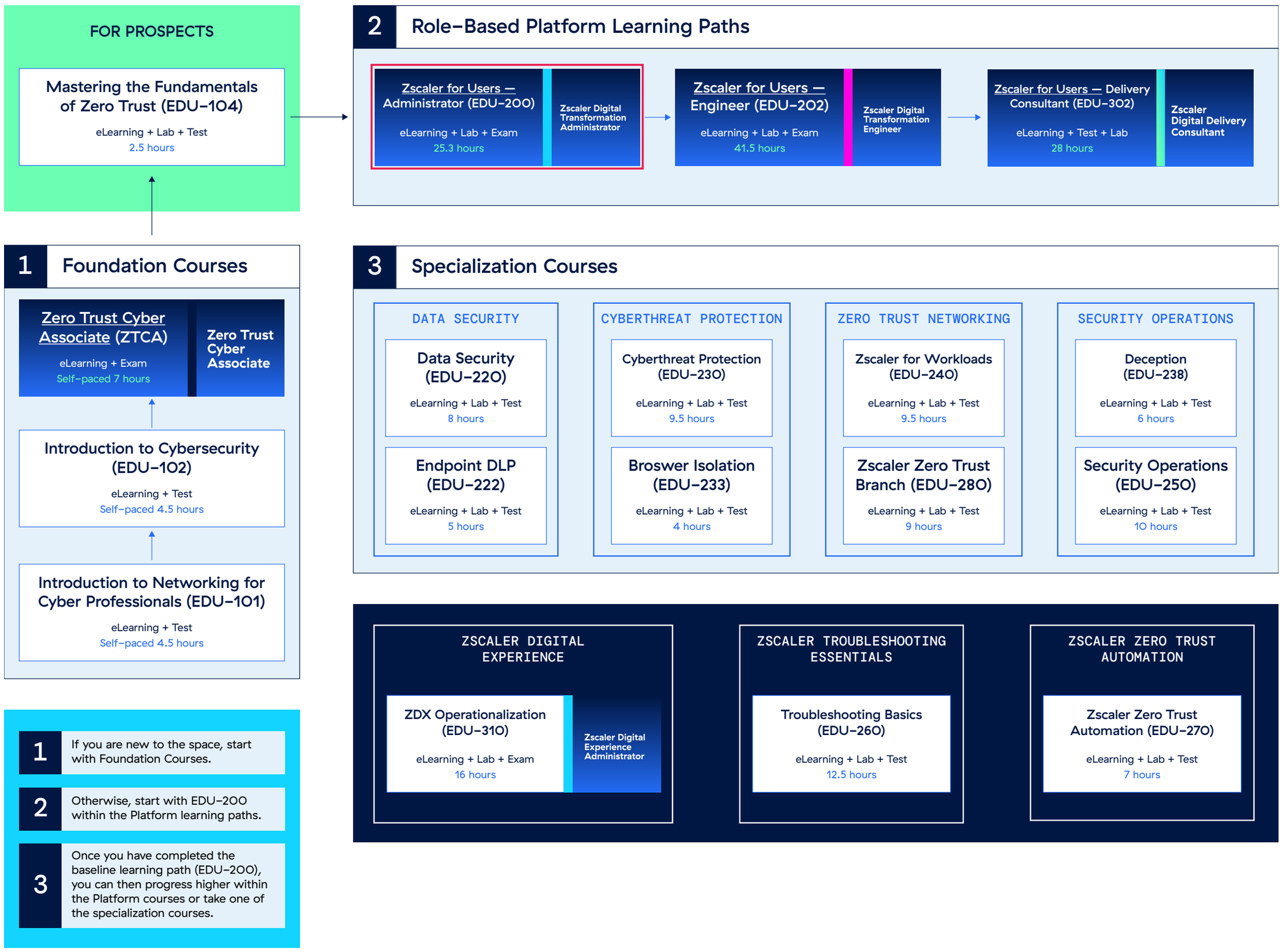
Zscaler Cyber Academy

Zscaler for Users Administrator – (EDU-200)

COURSE OUTLINE

Zscaler Cyber Academy Catalog



EDU-200 Learning Journey Map

The recommended path for the Zscaler for Users – Administrator learning journey is to complete the eLearning course, and then take the hands-on labs. Once these are completed, you can sign up for the certificate test. You will have 90 minutes to answer 50 questions. Upon passing the test, you'll earn the Zscaler Digital Transformation Administrator (ZDTA certificate).

