Solution Brief

Secure SAP Cloud Migration and App Modernization with Zscaler Private Access (ZPA)

Businesses are embracing digital transformation to reap the benefits of improved performance, reduced costs, and operational complexity. For SAP customers, digital transformation is also fueled by the end-of-support for SAP ERP Central Component (SAP ECC) 6.0, an on-premises enterprise resource planning system. This is unsurprising as Gartner estimates that by 2025, 95% of new digital workloads will be deployed natively in the cloud. However, end-user experience is an afterthought during the SAP S/4HANA migration process, remaining slow, complicated, or risky.

Legacy technology continues to place users on the network and leads to complexity that slows the migration to cloud, making it hard for enterprises to realize a return on their cloud investment. Simply put, castle-and-moat and hub-and-spoke architectures can't scale or deliver a fast, seamless user experience.

Introducing Zscaler Private Access (ZPA)

To accelerate SAP S/4HANA cloud migrations and ensure user experience and productivity throughout the transformation process, organizations can leverage Zscaler Private Access (ZPA) for seamless and consistent experiences, effortless application modernization, and application-based security. With 150+ points of presence peered with the world's largest cloud providers, customers such as Kubota, an agricultural machinery manufacturer, can quickly scale and expand operations, stating "The next time we add a warehouse, there is no need to wait for weeks and spend thousands of dollars on networking to connect to our SAP ERP systems for inventory management...we are up and running anywhere on day one."

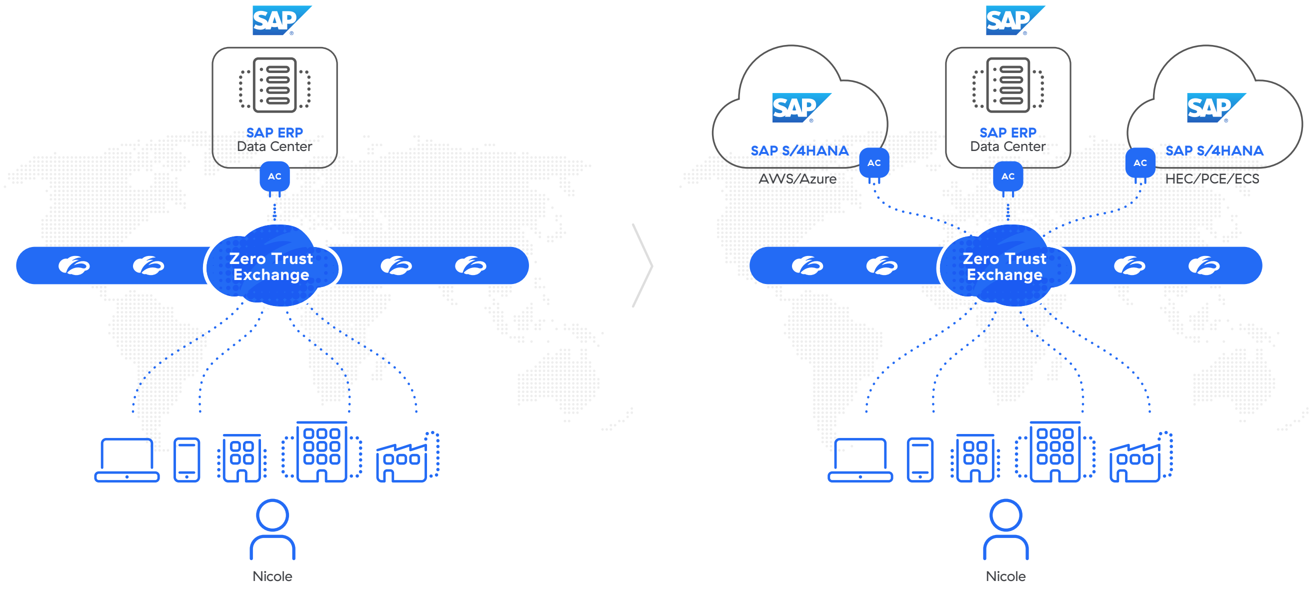
Acting as an abstraction layer between the user and the app, ZPA's single, global policy engine enforces zero trust principles across all devices, locations, and applications. Users connect the same way to apps running in the data center as they do to those in the cloud and from any device or location. The location of the app can be changed through a simple policy change, from datacenter to public cloud or VPC to VPC, securely connecting users directly to private apps and with a superior user experience.

