer requests Zscaler Endpoint Service from their SAP account rep or customer delivery manager.
2. SAP installs high availability App Connectors in SAP HEC/PCE on behalf of customer.
3. Customer provides SAP with the ZPA license to apply to App Connectors.

Step 3. Configure Client Connector

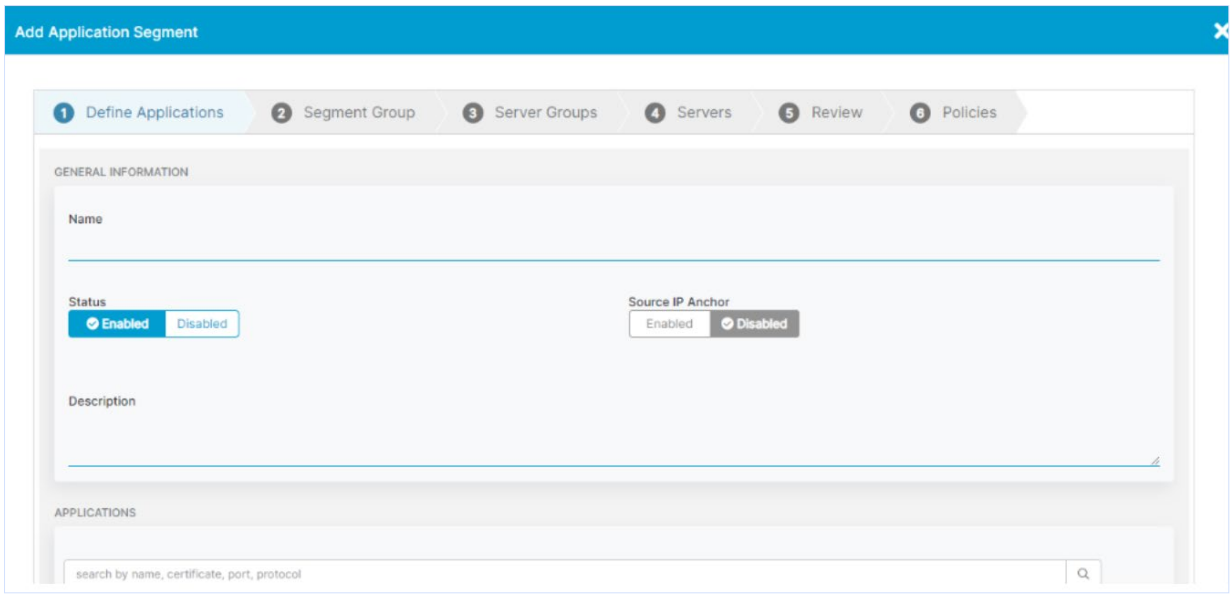


Zscaler Client Connector is a lightweight app that sits on users' endpoints—corporate-managed laptops and mobile devices, BYOD, handheld devices, and more—and enforces security policies and access controls regardless of device, location, or application. The Zscaler Client Connector app forwards traffic to the closest Zscaler Cloud point of presence, where the traffic is routed to SAP applications through the Zero Trust Exchange.

1. Complete system requirements and prerequisite tasks:
   - Configure appropriate security and access settings in the ZPA Admin Portal.
   - SAML-based authentication must be configured and users provisioned. You cannot use the Zscaler Client Connector Portal as an IdP for the ZPA service.
   - Ensure that Zscaler Client Connector properly processes traffic for ZPA.
2. Configure administration settings for Zscaler Client Connector. The acceptable use policy, update settings, forwarding policies, user access to support and logging, and fail open settings are all configurable.
2. Configure Client Connector Profiles. In the Zscaler Client Connector Portal, you can configure app profiles by adding policy rules to each profile. You can select the order of precedence among the rules as well as to whom each rule applies (i.e., to all users or to different groups of users). When a user enrolls the app with the Zscaler service, the app takes into account the order of precedence and the identity of the user in order to download an app profile with the appropriate policy rule.

4. Download Zscaler Client Connector from the Client Connector store
5. Customize Client Connector with installer options. You can configure a Zscaler Client Connector installer file with installation options that allow you to remove steps from the user enrollment process (e.g., allowing users to skip the enrollment page or the cloud selection prompt on Zscaler Client Connector).
6. Deploy Client Connector. You can install Zscaler Client Connector manually on individual devices or use your organization's device management mechanism to deploy Zscaler Client Connector on your users' devices.

Step 4. Add Applications Segments



An application segment is a collection of application instances. Applications are auto-discovered and can be grouped automatically based on matching criteria. An application segment can be anchored to one or more hosts or host segments. Application segments are used to accommodate policies that include or span multiple other segments.

Zscaler recommends the following best practices for configuring SAP App Segments:

- Create a single application segment for all SAP applications. This will allow the ZPA service to load balance user requests for these applications. However, if segmentation is required, then create multiple application segments for the SAP applications.
- Create application segments for SAP applications using FQDNs. If the SAP client is unsuccessful in resolving the host's FQDN, it will attempt to connect to the IP address. While the service supports IP addresses, it is more secure for zero trust models to connect with FQDNs.

- If the SAP hostname is not an FQDN, a DNS search domain is required. If the client has no search suffix, it cannot complete the FQDN to connect to SAP. The client will fall back to the IP address provided by the SAP message server, which might not be desirable or routable over the ZPA service.
- Use the Wireshark trace, or SAP configurations, to identify the IP addresses of all SAP servers, and create an application segment which includes only these IP addresses and the appropriate TCP ports. Do not advertise the entire subnet range (e.g., 192.168.1.0/24).
- If there is an access control list (ACL) configured in the SAP message server or application server, add the App Connector IP addresses to it. Since the ZPA service performs a source NAT for the client, all traffic is seen from the IP address of the App Connector. For the App Connector group associated with the application segments, ZPA will load balance user requests across App Connectors in this App Connector group. Because of this, it's recommended that the IP addresses for all the App Connectors in the App Connector group be added to the ACL.

Supporting SAP applications in ZPA requires you to configure application segments and DNS search domains.

1. Add an Application segment via the ZPA Amin Portal.
   - In the Add Application window, under Define Applications. Enter a fully qualified domain name (FQDN) that corresponds to the SAP applications. While it's possible to enter an IP address, Zscaler recommends you use FQDNs wherever possible as it's more secure. If the client has no search suffix, it cannot complete the FQDN to connect to SAP. The client will fall back to the IP address provided by the SAP Message Server.
   - To ensure Zscaler Client Connector Access make sure to enter the TCP Port ranges for the application.
2. Add a DNS Search Domain. For SAP, you can configure DNS Search Domains for FQDNs within the ZPA Admin Portal. This allows the SAP client to append the search suffix and build the FQDN. However, you can also configure SAP to provide an FQDN instead of a short name. Doing this removes the need to configure a DNS Search Domain.

Resources

ZPA Policies
ZPA: Supporting SAP Applications
RISE with SAP S/4HANA Cloud, private edition and SAP ERP, PCE

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com