LevelBlue Secure Service Edge with Zscaler Service Guide

Table of Contents

LevelBlue Secure Service Edge with Zscaler

Section Effective Date: 27-Apr-2021

The LevelBlue Secure Service Edge with Zscaler Service Guide consists of the following parts:

- Service Description (SD)
- Service Level Agreements (SLAs)
- Pricing (P)
- Country-Specific Provisions (CSP)

In addition, General Provisions are incorporated and apply as specified therein.

Service Description (SD)

SD-1. Overview

Section Effective Date: 27-Mar-2025

LevelBlue Secure Service Edge ("LevelBlue SSE") is a fully managed cloud-delivered security solution providing secure web gateway (SWG), zero trust network access (ZTNA), firewall as a service (FWaaS), and cloud access security broker (CASB).

SD-2. LevelBlue SSE with Zscaler

Actual features and capabilities of LevelBlue SSE with Zscaler depend on the Platform purchased. LevelBlue SSE with Zscaler only applies to traffic that has been forwarded to it. Customer must purchase subscriptions for specific individual Users for use of the Service ("Seats").

The LevelBlue SSE with Zscaler Platforms are:

- Zscaler Essentials Platform
- Zscaler Platform
- Zscaler ELA Platform

SD-2.1. Zscaler Essentials Platform

Zscaler Essentials Platform includes the following capabilities:

- Traffic Forwarding (Client connector, GRE, PAC, Proxy Chaining, IPSEC)
  - LevelBlue will perform no monitoring of the tunnel status or performance
- Multiple IDP, ZIdentity, API access, Authentication and Forwarding
- Internet Access
  - Content filtering, Antivirus, NSS, SSL inspection, SSL Private Certificate, File type control, Bandwidth Control and Internet Access Virtual Service Edge (as many as needed)
- Data Protection
  - Cloud App Control; Shadow-IT discovery; Tenancy Restriction; In-line Web DLP – Monitor mode and 2 custom dictionaries; SaaS API for 1 app
- Cyber Threat Protection
  - Advanced Threat Protection; Correlated Threat insights; Firewall Standard (10 firewall rules, 64 DNS rules); Guest Wifi using DNS Control; Sandbox Standard (.exe and .dll files only); Cyber Isolation Standard for URLs in Miscellaneous Category
- Zero Trust for Workloads
  - Zero Trust for Workloads Standard (Stateful filtering, Access Control Lists, Logging only) includes up to 1 GB of monthly traffic (Internet-bound) for Inline Unauthenticated Traffic, Cloud Workloads and/or on-premise DC servers
- Digital Experience
  - ZDX for Zscaler Platform (predefined probes, no user configuration required, basic endpoint monitoring)

For customers with more than 500 users:

- Internet Access
  - Cloud NSS; Source IP Anchoring for Private Access users

- Private Access
  - Private Access Standard (1 user for every 20 Platform Users; SAML authentication and SCIM provisioning support; Private Application and Server discovery; Standard Device Posture enforcement; up to 10 App Segments; App Connectors; Log Streaming Service and Health Monitoring)

SD-2.2. Zscaler Platform

Zscaler Platform includes the capabilities in Zscaler Essentials Platform and adds the following capabilities:

- Access to all Zscaler public DCs (excludes China Premium and regulated Middle East DC access)
- Data Protection
  - In-line DLP Web for SaaS/Internet, Private and GenAI Apps; 10 TB of one-time retro scan for SaaS API; Data Protection incident management including incident receiver (Virtual appliance)
- Private Access
  - Private Access Advanced for all Users; Segmentation (up to 20 app segments); ZPA Private Service Edge (as many as required up to system max);
- Zero Trust for Workloads
  - Zero Trust for Workloads Standard (Stateful filtering, Access Control Lists, Logging only) includes up to 2 GB of monthly traffic (Internet-bound) for Inline Unauthenticated Traffic, Cloud Workloads and/or on-premise DC servers
- Digital Experience
  - ZDX Standard (6 probes)

For customers with more than 500 users:

- Risk Management
  - Deception Standard
- Zero Trust SD-WAN

- ZT SD-WAN Standard (Virtual appliance) includes visibility, Internet and Private Access connectivity; 1 site per 500 users, max:10 sites, services for up to 10 devices (non-OT) and 20 GB of monthly traffic per site (devices and traffic is aggregated across all sites)

- Privileged Remote Access
  - PRA “Standard” for 10 systems (User Portal, Browser-based access, RDP/SSH/VNC, up to 1 GB per systems – pooled across all systems)

SD-2.3. Optional Add-on Features

The following features can be added to the Platforms outlined above.

