Solution Brief

Secure SAP Access for Supply Chain and Third Parties with Zscaler Private Access (ZPA)

Global enterprises with supply chain operations and OT and IIoT assets require third-party users, such as contractors and partners, to have agile and connected access to internal SAP business management applications. To maximize production uptime and avoid disruptions from equipment and process failures, organizations need to consider a modern user access approach that provides:

1. Agentless and secure remote access to supply chain users accessing the SAP Suite via a web browser from untrusted or unmanaged devices e.g. BYOD, contractors, factory floor workers, etc
2. A reduced SAP application attack surface exposure risks when granting supply chain access to enterprise applications i.e. users are connected directly to the SAP application without exposing other applications or the corporate network
3. Assurance that global access policies are consistently applied while maintaining user visibility and limiting excessive access permissions

Yet, the risk of extending access to third parties is extensive and supply chains are easy targets for ransomware and other sophisticated attacks. When disruptions occur, no matter how minor, they produce ripple effects that can impact the global economy. To mitigate risks, businesses have relied on VPNs to access necessary SAP ERP applications. However, in many cases, deploying a remote access client is not possible or requires additional IT infrastructure. In addition, partners may not have the necessary device-level privileges to install such clients or simply be unwilling to do so.

Introducing Zscaler Private Access (ZPA)

When access to SAP is crucial for supply chain operations, agentless Browser Access allows you to leverage a web browser for user authentication and application access over Zscaler Private Access (ZPA), without requiring users to connect to site-to-site VPNs or install the Zscaler Client Connector on their devices. This is pertinent for third-party users, such as contractors and partners, whose IT organization does not permit outside clients or whose bring-your-own-device (BYOD) cannot support clients.

For many customers like **Schmitz Cargobull**, an innovative manufacturer, accessing internal SAP applications using VPNs was no longer feasible after multiple access failures that jeopardized sensitive supply chain operations. After leveraging ZPA for secure access to SAP ERP, Michael Schöller, Head of Infrastructure, noted that "**employees and third parties can securely and reliably access SAP systems without exposing the entire network.**" When zero trust policies are enforced by default across all devices, locations, and applications, partners are never brought onto the network and the application is never exposed to the internet. By limiting unauthorized use, users are more productive and organizations are safeguarded from unwarranted lateral movement. ZPA admins can rely on the service for real-time visibility into user activity, identify users who access applications via browser access, and discover previously unknown apps.

Benefits of Zscaler for SAP

- **Secure agentless user and device access to SAP:** Never place third-party users or supply chain tools on your corporate network, reducing exposure to risks and lateral movement.
- **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.
- **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.
- **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.
- **Reduce operational complexity and costs:** With no hardware or software to manage, cloud-delivered zero trust network access (ZTNA) deployments eliminate infrastructure overhead.

How ZPA Agentless Access Works

ZPA/SAP Supply Chain Design

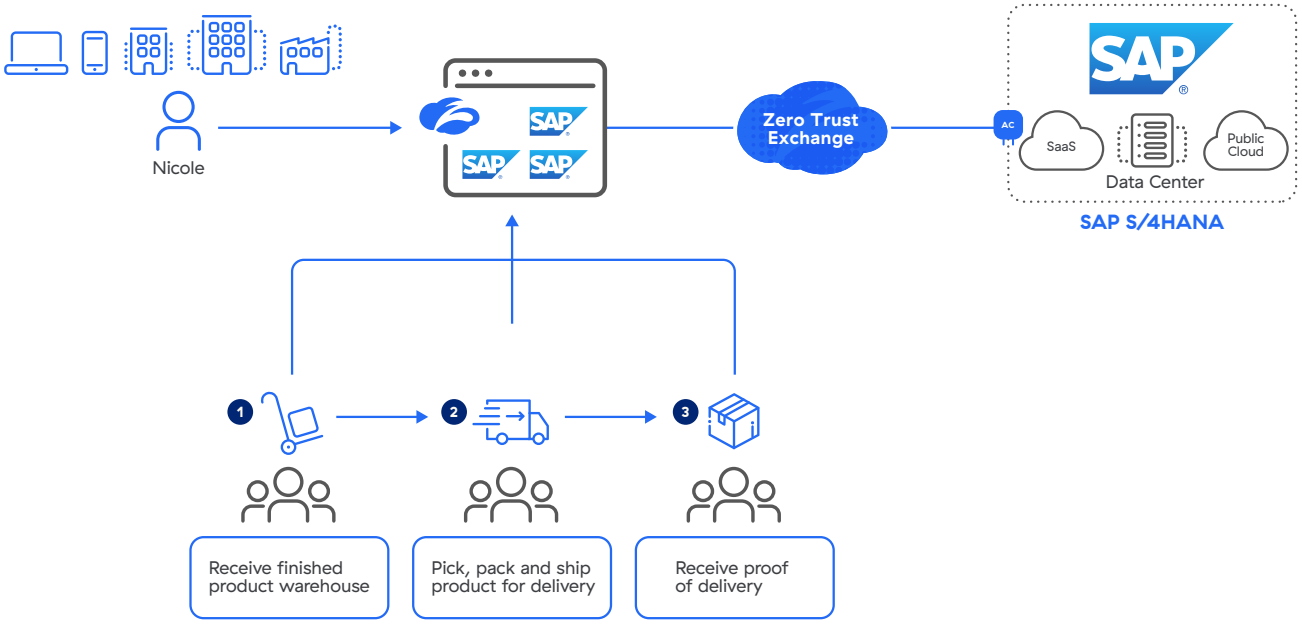


Figure 1: Employees and third-party users in the supply chain accessing SAP applications with ZPA Browser Access

ZPA/SAP Components

- App Connectors provide an authenticated secure interface between an organization's 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.
- Browser Access User Portals provide agentless users and devices access to authorized applications for an organization's employees or partners.
- 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.