Benefits of Zscaler Private Access (ZPA):

- Accelerate SAP application migration and cloud adoption
- Enable granular control of user access to SAP Suite applications
- Actively manage workload access pre- and post-migration
- Deliver end-to-end SAP application visibility and improved user experience

> "The next time we add a warehouse, there is no need to wait for weeks and spend thousands of dollars on networking, we are up and running anywhere on day one with our 4G-connected RF scanners using the Zscaler Client Connector to connect to our SAP ERP systems inventory management."
>
> **Jonathon Bonnici**
> IT Service Delivery Manager,
> Kubota Australia

How Zscaler Private Access Works

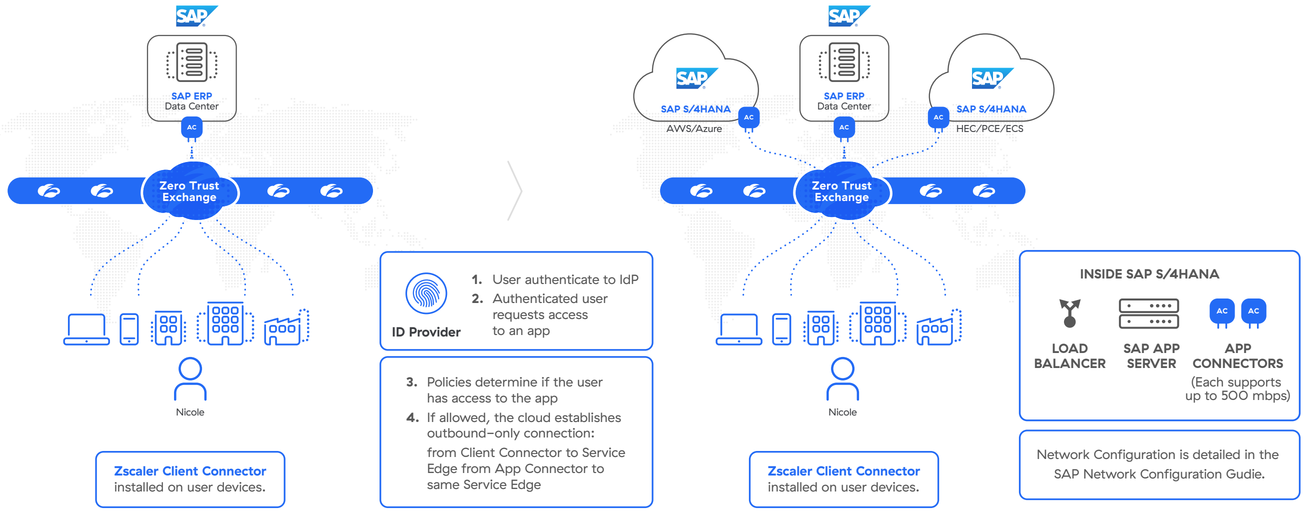


ZPA/SAP Components

- 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.
- Servers host applications made available for ZPA, the servers can be located in enterprise data centers or in virtual public clouds.
- Server Groups are a collection of servers. Each Application Segment must be mapped to a Server Group.
- SAP App Servers are servers that host SAP applications.

