Ultima ZScaler Zero Trust Security Cloud

Service type

Lot 2a: Infrastructure Software as a Service (iSaaS)

- **Service name**

Service name

Ultima ZScaler Zero Trust Security Cloud

Edit

- **About your service**

Service description

Zscaler is a cloud-based security platform that protects users, data, and applications wherever they are, delivering seamless, scalable internet and private app access with advanced security, Zero Trust access, and centralized policy management eliminating the need for traditional hardware appliances or legacy VPNs.

Edit

Service categories

- Systems Infrastructure Software
  - Security
    - Cloud native application protection platform
      - Cloud native application protection platform
    - Identity and access management
      - Access
      - Privilege
    - Endpoint security
      - Endpoint security
    - Network security
      - Trusted network access and protection
      - Active application security
    - Security analytics
      - Security analytics
    - Data security
      - Information protection
      - Digital trust
    - Governance, risk and compliance
      - Governance, risk and compliance

Edit

Multi cloud support

Yes

Edit

- **Service features and benefits**

Service features and benefits

Service features

- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)

- Zero Trust security for Cloud and Workloads
- SaaS Security
- AI Security
- Digital Experience Monitoring
- Cloud Firewall
- Data Loss Prevention (DLP)
- Security Operations
- Globally distributed and scalable Cloud-Native Architecture

Service benefits

- Improve overall Security posture
- Reduce risk of a Cyber attack
- Reduce the risk of Data Loss
- Reduce the risk of a Ransomware attack
- Reduce network and security complexity through technology consolidation
- Reduce cost
- Improve User Experience, Performance & Productivity
- Improve business agility and accelerate digital transformation initiatives
- Enable and simplify organisation transformation and scalability

Edit

- **Service scope**

Add-ons and extensions

Software add-on or extension

No

Edit

Cloud deployment model

Private cloud

Edit

Service constraints

There are no operational constraints to the service

Edit

System requirements

- Depends on use case and the Platform components being utilised
- System requirements can be found: https://help.zscaler.com/

Edit

- **Reselling**

Supplier type

Supplier type

I’m a reseller providing extra features and support not available from the original supplier

Organisation whose services are being resold

ZScaler

Edit

- **User support**

Email or ticketing support

Email or online ticketing support

Yes

Support response times

Zscaler offers 24/7 support across all tiers. For Essentials, high-priority (P1) support tickets receive an initial response within 30 minutes where as a P4 is within 4 hours. Please see further details of support SLA's here: https://www.zscaler.com/resources/data-sheets/zscaler-support-guide.pdf

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

WCAG 2.2 AA

Edit

Phone support

Phone support

Yes

Phone support availability

24 hours, 7 days a week

Edit

Web chat support

Web chat support

No

Edit

Onsite support

Yes, at extra cost

Edit

Support levels

Zscaler offers four main customer support levels to ensure organizations get the right assistance for their needs: •Essentials: Provides 24/7 access to support via phone, web portal, and admin console, including online training and resources. Initial response for highest-priority (P1) incidents is within 30 minutes. •Support Plus: Includes all Essentials features, faster initial response (15 minutes for P1), and adds proactive operational engagement like monthly case reviews, business continuity planning, health checks, and periodic service resiliency audits. •Premium Support Advanced: Adds deeper operational engagement and strategic planning, such as customized training, biannual architecture review, and annual security policy review. •Premium Support Advanced Plus: Offers dedicated focal support teams for escalation, and further strategic benefits including reviews for enhancement requests and prioritization. All tiers offer always-on coverage, escalation pathways, and resources tailored to maximize your Zscaler investment. As support spend increases, coverage and deliverables are enhanced to meet enterprise requirements. A full overview and comparison can be found here: https://www.zscaler.com/resources/data-sheets/zscaler-support-guide.pdf

Edit

Support available to third parties

Yes

Edit

- **How users work with your service**

Browsers

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Firefox
- Chrome
- Safari
- Opera
- Other

Edit

Installation

Application to install

Yes

Compatible operating systems

- Android
- iOS
- Linux or Unix
- macOS
- Windows
- ChromeOS
- Other

Edit

Mobile

Designed for use on mobile devices

Yes

Differences between the mobile and desktop service

Zscaler provides feature parity for users across supported mobile and desktop operating system platforms.

Edit

Service interface

Service interface

Yes

Description of service interface

The Zscaler administrator portal is a cloud-based console that provides a unified interface for managing security policies, user access, and monitoring traffic across the organization. Administrators use the portal to set and enforce policies, configure security and access controls, view analytics, and respond to threats in real time. With intuitive dashboards and reporting tools, IT teams can quickly identify issues, adapt policies, and ensure compliance—streamlining service management without the need for on-premises hardware.

Accessibility standards

WCAG 2.2 AA

Accessibility testing

Zscaler's Compliance team stays current with evolving accessibility requirements and partners with our product and engineering teams through the Software Development Lifecycle (SDLC) to help ensure our products, software, and services adhere to applicable accessibility laws and regulations. We document our conformance by self-publishing an Accessibility Conformance Report (ACR) for our solutions using the Voluntary Product Accessibility Template (VPAT)® v2.5,

aligned to Revised Section 508 and the Web Content Accessibility Guidelines (WCAG) Conformance Levels A and AA criteria.

Edit

User support

User support accessibility

WCAG 2.2 AA

Edit

API

API

Yes

What users can and can't do using the API

The Zscaler API empowers organizations to automate, customize, and streamline the management of their cloud security operations. With the API, users can programmatically control security policies, manage user accounts, update access rules, and integrate Zscaler with third-party platforms such as IT service management and SIEM tools. It enables bulk configuration changes, policy enforcement, and real-time monitoring without manual intervention. This gives enterprises the flexibility to tailor Zscaler's security services to their unique workflows, automate routine administrative tasks, generate dynamic reports, and quickly adapt to evolving cyber threats. Role-based access and detailed audit trails ensure secure, controlled automation. Overall, the Zscaler API extends the platform’s powerful cloud security capabilities, helping organizations boost efficiency, maintain compliance, and respond rapidly to business or regulatory needs.

API documentation

Yes

API documentation formats

- Open API (also known as Swagger)
- HTML
- PDF

API sandbox or test environment

Yes

Edit

Customisation

Customisation available

Yes

Description of customisation

Zscaler enables extensive customization to fit your organization’s security and access needs. Administrators can tailor security policies, internet and application access controls, user authentication integrations, reporting templates, and data loss prevention settings via the centralized Zscaler Admin Console. Role-based access control (RBAC) ensures that only authorized personnel can make and apply changes. Automation and further customization can be achieved using the Zscaler API, allowing bulk changes, policy updates, and integration with third-party IT or security systems. Customization can be handled by IT and security admins, depending on their assigned permissions, ensuring secure, efficient adaptation of the platform to your business requirements.

Edit

- **Onboarding and offboarding**

Getting started

Zscaler streamlines the customer onboarding process, ensuring organizations can quickly and securely start using its cloud security services. Deployment is swift—proof-of-concept setups can be ready in as little as one day—thanks to Zscaler's cloud-native platform that does not require hardware installation or complex network changes. Customers are guided through initial setup steps such as connecting users, integrating identity providers, and configuring security policies via the centralized Zscaler Admin Console. Extensive support is available from day one, with always-on access to help via phone, web portal, and online resources, tailored by support level (from Essentials to Premium tiers). Role-based access controls and automation options (including APIs) enable IT teams to efficiently customize policies and onboard users while maintaining centralized control and compliance. Comprehensive resources—including online training, health checks, and periodic reviews—help organizations get up to speed quickly and ensure smooth adoption. The Zscaler team partners with customers through every stage, from proof-of-concept to full production, minimizing disruption and supporting a seamless transition to secure, scalable cloud-based security. Documentation on deployment guides, help portals can be found on Zscaler Help: https://help.zscaler.com/ All online training can be accessed by Zscaler Academy: https://www.zscaler.com/zscaler-academy

Edit

Documentation

Service documentation

Yes

Documentation formats

- HTML
- PDF

Documentation accessibility standard

WCAG 2.2 AA

Edit

End-of-contract data extraction

The reports here give different options to extract data from the tenants: https://help.zscaler.com/zia/dashboard-analytics/reports

Edit

End-of-contract process

Customers can download their data and documentation at no additional cost during the agreed retrieval period. After the contract expires or is terminated, Zscaler will delete customer data from its platform, usually within 60 days. If the customer requests extended termination assistance, such as transition beyond the standard period, a separate statement of work (SOW) will specify any additional fees for such services. Continued use of Zscaler services—including Premium Support—during the transition period requires a separate order and payment of applicable fees.

