ZSCALER AND SAP S/4HANA CLOUD PRIVATE EDITION DEPLOYMENT GUIDE

NOVEMBER 2026, VERSION 2.0

BUSINESS DEVELOPMENT GUIDE

Contents

About This Document 5
- Zscaler Overview 5
- SAP Overview 5
- Audience 5
- Software Versions 5
- Request for Comments 6

Zscaler and SAP Introduction 7
- Private Access Overview 7
- Zscaler Cloud Connector Overview 7
- SAP S/4HANA Cloud Private Edition Overview 8
- SAP Resources 8

Private Access and SAP S/4HANA Cloud Private Edition 9
- Connectivity Out of the SAP S/4HANA Managed Platform 9
- Ordering SAP S/4HANA Cloud Private Edition Managed Services 9
- SAP S/4HANA Cloud Private Edition Supported Use Cases 11
  - Zscaler Zero Trust Network Access 11
  - Zscaler Zero Trust Browser Access 11
  - Zscaler BYOD Browser-Based Access 11
  - Zscaler Data Protection with Private Access Zero Trust Browser 11
  - Zscaler Digital Experience Monitoring for Private Applications 11
- SAP S/4HANA Cloud Private Edition Configuration for Managed 12
- Private Access Configuration for SAP S/4HANA Cloud Private Edition 12
- Provisioning Key 14
- App Connector Auto Delete 16
- Finalize Configuration 16

©2026 Zscaler, Inc. All rights reserved.

Zero Trust Security for Workloads 17
Cloud Connector Configuration 17
VNet/VPC Peering Guidance 21
Zscaler for SAP S/4HANA AWS, Azure, and GCP 21
Private Access 21
Zero Trust Security 21
Appendix A: App Connector Updates and Responsibility Framework 23
Customer Responsibilities 23
SAP Responsibilities 23
Shared Responsibilities 23
Appendix B: Requesting Zscaler Support 24
Requesting SAP Support 24
Requesting Zscaler Support for Private Access 24

©2026 Zscaler, Inc. All rights reserved.

Trademark Notice

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Internet & SaaS (ZIA) and Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see Zscaler's website.

SAP Overview

SAP (Trading Index: SAP SE) Founded in 1972, the company was initially called System Analysis Program Development (Systemanalyse Programmentwicklung), later abbreviated to SAP. Since then, it has grown from a small, 5-person endeavor to a multinational enterprise headquartered in Walldorf, Germany, with more than 105,000 employees worldwide.

With the introduction of its original SAP R/2 and SAP R/3 software, SAP established the global standard for enterprise resource planning (ERP) software. Now, SAP S/4HANA takes ERP to the next level by using the power of in-memory computing to process vast amounts of data, and to support advanced technologies such as AI and machine learning.

The company's integrated applications connect all parts of a business into an intelligent suite on a fully digital platform, thereby replacing the process-driven, legacy platform. Today, SAP has more than 230 million cloud users, more than 100 solutions covering all business functions, and the largest cloud portfolio of any provider.

Christian Klein leads the company, heads up the Executive Board of SAP SE, and is one of the youngest CEOs of any major enterprise on Germany's DAX blue chip market index. To learn more, refer to SAP's website.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- SAP Resources
- Appendix B: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

©2026 Zscaler, Inc. All rights reserved.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

©2026 Zscaler, Inc. All rights reserved.

Zscaler and SAP Introduction

Overviews of the Zscaler and SAP applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

Private Access Overview

Private Access is a cloud service that provides secure remote access to internal applications running on a cloud or service location using a zero trust framework. With Private Access, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

Private Access provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the Zcaler Admin Console and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Cloud Connector Overview

Enabled by the Zero Trust Exchange (ZTE), Zscaler Cloud Connector is a virtual machine that extends the capabilities of Internet & SaaS and Private Access to cloud native workloads and applications. This allows enterprises to secure all workload communications over any network and have a granular security policy applied. Generally, where a SAP workload is communicating to a public workload through the ZTE, this uses the Internet & SaaS platform through Cloud Connector; and where an SAP workload is communicating with another private workload through the ZTE, this uses the Private Access platform.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
Private Access Help Portal	Help articles for Private Access.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
Private Access Help Portal	Help articles for Private Access.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

©2026 Zscaler, Inc. All rights reserved.

SAP S/4HANA Cloud Private Edition Overview

SAP S/4HANA Cloud Private Edition is a tailored-to-fit cloud ERP that adapts to your organization's unique transformation while enabling the migration of your on-premises ERP investment from SAP, such as SAP ERP Central Component (SAP ECC), SAP S/4HANA , and SAP ERP.

SAP Resources

The following table contains links to SAP support resources.

Name	Definition
SAP S/4HANA Cloud Private Edition	Description of SAP Cloud ERP Private edition.
SAP for Me	SAP for Me is a customer portal that provides a central location for SAP products, support, and services.
SAP Store	SAP Marketplace to order SAP Container Service.

©2026 Zscaler, Inc. All rights reserved.

Private Access and SAP S/4HANA Cloud Private Edition

Zscaler and SAP Enterprise Cloud Services (ECS) have created an ECS-managed service which deploys Zscaler App Connectors inside a customer's ECS managed service environment on the AWS, Azure, or GCP hyperscalers.

The App Connectors permit a customer to establish zero trust connectivity from their desktop-based client devices to the SAP applications running in the ECS environment.

The ECS service consists of a pair (two) of Zscaler App Connectors deployed in two availability zones. This offers the resilience that supports the offered 99.9% SLA.

One pair provides 500 Mbps of supported traffic volume. You can provide additional traffic volume by adding more pairs of connectors. Constrain total desired traffic volume by available internet bandwidth on the SAP entry points. The following are key features and benefits:

- Enhanced Security for SAP S/4HANA Cloud Private Edition: Application-specific connectivity without ever bringing users on-net.
- Real-Time Visibility: Dashboards provide unparalleled visibility into your users and applications and the health of your organization's SAP S/4HANA applications.
- Private Access S/4HANA App Connectors become part of SAP S/4HANA SLAs.
- App Connectors are closer to critical apps for lower latency and higher efficacy of Zero Trust Network Access (ZTNA).
- App Connectors are hosted in an SAP-managed Kubernetes-based architecture for high availability and rapid scalability for mission-critical applications.

Connectivity Out of the SAP S/4HANA Managed Platform

To facilitate outbound traffic from the ECS-managed service (such as for connecting to desktop printers or other IoT/OT devices within the customer's network), Zscaler recommends routing this traffic through a Cloud Connector appliance. Cloud Connector appliances accept traffic from the ECS-managed service via VPC peering (such as with AWS Transit Gateway). Likewise, standard AWS route tables are leveraged to direct traffic to the Cloud Connector Gateway Load Balancer which, in turn, distributes this traffic across multiple highly-available appliances.



Zscaler Cloud Connector is not currently offered as a SAP-managed service. Zscaler recommends you deploy Zscaler Cloud Connectors in a SAP peer-connected VNet VPC.

Ordering SAP S/4HANA Cloud Private Edition Managed Services

SAP ECS is a managed service offering for hosting the App Connectors deployed inside a customer's ECS service environment.

To activate the service, order Private Access for SAP S/4HANA from the **SAP Store** or contact your SAP account team. The service only provides Zscaler App Connector hosting and does not include Private Access licensing.

©2026 Zscaler, Inc. All rights reserved.

SAP does not currently offer SAP PCE Long Distance Disaster Recovery (LDDR) for Private Access. When offered in the future, this consists of another pair of Zscaler App Connectors hosted in another region for SAP PCE.

SAP PCE Cross Region Resilience architecture might vary between SAP PCE tenants. The DNS namespace also differs from a production tenant region to a replication tenant region.

The following diagram shows a conceptualization of the integration.

