+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 10/06/2026

Sign Up

Zscaler Private Access (ZPA) Training

3 days (21 hours)

Overview

Zscaler Private Access is a ZTNA solution that secures access to private applications without exposing the network to users. Using App Connectors and contextual policies, ZPA connects each user only to authorized applications, in accordance with the principles of Zero Trust and least privilege.

Our Zscaler Private Access (ZPA) training will enable you to master the deployment, administration, and security of private access. This self-paced, intermediate-level course prepares you for common scenarios encountered in production environments.

You'll learn how to organize Application Segments and associated groups, configure Client Connector, and integrate an identity provider. You'll build policies that combine user groups, endpoint posture, and connection context.

By the end of the course, you will be able to publish applications using Browser Access and determine the uses of a Private Service Edge in a resilient architecture. You will also know how to prepare for a phased migration from VPN to ZPA.

This training covers diagnostics, logs, and operational best practices. Hands-on workshops on deployment, access configuration, and incident resolution will help you ensure the reliability of your environments.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Deploy App Connectors and verify their availability

- Organize Application Segments and their groups to restrict access to authorized applications
- Integrate identity and configure context-aware access policies based on the principle of least privilege
- Configure the Client Connector and publish an application with Browser Access in a test environment
- Define an architecture using Private Service Edge and prepare for a phased migration from VPN
- Diagnose and resolve access incidents using logs and connectivity checks

Target Audience

- Network and security administrators
- System administrators
- Security Engineer
- Infrastructure architect
- Network Support Engineer

Prerequisites

- Proficiency in TCP/IP fundamentals and DNS resolution in a professional environment
- Knowledge of remote access via VPN and the principles of network filtering
- Experience administering Windows or Linux systems and virtual machines
- Basic understanding of identity federation with SAML 2.0 and multi-factor authentication

Technical Prerequisites

- Windows 11 workstation with installation privileges and a recent browser
- Stable internet connection and the ability to install the Zscaler Client Connector
- Access to a Zscaler Private Access lab environment provided or set up for the training
- Lab environment allowing you to work with App Connectors, identity, and private applications

Our Zscaler Private Access (ZPA) Training Curriculum

[Day 1 - Morning]

Zero Trust architecture and deployment preparation

- Principles of ZTNA, application access, and differences from a VPN that provides network access
- ZPA architecture, roles of Public Service Edges, App Connectors, and Client Connectors
- Private connection path, microtunnels, and DNS resolution with synthetic addresses
- Tenant preparation, administrative roles, and inventory of private applications and their dependencies

- App Connector Deployment Prerequisites: Platforms, Outbound Connectivity, DNS, and Network Placement
- Hands-on Workshop: Mapping a lab architecture and verifying network and DNS prerequisites before deployment.

[Day 1 – Afternoon]

Deploying connectors and application segmentation

- Installation and enrollment of App Connectors, OAuth tokens, and provisioning keys according to the chosen method
- Organizing App Connector Groups, redundancy, and verifying the availability of the connectors
- Defining Application Segments by domain names, addresses, and required ports
- Mapping Server Groups to connector groups and dynamic server discovery
- Organization of Segment Groups, segmentation granularity, and management of overlaps between segments
- Hands-on Workshop: Deploy two App Connectors, create their groups, and define the segments for two applications along with their Server Groups.

[Day 2 - Morning]

Identity and access from user workstations

- Integrating the identity provider with SAML 2.0, metadata, certificates, and user attributes
- Provisioning users and groups with SCIM, distinguishing between synchronization and authentication
- Installation and enrollment of the Zscaler Client Connector on test workstations
- Application profiles, forwarding profiles, and Client Forwarding Policy to route requests to ZPA
- Initial access policies by user group and application, authorization validation, and denials
- Hands-on workshop: Integrate a test identity provider, enroll a device, and verify access for two user profiles.

[Day 2 - Afternoon]

Contextual Policies and Browser Access

- Creating contextual access policies that combine identity, groups, applications, and client type
- Endpoint posture checks and trusted network criteria in access rules
- Top-down rule evaluation, best match, and selection of the most precise application segment

- Application of the principle of least privilege, reduction of overly broad segments, and non-regression testing
- Publication with Browser Access, agentless web access, domains, certificates, and application compatibility constraints
- Hands-on workshop: Apply a posture rule, test authorized and denied access, and then publish a web application with Browser Access.

[Day 3 - Morning]

Private Service Edge and migration from VPN

- Uses of Private Service Edge, differences from Public Service Edges, and operational responsibilities
- Deployment prerequisites, sizing, groups, enrollment, and inbound and outbound traffic for the Private Service Edge
- Path preference with redirection policies, availability, and fallback scenarios to validate
- Secure administration of components, updates, and monitoring the resilience of application access
- VPN migration to ZPA, dependency inventory, pilot cohort, controlled coexistence, and rollback criteria
- Hands-on workshop: Configure a pre-configured Private Service Edge, verify the access path, and then perform a pilot switchover of an application with a rollback test.

[Day 3 - Afternoon]

Operations and incident resolution

- Step-by-step troubleshooting method, scoping, and reproducing an incident
- Reviewing user activity diagnostics, connection events, policy denials, and application errors
- Diagnosing Client Connector incidents, authentication, identity attributes, and endpoint
- Verifying App Connectors, DNS resolution, application ports, and associations between segments and groups
- Collecting logs, principles of the Log Streaming Service, SIEM integration, and creating an escalation report
- Hands-on workshop: Resolving simulated DNS, policy, and connector incidents, verifying that access has been restored, and documenting corrective actions.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams on new, advanced IT technologies or to acquire specific business knowledge or modern methodologies.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon

final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg