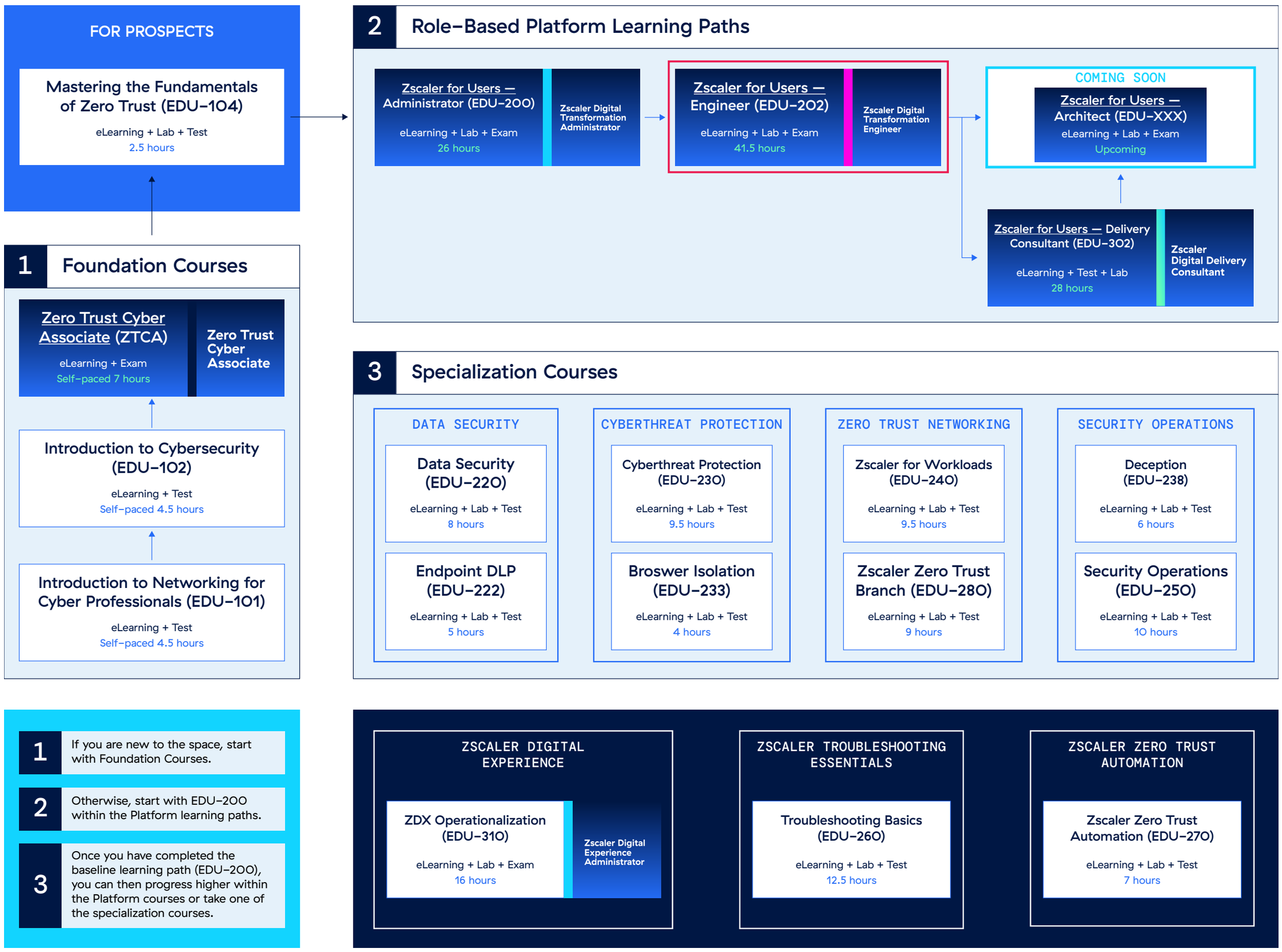
Zscaler Cyber Academy

Zscaler for Users – Engineer (EDU-202)