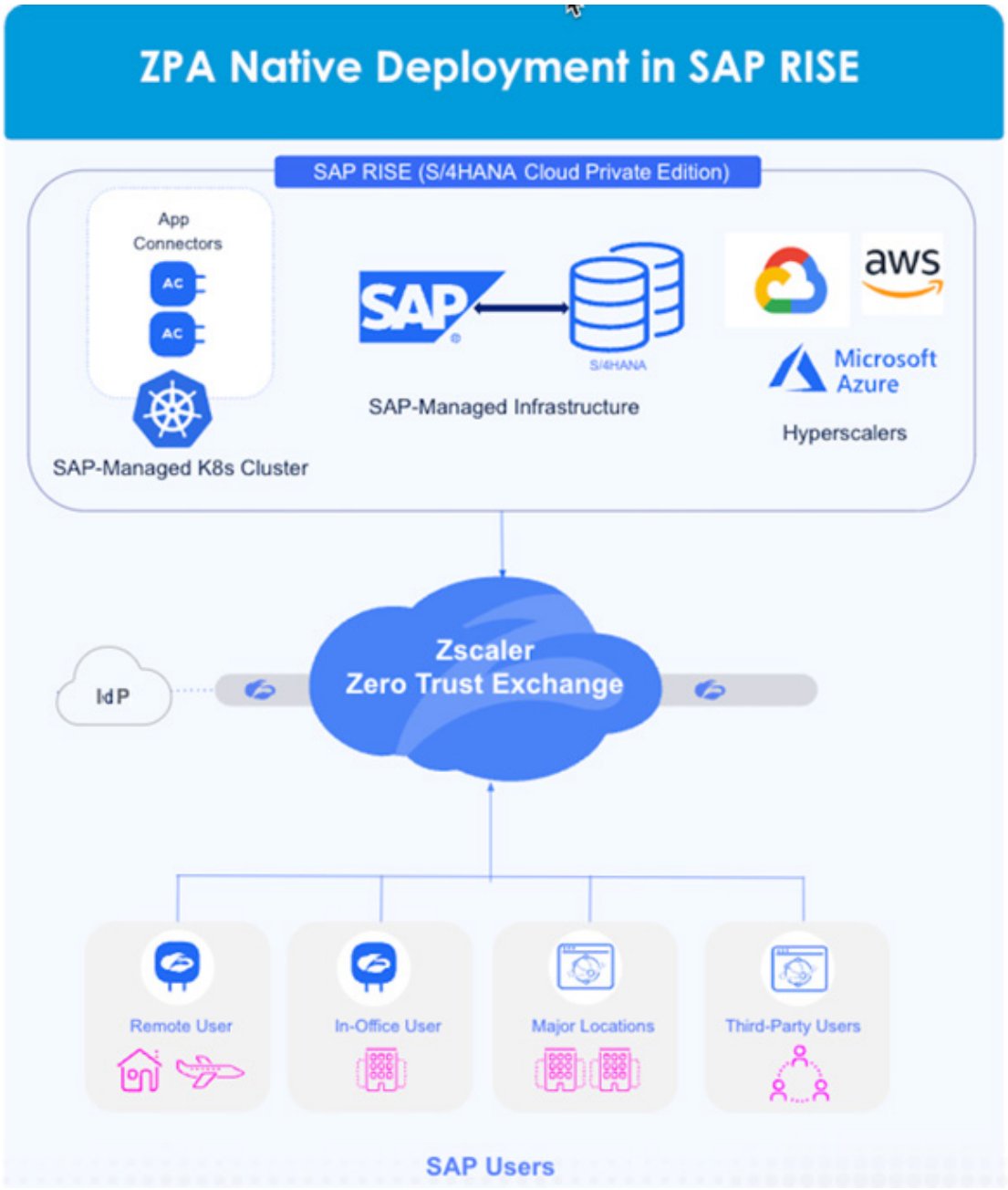


Figure 1. Zscaler and SAP architecture

©2026 Zscaler, Inc. All rights reserved.

SAP S/4HANA Cloud Private Edition Supported Use Cases

The following sections describe the supported used cases.

Zscaler Zero Trust Network Access

The Private Access service enables ZTNA to provide access to internal applications and services while ensuring the security of their networks. Unlike VPNs, which require users to connect to your network to access your enterprise applications, Private Access allows you to give users policy-based secure access only to the internal apps they need to get their work done. With Private Access, application access does not require network access. To learn more about configuration for this use case, see **What Is Private Access** (government agencies, see **What Is Private Access**).

Zscaler Zero Trust Browser Access

Browser Access allows you to leverage a web browser for user authentication and application access over Private Access, without requiring users to install Zscaler Client Connector on their devices. To learn more about configuration for this use case, see **About Browser Access** (government agencies, see **About Browser Access**).

Zscaler BYOD Browser-Based Access

The unified Zscaler solution brings together Browser Access, Zero Trust Browser, AppProtection, and Privileged Remote Access. The solution is both a more secure alternative to VPNs and a more cost-effective alternative to VDI, offering significantly improved user experiences to boost productivity. To learn more about configuration for this use case, see **About Browser Access** (government agencies, see **About Browser Access**).

Zscaler Data Protection with Private Access Zero Trust Browser

Using the Zero Trust Browser policy, you can create rules that define when application requests are redirected to Isolation. Isolation policies provide secure clientless access to critical SAP applications via a containerized isolated browser on the Zscaler cloud, ensuring the posture of a user's machine doesn't affect the related SAP applications. Additionally, enforce data exfiltration controls by ensuring users are unable to copy, paste, upload, or download files between their computers and the applications they are accessing. To learn more about configuration for this use case, see **About Isolation Policy** (government agencies, see **About Isolation Policy**).

Zscaler Digital Experience Monitoring for Private Applications

The Zscaler Digital Experience (ZDX) service is built as a multi-tenant, cloud-based monitoring platform to probe, benchmark, and measure the digital experiences for every single user within an organization, including SAP Private Applications. ZDX relies on the Zscaler Client Connector to perform synthetic probing to a desired Software as a Service (SaaS) application or internet-based service (e.g., OneDrive, Gmail, etc.). Zscaler Client Connector is the unified client that supports our Internet & SaaS and Private Access services today. ZDX support is natively integrated within Zscaler Client Connector and runs as a standalone lightweight module that is upgraded independently of the Zscaler Client Connector core process. To learn more about configuration for this use case, see **What Is Zscaler Digital Experience** and **Visualizing User Connectivity with Zscaler Digital Experience** (government agencies, see **What Is Zscaler Digital Experience** and **Visualizing User Connectivity with Zscaler Digital Experience**).



Zscaler Privileged Remote Access is not supported with SAP Cloud Private Edition. Additionally, SAP Premium Supplier clouds do not currently support SAP container-based deployments.

©2026 Zscaler, Inc. All rights reserved.

SAP S/4HANA Cloud Private Edition Configuration for Managed

In the SAP S/4HANA Cloud Private Edition, App Connectors are hosted by SAP. No Private Access administrator activities are required to configure and manage the App Connector other than creating the provisioning key and the associated application segments.

Private Access Configuration for SAP S/4HANA Cloud Private Edition

Follow the recommended configuration steps for new Private Access deployments. To learn more, see the Private Access Help (government agencies, see Private Access Help).

From the Zcaler Admin Console, you can create App Connectors, App Connector groups, and provisioning keys. For a complete list of ranges and limits per feature, see Ranges & Limitations (government agencies, see Ranges & Limitations).

To add a new App Connector:

1. Log on to the Zscaler Admin Console and go to **Private Access** > **Private Infrastructure** > **App Connectors**.
2. Click **Add**.
3. In the **Add App Connector** window that appears, and in the **Choose Key** tab:
   a. Select an **App Connector Group** (or create one if required).
   b. To Add App Connector Group, go to **Private Access** > **Private Infrastructure** > **App Connector Groups**.
   c. Select **Add**. The **Add App Connector Group** panel appears.
      - **Name**: Enter a name for the group. The name can only use the period (.), hyphen (-), and underscore (_) special characters.
      - **Status**: Make sure **Enabled** is selected.
      - (Optional) **Description**: Enter a description for the group.
      - **Enrollment Certificate**: From the drop down select the enrolment certificate.
      - **DNS Resolution Option**: Ensure IPv4 is selected. For the DNS resolution checks to work, the App Connector must have the corresponding interface or interfaces enabled, and the servers hosting your applications must support the selected interface or interfaces. By default, IPv4 and IPv6 are selected. IPV6 is not supported in SAP RISE.
      - **TCP Quick Acknowledgement**: Disable. TCP Quick Acknowledgement for the App Connector group to perform TCP Quick Ack for applications. TCP Quick Acknowledgement is used to improve the performance of applications that use specific protocols (e.g., Server Message Block Protocol). This configuration is not typically enabled for SAP PCE.
      - **Disaster Recovery**: Enable to designate the App Connector Group for disaster recovery. App Connector groups that are designated for disaster recovery bypass the ZPA cloud to ensure business continuity in the event of a disaster scenario. You must associate the App Connector Group designated for disaster recovery with a server group that serves an application segment designated for disaster recovery. Disaster recovery is disabled by default. To learn more, see Understanding Disaster Recovery and About Disaster Recovery App Connector Groups (government agencies, see Understanding Disaster Recovery and About Disaster Recovery App Connector Groups).

©2026 Zscaler, Inc. All rights reserved.

d. Version Profile configuration:

- **Persist Local Version Profile**. Displays the current Version Profile. The default value is set to Inherit. To learn more, see Configuring a Version Profile (government agencies, see Configuring a Version Profile).
- **Software Update Schedule**: Choose the day of the week and start time for the periodic update.
- **Hosting Detection**: Default Automatic. Allows ZPA to automatically detect data center hosting information, or you can enter it manually.
- **App Connector Location**: Enter the location where the App Connectors in the group are set up. The map displays the location you entered. If you click the location marker on the map, the Latitude, Longitude, and Location Address fields are automatically populated. For SAP Managed identify the location by contact SAP support.
  - **Latitude**: Displays the latitude coordinate.
  - **Longitude**: Displays the longitude coordinate.
  - **Country Code**: Displays the country code for the location address you entered.
  - **Location Details**: Displays the location address you entered.

e. Click **Save**.

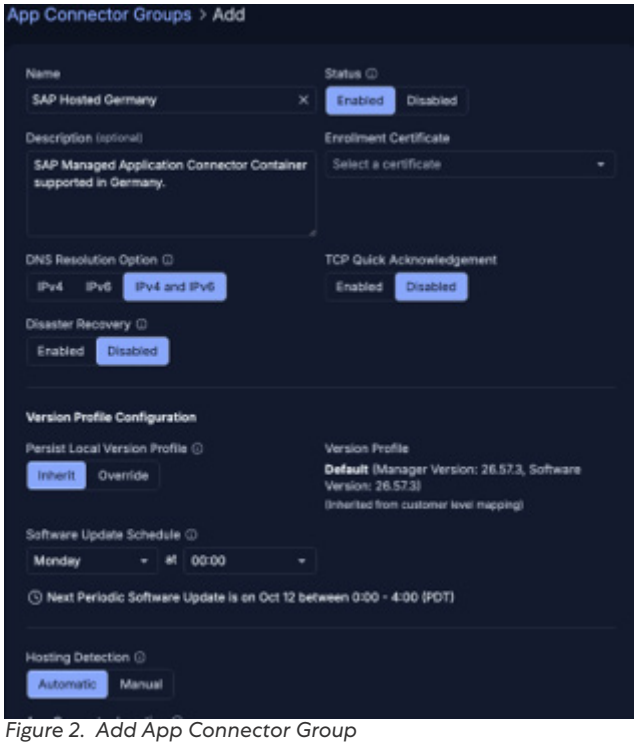


Figure 2. Add App Connector Group

©2026 Zscaler, Inc. All rights reserved.

The following shows adding an App Connector Group location.

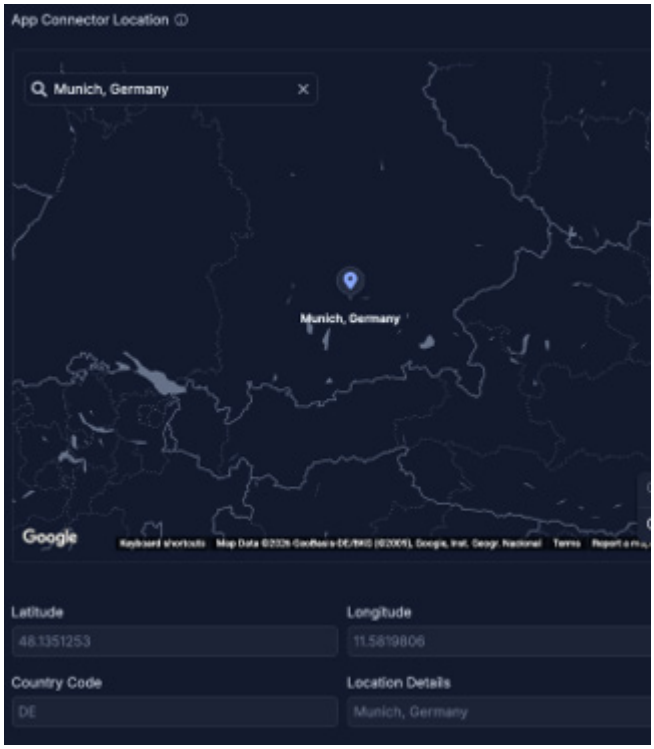


Figure 3. Add App Connector Group Location

If you need help in determining where the App Connectors are deployed in the SAP PCE Cloud, contact SAP to identify the region and location.

Provisioning Key

Create a provisioning key or choose an existing one. The provisioning key is a secure random text string that you need to enter when you deploy the App Connector on a platform. Each key is associated with a specific App Connector group and functions like an ID for the App Connector.

Zscaler recommends using a unique provisioning key for the SAP S/4 HANA Cloud Private Edition for the integration. Once the provisioning key is created it will need to share with SAP for app connector provisioning. The recommended SAP protocol for sharing is open a case with me.SAP.com.

SAP RISE is a flat network with no logical separation between production and no production workloads. Deploying multiple application connector pairs for production and no production is not needed. Zscaler recommends policy segmentation be applied in the ZPA Policy.

©2026 Zscaler, Inc. All rights reserved.

To create a Provisioning Key:

1. Log on to the Zscaler Admin Console and go to **Private Access** > **Private Infrastructure** > **App Connectors** > **App Connector Keys**.
2. Click **Add** and the **Add App Connector Provisioning Key** blade appears.
   a. **Name**: Enter a name for the provisioning key. The name can only use the period (.), hyphen (-), and underscore (_). special characters.
   b. **App Connector Group**: Selected the App Connector Group previous created.
   c. **Maximum Reuse of Provisioning Key**: Set a maximum reuse for the provisioning key. Due to the nature of SAP containers hosting the app connectors they key can be consumed as the containers are updated.
   d. **Signing Certificate**: Select Connector.

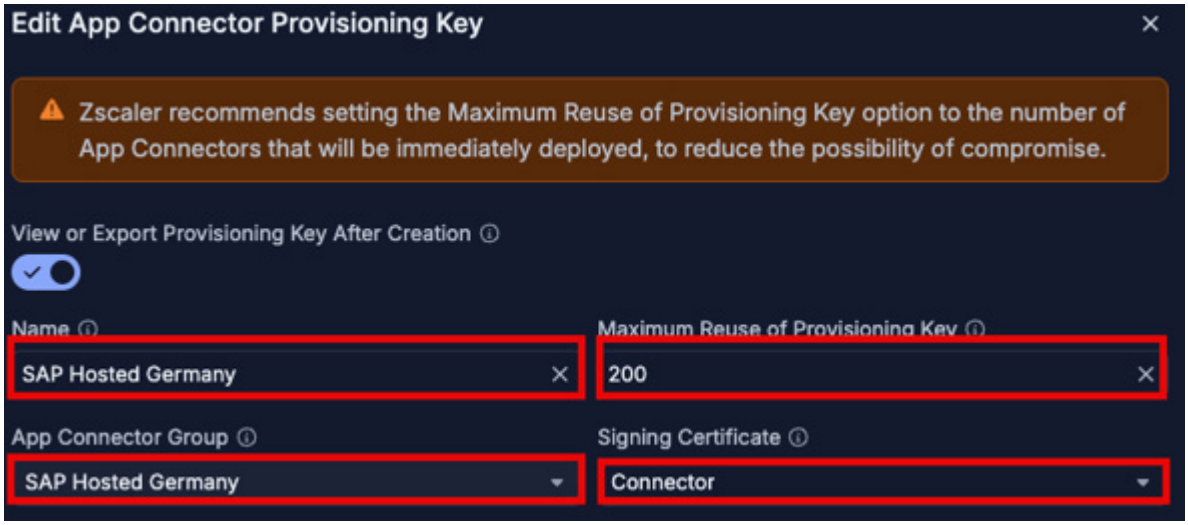


Figure 4. Provisioning Key

Zscaler recommends setting containerized deployments for App Connectors to 100 or higher.