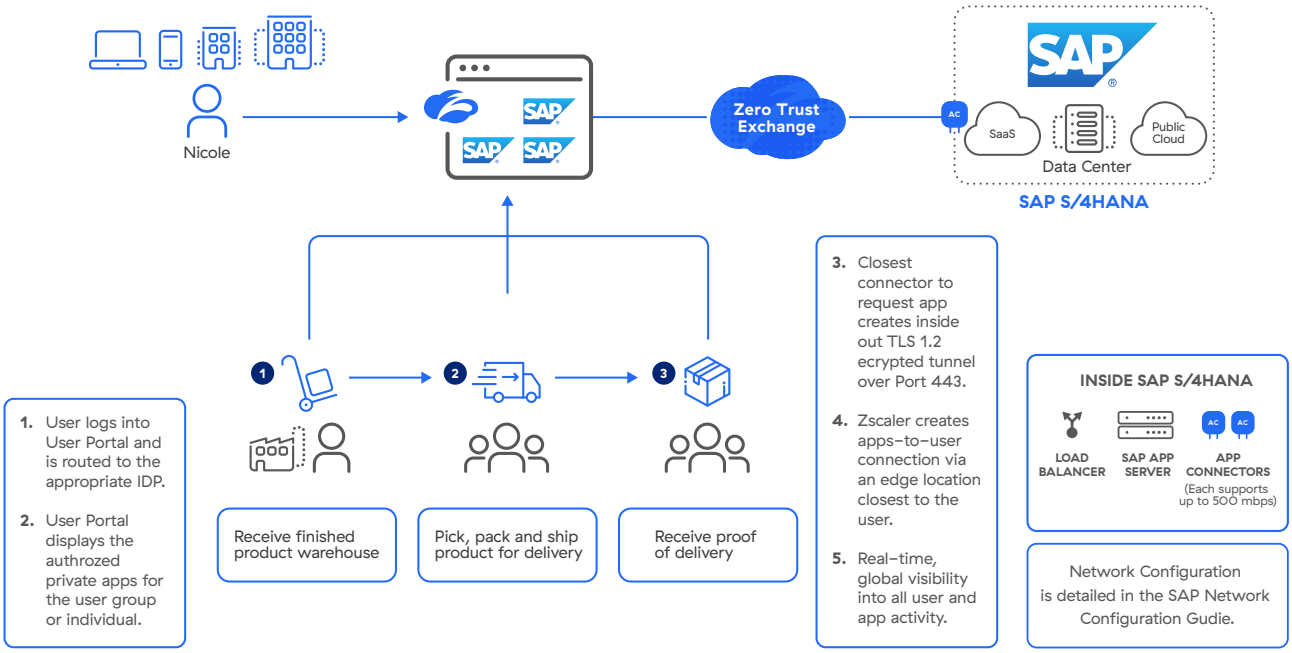
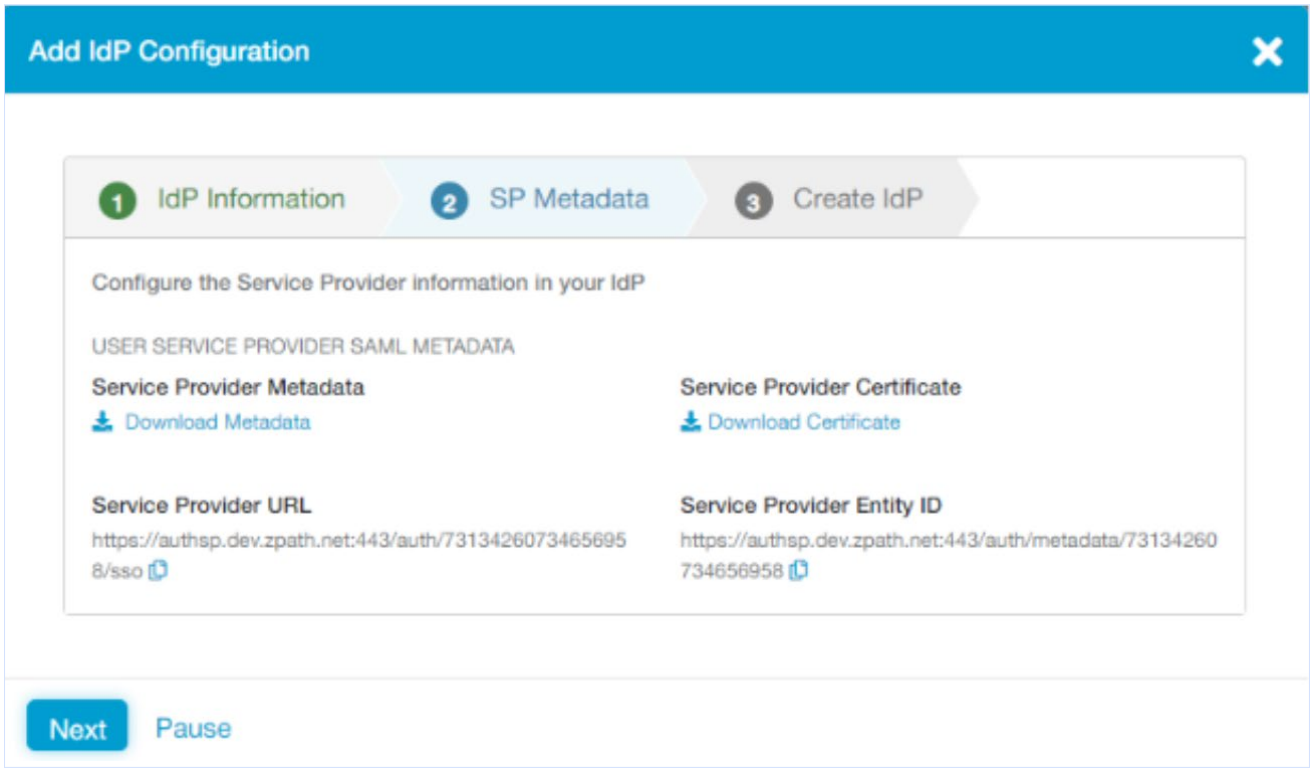


Figure 2: Employees and third-party users in the supply chain accessing SAP applications with ZPA Browser Access (additional details)

Figure 1 and 2 depict a ZPA deployment for a hybrid SAP environment. Nicole is an employee at ACME who needs to track products as they move through the supply chain. Paul is an employee at a warehouse that stores ACME products before they are shipped to customers. When Paul receives a shipment, he alerts ACME and Nicole via a ZPA Browser Access portal. Paul browses to ACME's user portal on his tablet and is redirected to his Identity Provider (IDP). After Paul authenticates, the user portal will display the appropriate applications for Paul. Paul selects the SAP Application he needs, and behind the scenes the closest App Connector to the requested SAP Application creates a Z-Tunnel, an encrypted TLS connection, to the Zscaler cloud. The Zscaler cloud then stitches the connection from the user portal to the SAP Application. Paul now has access and can update ACME, and Nicole, on their product locations. It's important to note that Paul doesn't need an ACME specific device, the device is agentless and can be unmanaged or untrusted, and only needs a web browser to access the ZPA Browser Access port for connecting to SAP applications.