COURSE OUTLINE

Zscaler Cyber Academy Catalog

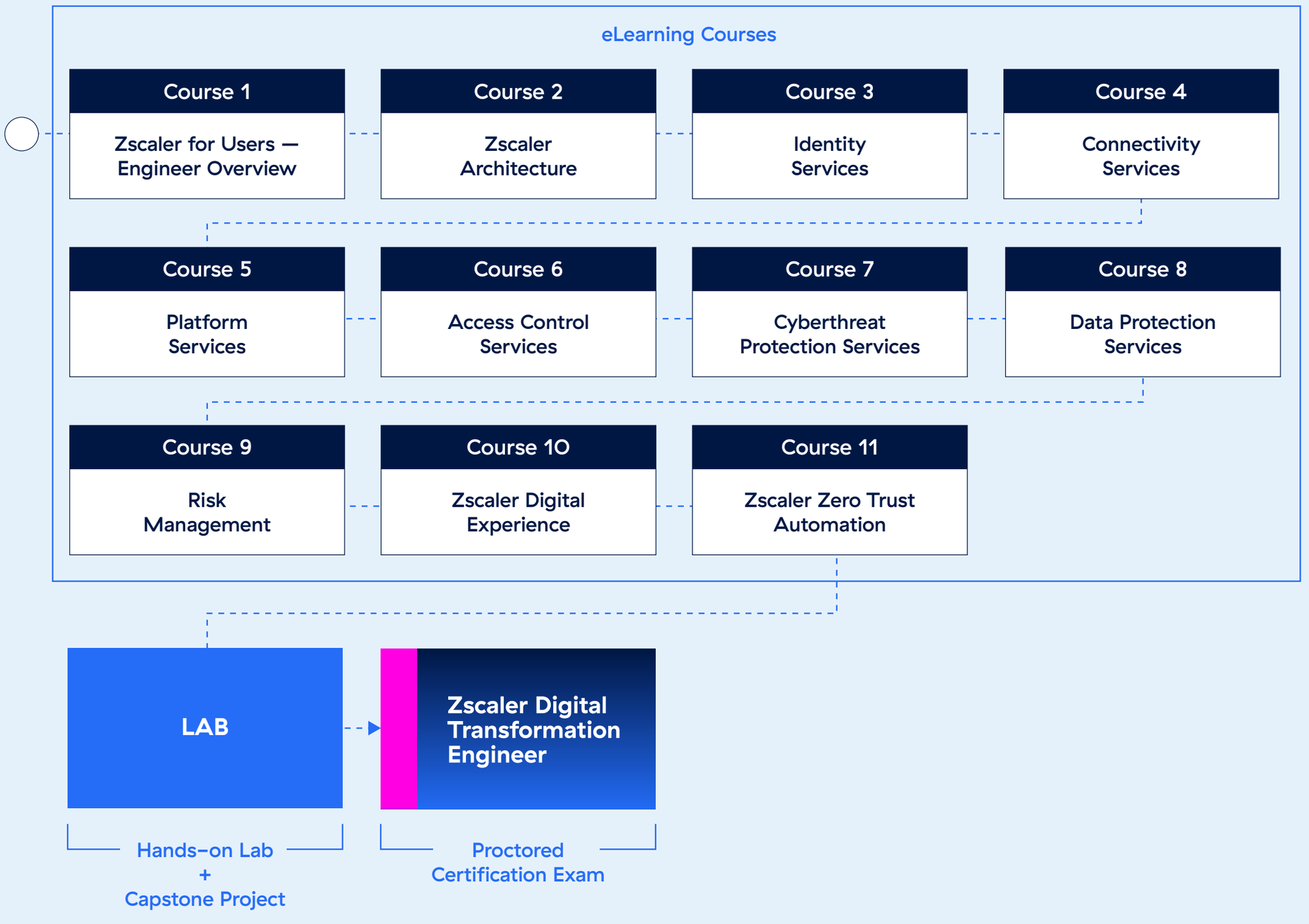


Zscaler for Users – Engineer (EDU-202) Learning Journey Map

The recommended path for completing the Engineer journey is to complete the 11 eLearning courses and then take the hands-on labs. Once this is completed, you can sign up for taking the proctored exam. Upon the successful completion of this exam, you'll be awarded the Zscaler Digital Transformation Engineer (ZDTE) Certification.

OUR LEARNING PATH

Zscaler for Users – Engineer (EDU-202) Learning Path



LEARNING OUTCOMES

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

- Discuss the architecture of the Zscaler platform, including its global scale, additional capabilities offered, and API infrastructure
- Configure advanced connectivity options such as Browser Access, SD-WAN, Client Connector, Branch Connector, and Cloud Connector
- Configure advanced cybersecurity services and Zscaler Digital Experience for applications, call quality monitoring, probes, diagnostics, alerts, and role-based administration

eLearning Details

Prerequisites	Zscaler Digital Transformation Administrator certificate
Proficiency	Advanced
Description	In this course, you will go beyond your initial deployment and provisioning to learn about advanced configuration of the identity, platform services, connectivity, access control, digital experience monitoring, security, and data protection services of the Zscaler Zero Trust Exchange. You will also learn about risk management and Zscaler Zero Trust Automation.
Duration	24 hours
Type	Self-paced
Completion Criteria	Complete the eLearning
Available Language(s)	English
Price per Seat	Free