After the Provisioning Key is created, send the provisioning key to SAP to be associated with your SAP tenant. To learn more, refer to SAP for Me.

After the provisioning key is added to the Application Connectors deployment in SAP S/4 HANA Cloud Private Edition, the App Connector launches and makes initial contact with the ZPA cloud. It presents a key as its ID, allowing the ZPA cloud to verify that this is an authentic App Connector and to identify which App Connector group it belongs to. ZPA then automatically completes the deployment process.

Zscaler can support multiple SAML and OIDC identity providers. To learn more, see Understanding SAML (government agencies, see Understanding SAML).

This does not mean their SAP applications must have been set up with SSO using SAML. This is not a requirement.

©2026 Zscaler, Inc. All rights reserved.

App Connector Auto Delete

The App Connectors settings allow you to disable Auto Delete for App Connectors with a disconnected status.

To verify the Auto Delete configuration settings:

1. Log on to the Zscaler Admin Console and go to **Private Access** > **Private Infrastructure** > **App Connectors**.
2. Click the **Settings** icon. The **App Connector Settings** blade appears.
3. Verify **Enabled** is set.
4. Set the number of days to **5 Default** before App Connectors with a disconnected status are deleted.
5. (Optional) To delete disabled App Connectors at the set time, select the **Include disabled App Connectors** checkbox.
6. Click **Save**.

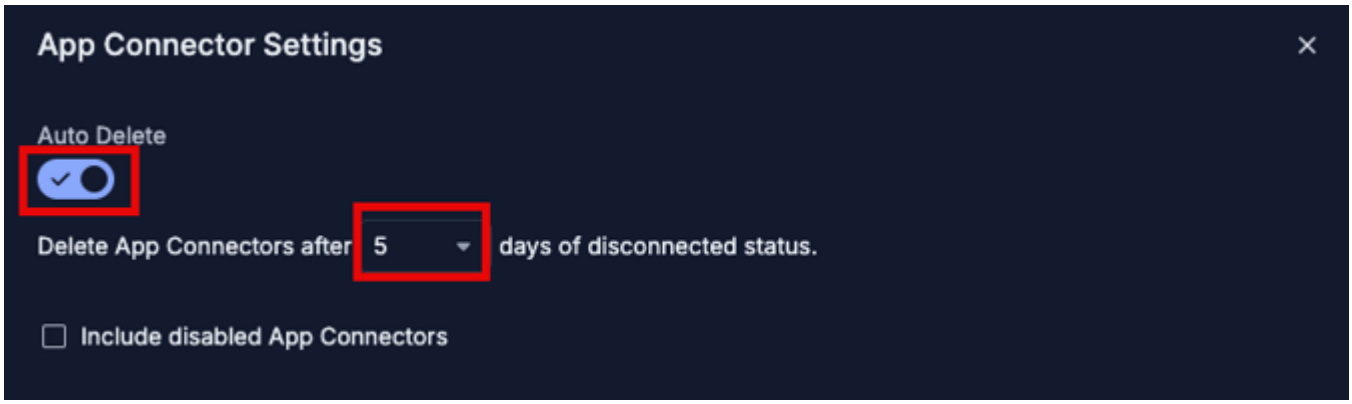


Figure 5. Review Documentation

In configuring Zscaler Application Segments (government agencies, see Zscaler Application Segments) for an SAP PCE tenant, an organization might deploy SAP clients' SAP GUI on endpoints for power users. The SAP client port and protocol can vary based on each organization's needs and design criteria.

For SAP, you can configure DNS Search Domains for FQDNs within the Zcaler Admin Console. 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.

To learn more about SAP Application support and best practices, see Supporting SAP Applications (government agencies, see Supporting SAP Applications).

Finalize Configuration

To complete the ZPA SAP integration, follow the guidance outlined in Private Access Help .

1. For clientless Browser Access, follow the guidance outlined in About Browser Access (government agencies, see About Browser Access).
2. For Data Protection, follow the guidance outlined in About Browser Isolation (government agencies, see About Browser Isolation).

©2026 Zscaler, Inc. All rights reserved.

Zero Trust Security for Workloads

(Optional) Zero Trust Security for SAP PCE workloads is not currently supported as managed services in the SAP ECS (PCE) environments. For organizations desiring Zero Trust Security, instantiate Zscaler Cloud Connector appliances within the customer-managed VNet/VPC and DNS Conditional Forwarding as a steering mechanism.

Cloud Connector Configuration

Outbound connectivity towards on-premises devices or other hyperscaler environments is necessary, instantiate Cloud Connector appliances within the customer-managed VNet/VPC and route traffic through them.

Follow the recommended configuration steps for new Zscaler Cloud Connector deployments. To learn more, see the Step-by-Step Configuration Guide for Zscaler Cloud Connector (government agencies, see Step-by-Step Configuration Guide for Zscaler Cloud Connector).

For Private Access functionality to operate correctly, Cloud Connector must see the initial DNS request from the SAP application towards the on-premises device. To facilitate this, ensure that DNS servers within the SAP-managed VNet/VPC are configured to forward queries for on-premises devices towards an upstream DNS server in which the request crosses over the Cloud Connector. You can accomplish this through normal routing mechanisms, or via cloud native services like AWS Route 53. For more information, see Handling DNS Resolutions for Zscaler Cloud Connector (government agencies, see Handling DNS Resolutions for Zscaler Cloud Connector).

Alternatively, if DNS is unavailable for Private Access-bound traffic, use real IP addresses to route traffic through the Cloud Connector appliances (you must ensure that Application Segments reference real IP addresses, however).

The following provides configuration guidance using Amazon (AWS) nomenclature. However, you can substitute Microsoft Azure or GCP nomenclature and services where appropriate.

To route traffic from the SAP-managed VPC to the customer-managed VPC, you must use AWS Transit Gateway. In this option, a pair of redundant Cloud Connector appliances is installed within a customer-managed Gateway VPC (also known as a Transit or Egress VPC). Peer this VPC with the Transit Gateway. Spoke VPC workloads as well as the SAP-managed VPC requiring Private Access are simply directed towards the Transit Gateway, where they are then directed towards the Cloud Connector appliances for outbound routing. You can leverage AWS Auto Scaling to automatically grow or shrink the Cloud Connector cluster based on the demands of the business.

Ensure that the Cloud Connector Forwarding Policy is set to send traffic to Internet & SaaS (or Private Access, depending on the use case). This is the default configuration, unless otherwise modified. Cloud Connector automatically downloads Application Segments configured in the other sections of this document.

Ensure that Private Access policy is configured to accept inbound traffic from SAP-sourced locations (VPC) and allowed (or denied) access to the private destinations.

Zscaler recommends using a NAT Gateway. This is not required since the Cloud Connector appliances can perform NAT on their own. However, it is recommended when implementing Auto Scale functionality because it allows the appliances to use RFC1918 address space behind a single AWS Elastic IP, rather than using multiple Elastic IP addresses across multiple Cloud Connector appliances.

©2026 Zscaler, Inc. All rights reserved.

To configure traffic routing through the new Cloud Connector:

1. Create a dedicated attachment Subnet within the customer-managed Gateway VPC that is used to accept outbound traffic from the Transit Gateway towards the Cloud Connector appliance. This Subnet is referenced in the TGW peering with the Gateway VPC. You might need more than one attachment Subnet, based on the Availability Zones in use.