ZPA and SAP Design



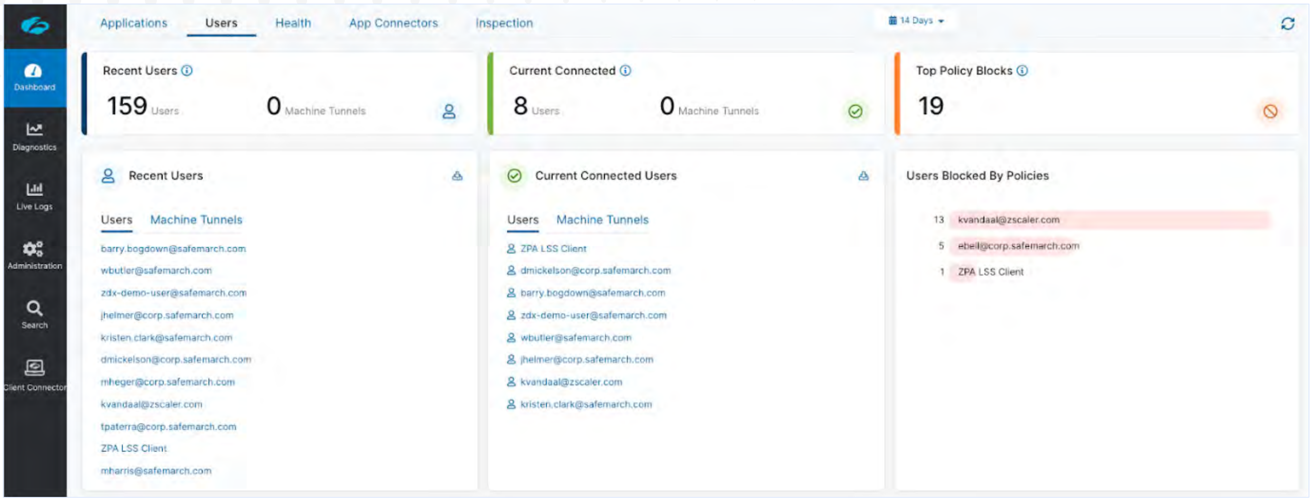
1. User authenticate to IdP
2. Authenticated user requests access to an app
3. Policies determine if the user has access to the app
4. If allowed, the cloud establishes outbound-only connection: from Client Connector to Service Edge from App Connector to same Service Edge

Zscaler Client Connector installed on user devices.

Network Configuration is detailed in the SAP Network Configuration Gudie.

For example, ACME currently hosts their SAP ERP system in an on-premise data center at company headquarters. The enterprise is in the process of network and application modernization with plans to migrate all of the company's SAP applications to the S/4HANA on AWS and Azure. Fortunately, ACME is leveraging ZPA, a part of Zscaler Zero Trust Exchange (ZTE), at the start of their transformation journey, reducing friction throughout the process to ensure a simple and seamless experience.

When Nicole, an employee at ACME, requests access to an SAP application hosted in the on-premise data center, she is prompted to authenticate with ACME's Identity provider (IdP). After authentication, the ZTE evaluates Nicole's application request against existing policy. If Nicole is permitted to access the application determined by identity and context, the ZTE 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 ZTE. Simultaneously, the ZTE will initiate an inside out Z-Tunnel from the Client Connector on Nicole's device back to the ZTE. The ZTE will then stitch the Z-Tunnels together and form an M-Tunnel, an end-to-end communication channel between Nicole and the application, inside of it.This same process happens when ACME migrates their SAP Applications to the cloud. ACME simply duplicates the applications from the on-premise data center to the cloud. When ready, ACME simply removes the applications from the on-premise data center. Now, when Nicole goes to access her SAP applications, she's automatically routed to the applications in the cloud.