©2026 Zscaler, Inc. All rights reserved.

OUR LEARNING PATH

Zscaler for Users — Administrator (EDU-200) Learning Path



LEARNING OUTCOMES

Once you complete this course, you will be able to:

- Build proficiency in ZIdentity and Experience Center to strengthen identity management and user experience
- Deploy and manage Zscaler Client Connector, understand tunneling, and use health metrics for monitoring and troubleshooting
- Implement and operate ZIA/ZPA integrations (network integration, App Connectors, Private Service Edges) and understand OneAPI fundamentals
- Configure and manage core security controls: traffic control, web/app access, SSL inspection, malware protection, and zero trust least-privilege ZPA policies
- Create and enforce data protection and SaaS controls: DLP policies/incidents and CASB for sanctioned/unsanctioned apps to meet compliance needs
- Use dashboards, logs, analytics, and ZDX (ThreatLabz, Risk360, alerts) to detect threats, monitor experience/performance, investigate root causes, remediate issues, and continuously optimize integrations and policies

©2026 Zscaler, Inc. All rights reserved.

eLearning Details

Prerequisites	A working understanding of computer networking, network monitoring and configuring. Familiarity with enterprise IT infrastructure and experience in using web-based management portals is recommended
Proficiency	Intermediate
Description	This in-depth course equips administrators to confidently administer, and continually optimize the Zscaler Zero Trust Exchange across ZIA, ZPA, and ZDX. Administrators gain hands-on experience with Zero Trust approaches to user/device management, platform setup, advanced policy management, monitoring/reporting, and troubleshooting Zscaler deployments.
Duration	15.8 hours
Type	Self-paced
Completion Criteria	Complete the eLearning
Available Language(s)	English
Price per Set	Free

eLearning Outline

Module	Topic	Sub Topic
Module 1: Introduction to Zero Trust Exchange (ZTE)	The Need for Digital Transformation / Introduction to Zero Trust Exchange	• Traditional Perimeter Network Security Architecture • Why Perimeter Network Security Architecture Is No Longer Effective • Zscaler Zero Trust Exchange • 5 Key Attributes of the Cloud Native Zero Trust Exchange • Benefits of Zscaler Zero trust Exchange Over Perimeter Network Security Architecture • Zscaler's Comprehensive and Integrated Solutions (Using Experience Centre UI) • Zscaler Zero Trust Exchange – Functional Diagram • Who Uses Zscaler Services?

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
Module 2: User Management	Introduction to Zero Trust Exchange	• Traditional Perimeter Network Security Architecture • Why Perimeter Network Security Architecture Is No Longer Effective • Zscaler Zero Trust Exchange • How the Zero Trust Exchange Works
	Understanding ZIdentity	• **Identity Fundamentals** » Security Assertion Markup Language (SAML) » SAML Components » OAuth 2.0 » OAuth 2.0 Authentication components » OAuth 2.0 Flow » OpenID Connect (OIDC) » Key Differences Between SAML and OIDC • **Introduction to ZIdentity** » ZIdentity Features (Automated Identity Management, Centralized Entitlement, Streamlined Authentication) » Common Identity Service Benefits » Key Features and Benefits » ZIdentity–Supported External Identity Providers • **Authentication with ZIdentity** » Configuring Microsoft Entra ID as an External Identity provider (IdP) » IDP and SP initiated SSO ZIdentity » IDP initiated SSO » SP initiated SSO • **Authorization with ZIdentity** » System for Cross–Domain Identity Management » SCIM Provisioning Flow – Azure » Configuring SCIM
	Managing users in Experience Center	• **Introduction to the Experience Center** » Getting Started with ZIdentity Administration » Zscaler Experience Center » Why Experience Center » Five Verticals of the Zscaler Experience Center (Analytics, Administration, Policies, Infrastructure, Logs) • **User Management in the Experience Center** » Accessing and Navigating the ZIdentity User Management » User & User Groups » Attributes » User Attributes