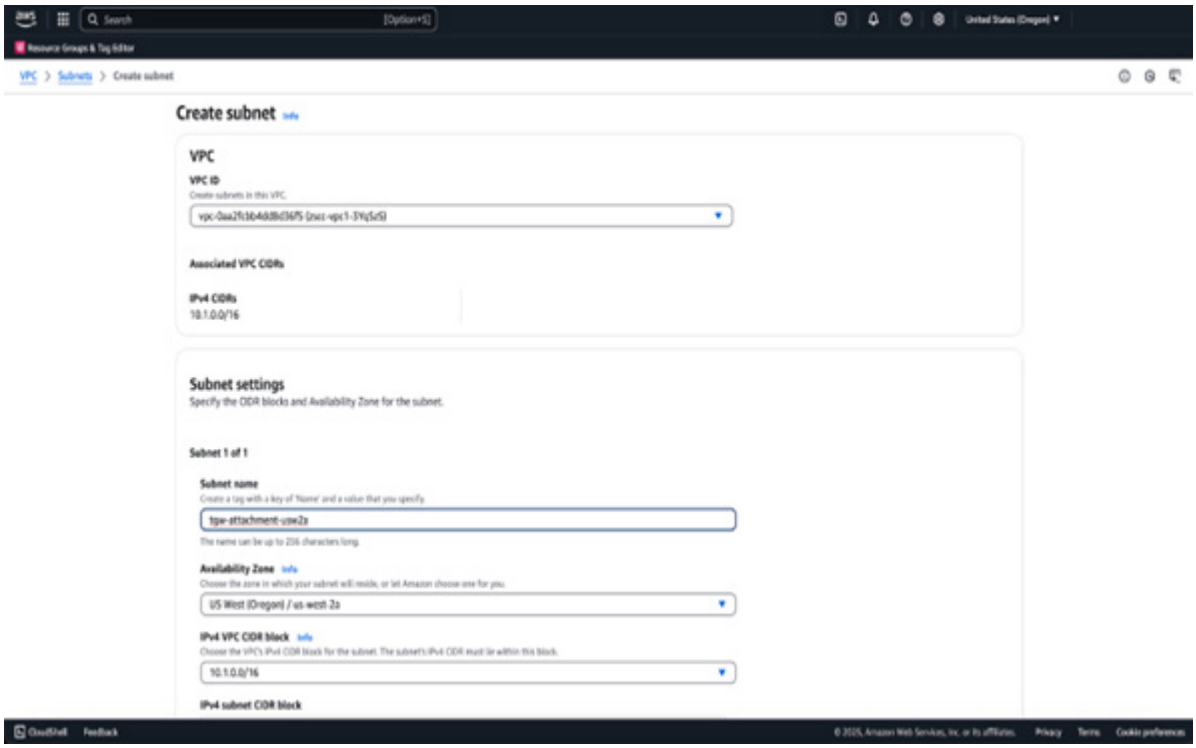


Figure 6. Attachment Subnet

2. Create a Route Table for the attachment Subnet and associate the two.

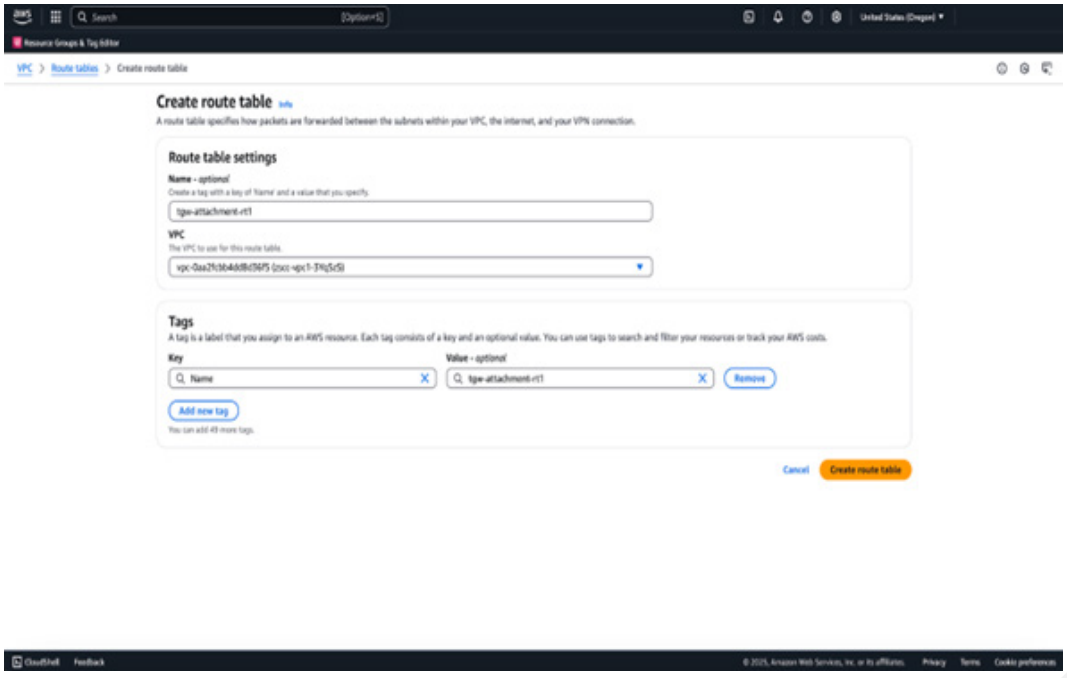


Figure 7. Route Table

©2026 Zscaler, Inc. All rights reserved.

The following figure shows subnet associations.

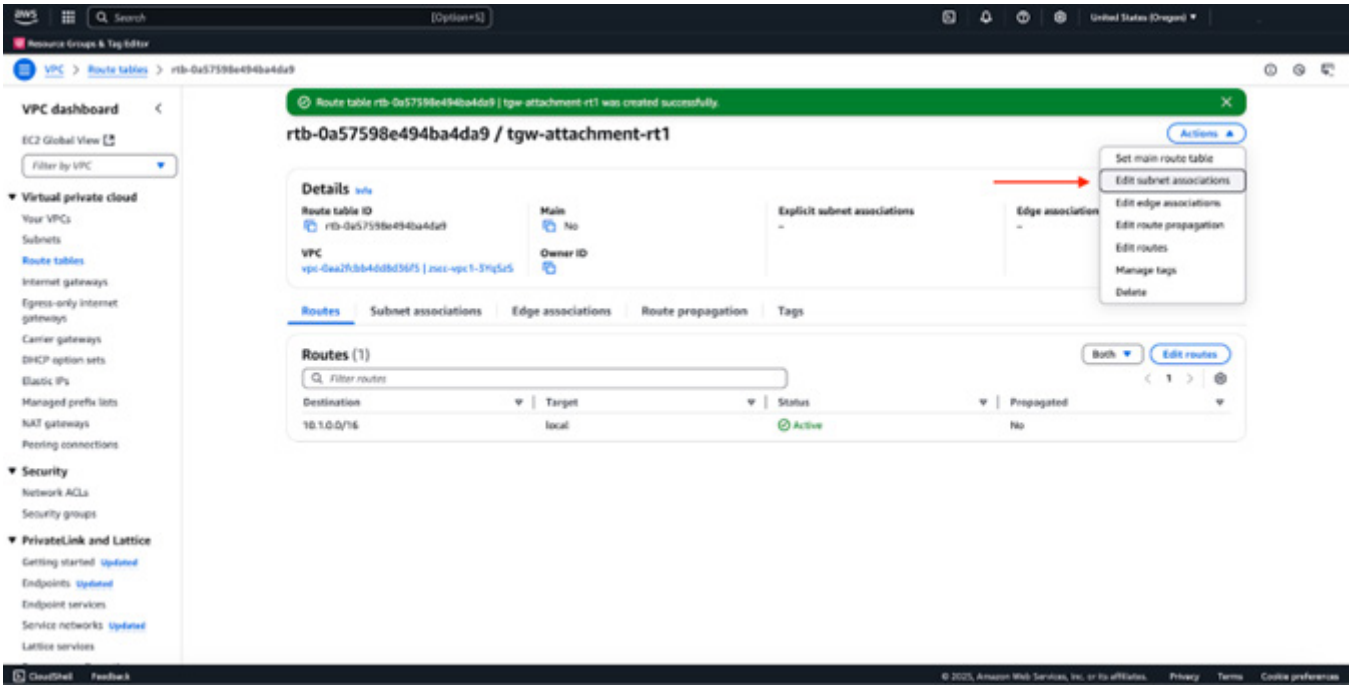


Figure 8. Edit Subnet Associations

3. Update the new Route Table and install two routes that point towards the GWLBE that was created when deploying the Cloud Connectors:
   a. **Synthetic IP address space**: By default, 10.254.0.0/19.
   b. **(Optional) Private IP address space**: On-premises actual IP address prefixes.