Recent Users: 159 Users, 0 Machine Tunnels

Current Connected: 8 Users, 0 Machine Tunnels

Top Policy Blocks: 19

Recent Users (Users | Machine Tunnels)

- barry.bogdown@safemarch.com
- wbutler@safemarch.com
- zdx-demo-user@safemarch.com
- jhelmer@corp.safemarch.com
- kristen.clark@safemarch.com
- dmickelson@corp.safemarch.com
- mheger@corp.safemarch.com
- kvandaal@zscaler.com
- tpaterra@corp.safemarch.com
- ZPA LSS Client
- mharris@safemarch.com

Current Connected Users (Users | Machine Tunnels)

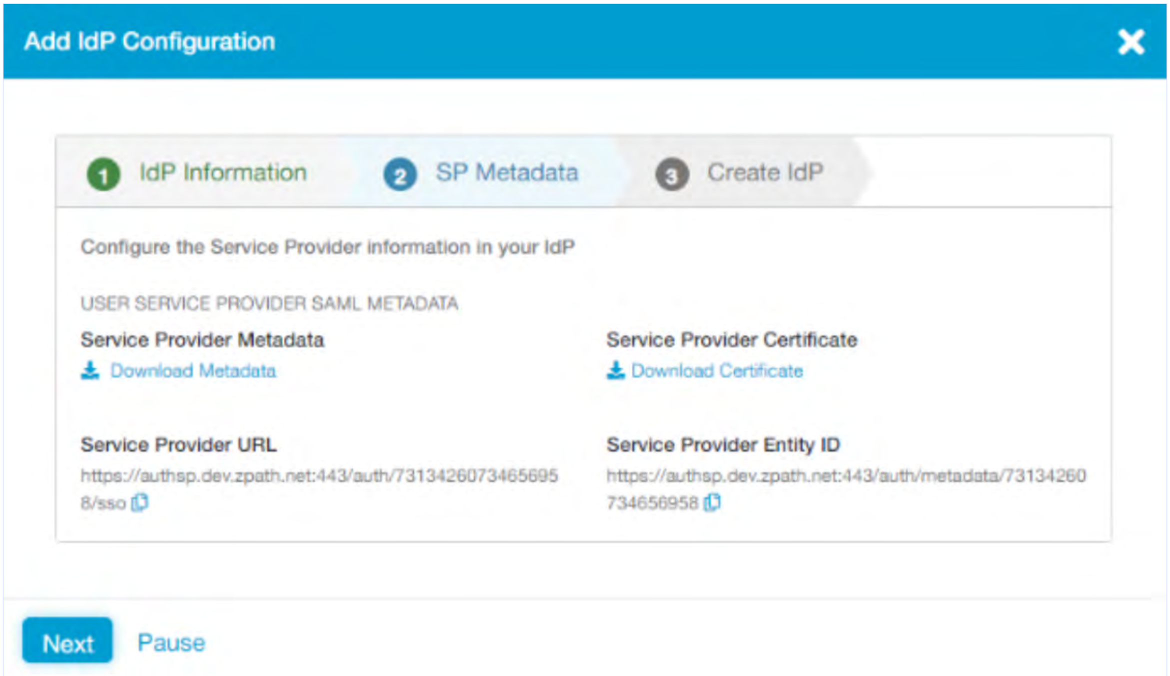
- ZPA LSS Client
- dmickelson@corp.safemarch.com
- barry.bogdown@safemarch.com
- zdx-demo-user@safemarch.com
- wbutler@safemarch.com
- jhelmer@corp.safemarch.com
- kvandaal@zscaler.com
- kristen.clark@safemarch.com

Users Blocked By Policies

13	kvandaal@zscaler.com
5	ebell@corp.safemarch.com
1	ZPA LSS Client

Getting started with Cloud Migration and App Modernization

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



Configure the Service Provider information in your IdP

USER SERVICE PROVIDER SAML METADATA

Service Provider Metadata

Service Provider Certificate

Service Provider URL: https://authsp.dev.zpath.net:443/auth/73134260734656958/sso

Service Provider Entity ID: https://authsp.dev.zpath.net:443/auth/metadata/73134260734656958