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
		» Session Attributes » ZIdentity Admin Roles » Service Entitlements » Administrative Entitlements • **Policies and Audit Logs** » Admin Sign–On Policies » Password Policies » Audit Logs • **Multifactor Authentication** » MFA in ZIdentity » Enabling MFA or FIDO2 in Zidentity » Integrate with IdP's MFA for User Authentication » Skip Second–Factor Authentication
Module 3: Device Management	Understanding Network Tunneling	• **Introduction to Tunneling** » What Is Tunneling? » Types of Tunnels » Benefits of Tunneling • **Introduction to Z–Tunnel** » Introduction » Difference Between Z–Tunnel 1.O and 2.O » Z–Tunnel Best Practices
	Installing and Deploying Zscaler Client Connector	• **Introduction Zscaler Client Connector** » Zscaler Client Connector Portal: Introduction » Key ZCC Configuration Elements » Accessing the Zscaler Client Connector Portal • **Deploying Zscaler Client Connector** » Selecting the Client Connector Release to Deploy » Downloading the Zscaler Client Connector Installer File » Installing the Zscaler Client Connector » Installing on Windows and Supported Parameters » Installing on macOS and Supported Parameters » Installing on Linux and Supported Parameters » Installing on iOS and supported parameters » Installing on Chrome/Chrome OS on Android and supported parameters » Deploy ZIA CA certificate for SSL Inspection » Deploying ZCC with Strict Enforcement » Best Practices for Deploying Client Connector • **Zscaler Client Connector Settings Overview** » Client Connector Refresh Intervals » Overview of Client Connector Global and Supportability Settings

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
		» Overview of Client Connector End User Notification settings » What are PAC FIles? Types of PAC files • **Zscaler Client Connector – Forwarding Profile** » Zscaler Client Connector Forwarding Profile » Configure Client Connector Forwarding Profile – General Settings » Configure Client Connector Forwarding Profile for Z–Tunnel 2.0 » Trusted Networks • **Zscaler Client Connector – App Profile** » Zscaler Client Connector – App Profiles » Configuring Client Connector App Profile • **Zscaler Client Connector – Device Postures and Polices** » Device Posture Overview » Device Posture Platform Support and Usage Guidelines » Leveraging device postures for service entitlement » Leveraging device postures for App Profile selection » Leveraging device postures for ZPA Access Policies » Leveraging device postures with ZIA enforcement policies
	Collecting Client Connector Health Metric	• **Understanding ZCC Telemetry** » ZCC telemetry » Why is it beneficial » How does it work? » How to enable this feature
Module 4: Core Platform Management	Understanding ZIA – Network Integration	• **ZIA Location Fundamentals** » What is a Location? » Why do we need Locations? » Understanding Sub Locations » What are Location Groups? • **ZIA Connectivity: Static IP, GRE, IPSec** » Static IP » Benefits of Static IP » GRE Tunnels » GRE Tunnel from Router » Key Features and Benefits » IPSec VPN » About IPSec Tunnel » Key Features and Benefits » Comparison between GRE and IPSec Tunnels

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
	ZPA: Deploying App Connectors and Understanding Private Service Edges	• **App Connector Deployment** » App Connector » Application, Application Segment and Segment Group » App Connector, App Connector Group and Server Group » Pulling it Together – Where Each Component Fits » Deploying App Connectors » Deploying App Connectors in Various Environments » Deploy App Connectors » Deploy App Connectors Architecture » Provisioning Keys » Deploy App Connector Process – Provisioning Keys & Certificates » Deploy App Connectors – Connector Group » Map App Connectors to Server Groups » Define Application & Server Group Mapping • **Private Service Edge Fundamentals (ZPA)** » What is Private Service Edge? » ZPA Private Service Edge – Features » ZIA Private Service Edge – Features
	Managing ZIA – Forwarding Control and DNS Control	• **Forwarding Control** » Forwarding Control » Configuring Forwarding Policy » Configuring Forwarding Rules » Use Case 1: Configuring Forwarding Rules for Dedicated IP » Use Case 2: Configuring Forwarding Rules for Geo IP » Use Case 3: Configuring Forwarding Rules for SIPA » Use Case 4: Configuring Forwarding Rules for Proxy Chaining • **DNS Control** » DNS Control is about Security and Performance » Zscaler DNS Control » DNS Performance » Zscaler Trusted Resolver » Forwarding DNS Traffic to ZIA » DNS Security across the Killchain » DNS Security to Enable Local Internet Breakout » DNS Granular Policy Examples » Use Cases » Best Practices