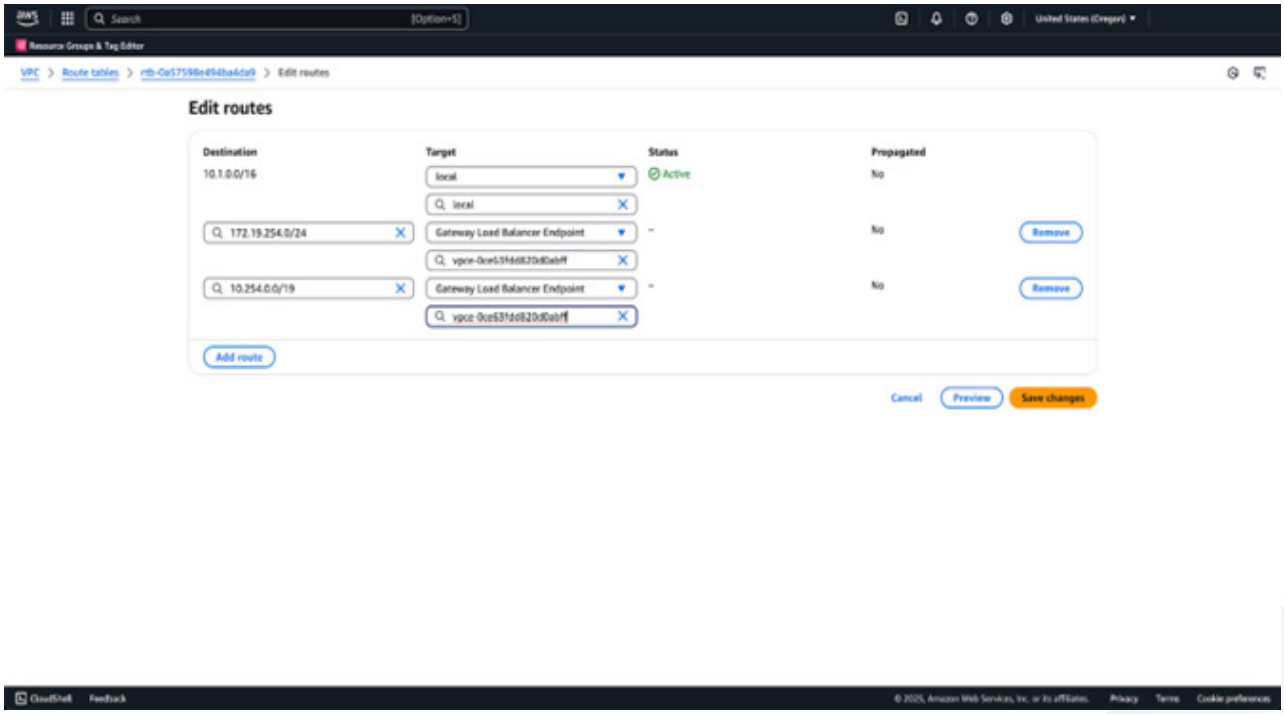


Figure 9. Edit Routes Save Changes

©2026 Zscaler, Inc. All rights reserved.

4. If needed, install a return route in the attachment Subnet to direct return traffic back towards the TGW for SAP Subnets.
5. Verify that Security Groups are updated to allow traffic from the SAP VPC towards the Cloud Connector appliances. By default, these Security Groups only allow traffic from the local Gateway VPC.

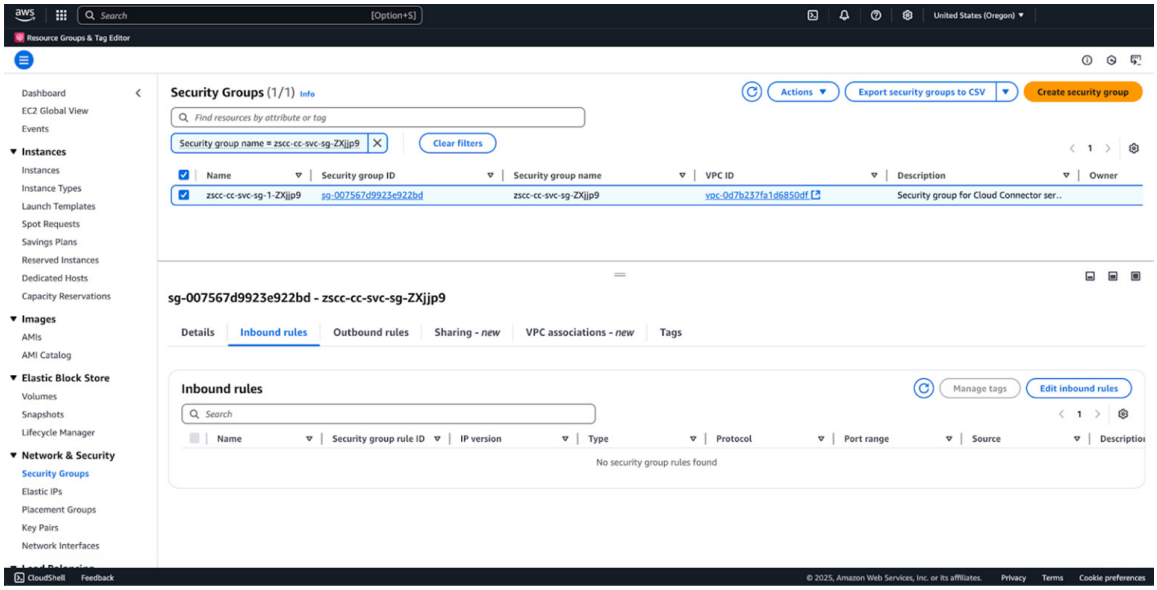


Figure 10. Edit Security Groups

6. Update each of the SAP-managed VPCs Route Tables with the following routes towards the Transit Gateway:
   a. **Synthetic IP address space owned by Cloud Connector**: By default, 10.254.0.0/19.
   b. **(Optional) Private IP address space**: On-premises actual IP address prefixes.
7. Update the TGW Routing Table to point towards the TGW Peering for the following prefixes:
   a. **Synthetic IP address space owned by Cloud Connector**: By default, 10.254.0.0/19.
   b. **(Optional) Private IP address space**: On-premises actual IP address prefixes.