Getting Started with ZPA Agentless Access for SAP

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



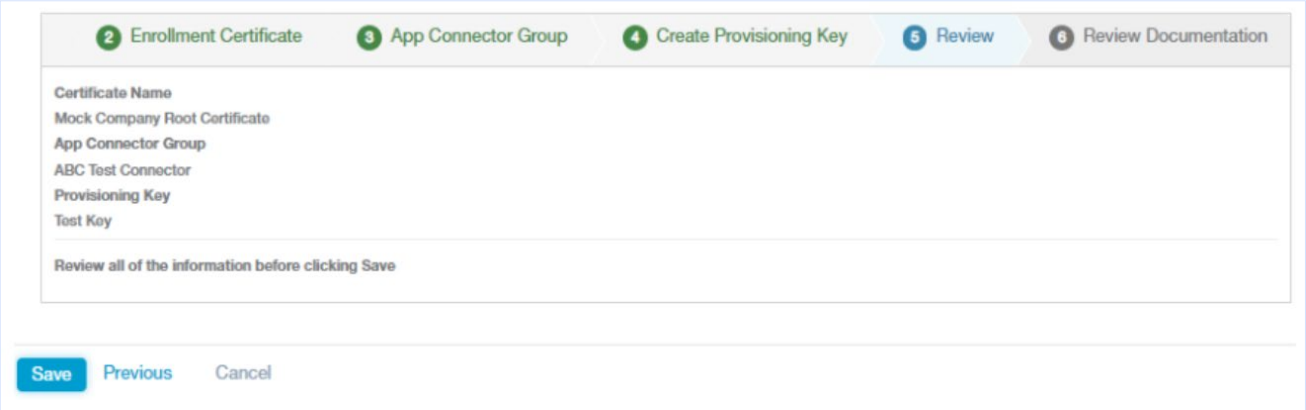
ZPA leverages user identities from an organization's existing Identity Provider (IdP), and can be configured to support one or multiple IdP solutions. ZPA supports single sign-on (SSO) via SAML so that your remote users can access enterprise applications without having to log in separately to ZPA.

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.

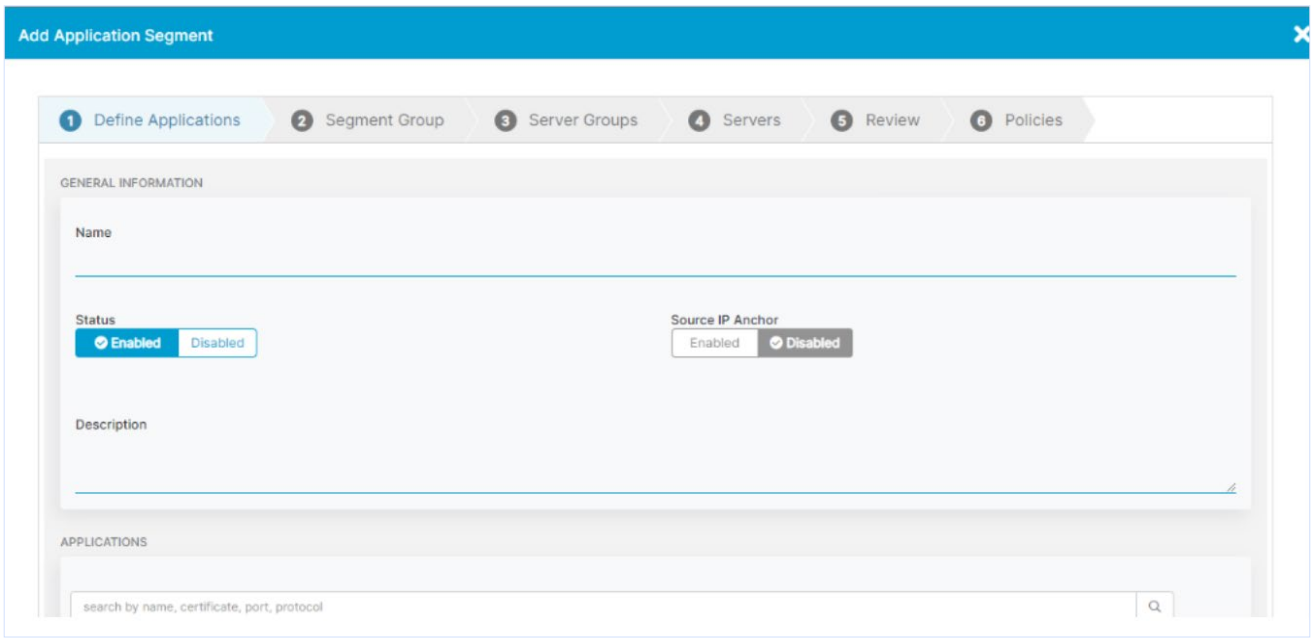
Standard App Connector configuration consists of two main steps:

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 Application Segments for Browser Access



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:

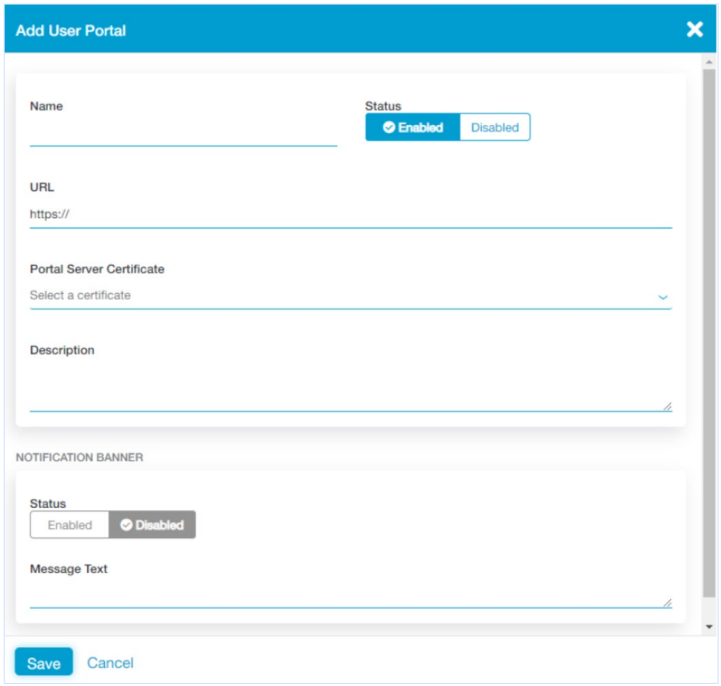
- Create a single application segment for all SAP applications. This will allow the ZPA service to load balance user requests for these applications. However, if segmentation is required, then create multiple application segments for the SAP applications.
- Create application segments for SAP applications 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.
   - Select Browser Access to enable the Application Segment for Browser Access.
2. Navigate to the Browser Access page in the ZPA Admin Portal and expand the Application Segment that was just configured for Browser Access. Copy the Canonical Name (CNAME).
3. Add the CNAME information you just copied to your public DNS and verify that the FQDN for the user portal resolves to the record.
4. 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 4. Configure Browser Access Portal



1. Configure a Browser Access Portal via the ZPA Admin Portal. When adding a new portal, you will be prompted to add the name of the portal, the URL, the portal server certificate, a description, as well the option to add a display banner for users.

2. On the User Portals page in the ZPA Admin Portal, expand the row to view the portal details within the table, then click the Copy icon next to the Canonical Name (CNAME). You will need this CNAME record for your public DNS.

3. Add the CNAME information you just copied to your public DNS and verify that the FQDN for the user portal resolves to the record.

4. Next add portal links, which are the links of the Browser Access enabled Applications that will be displayed on the Browser Access User Portal.

5. Navigate to the Portal Links page in the ZPA Admin portal. From here, you can configure the name, the protocol (HTTPs/HTTP), the description, and the icon/image for each application that will display on the portal.

Resources

ZPA: Browser Access
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