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
	Understanding OneAPI	• **API Key/Integration Management** » Introduction to APIs » What is an API? » How API works? » Why do we Need APIs? » RESTful APIs » Traditional Automation Framework: Challenges » Traditional Zscaler Automation Framework: Workflow » Solution: Zscaler Zero Trust Automation » Key Benefits of Zscaler Zero Trust Automation » What is OneAPI? » OneAPI Workflow » Key Features of OneAPI
Module 5: Understanding ZIA Policies	Network and Traffic Control	• **Firewall Rules** » Zero Trust Firewall and use cases » Firewall Control Policy » Configuring and Ordering Firewall Policies » Understanding Firewall Criteria (Logical AND) – Creating Firewall Actions • **Bandwidth Control** » Bandwidth Control Policy Overview » Bandwidth Control Policy – Configuration » Monitor bandwidth usage against Policies • **File Type Control** » File Type Control Overview, Importance and identification » Define and categorize allowed/blocked file types for upload/download » Apply file-type control policies to specific users or groups » Monitor and review file transfer activities
	Web and Application Access Management	• **URL Filtering / Cloud App Controls** » Overview of URL Filtering functionality, importance and configuration » Applying URL Filtering to Custom URL Categories » Overview of Cloud App Control functionality, importance and configuration » Policy Enforcement Order » Tenancy Restriction Policy and configuration

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
	Encryption and Traffic Inspection	• **SSL/TLS Inspection** » Overview of TLS/SSL Inspection » Understanding how ZIA TLS Inspection/TLS Proxy Works and why it is needed. » Deploying SSL/TLS Inspection » Define specific domains and categories to bypass SSL inspection » Understanding Certificate Chain with TLS/SSL Inspection » Reviewing common SSL inspection issues
	Malware and Threat Detection	• **Advanced Threat Protection** » ATP Overview & command and control channels » Advanced Threat Policy » Configure Safe Search Enforcement • **Malware Protection** » Malware Protection Overview and Types of Malware » Malware Protection Policy • **Sandbox Policy** » Zscaler Sandbox Overview and Policy Flow » Configure actions based on sandbox results » Review sandbox reports to analyze threat verdicts
Module 6: Configuring DLP Policies	Policy and Security Capabilities	• **Data Loss Prevention (DLP – Inline/eDLP)** » Data Loss Prevention (DLP) Policy Overview » Data Classification and Content Inspection Capabilities » Data Loss Prevention Policies – Content & Context–driven » Content Inspection Rules and Patterns and Matching Options » Web DLP Policies and Use cases • **Cloud App Security (CASB)** » Shadow IT Discovery overview and monitoring » Importance of discovering Application Types » Discover sanctioned/unsanctioned SaaS applications » Enforce granular controls for app usage • **Smart Browser Isolation** » Smart Browser Isolation Overview » How it works

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
Module 7: Implementing ZPA Policies	Configuring ZPA Policies	• **Access Policy** » Access Policy Overview » Configuring Granular Access » Access Policy: ACTION & CRITERIA » Posture Check Access Policy Configuration • **Client Forwarding Policies** » Client Forwarding Policy: Overview » Policy Configuration: Actions » Default Client Forwarding Policy: Forward to ZPA » Client Forwarding Policy: Bypass ZPA • **Timeout Policy** » Timeout Policy Overview » Timeout Policy: Authentication & Idle Connection Timeout
Module 8: Reviewing Dashboard and Logs	Log, Insights, and Dashboard	• **ZIA Logs** » ZIA Overview, Filtering Logs, Searching Logs, Analyzing Logs » Insights Logs, Web Insights Logs, Firewall Logs, Mobile Insight Logs » DNS Insights and Tunnel Insights • **ZPA Access Logs** » ZPA Logs: Overview, ZPA – Events Diagnostics, Private Access Logs » Reviewing Application Usage Pattern in ZPA, Tools for Monitoring Usage and Benefits of Reviewing Usage Patterns • **ZIdentity Audit Logs** » ZIdentity Audit Logs: Overview » What Audit Logs Captures? • **ZCC Logs** » ZCC Logs: Overview » Pop-up Notifications » Configure Policy Logging and Notifications » Logging Modes in Zscaler Client Connector • **Log Streaming** » How Log Streaming Works? » VM-Based and Cloud NSS Feeds: Overview » Log Streaming Services Overview