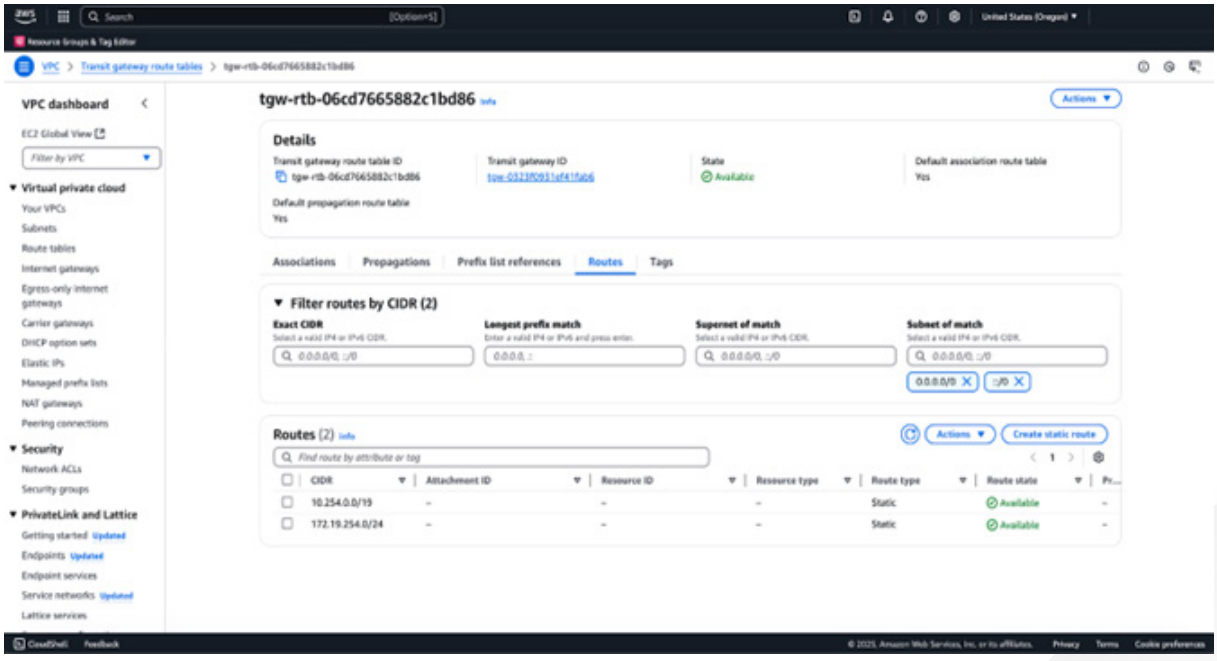


Figure 11. Edit Security Groups Details

©2026 Zscaler, Inc. All rights reserved.

VNet/VPC Peering Guidance

- Customer typically manages peering security.
- Contact SAP technical support for guidance in establishing the peering service.
- Cloud Connectors require deployment in an organizationally managed VNet or VPC network that is VNet or VPC peer connected to SAP PCE.
- Install this VNet/VPC on the same hyperscaler (AWS, Azure, or GCP) used for the organization's SAP PCE tenant.
- Zscaler recommends that the VNet/VPC network be in the same region for the lowest possible latency connecting to SAP PCE.
- App Connectors and Cloud Connectors require DNS resolution to connect to SAP PCE applications.

Zscaler for SAP S/4HANA AWS, Azure, and GCP

The following sections describe Zscaler for SAP S/4HANA AWS, Azure, and GCP (non-PCE-managed) users.

Private Access

If organizations prefer more control over hosting App Connectors, alternative architectural approaches are possible. The SAP user to Application VNet/VPC Peering approach might best fit an organization's needs in this scenario. It is important to note that the App Connectors are external to SAP PCE and are able to access SAP PCE application resources by utilizing a VNet/VPC peer connection to the SAP ECS.

Zero Trust Security

(Optional) You can also use Zscaler Cloud Connector appliances to facilitate outbound connectivity from the SAP ECS and customer hyperscaler environment. Since the customer, or Solutions Integrator (SI), manages both the SAP infrastructure and the gateway VNet/VPC, more flexibility exists in how traffic is routed to Zscaler. The following guidance is provided for organizations desiring Zero Trust Security when deployed directly into AWS, Azure, or GCP.



Follow the recommended configuration steps for new Zscaler Cloud Connector deployments. To learn more, see the **Step-by-Step Configuration Guide for Zscaler Cloud Connector** (government agencies, see **Step-by-Step Configuration Guide for Zscaler Cloud Connector**).

For Private Access functionality to operate correctly, Cloud Connector must see the initial DNS request from the SAP application towards the on-premises device. To facilitate this, ensure that DNS servers within the SAP-managed VNet/VPC are configured to forward queries for on-premises devices towards an upstream DNS server in which the request crosses over the Cloud Connector. You can accomplish this through normal routing mechanisms, or via cloud native services like AWS Route 53. For more information, see **Handling DNS Resolutions for Zscaler Cloud Connector** (government agencies, see **Handling DNS Resolutions for Zscaler Cloud Connector**).

Alternatively, if DNS is unavailable for Private Access-bound traffic, you can use real IP addresses to route traffic through the Cloud Connector appliances (you must ensure that Application Segments reference real IP addresses, however).

©2026 Zscaler, Inc. All rights reserved.

There are two models in which you can deploy Cloud Connector: distributed or centralized. When in a distributed model, Cloud Connector appliances are instantiated directly within the SAP VNet/VPC that the customer (or SI) manages. In a centralized model, the Cloud Connectors sit in a hub VNet/VPC that is peered with the SAP VNet/VPC:

- Distributed Model: In this model, Cloud Connectors sit adjacent to the individual SAP workloads they service. The primary benefit to this design option is its simplicity and time to implement. Since each Cloud Connector instance is spawned within the SAP VPC that it services, routing is made simple. However, for customers with many SAP VPCs, this design option can be cumbersome and expensive. This option requires the modification of many Route Tables to direct traffic accordingly, which is further complicated when high availability enters the picture. For more information, review the **AWS**, **Azure**, or **GCP** Reference Architecture section *Use Case: Direct to Internet Using Internet & SaaS*.
- Centralized (Hub-and-Spoke) Model: In this model, Cloud Connectors operate in a hub that SAP traffic routes through (in addition to other workload traffic outside the SAP VPC that the customer might want to route through Zscaler):
  - AWS Transit Gateway: Detailed in the preceding section, the Transit Gateway option deploys Cloud Connectors into a Gateway VPC, which is then peered with the SAP VPC and Route Tables are updated accordingly. For more information, see the **AWS Reference Architecture** section titled *Use Case: Integrating with AWS Transit Gateway*.
  - AWS Gateway Load Balancer Endpoint Distribution: Cloud Connectors are installed using Gateway Load Balancer as a best practice for high availability. In lieu of Transit Gateway and VPC peering, you can extend the Gateway Load Balancer endpoints directly into the SAP VPC directly. This option offers the benefit of the distributed model, without requiring the customer to deploy multiple Cloud Connector appliances. For more information, see the **AWS Reference Architecture** section titled *Use Case: Distributed Gateway Load-Balancing Endpoints*.
  - Azure VNet Peering: Deploying Cloud Connector using a Gateway VNet allows the organization to simplify cloud routing and, more importantly, reduce the compute footprint required when deploying directly to the SAP VNets. In this option, only a single cluster of Cloud Connector appliances is necessary for a Gateway VNet. SAP VNet workloads are directed towards the front-end load balancer IP address using a simple default route, where you can direct them towards the Cloud Connector appliances for outbound routing. For more information, see the **Azure Reference Architecture** section titled *Use Case: Leveraging VNet Peering*.
  - Azure vWAN (VHub): Here, SAP VNets send traffic to the vHub, which then directs the traffic toward the Gateway VNet (Cloud Connector) for processing. In this model, you generally rely on the vHub route table to influence traffic from spoke locations to the Cloud Connector appliances by propagating a default route. SAP VNets then inherit this default route via vHub propagation and the hub/Gateway VNet uses the default internet route that Microsoft installs directly. For more information, see **Securing Microsoft Azure vWAN**.
  - GCP Shared VPC: In this option, Cloud Connector receives traffic from SAP VPCs (or other workload VPCs) through a hub Shared VPC. Deploying Cloud Connector using a Shared VPC allows the organization to simplify cloud routing and reduces the compute footprint required when deploying directly to the SAP VPCs. In this option, only a single cluster of Cloud Connector appliances is necessary for the Shared VPC. SAP VPC workloads are simply directed towards the internal passthrough Network Load Balancer using a default route (or specific prefixes), where they are then directed towards the Cloud Connector appliances for outbound routing. For more information, see the **GCP Reference Architecture** section titled *Use Case: Integrating with a Shared VPC*.

After the appliances have been instantiated, routing through the Cloud Connector appliances follows the standard methodology outlined in the documentation linked previously and detailed earlier in this document.



Zero Trust Security for SAP PCE Workloads is not currently supported for managed services in the SAP ECS (PCE) environments.