SD-2.3.1 Data Protection

- Zscaler Data Protection (Choose up to 4 depending on the package purchased)
  - Email: Annual subscription to inline Email data protection for Exchange and Gmail for outbound Email (does not include inbound email) and Out-of-band Email API for Exchange and Gmail for Email monitoring
  - Endpoint: Annual subscription to Endpoint DLP. Includes: Data discovery on the endpoint; Print, personal cloud, removable storage and local network shares; Monitoring of end-user activity with dashboards and reports
  - SaaS Security: Annual Subscription to Data Protection – SaaS Security Advanced. Includes Out-of-band CASB for all SaaS Apps (excluding Email – Exchange and Gmail); 1 TB per 1000 users (Max: 20 TB) of historical data scanning; and unlimited forward data scanning; SaaS Security Posture Management; SaaS Security for Third party apps
  - Classification and Encryption Advanced: Annual subscription to Classification and Encryption Advanced. Includes: sensitive file encryption, redaction, watermarking and data classification features including EDM, IDM, OCR.

- Data Protection: Inline All Apps
  - Annual subscription to inline Data Loss Prevention Web for SaaS, Private and Gen AI applications and Data Protection incident management including incident receiver (Virtual appliance)
  - Data Protection: Browser Isolation Advanced

- Annual Subscription to Data Protection Browser Isolation for Pvt /SaaS applications. This is applicable to BYOD, B2B, VDI replacement and other managed devices use cases (Cloud App control or user-risk or device-risk based Isolation). Includes User Portal 2.0, Identity proxy, Unmanaged/Managed devices, mobile browser support, prevent upload/download, print restriction, clipboard controls, local browser rendering, persistent and customizable end-user notification, persistent URL, cookie persistence, region selection, watermarking, view-office files, protected storage for file transfer and browser-in-browser mode. Fair Usage: 1.5 GB per user of monthly isolation data (measured across all isolation users)

SD-2.3.2 Cyber Threat Protection

- Zscaler Inline Threat Protection (Choose up to 3 depending on the package purchased)
  - Sandbox Advanced: Annual subscription to inline Sandbox Advanced performing AI Instant Verdict and advanced behavioral analysis, simplified policy management with granular controls, Sandbox API for up to 3,000 files per month per customer and advanced reporting including Zero Day malicious payload analysis.
  - Firewall Advanced: Annual subscription to App Identification, Auto-proxying, Dynamic Risk Based Policy, Dynamic SSL Inspection on any port, DNS Filtering and Security with 1k+ rules, DNS Tunnel Detection, Network and Application Services, Location, User and Application Awareness, detailed logging and IPS Control
  - Cyber Browser Isolation Advanced: Annual subscription to Cyber Browser Isolation Advanced for internet bound traffic. Includes URL, Cloud App control, user-risk, device-risk based and managed devices; Provides mobile browser support, prevent upload/download, clipboard controls, read-only access, local browser rendering, persistent and customizable end-user notification, persistent URL, cookie persistence, region selection, view-office files, protected storage for file transfer, AI-powered Isolation, Downloaded Flattened File (CDR) and Browser in Browser; Includes up to 1.5 GB per user of monthly isolation data (measured across all isolation users)

- Cyber Browser Isolation Unlimited
    - Annual subscription to Annual subscription to Cyber Browser Isolation Unlimited for internet bound traffic. Includes URL, Cloud App control, user-risk, device-risk based and managed devices; Provides mobile browser support, prevent upload/download, clipboard controls, read-only access, local browser rendering, persistent and customizable end-user notification, persistent URL, cookie persistence, region selection, view-office files, protected storage for file transfer, AI-powered Isolation, Downloaded Flattened File (CDR) and Browser in Browser

SD-2.3.3 Private Access

- Zscaler Private Access (Choose up to 2 depending on the package purchased)
    - Private Access Segmentation: Annual Subscription to Segmentation. Including: App segments (as many as required up to system max), Segmentation Insights (90-day Lookback), AI/ML Segmentation Accelerator (recommendations every 2 weeks), App Connectors (as many as required up to system max), App Migration (Call Weighted Load Balancer) and Virtual Private Service Edges (as many as required, software only)
    - Private Access App Protection: Annual subscription to Zscaler App Protection (Private Web Application Protection)
- Zscaler Private Access Platform
    - SAML authentication and SCIM provisioning support, Secure Private application access, Zscaler Client Connector, Application and Server discovery, Standard Device Posture enforcement, up to 20 App Segments included, App Connectors (as many as required up to system max), ZPA Virtual Service Edge (as many as required up to system max, Software only), Multiple IdP, Log Streaming Service, Source IP Anchoring, Health Monitoring, ZDX Standard, Browser-based access.
    - Privileged Remote Access Standard for 10 systems (User Portal, Browser-based access, RDP/SSH/VNC, up to 1 GB per systems – pooled across all systems) enforcement, up to 20 App Segments included, App Connectors (as many as required up to system max), ZPA Virtual Service Edge (as many as required up to system max, Software only), Multiple IdP, Log Streaming Service, Source IP Anchoring, Health Monitoring, ZDX Standard, Browser-based access (For customers with more than 500)