Edit

- **Data importing and exporting**

Data export approach

With Zscaler Internet Access (ZIA), you can download data in CSV format, for any specified date/time range, within the available 6-month window. Audit Logs can also be retrieved via API, enabling easy integration to SIEM and third-party auditing tools. To learn more, see: https://help.zscaler.com/zia/audit-log-use-cases Zscaler also aligns with the EU Data Act for customer data exports - https://www.zscaler.com/legal/data-act-addendum

Edit

Data export formats

Data export formats

- CSV
- Other

Other data export formats

JSON

Edit

Data import formats

Data import formats

Other

Other data import formats

N/A

Edit

- **Analytics**

Metrics

Service usage metrics

Yes

Metrics types

Zscaler provides real-time traffic and security analytics, giving organizations visibility into user activity, threats, and policy enforcement across their network. Metrics include detailed reports on internet usage, security incidents, cloud application access, and policy compliance. Pre-built templates (such as Executive Overview and Security Policy Audit) and SIEM integration enable comprehensive monitoring, compliance, and audit readiness.

Reporting types

- Through an API
- Real-time dashboards
- Regular reports
- Reports on request

Resource tagging

Yes

FOCUS resource tagging

No

Edit

- **Scaling**

Independence of resources

Zscaler guarantees that users are not impacted by other users' demands through its cloud-native, multi-tenant architecture and over 160 globally distributed nodes. The platform elastically scales resources as needed, providing consistently high performance for all users. Zscaler’s 99.999% SLA ensures service reliability and availability even under heavy load.

Edit

- **Public sector networks**

Public sector networks

Connection to public sector networks

No

Edit

- **Data-in-transit protection**

Protection between networks

Data protection between buyer and supplier networks

- TLS (Version 1.2 or above)
- IPsec or TLS VPN gateway
- Legacy SSL and TLS (under 1.2)

Edit

Protection within your network

Data protection within supplier network

TLS (Version 1.2 or above)

Edit

- **Asset protection**

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

- United Kingdom
- European Economic Area (EEA)
- Other locations

User control over data storage and processing locations

Yes

Edit

Datacentre security standards

Managed by a third party

Edit

Penetration testing

Penetration testing frequency

At least once a year

Penetration testing approach

Another external penetration testing organisation

Edit

Protection of data at rest

Protecting data at rest

- Physical access control, complying with SSAE-18 / ISAE 3402
- Physical access control, complying with another standard
- Encryption of all physical media
- Scale, obfuscating techniques, or data storage sharding
- Other

Other data at rest protection approach

For data at rest, Zscaler uses tokenization to mask personal information as customer transactions pass through our products. Tokenization converts meaningful data, such as a user ID, into a random string that points to the original value. Unlike encryption, no key or algorithm can recreate the original data. Tokens do not require a direct relationship to the source data to function, but customers may use a token vault to store mappings between tokens and their corresponding original data. This approach strengthens privacy controls while preserving necessary functionality and supports compliance with data protection requirements across varied operational environments and systems.

Edit

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

- Data Erasure
- Explicit overwriting of storage before reallocation / Secure Erase
- Degaussing
- Physical Destruction / Hardware containing data is completely destroyed

Edit

Equipment disposal approach

A third-party destruction service

Edit

- **Availability and resilience**

Guaranteed availability

"Zscaler guarantees industry-leading service availability through its cloud-native, multi-tenant architecture with more than 160 globally distributed nodes. The platform offers a 99.999% service level agreement (SLA) for availability, ensuring that users experience virtually uninterrupted access to security services and business-critical applications—even under heavy global demand. If Zscaler fails to meet its SLA for availability, the customer is typically entitled to compensation as outlined in their contract. This usually takes the form of service credits or refunds, calculated based on the degree and duration of the outage compared to the agreed SLA. The process for obtaining compensation requires the customer to submit a request in accordance with contract terms, and service credits are then applied to future invoices or fees. However, the specific terms—including eligibility, calculation formula, and limits—are determined by each customer's individual agreement with Zscaler. Overall, Zscaler's robust architecture and high SLA minimize downtime risk, and their contractual remedies provide reassurance that customers are protected financially if service levels are not met."