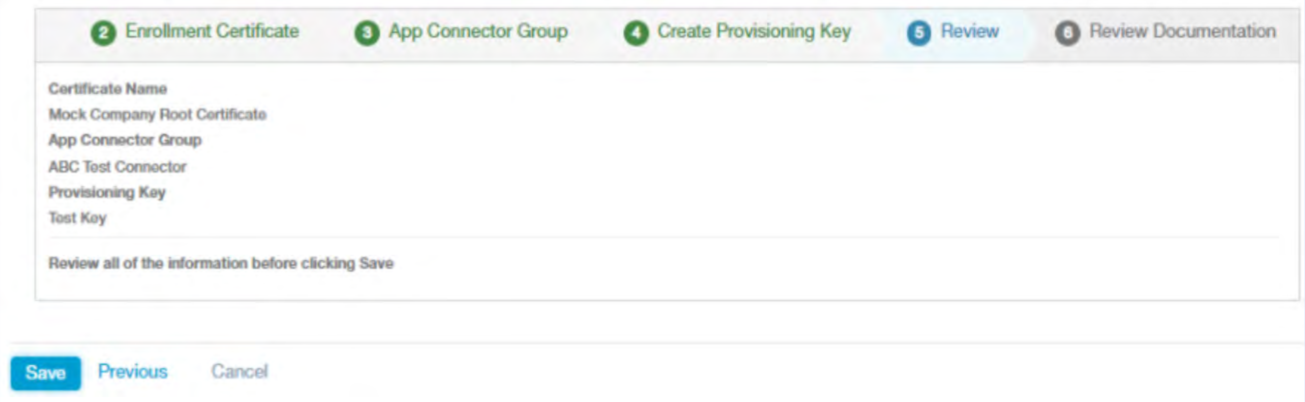
ZPA leverages user identities from an organization's existing Identity Provider (IdP), and can be configured to support one or multiple IdP solutions. ZPA supports single sign-on (SSO) via SAML so that your remote users can access enterprise applications without having to log in separately to ZPA.

In order for users to access your applications via ZPA, they must first authenticate into Zscaler Client Connector with 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. Configure App Connectors and App Connector Groups



Certificate Name
Mock Company Root Certificate
App Connector Group
ABC Test Connector
Provisioning Key
Test Key

Review all of the information before clicking Save

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 are further organized into App Connector Groups. Every App Connector belongs to a specific App Connector Group and every App Connector group is associated with at least one Server Group to serve any application. 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.

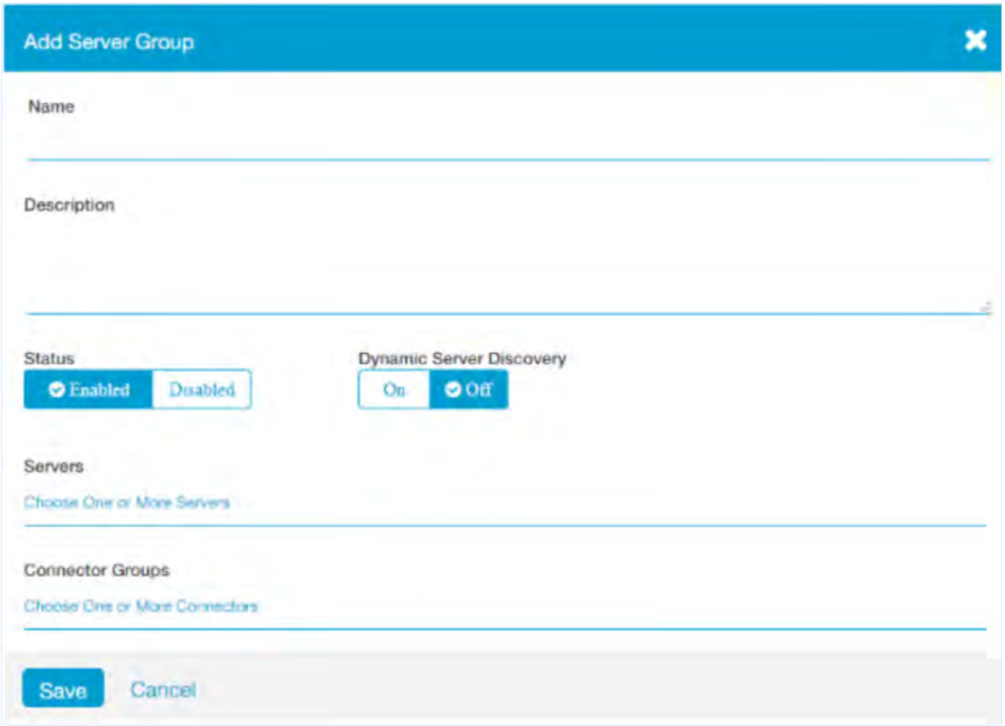
2. Deploy App Connectors on the supported platform of your choice.

3. For cloud migration, App Connectors will need to be associated with the Server Group for the on-prem data center and the Server Group for the cloud.

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 the customer.
3. Customer provides SAP with the ZPA license to apply to App Connectors.

Step 3. Configure Servers and Server Groups



Add Server Group

Name

Description

Status: ● Enabled | Disabled

Dynamic Server Discovery: On | ● Off

Servers: Choose One or More Servers

Connector Groups: Choose One or More Connectors

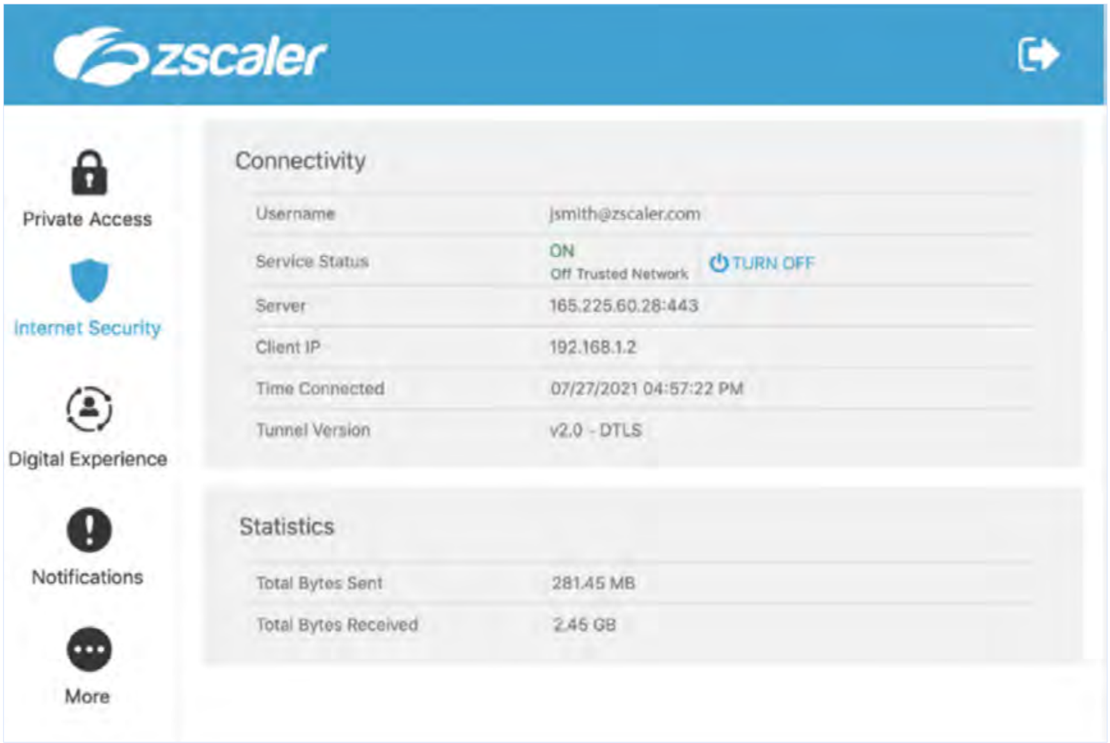
You must configure servers that host the applications you want to make available for ZPA, whether the servers are in your enterprise data center or in a virtual public cloud (VPC).