- Zscaler Privileged Remote Access Advanced
    - Annual subscription to Zscaler Privileged Remote Access Advanced for SSH, RDP and VNC system with Privileged Capabilities – Interactive Authentication, Clipboard and File Transfer, Time-bound, Emergency Access (with External IdP), Credential Mapping and Injection, Session Recording (10 hours monthly recording per system pooled across tenant systems) and Session Monitoring; OT System Emergency Access (for up to 100 users) (Fair Use limit: App Connectors used for Clientless Access – 1 pair per systems, includes up to 10 GB per system of monthly PRA data, pooled across all systems)

SD-2.3.4 Zero Trust for Workloads

- Zero Trust for Workloads Standard
    - Annual subscription to 1 GB of monthly traffic for Zero Trust for Workloads Standard; Includes Stateful filtering and Cloud Connector (where available)
    - Monthly traffic measured across all workloads in public cloud, private cloud/ on-premises DC and from inline unauthenticated traffic.
- Zero Trust for Workloads Advanced
    - Annual subscription to 1 GB of monthly traffic for Zero Trust for Workloads Advanced; Includes Cloud Connector (where available)
        - Internet Access for Workloads: SSL/TLS inspection, Advanced Threat Protection, Cloud NSS, Source IP Anchoring
        - Private Access for Workloads: App Segments, Sub-location, LSS Standard Logging and Reporting.
        - Data Protection for Workloads: Inline web (in monitor mode only)
        - Cyber Protection for Workloads: Standard Firewall, DNS control
        - Monthly traffic measured across all workloads in public cloud, private cloud/on-premises DC and from inline unauthenticated traffic

- Zero Trust for Workloads Advanced Plus
  - Annual subscription to 1 GB of monthly traffic for Zero Trust for Workloads Advanced Plus; Zero Trust Workloads Advanced as well as
    - Data Protection for Workloads: Data Protection inline and Advanced classification
    - Cyber Protection for Workloads: Firewall Advanced for Workloads, Sandbox Advanced for Workloads
  - Monthly traffic measured across all workloads in public cloud, private cloud/ on-premises DC and from inline unauthenticated traffic

SD-2.3.5 Digital Experience

- ZDX Advanced
  - Annual subscription to ZDX Advanced. Includes: 30 configurable user probes; hop by hop analysis; UCaaS monitoring; Deep tracing (25 sessions); 5 mins Polling interval; 25 alert rules; 14 days of data retention; 10 webhook integrations.
- ZDX Advanced Plus
  - Annual subscription to ZDX Advanced Plus including ZDX Advanced as well as:
    - Total 100 probes (max probes per user is 30), Software process monitoring and incident reporting, ZDX Co-pilot Essentials,
    - ZDX Hosted Monitoring: (1 Hosted Monitoring Probe Location per 1,000 users)

SD-2.3.6 Other Products

- Source IP Anchoring
  - Annual subscription to Source IP Anchoring to Selectively steer application traffic which needs source IP whitelisting up to 200MB per user per month (measured at a tenant level)
  - Zscaler Test Environment

- Annual subscription to a Zscaler test environment (1 tenant) for up to 50 users that replicates the entitlements of the production environment
- Only available for customers with more than 5000 users

- Zscaler Test Environment Essentials
  - Annual subscription to a Zscaler test environment (1 tenant) for up to 50 users that replicates the entitlements of the production environment
  - Only available for customers with fewer than 5000 users

SD-2.3.7 Customer Managed Features

Customer is fully responsible for implementation and management of the following features

- ZDX for Zscaler Platform
- ZDX Standard
- ZDX Advanced
- ZDX Advanced Plus
- SaaS Security (OOB CASB)
- Identity Proxy
- Deception Standard
- Deception Advanced
- Zscaler Test Environment
- Zscaler Test Environment Essentials
- Risk360 Advanced
- Workflow Automation
- Unified Vulnerability Management Advanced

SD-2.3.8 Service Limitations

- Customer is responsible for hosting, deploying, configuring, and managing all virtual machines. The Service will automatically update the Virtual Service Edge(s) without Customer notification.
- LevelBlue supports the creation of custom DLP engines utilizing predefined dictionaries. Custom DLP dictionaries will be entirely self-managed by the customer.
- LevelBlue will only support the creation of one Source IP Address per one application segment.
- Customer must utilize a SAML 2.0 compliant identity provider (IdP) to authenticate to the mobile application in order for users to access Customer applications via Private Access.

SD-3. Service Activation

Section Effective Date: 27-Apr-2021

LevelBlue provides activation for the Service ("Service Activation"). Service Activation consists of the following elements:

- Customer confirmation on readiness to submit the order by written notice to Service Implementation Manager (SIM)
- LevelBlue procurement of customer components for their Service

The Service Activation will occur when LevelBlue has determined that the above steps are complete. Billing will begin upon Service Activation.

Cross References

SD-5.1.1. Security Implementation Management (SIM)

SD-4. Deployment Services

Section Effective Date: 12-Nov-2022

Deployment Services refers to LevelBlue Cybersecurity's effort to work collaboratively with the customer's IT resources to implement and migrate a customer to the Service.