Edit

Approach to resilience

Zscaler is engineered for resilience through its cloud-native, multi-tenant architecture and extensive global footprint—comprising over 160 distributed nodes. This design ensures seamless scalability, with resources automatically adjusted to handle spikes in user demand and maintain high performance for all customers. The platform's redundancy and failover capabilities safeguard security services against outages and disruptions, supported by a 99.999% availability SLA that guarantees extremely reliable access to business-critical applications and data. Each security service is delivered directly from the cloud rather than relying on potentially vulnerable on-premise hardware, minimizing single points of failure. Zscaler's distributed infrastructure eliminates bottlenecks, providing automatic load balancing and disaster recovery to keep users protected and connected. High availability DNS integration and elastic resource allocation further enhance continuity, ensuring that core functions remain operational even during maintenance or unexpected events. In summary, Zscaler's resilient architecture protects users from service degradation caused by external factors or other tenants on the platform, maintains security and productivity, and delivers industry-leading uptime through proactive cloud engineering and robust contractual safeguards.

Edit

Outage reporting

a public dashboard and email alerts.

Edit

- **Governance**

Named board-level person responsible for service security

Yes

Edit

Security governance

Software Security Code of Practice

Yes

Security governance certified

Yes

Security governance standards

- ISO/IEC 27001
- Other

Other security governance standards

Global Certifications: FedRAMP, DoD IL5, CMMC 2, ITAR & CJIS Commercial Standards: ISO 27001/ 27701 / 27017 / 27018, SOC 2 & SOC 3, CSA STAR 2 Other: UK Cyber Essentials Plus, HIPAA, HITRUST CSF v11, PCI DSS 4.0, IRAP, ENS High, CPSTIC, C5 https://www.zscaler.com/privacy-compliance/compliance-and-standards

Edit

Information security policies and processes

Zscaler's information security program is anchored by its Master Information Security Policy, which sets a rigorous framework to protect the confidentiality, integrity, and availability of company and customer assets. This approach is validated by globally recognized certifications, including ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2, and SOC 3, which are externally audited on an annual basis. Compliance & Transparency: Customers may request detailed compliance documentation or audit reports (including ISO, SOC 2, penetration test outcomes, and vulnerability scans) through Zscaler's Compliance portal Zscaler's security policies and processes are structured to meet and exceed major regulatory and industry requirements, adapting rapidly to changes in threats or legislation. In summary, Zscaler's security policies and processes deliver a holistic, certified approach to protecting information and minimizing risk, with strong governance, continuous improvement, and proactive compliance at their core.

Edit

- **Operational security**

Configuration and change management standard

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Configuration and change management approach

Zscaler's Configuration and Change Management policies and procedures are part of our ISO 27001 and SOC 2 Type 2 certifications, which are audited annually by an independent third party. Compliance certificates and reports are available for download or through a request form on our public-facing webpage: https://www.zscaler.com/company/compliance. All change requests must be approved prior to modification, and for emergency changes, formal approval is obtained afterward. Formal operational change management processes under our ISO 27001 and SOC 2 Type II certification include change control requirements, clear roles and responsibilities, segregation of duties, and security requirements.

Edit

Vulnerability management type

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Vulnerability management approach

Zscaler has documented Security Audits, Vulnerability Management and Patch Management standards, created in accordance with international cybersecurity frameworks. These standards define the process for conducting security audits/vulnerability testing, evaluating information system technical vulnerability results, and remediating technical vulnerabilities or implementing appropriate measures to address associated risk (including patching). These standards implementation are audited by external auditors annually - SOC 2 Type II, ISO 27001, ISO 27701, ISO 27017, ISO 27018, CSA Star, and other major global frameworks: https://www.zscaler.com/compliance/overview

Edit

Protective monitoring type

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Protective monitoring approach

Zscaler monitors the daily business and operational activities, including the internal control environment, as a routine part of business. Zscaler has implemented a set of logging and monitoring tools that are configured to collect data from system infrastructure components to monitor system performance, potential security threats and vulnerabilities, resource utilization and alert IT operations upon detection of unusual system activity or service requests. The in-scope systems are monitored using enterprise monitoring applications that track system performance, responsiveness, availability and vulnerabilities.