There are two main methods for server configuration:

- **Explicitly define servers and server groups:** You can explicitly define every server that hosts one or more applications. For each server, you provide a name as well as an IP address or a fully qualified domain name (FQDN). Then, you can manually arrange those servers into server groups.
- **Enable Dynamic Server Discovery:** Instead of explicitly defining each server, you can enable dynamic server discovery so that ZPA can discover the appropriate servers for your applications as users request them. For this method, you only need to create an empty server group that has dynamic server discovery enabled.

Each Application Segment will be associated with a server and server group. If Dynamic Server Discovery is enabled, then when the application is migrated to the cloud, ZPA will automatically register the change and route customers to the application in the cloud. If Dynamic Server Discover is not enabled, then the ZPA Admin will need to manually change the server and server group associated with the application that now resides in the cloud.

Step 4. Configure Client Connector



Connectivity

Username	jsmith@zscaler.com
Service Status	ON Off Trusted Network
Server	165.225.60.28:443
Client IP	192.168.1.2
Time Connected	07/27/2021 04:57:22 PM
Tunnel Version	v2.0 - DTLS

Statistics

Total Bytes Sent	281.45 MB
Total Bytes Received	2.45 GB

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 the 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.

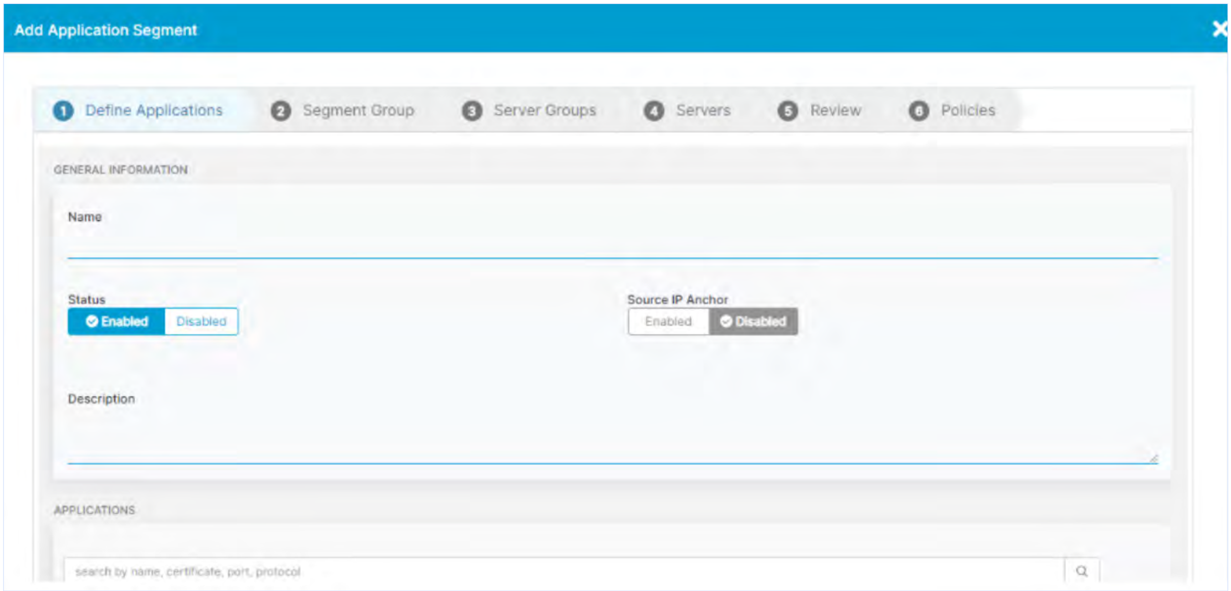
3. Configure Client Connector Profiles. In the Zscaler Client Connector Portal, you can configure app profiles by adding policy rules to each profile. You can select the order of precedence among the rules as well as to whom each rule applies (i.e., to all users or to different groups of users). When 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 5. Add Applications Segments



Status: Enabled | Disabled (Enabled selected)

Source IP Anchor: Enabled | Disabled (Disabled selected)

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.