The customer must purchase a deployment package as set forth in the Service Agreement based on the service level, user count, and complexity of the proposed project.

Customer must purchase a deployment package as set forth in the Service Agreement based on the service level, user count, and complexity of the proposed project. These deployment services packages will ensure that the deployment is sufficient to be judged complete as contracted.

SD-5. LevelBlue SSE Implementation

Section Effective Date: 20-Jan-2023

LevelBlue's structured process for implementation includes developing and gathering documentation and credentials, establishing a baseline of deliverables, timelines, and responsibilities, and verifying performance prior to LevelBlue assuming management of steady-state operations.

SD-5.1. Resources

SD-5.1.1. Security Implementation Management (SIM)

Section Effective Date: 27-Apr-2021

LevelBlue will assign a Cybersecurity Security Implementation Manager (SIM) to facilitate the LevelBlue SSE Deployment. The SIM resource is a service delivery technical implementation manager supporting the ordering, tracking, installation, and testing of the MSS services globally. This resource is designated to the customer order and will set up a kickoff call to discuss the Customer's LevelBlue SSE service. The SIM is responsible to deliver the overall solution to see to it that the Customer is supported end-to-end, from post sales through service operations.

SD-5.2. Technical Implementation

SD-5.2.1. Kickoff Call

Section Effective Date: 27-Apr-2021

As part of the Technical Implementation, the SIM for the Customer order will work with the Customer to establish a kickoff call to:

- Introduce key contacts from LevelBlue
- Set expectations for the implementation process and outline steps for process
- Demonstrate how to complete the OLTPD

- Answer any questions and address any concerns from the customer

SD-6. Support and Management

Section Effective Date: 27-Apr-2021

The following describes the support and management capabilities included in LevelBlue SSE.

SD-6.1. Network Monitoring and Management

Section Effective Date: 27-Apr-2021

LevelBlue's Security Network Operations Center (LevelBlue SNOC) provides 24/7 management of the Service.

SD-6.2. Help Desk Support

Section Effective Date: 27-Apr-2021

All issues, questions or requests for assistance related to LevelBlue SSE are made to the LevelBlue SNOC on a 24/7 basis by Customer-designated points of contact. Where possible, problems and incidents will be mitigated remotely by LevelBlue SNOC technicians.

A Trouble Ticket, defined as the individual incident report LevelBlue opens for each outage or other issue, will be opened for each incident. The Trouble Ticket begins when an LevelBlue SNOC has acknowledged and validated a problem that is a result of the Customer's Service, and when an LevelBlue generated ticket is opened. A Trouble Ticket is deemed "Resolved" when the Incident has been addressed and the Service is restored, at which time the Trouble Ticket is closed. The LevelBlue SNOC provides 24/7 problem assistance excluding the periods for maintenance.

SD-6.3. Policy Administration

Section Effective Date: 12-Nov-2022

The following options are available for Policy Administration for the Service:

- LevelBlue Managed Policy, or
- Customer Managed Policy

Whether LevelBlue Managed Policy or Customer Managed Policy is set forth in Customer's Service Agreement, Customer may manager their own security policy for the Service, as further described below.

SD-6.3.1. LevelBlue Managed Policy

Section Effective Date: 27-Apr-2021

LevelBlue will assume sole policy management for the Service. Customer will use BusinessDirect to request policy changes.

Customer will self-manage whitelist/blacklist policies in LevelBlue SSE with Zscaler.

SD-6.3.1.1. Content Security Policy and Configuration Changes

Section Effective Date: 27-Apr-2021

- Following implementation of the LevelBlue SSE service, Customer will be shown how to use the LevelBlue Change Management Portal to submit security policy changes.
- When using the LevelBlue SSE service, Customer designs and sets all filtering and interception policies (Security Policies). LevelBlue undertakes only to implement the Security Policies as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings.
- All changes to the Security Policies must be provided by a customer identified Security Liaison designated by Customer to be the point of contact to work with LevelBlue to notify and assist with problem resolution regarding the Customer environment.
- Customer will follow the LevelBlue Change management process. This includes the use of the LevelBlue MSS Change Management System to request policy changes.
- If changes to Customer's security policy are necessary, Customer will provide LevelBlue with Minimum Data Set for policy change.

SD-6.3.2. Customer Managed Policy

Section Effective Date: 07-Jun-2024

Customer can manage its security policy from the Service Management Portal in LevelBlue SSE with Zscaler. Customer may designate Customer Users that will be provided Role-Based Access Credentials (RBAC) allowing them access privileges to the LevelBlue SSE Portal (RBAC Users).

RBAC will only be provided to Customer after the LevelBlue Service Implementation Manager (SIM) confirms Service Activation of the LevelBlue SSE Service.

Customer is solely responsible for any resulting incident(s), including but not limited to Service(s) interruptions and any security intrusions, exploitations and/or breach-related incidents due to changes in policies made by Customer or Users through the LevelBlue SSE Portal.

Customer's designated RBAC Users will have the following access privileges in the LevelBlue SSE with Zscaler Portal:

ZIA

- Full Read/Write access to Dashboards
- Full Read/Write access to Reporting
- Read Only access to Insights
- Full Read/Write access to Policy Access
- Read Only access to Administrators Access
- Full Read/Write access to Alerts Access
- Full Read/Write access to Data Loss Prevention module
- Full Read/Write access to Security module
- Full Read/Write access to SSL policy
- Full Read/Write access to Firewall, DNAT, DNS and IPS module
- Full Read/Write access to NSS Configuration
- Full Read/Write access to Access control (Web and Mobile)

- Full Read/Write access Traffic Forwarding
- Full Read/Write access to the following Authentication Configuration settings
  - Authentication Settings
  - User Management
  - Identity Proxy Settings

ZPA

- Full Read/Write access to Authentication excluding:
  - IdP Configuration
  - Remote Assistance
  - Settings
- Full Read/Write access to Certificate Management
- Full Read/Write access to Configuration
- Full Read/Write access to App Connector Management
- Full Read/Write access to Dashboard
- Full Read/Write access to Diagnostics
- Full Read/Write access to Dashboard
- Full Read/Write access to Cloud Connector Management
- Full Read/Write access to Log Streaming
- Full Read/Write access to Machine Management
- Full Read/Write access to Policies excluding:
  - IdP Configuration
- Full Read/Write access to SCIM Management excluding:
  - IdP Configuration
- Full Read/Write access to Service Edge Management

- Full Read/Write access to User Portal
- Full Read/Write access to Client Connector Portal

RBAC Users shall only utilize their RBAC privileges to complete the functions noted above.

For policy changes other than those listed above, Customer will use BusinessDirect to request that LevelBlue make policy changes (a Change Request). LevelBlue retains super administrative rights to the LevelBlue SSE Portal, which means that LevelBlue retains overall control and administration of the Portal.

SD-6.4. Special Projects

Section Effective Date: 27-Apr-2021

Special Projects are requests not specified in this Service Guide or Customer's Service Agreement. Special Projects will require further assessment, and additional charges will be applied to projects and will be negotiated between LevelBlue and Customer.

SD-7. Ordering

Section Effective Date: 27-Apr-2021

The Service Components and quantities purchased by Customer will be reflected on each Order submitted by LevelBlue. Purchase of additional Service Components will be reflected on subsequent Order(s). Unless otherwise specified in the relevant Order, additional Orders will be coterminous with the expiration of the existing Service Agreement.

SD-8. Customer Responsibilities

SD-8.1. Customer Responsibilities for Service Delivery and Use

Section Effective Date: 26-May-2022

Prior to Service Activation, Customer shall:

- Customer must place initial order within 90 days of contract signature. If Customer fails to place initial order within 90 days, the contract is subject to cancellation by LevelBlue in its sole discretion.

- Provide a site contact who will participate in delivery of service, configure on-premises customer-managed or third-party managed systems (e.g. routers, switches, firewalls), perform troubleshooting (as deemed necessary by LevelBlue), and who will conduct pre-installation and post-installation User acceptance testing.
- Participate in pre-delivery configuration and architectural reviews.
- Supply LevelBlue with all technical data and any additional information required for LevelBlue to activate LevelBlue SSE.
- Back-up configuration information prior to Service Activation.
- Manage installation of LevelBlue SSE and related software on all end-user laptops and mobile devices, and configure Customer applications, if needed.
- Provide equipment and application logs and network traces, if required, for troubleshooting and testing of installations.
- Review and provide relevant comments (in the form of additional data requirements, preliminary conclusions, or recommended technical architecture) or subject matter expert resources from applicable information technology departments or business units to assist in completing LevelBlue deliverables in a timely manner.
- Configure traffic forwarding from any Customer-owned/managed tunnel termination devices, if needed. LevelBlue will configure traffic forwarding from LevelBlue-managed tunnel termination devices only.
- Provide the necessary certificates signed by Customer's certificate authority as needed, for use with the SSL inspection and granular inspection capabilities of LevelBlue SSE.

During use of the Service, Customer shall:

- Undertake all necessary steps to keep confidential and not reveal or disclose to any third party, without prior permission from LevelBlue, any username or password information provided to Customer by LevelBlue. Customer is solely responsible for monitoring and controlling access to the Service, maintaining the confidentiality of the passwords and for any use of the Service that occurs during the use of the passwords. If for any reason LevelBlue believes that there has been a security related breach, LevelBlue may take whatever action LevelBlue deems appropriate to remedy the situation.