eLearning Outline

Topics	Sub Topic
Zscaler for Users — Engineer Overview	• Recap of Zscaler for Users — Administrator (EDU-200) • Introduction to Zscaler for Users — Engineer (EDU-202)
Zscaler Architecture	• Multitenant Cloud Security Architecture • Architecture Deep Dive • ZIA, ZPA, ZDX, and ZIdentity Architecture Overview • Additional Capabilities • Zscaler API Architecture
Identity Services	• Essentials of ZIdentity Authentication • Configuring Authentication Levels, Methods, and Types • ZIdentity Integration • ZIdentity Policies

Topics	Sub Topic
Connectivity Services	• Zscaler Client Connector — Tunnel Mode • GRE Tunnel Options • IPsec Tunnel Options • Forwarding Profile PAC vs App Profile PAC • Zscaler Branch Connector • Zscaler Cloud Connector • Browser Access • Configuring Browser Access and User Portals • Privileged Remote Access • Configuring Privileged Remote Access • SD-WAN / Any Router
Platform Services	• Zscaler Private Service Edges • ZPA Private Service Edge • ZIA Private Internet Service Edge • Traffic Forwarding — Source IP Anchoring • Policy Framework • Analytics & Reporting
Access Control Services	• Firewall • DNS Control • DNS Configuration Use Cases & Best Practices • Zscaler DNS Policy Demonstration • Tenant Restrictions • Zscaler Tenant Restrictions Demonstration • Cloud App Instances / Cloud App Control Policy • Segmentation & Conditional Access Through Policies • Access Control Services Configuring Private Application Access • Segmentation • Microsegmentation • App Segmentation • Client to Client connectivity • Server to Client connectivity

Topics	Sub Topic
Cyberthreat Protection Services	• Recap from Cyberthreat Protection Services: Course 6 of 10 (EDU-200) • Advanced Threat Protection • Cloud Sandbox • Cloud Sandbox Policies • Intrusion Prevention System (IPS) • Browser Isolation • Setting Up Zero Trust Threat Isolation • Zscaler Browser Isolation • Browser Isolation Configuration • Zscaler Deception • What is Zscaler Deception? • Zscaler Deception Workflow • Set up a Zscaler Deception Campaign • Zscaler ITDR • Zscaler ITDR Demo • Private Access AppProtection • Private Access AppProtection Video 1 • Private Access AppProtection Video 2 • Private Access AppProtection Configuration
Data Protection Services	• Secure Data in Motion • Secure SaaS Data • Secure Cloud Data and Endpoint Data • Secure SaaS Access from BYOD • Incident Management

Topics	Sub Topic
Risk Management	• What is Risk Management? • Risk Management Overview • Risk Based Business Decisions • Risk Management Process • Risk360 — Risk Quantification Visualization Framework • Contributing Factors to Organizational Risk Score • Investigate Workflows Using Risk360 • Exclude/Include Risk Factors • Exclude/Include Entity Contributing to the Risk Factors • Annotated Risk Score Trend Chart • Alerts • Mapping to Security Risk Framework • Financial Analysis • Data Fabric for Security • Unified Vulnerability Management • Deception: Architecture and Use Cases • ITDR Posture • EASM • Breach Predictor
Zscaler Digital Experience	• Introduction to ZDX • ZDX Metrics • Probe • Configuring Probes • Diagnostics • Configuring Diagnostics • Alerts • Configuring Alerts • Device Software and Process Inventory • Configuring Applications • Integration with Intune • Integration with Service Now • Configuring Call Quality Monitoring • Configuring Self Service Settings • Configuring Data Explorer • Configuring Inventory Settings in ZDX • Role-Based Administration • Configuring RBAC • ZDX Dashboard • Analytics • Hosted Monitoring • Visualization and Reporting • AI Influence in ZDX • ZDX: Workflow Automation Integration

Topics	Sub Topic
Zscaler Zero Trust Automation	• Recap of EDU-200 • Legacy Automation Architecture • Zscaler Zero Trust Automation Framework • Components of OneAPI • Configuring OneAPI • Sample API Call Using OneAPI • Use cases