Edit

Incident management type

Complies with a recognised standard, for example, CSA CCM v4.0 or ISO/IEC 27035:2011 or SSAE-18 / ISAE 3402

Edit

Post-quantum cryptography secure

Yes

Edit

Incident management approach

Zscaler’s incident management process follows a formal Incident Response Plan to rapidly detect, assess, respond and communicate security events. Defined procedures, escalation channels, and post-incident reviews drive efficient handling and continuous improvement. The process ensures prompt communication, minimizes disruption, and incorporates lessons learned to protect customer information and reinforce overall security. Zscaler provides transparency around service availability and changes to our customers. https://trust.zscaler.com/zscalertwo.net

Edit

- **Staff security**

Staff security clearance

Staff screening performed but doesn’t conform with BS7858:2019

Edit

Government security clearance

Up to Developed Vetting (DV)

Edit

- **Secure development**

Approach to secure software development best practice

Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v4.0)

Edit

- **Identity and authentication**

User authentication

User authentication needed

Yes

User authentication

- Multi-Factor Authentication (MFA)
- Username or password
- Other

Other user authentication

Zscaler supports SSO via SAML 2.0 and OIDC with your IdP, including MFA (e.g., TOTP, push, FIDO2). ZIA inline auth supports Kerberos (SPNEGO), NTLM fallback, and Basic/Captive Portal. Zscaler Client Connector authenticates via SSO and can use device certificates; traffic uses mutual TLS (Z-Tunnel 2.0). Network forwarding supports IPsec (IKE PSK); GRE has no encryption/auth. ZPA uses SSO with optional posture checks; App Connectors communicate over mutually authenticated TLS. APIs: ZPA uses OAuth 2.0 (client credentials); ZIA/ZDX use API keys/tokens. SCIM is supported for provisioning (not authentication).

Edit

Access restrictions in management interfaces and support channels

Zscaler’s administrator portal restricts access through role-based access controls allowing organizations to define permissions for each administrator. Only authorized users can log in, and their activities are limited to roles assigned Integration with identity providers enables single sign-on and multi-factor authentication, further securing the portal and ensuring only approved personnel can manage or modify security settings. Zscaler restricts access to who can log support calls by allowing only authorized users listed in the organization’s support profile to submit requests. Access is controlled via user authentication, typically integrated with single sign-on, ensuring only approved personnel can access the support portal/open tickets.

Edit

Access restriction testing frequency

At least every 6 months

Edit

Management access

Management access authentication

- Multi-Factor Authentication (MFA)
- Username or password
- Other

Description of management access authentication

Zscaler supports SSO via SAML 2.0 and OIDC with your IdP, including MFA (e.g., TOTP, push, FIDO2). ZIA inline auth supports Kerberos (SPNEGO), NTLM fallback, and Basic/Captive Portal. Zscaler Client Connector authenticates via SSO and can use device certificates; traffic uses mutual TLS (Z-Tunnel 2.0). Network forwarding supports IPsec (IKE PSK); GRE has no encryption/auth. ZPA uses SSO with optional posture checks; App Connectors communicate over mutually authenticated TLS. APIs: ZPA uses OAuth 2.0 (client credentials); ZIA/ZDX use API keys/tokens. SCIM is supported for provisioning (not authentication).

Edit

- **Audit information for users**

Audit for buyers' users' actions

Access to user activity audit information

Users have access to real-time audit information

How long user audit data is stored for

Between 1 month and 6 months

Edit

Audit for suppliers' users' actions

Access to supplier activity audit information

You control when users can access audit information

How long supplier audit data is stored for

At least 12 months

Edit

How long system logs are stored for

At least 12 months

Edit

- **Pricing**

Discount for educational organisations

No

Edit

Free or trial versions

Free trial available

Yes

Description of free trial

A Zscaler free trial typically last for 30 days and includes access to cloud-based security services, such as secure internet and private app access, centralized policy management, advanced threat protection, reporting tools, and integration options, allowing testing of scalability, performance, and key platform features without hardware installation or long-term commitment.

Edit