- Patching or removing security threats on Customer-maintained equipment, including all host and server equipment connected to LevelBlue-managed security devices and services.
- Ensure that all Customer systems and networks (including but not limited to those which are outsourced), that connect with those belonging to LevelBlue, implement appropriate security controls which are designed to prevent loss, disclosure, unauthorized access, or service disruption. Customer must also ensure LevelBlue will have access to LevelBlue's assets, either via remote access or physical access as appropriate, for the proper operation of the Service. The process in which LevelBlue will access these assets will be mutually agreed upon between LevelBlue and Customer. Customer must also restrict access to and use of these systems and assets only by authorized Customer personnel. The use of the LevelBlue network and its facilities is intended for use by the Customer only, and not for those who may be interconnected with Customer's systems and network.
- Notify LevelBlue if a customer suspects a security breach within Customer's network.
- Define and maintain Customer's own security policy and internal security response procedures. In the event there is an incident generated either from the Internet or within Customer's enterprise, it is Customer's responsibility to have appropriate mitigation contacts, processes, and procedures in place. LevelBlue will work with the Customer's designated security contacts according to LevelBlue procedures and notify the Customer of incidents identified by its Service management team.
- Design all filtering and interception polices (Security Polices). LevelBlue undertakes only to implement Security Policy as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings.
- Maintain and manage all credentials of authorized Users as well as restrict access to and use of LevelBlue SSE only by authorized Users. Customer must immediately notify LevelBlue if there is a change in authorized Users.
- Notify LevelBlue at least five (5) working days in advance of any scheduled maintenance, planned outages, or LevelBlue SSE configuration changes that may interfere with monitoring of LevelBlue SSE. Customer must notify LevelBlue immediately of any unscheduled activities that may interfere with the LevelBlue SSE service.
- Direct end-user support remains the responsibility of the Customer, this includes but is not limited to:
  - Issues on machines of end users

- End-to-end network connectivity (e.g., Customer's network, Internet Service Provider)
- Identity source management

SD-8.2. Customer Compliance Responsibilities

SD-8.2.1. Monitoring of Communication

Section Effective Date: 27-Apr-2021

LevelBlue is providing this Service for a cybersecurity purpose as defined in and consistent with the Cybersecurity Information Sharing Act of 2015 ("CISA"). In the United States, Customer agrees to undertake any monitoring of its network, undertake defensive measures, and share cyber threat indicators or defensive measures consistent with CISA. In the U.S and globally, Customer agrees that it is responsible for setting all security policies, including monitoring policies, and will implement any and all security policies pursuant to CISA or other applicable law. LevelBlue retains the right to reject any security policies Customer asks it to implement that in LevelBlue's sole judgment are not for a cybersecurity purpose or as defined in or are inconsistent with CISA or other applicable law. Customer consents to the monitoring of the communications, and agrees that during the Service contemplated here, its Users will be provided notice through bannering or otherwise and will consent that they have no right of privacy in the communications or information transmitted over Customer's network and that Customer or its contractors may monitor those communications for any lawful purpose.

SD-8.2.2. Cooperation with Requests

Section Effective Date: 27-Apr-2021

Customer agrees to, and will secure User agreement to, cooperate with, and assist LevelBlue in connection with responses to requests or requirements of a regulator, authority or governmental body concerning the Service.

SD-8.2.3. Importation of Technology

Section Effective Date: 27-Apr-2021

When using the Service, Customer is responsible for compliance with all applicable laws in the jurisdictions in which the Service is used. In certain countries, Customer may be deemed to be the importer of technology. This technology includes encryption

software that may be subject to restrictions with respect to its importation and/or use in certain countries. Customer agrees that it and/or its Users will not attempt to import such technology into any countries where LevelBlue does not offer the Service. Any violations of this provision shall entitle LevelBlue to immediately terminate Customer's Service Agreement.

SD-9. Use of Service

SD-9.1. Audits

Section Effective Date: 27-Apr-2021

Consistent with the terms and conditions herein, LevelBlue may conduct audits of Customer's use of the Service, including total number of Seats accessing the Service and/or Customer's bandwidth consumption to determine if the Customer's use of the Service has expanded beyond what has been ordered. In the event an audit reveals a Service use increase, the parties will work in good faith to immediately resolve these issues. (See Section on "Restrictions of Use of the Service").

SD-9.2. Excessive Bandwidth Consumption

Section Effective Date: 12-Nov-2022

If Customer's bandwidth consumption materially increases (an increase greater than 50% shall be deemed a material increase) from the average bandwidth level over the ninety-day period following Service Activation without an increased amount of Customer Seats, LevelBlue will notify Customer in order to agree on a bandwidth reduction plan, or to work in good faith to renegotiate pricing for remaining balance of the Service term. If the Parties are unable to reach a mutually agreeable solution, LevelBlue may terminate the remaining Service term of the Customer and early termination fees may apply.

SD-9.3. Excessive Seats

Section Effective Date: 12-Nov-2022

During the Service Term, if the number of Customer's Seats increases by more than five percent (5%) of the then purchased number of Seats, LevelBlue will notify Customer in order to agree on a reduction plan, or to work in good faith to renegotiate pricing for remaining balance of the Service Term. If the Parties are unable to reach a mutually agreeable solution, then LevelBlue may terminate the remaining Service Term of the Customer and early termination fees may apply.

SD-9.4. Acceptable Use

Section Effective Date: 27-Apr-2021

Users shall not use the Service for any purpose other than as expressly authorized.