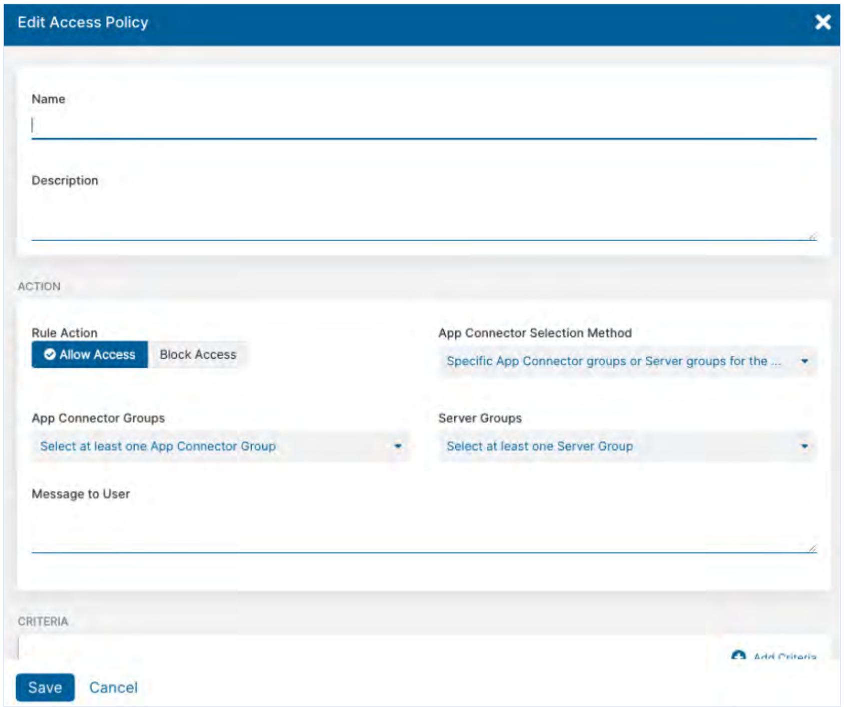
Zscaler recommends the following best practices for configuring SAP app segments:

- 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 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.

Step 6. (Optional) – App Migration via Policy


Edit Access Policy
Name
Description
ACTION
Rule Action
Allow Access
Block Access
App Connector Selection Method
Specific App Connector groups or Server groups for the ...
App Connector Groups
Select at least one App Connector Group
Server Groups
Select at least one Server Group
Message to User
CRITERIA
Add Criteria
Save
Cancel

During typical cloud migrations there are no additional policy changes necessary to complete the user access migration from legacy application to cloud application.In some cases, organizations may not want to migrate all users at once to cloud applications. For example, they may want to test the cloud applications with a small group of users before migrating every user. In this scenario, organizations can use a policy based approach to cloud migration.

1. In the ZPA Admin portal, create a policy for the users that will be accessing the applications in the cloud, and select the option for “Specific App Connector groups or Server groups”.

2. Next, Select the App Connector group for the applications hosted in the cloud.

3. Repeat this process for the users that will access applications in the data center. Make sure to select the App Connector group for the applications in the on prem data center.

4. When ready, migrate the rest of the users to the cloud by updating the policy with the App Connector groups associated with the cloud.

Resources

ZPA Policies

ZPA: Supporting SAP Applications

RISE with SAP S/4HANA Cloud, private edition and SAP ERP, PCE

> “ZPA gives us flexibility to terminate users wherever we need to so we can run SAP in one region in AWS but fail over to another region & have those users connect seamlessly by a policy change. ZPA allows users access to legacy apps as well as our new SAP environment in the cloud.”
>
> **Growmark**

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that 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. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.