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
Module 9: Security Reporting and Risk Analytics	Strategic Security Reporting and Risk Assessment	• **Security Reports (Threats, DLP)** » Threat Landscape Reports (Malware, Phishing, GenAI): Purpose & Value » ZIA Analytics, ThreatLabz Contribution » DLP Incident Reports: Overview • **Risk360** » Monitor your domains for external surface attacks, identify and report exposed assets, and quantify risk using Risk360 » How Risk360 benefits administrators » Critical Risk Identification & Identifying Root Causes of Increased Incidents » Quantifying potential financial losses resulting from cybersecurity risks » Board-ready Reporting, Risk Mapping, and Guidance
Module 10: Monitoring using ZDX	User Experience Monitoring and Insightful Reporting	• **ZDX Overview** » Zscaler Digital Experience (ZDX): Proactively Identify and Resolve Performance Issues » ZDX — Operational View » ZDX — High Level Architecture • **User Experience Monitoring** » Web/Cloud Path Probes – Overview » Monitoring Network Path Performance & Latency » Tracking Application Response Times & Availability » Analyzing User Digital Experience Scores » Key Score Types in ZDX » Introduction to ZDX Copilot » How Copilot Works? » The End-to-End Latency ZDX Copilot: AI-Driven Assistance • **Application Performance Management** » Application and Path Monitoring » Key Offerings of ZDX Monitoring, Performance Dashboard » Benefits of Application Performance Management » Diagnose Issues Impacting End-User Productivity

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
		• **Visualization and Reporting** » ZDX Dashboard Overview » Performance Overview & Filtering Options » Key Dashboard Metrics » Visualizing Performance Issues » Monitoring User and Device Wi-Fi Performance • **Alerts and Rules** » Defining and Managing Alert Rules in ZDX » Defining Rules in the ZDX Administrator Portal » Dynamic Alerts
Module 11: Trouble-shooting & Incident Response	Analyzing the Common Root Cause	• **Connectivity Issues Using ZDX Diagnostics** » Utilize ZDX diagnostics (diagnostics, log, packet capture) » Perform network troubleshooting (traceroute, MTR, ping) » Analyze network traffic flow through Zscaler » Analyze UCaaS applications poor performance based on the ZDX score » Filter User/Network/Location activites with poor ZDX score • **Policy Enforcement Failures** » Review policy rule order and hierarchy » Verify user/group membership for policy matching • **Application Access Problems (ZPA)** » Verify App Segment configuration and associated policies » Check ZPA App Connector health and reachability to applications » Analyze Live logs for tracking user activities/status, and application activities » Review ZPA access logs for denied connections • **Performance Bottlenecks** » Analyze Zscaler dashboards for bandwidth and latency metrics
	Implementing Incident Response & Remediation	• **Malware/Phishing Alerts** » Isolate affected users/devices » Block malicious domains/IPs in Zscaler policies » Coordinate with SOC/IR teams for broader remediation

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
		• **DLP Incidents Investigation** » Review DLP logs and content of leaked data » Identify source of DLP violationand contact affected parties » Implement additional controls to prevent recurrence • **Account Compromise** » Review User Risk Score » Force password resets or MFA re-enrollment » Review audit logs for unauthorized access • **Service Disruptions** » Monitor Zscaler trust.zscaler.com for platform status » Communicate outages/degradations to users » Implement temporary workarounds if necessary
Module 12: Integrations & Optimization	Managing Ecosystem Integrations	• **SIEM** » Configure log forwarding (NSS/LSS) to SIEM platforms • **IdP (Okta, Azure AD, Ping)** » Manage IdP configurations and attribute mappings » Troubleshoot authentication and synchronization issues
	Optimizing Policies	• **Policy Cleanup/Consolidation** » ZIA-Based: Regularly review and remove unused/stale policies » Improve policy efficiency by merging redundant rules and objects for Cloud App Control and URL Filtering » ZPA-Based: Ensure streamlined app access by removing outdated or unused ZPA policies » Streamline secure access by consolidating redundant rules and objects within application access policies • **Performance Tuning** » Optimize policy order for efficiency » Review and refine SSL inspection bypasses » Monitor and adjust resource allocation for Private Service Edges/Connectors
	Maintaining Platform	• **ZCC Version Updates** » Plan and schedule ZCC client upgrades » Test new ZCC versions in a pilot group » Deploy updates to the broader user base • **App Connector Health & Updates** » Monitor health metrics of ZPA App Connectors » Schedule and perform software updates for Connectors

©2026 Zscaler, Inc. All rights reserved.