SD-9.5. Reservations of Rights; Ownership, Terms of Service

SD-9.5.1. Reservations of Rights; Ownership

Section Effective Date: 27-Apr-2021

All right, title, and interest in and to the Service, any applicable Software and related Documentation are and shall remain the exclusive property of LevelBlue and/or its suppliers. Customer acknowledges and agrees that: (i) the Service is protected under U.S. and foreign copyright and other intellectual property laws; (ii) LevelBlue and its suppliers retain all copyrights and other intellectual property rights in the Service; (iii) there are no implied licenses and any rights not expressly granted to Customer hereunder are reserved by LevelBlue or its suppliers; and (iv) Customer acquires no ownership or other interest in the Service (other than right to access and use the Service as stated herein).

SD-9.5.2. Terms of Service

Section Effective Date: 27-Apr-2021

Use of the Service may require download of application software to User devices from an app store or from a third-party site. LevelBlue is not licensing or furnishing such software.

SD-9.6. Restrictions on Use of the Service

Section Effective Date: 20-Jan-2023

Customer shall use the Service solely for internal business purposes and Customer shall only permit access to the Service by its Users as stated herein. Customer is prohibited from: (i) modifying, copying, or making derivative works based on the technology of the Service; (ii) disassembling, reverse engineering, or decompiling any of the technology of the Service; or (iii) creating Internet “links” to or from the Service, or “frame” or “mirror” any of the Service s content which forms part of the Service (other than on Customers’ own internal intranets).

- Customer shall not (and will not allow any third party to): (i) access the Service in order to build a competitive product or service, or copy any ideas, features, functions or graphics of the Service; (ii) use the Service to send spam or otherwise duplicative or unsolicited messages in violation of any applicable laws and/or regulations; (iii) use the Service to send infringing, obscene, threatening, libelous, or otherwise unlawful material; (iv) use the Service to access blocked services in violation of any applicable laws and/or regulations; (v) upload to the Service or use the Service to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (vi) interfere with or disrupt the integrity or performance of the Service or the data contained therein; (vii) attempt to gain unauthorized access to the Service or its related systems or networks; (viii) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Service; (ix) perform penetration or load testing on the Service without the prior written consent of LevelBlue and agreeing to certain conditions and requirements for such penetration or load testing; or (x) without the express prior written consent of LevelBlue, conduct any benchmarking or comparative study or analysis involving the Service for any reason or purpose except, to the limited extent absolutely necessary, to determine the suitability of Service to interoperate with Customer's internal systems.
- Customer shall: (i) comply with any User instructions, and training materials for the Service ("Documentation") provided to it by LevelBlue; (ii) be solely responsible for its activities in using the Service, including without limitation the activities of its Users, or any third parties that Customer allows to utilize the Service; and (iii) supply all technical data reasonably requested from time to time in order for the Services to be provided to Customer.
- The Service must not be used for running automated queries to web services (e.g. a Customer running a script for searching on an internet search engine that would flag the internet search engine to blacklist LevelBlue's internet protocol) and in case of misuse offending source IP addresses may be blocked.

SD-9.7. Customer Data

SD-9.7.1. Definition of Customer Data

Section Effective Date: 27-Apr-2021

In its provision of the Service, the Service may receive, store and/or process network traffic data ("Traffic Data"), such as time of transaction, User IP address, username, URL, URL category, status (success or error), file type, filter result (allowed or denied), virus id, and other metadata (e.g. browser software used), and any other network traffic

(and data related thereto) sent to or received from Customer through use of the Service, in detail and/or in an aggregate form. In such cases, LevelBlue is acting in its capacity as a data processor and will process the Traffic Data of Customer only on behalf of and under the direction of Customer (and its designees). In addition, LevelBlue may receive, store, process and retrieve other personally identifiable information uploaded through the LevelBlue SSE Portal or other means ("Administrative Data"). Administrative Data includes, for example, administrator identifying information, User and group names, and other personally identifiable information. "Customer Data" means Traffic Data and Administrative Data.

SD-9.7.2. Limited Use

Section Effective Date: 27-Apr-2021

LevelBlue may store, process, retrieve, and disclose Customer Data for the following purposes: (i) providing the Service to Customer; (ii) analyzing, maintaining and improving the Service; (iii) complying with legal, or governmental requirements if LevelBlue is required to do so; (iv) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service; and (v) anonymously aggregating and statistically analyzing malicious or unwanted content.

SD-9.7.3. Customer Transaction Logs

Section Effective Date: 12-Nov-2022

In order to perform the Services, LevelBlue and its supplier shall have the right to use, reproduce, store, modify, distribute, and display the content of all network traffic sent to or received from customers through use of the Services (the "Customer Transaction Logs"). Customer Transaction Logs will not be accessed, read, or copied other than by electronic methods and for the purposes of providing the Services. The malware, spam, botnets, or other information related to the Services may be utilized for the purpose of: (i) maintaining and improving the Services, (ii) complying with all legal or contractual requirements, (iii) making malicious or unwanted content anonymously available to its licensors; and (iv) anonymously aggregating and statistically analyzing the content.