Hands-On Lab Details

Prerequisites	Zscaler for Users – Engineer (EDU-202) self paced eLearning course
Proficiency	Advanced
Description	The Zscaler For Users – Engineer (EDU-202) Hands-On Lab builds on the Zscaler For Users – Engineer (EDU-202) eLearning by allowing students to practice the skills they learned in the eLearning portion. This lab session will help you: 1. Gain an overview of the advanced concepts of Zscaler's Zero Trust Exchange and the advanced use cases for adopting the Zscaler for Users platform of solutions 2. Configure the advanced functions of ZIA, ZPA, and ZDX and monitor them 3. Explore the advanced services and their capabilities offered by the Zero Trust Exchange including connectivity, platform, access control, cyber security, data protection, and digital experience
Duration	1.5 days, 12 hours
Type	Instructor-led hands-on lab
Completion Criteria	Complete all hands-on labs
Available Language(s)	English
Price per Set	$1200 (6 credits)

Lab Outline

Task	Sub Task
Lab 1: Connecting to the Virtual Lab	• Task 1.1: Test Your Lab Access and Start Your Environment • Task 1.2: Signing into ZIdentity landing page • Task 1.3: Verify Lab Access
Lab 2: Create ZIdentity user account and verify service entitlement	• Task 2.1: Create a user Account, assign to user group and verify access
Lab 3: Connectivity Services—Configure Browser Access for 3rd Parties	• Task 3.1: Provision App Connector • Task 3.2: Create HVAC Application Web Server Certificate • Task 3.3: Create HVAC Application and Access Policy for Browser Access • Task 3.4: Create DNS CNAME Record for the HVAC Application • Task 3.5: Test Browser Access to the HVAC Application
Lab 4: Platform Services—Configure Log Streaming	• Task 4.1: Provision Dedicated App Connector for Log Streaming • Task 4.2 : Add Log Receiver • Task 4.3: Add SSH Access to SIEM Server in Private Data Center • Task 4.4: Verify Log Feed
Lab 5: Access Control Services—Configure & Examine Firewall Policies	• Task 5.1: Verify Client Connector Forwarding to Firewall • Task 5.2: Verify Tunnel Version v2.0 DTLS Forwarding on User's Device • Task 5.3: Test Non-web Traffic with Firewall Default Block • Task 5.4: Configure Firewall Policies • Task 5.5: Examine Firewall Traffic • Task 5.6: Check Firewall Filtering Rule Log Data
Lab 6: Securing Access to Internet	• Task 6.1: Configure SSL Inspection Policy & Verify SSL Decryption
Lab 7: Cyberthreat Protection Services—Configure Sandbox File Inspection	• Task 7.1: Configure Sandbox Policies
Lab 8: Cyberthreat Protection Services—Browser Isolation	• Task 8.1 Build Isolation Profile • Task 8.2 Implement Isolation Policy • Task 8.3: Add URL/Cloud App Isolate Control Policies

Task	Sub Task
Lab 9: Cyberthreat Protection Services—Deception-Based Active Defense	• Task 9.1: Generate Recon Activity • Task 9.2: Investigate Deception Alerts • Task 9.3: Explore Orchestrate Menu in Deception Dashboard
Lab 10: Policy Enforcement with Unified DLP for Multi-Channel	• Task 10.1: Protect PII Information in Unsearchable PDF/ documents for Data in Motion
Lab 11: Manage Incidents with Zscaler Workflow Automation (ZWA)	• Task 11.1: Enroll with Zscaler Client Connector • Task 11.2: View Current DLP Incidents • Task 11.3: Modify Incident Metadata • Task 11.4: Test User Notification/Coaching & Escalation Workflow • Task 11.5: Configure Automated Workflows
Lab 12: Analyzing Risk with MITRE ATT&CK and NIST CSF	• Task 12.1: Analyzing Risk MITRE ATT&CK Framework • Task 12.2: Analyzing Risk with NIST CSF
Lab 13: Configuring Cloud Applications Monitoring	• Task 13.1: Configure a Custom Application • Task 13.2: Create a Custom Probe
Lab 14: Zscaler Digital Experience—Configure Alerts & Diagnostics	• Task 14.1: Create an Alert Rule • Task 14.2: Configure a Diagnostic Session
Lab 15: Adding API Clients	• Task 15.1: Adding API Clients • Task 15.2: Testing API endpoint using POSTMAN • Task 15.3: Adding APP Connector Group using OneAPI Endpoint
Lab 16: Capstone Project	• Task 16.1: Apply Identity Services Best Practices • Task 16.2: Apply Access Control Services Requirements • Task 16.3: Apply Cyberthreat Protection Services Requirements • Task 16.4: Apply Data Protection Services Requirements • Task 16.5: Apply Zero Trust Automation Requirements

Certificate Exam Details

Prerequisites	Zscaler for Users – Engineer eLearning; ILT 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**.

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

Zero Trust Everywhere