Module	Topic	Sub Topic
		» Ensure high availability and failover management of App Connector groups • **Multi-Session VDI** » VDI Workflow » Configure VDI Templates (Forwarding Profiles, Groups, Devices) • **Staying Informed on Zscaler Roadmap/Features** » Participate in Zscaler webinars and product briefings » Read release notes and security advisories » Engage with Zscaler support and community forums » Review and track product release notes and notifications
	Documentation & Best Practices	• **Security Posture Reviews** » Conduct regular audits of Zscaler configuration against best practices » Identify and address configuration drift » Ensure compliance with internal security policies

Hands-On Lab Details

Prerequisites	Zscaler for Users – Administrator (EDU-200) self paced eLearning course
Proficiency	Intermediate
Description	Practice what you learned in training using our remote lab. Manage organizational access by creating and assigning departments, groups, entitlements, and admin roles, while configuring secure traffic forwarding with Zscaler Client Connector and dedicated IPs. They'll implement and troubleshoot firewall and content-filtering policies, enable SSL inspection with appropriate exemptions, and apply DNS security and unified DLP to protect sensitive data. The course also covers deploying ZPA for secure access to internal apps and diagnosing connectivity issues, plus using ZDX dashboards and advanced analytics to improve performance and resolve root-cause issues impacting user experience.
Duration	8 hours
Type	Instructor-led hands-on lab
Completion Criteria	Complete all hands-on labs
Available Language(s)	English
Price per Seat	US $1200 (2 credits)

©2026 Zscaler, Inc. All rights reserved.

Lab Outline

Task	Sub Task
Connecting to the Virtual Lab	• Test Your Lab Access and Start Your Environment • Signing in to the Experience Center Landing Page
Configure User and Administrator Access Entitlements	• Create Departments and User Group • Creating Users • Adding Administrative and Service Entitlements • Verify Entitlement Access for Users
Forwarding Traffic with the Zscaler Client Connector	• Configure Forwarding Options • Log into the Zscaler Client Connector and Verify Protection
Understanding Firewall Filtering Policy	• Test Non-web Traffic with Firewall Default Block • Configure Firewall Policy for allowing outbound SSH and ICMP traffic • Configuring a Firewall Filtering Policy to Restrict Application
Configuring SSL Inspection Policies	• Enable SSL Inspection for All Destinations • Verify Zscaler CA Installation [Optional] • Certificate Pinning Error
Content Filtering & Access Control	• View Threat Protection Reports • Configure Content Filtering Controls • Test End User Experience with URL Filtering • Configure Cloud App Control
DNS Security	• Configure App Profile • Configure DNS control policy • DNS Insight Logs
Policy Enforcement with Unified DLP for Multi-Channel	• Protect PII Information for Data in Motion
Provisioning ZPA Infrastructure	• Provision an App Connector • Activate the App Connector
Add a Corporate Application	• Configure a Wildcard Application Segment for Internal Applications • Configure User-Specific Access for the Intranet Application • Block Intranet Access for Unauthorized Users • Enabling ICMP Access

©2026 Zscaler, Inc. All rights reserved.

Task	Sub Task
Accessing the Internal Application using Remote Desktop Protocol (RDP) for troubleshooting	• Ensuring access to internal application using RDP
Troubleshooting access to the internal application for a specific user	• Tracking the root cause for access issue to the internal application • Troubleshooting for access issue to the internal application
Traffic Forwarding through SIPA	• Configure Source IP Anchor (SIPA) in ZPA • Configure ZIA Forwarding for Source IP Anchor • Verify Source IP Anchor (SIPA) Functionality
Navigating the Incident, Self-Service, Application Overview Dashboard	• View ZDX Performance Dashboard • View Incidents Dashboard and Self Service Dashboard and identify the key issue • View Application Overview Dashboard • View User Overview Dashboard
Troubleshooting Poor Wi-Fi	• View User ZDX Score for an Application • Analyze Poor ZDX Score Interval • Compare Poor ZDX Score to Last Known Good Score • Isolate High Latency Hop • View User Device Events Associated with ZDX Score Changes
Troubleshooting Slow DNS Response	• Use ZDX Copilot for Root Cause Analysis • View User ZDX Score Over Time • Analyze High Page Fetch Time

Certificate Exam Details

Prerequisites	Zscaler for Users – Administrator Hands-On Lab
Duration	90 minutes
Test Format	50 multiple-choice questions
Available Language(s)	English
Price per Attempt	US $300 (1 credit)

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 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.

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

zscaler™

Act Fast.
Stay Secure.