©2026 Zscaler, Inc. All rights reserved.

Appendix A: App Connector Updates and Responsibility Framework

The following sections describe the App Connector updates and responsibility framework.

Customer Responsibilities

1. The Private Access Administrator provides the App Connector provisioning key for Private Access. The process for providing the App Connector provisioning key follows SAP's third-party software procedure in the SAP for Me.
2. Except for the SAP-managed App Connector, the Private Access Administrator manages the Private Access solution, including Application Segments and Access policies for SAP application access.
3. Updating App Connector is a shared responsibility between SAP and the Private Access Administrator.

SAP Responsibilities

1. SAP installs the customer-provided App Connector provisioning key.
2. SAP maintains the underpinning workload, including containers, OSs, and VMs, to support the App Connector and ensure availability.

There is no option to scale up to change the containers' resource sizes (CPU, RAM, disk).

The service is only delivered if the customer is using SAP Cloud Private services.

This service is only provided in the SAP Cloud Private portfolio.

Shared Responsibilities

App Connector updates are shared by SAP and the Private Access Administrator. Details are outlined in the following App Connector Shared Responsibilities table.

Component	Who Updates	How Updates Happen	Frequency
Zscaler Manager	SAP Updates	Manually Triggered Understanding the Manager Software	Typically Quarterly Most updates are optional. Required updates are rare and planned (e.g., Zscaler issued only one required update in 2023).
App Connector Child	Customer Updates Customer schedules updates for all App Connectors across their full estate from their Zcaler Admin Console.	Automated or Manually Triggered Customer can configure the schedule for auto-updates; Option to manually override. Auto update process Manual update process	Updates released approximately every four weeks.

©2026 Zscaler, Inc. All rights reserved.

Appendix B: Requesting Zscaler Support

You might sometimes need Zscaler Support to provision certain services or troubleshoot configuration and service issues. Both SAP Support and Zscaler Support are available 24/7/365.

Requesting SAP Support

The following link access the SAP Support Portal:

SAP Support

Requesting Zscaler Support for Private Access

You might sometimes need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Adminstration** > **Organization**.
2. Copy the **Company ID**.

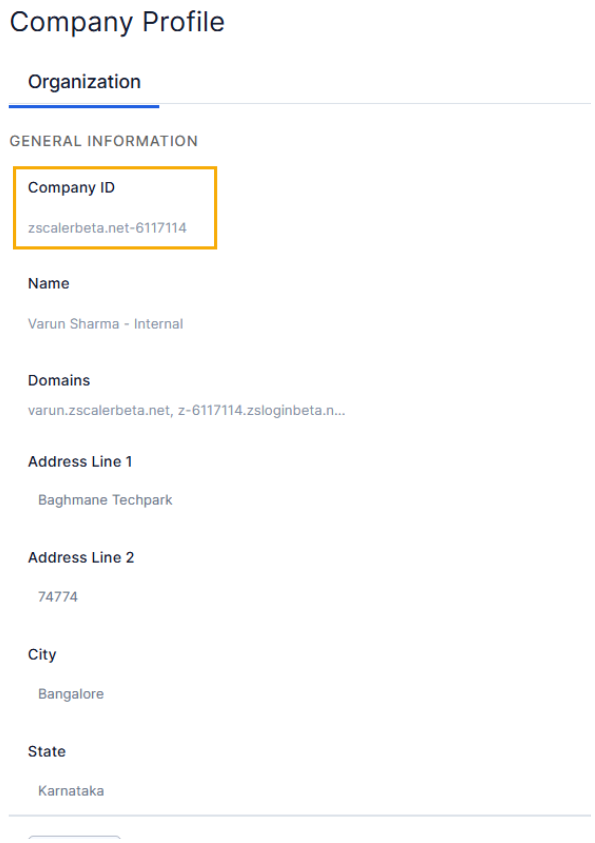


Figure 12. Collecting Company ID to open support case with Zscaler TAC

©2026 Zscaler, Inc. All rights reserved.

3. Now that you have our company ID, you can open a support ticket. Go to the **Help** icon and select **Tools and Resources**.
4. Click **Support Portal**.

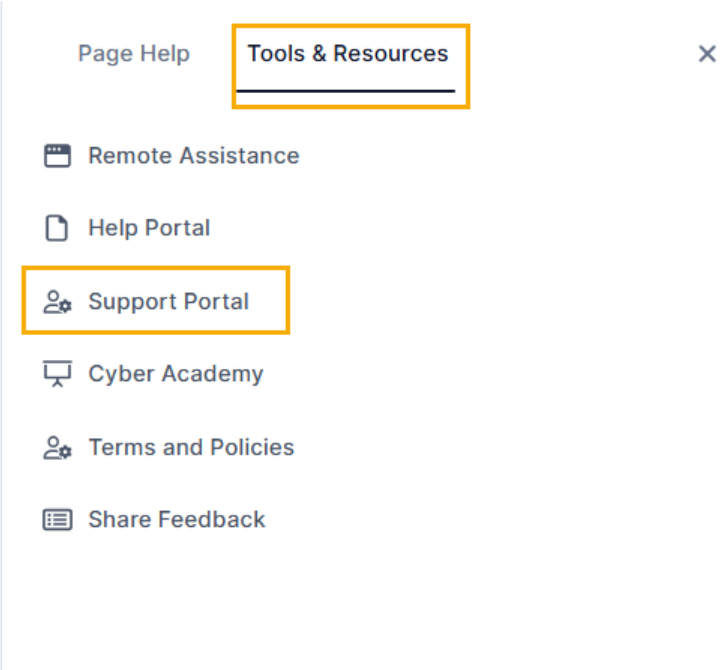


Figure 13. Open the Support Portal

5. Log in to the Support Portal and enter the issue or help request.

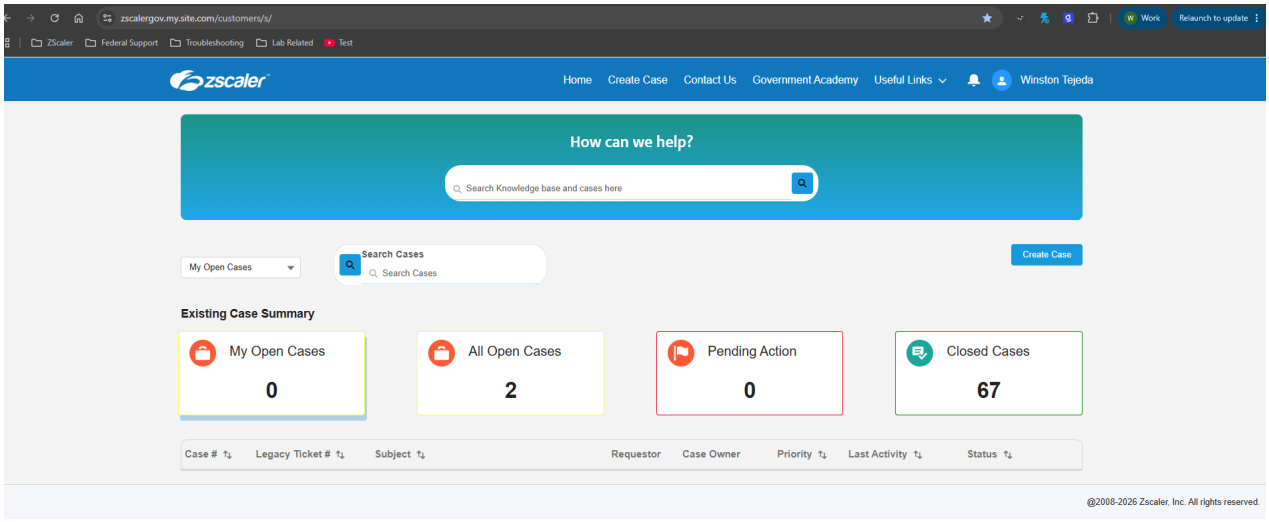


Figure 14. Support Portal

You can also use Zscaler's Support phone numbers. To learn more, see [Support Scope & Communication Methods].

©2026 Zscaler, Inc. All rights reserved.