Service Level Agreement (SLA)

SLA-1. Service Level Agreement Terms – LevelBlue SSE with Zscaler

Section Effective Date: 27-Apr-2021

LevelBlue has established performance objectives for the Service. While LevelBlue does not guarantee performance objectives, LevelBlue will provide credits to an eligible Customer when a performance objective is not met. If an SLA states that a Customer is eligible for an SLA credit, this means that the Customer is eligible subject to the terms, definitions and any exclusions or limitations stated herein.

SLA-1.1. Definitions

Section Effective Date: 24-Jun-2021

The definitions below apply to the Service Level Agreements described in this Service Guide.

- "Data Packet" means a unit of data made into a single Internet Protocol (IP) packet that travels along a given network path.
- "Excluded Transactions and Sessions" means Transactions and Sessions that are not processed due to (a) failure by Customer's network to forward traffic to the Service; (b) failure by an intermediate ISP to deliver traffic to the Service; (c) a Customer-implemented policy change that causes Transactions and Sessions to drop; (d) scheduled maintenance as notified to Customer.
- "Known Virus" means a virus for which, at the time of receipt of content by the Service: (i) a signature has already been made publicly available for a minimum of one (1) hour for configuration by the Service; and (ii) is included in the Wild List located at http://www.wildlist.org and identified as being "In the Wild" by a minimum of three (3) Wild List participants.
- "Qualified Transactions and Data Packets" means the following: (i) less than 1MB HTTP GET request and response; (ii) not SSL-intercepted; (iii) not related to streaming applications; (iv) not subject to bandwidth management rules; and (v) a reasonable number of Transactions and Data Packets per User (based on the Service's cloud-wide average).
- "Session" means any non-HTTP or non-HTTPS request sent to or from Customer through its use of the Service.

- "Outage" is (unless stated otherwise) measured in minutes and is the time Service is unavailable on an unscheduled basis. An Outage does not include time when Service is unavailable during a scheduled period for maintenance, repair or upgrade.
- "Maintenance" time or "Planned Down Time" can be either for "Scheduled Maintenance" or "Emergency Maintenance". "Scheduled Maintenance" is maintenance, repair or updating activities that are performed during a maintenance window established by LevelBlue or a maintenance window agreed to by LevelBlue and Customer. LevelBlue may also perform Scheduled Maintenance by providing Customer a minimum of five (5) business days' notice prior to the day the Scheduled Maintenance will occur. "Emergency Maintenance" is unscheduled maintenance, repair or updating activities that are necessary in order to protect LevelBlue facilities, network services or the security of Customer equipment or property. LevelBlue will attempt to provide reasonable notice to the Customer when LevelBlue determines that it is required to perform Emergency Maintenance prior to the maintenance activity being performed.

SLA-1.2. SLA Exclusions

Section Effective Date: 27-Apr-2021

Notwithstanding any other clause herein, no commitment is made hereunder with respect to: (i) the Service being used in conjunction with hardware or software other than as specified by LevelBlue in the Initial Order (ii) alterations or modifications to the Service, unless altered or modified by LevelBlue (or at the direction of or as approved by LevelBlue); (iii) defects in the Service due to accident, hardware malfunction, abuse or use other than in accordance with LevelBlue's published documentation (unless caused by LevelBlue or its agents); (iv) an evaluation of the Service or other trial provided to Customer at no charge and (v) any problems or issues of connectivity due to the network or internet connection of Customer.

The SLA becomes active after a 3-month service baseline period following the Service Activation date. After the baseline period LevelBlue and customer will review the SLAs in good faith.

SLA-1.3. SLA Reporting and Claims

Section Effective Date: 27-Apr-2021

To file a claim or termination notice with refund claim, as applicable, Customer must include in a written notice the following details:

- Downtime information detailing the dates and time periods for each instance of claimed downtime or Average Latency failure, as applicable, during the relevant month (or calendar quarter for termination with a refund claim).
- An explanation of the claim made under this Service Level Agreement, including any relevant calculations.

Claims may only be made on a calendar month basis and only for the previous calendar month or part thereof. All claims must be made within 10 days of the end of each calendar month. A termination notice with a refund claim must be made within ten (10) days of the end of a calendar quarter.

All claims will be verified against LevelBlue's system records. Should any claim submitted by Customer be disputed, LevelBlue will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide to Customer a record of Service availability for the period in question. The record provided by LevelBlue shall be definitive. LevelBlue will provide records of Service availability in response to valid Customer claims upon Customer's request. LevelBlue shall respond to a Customer claim within ten (10) business days of claim submission.

All remedies referred to herein are subject to Customer having paid all applicable fees and fulfilled all its obligations hereunder.

Notwithstanding any other clause herein, the remedies herein do not apply to any matters arising due to any of the following:

- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
- Excused Outages.
- Hardware, software or other data center equipment or services not in the control of LevelBlue or outside the scope of the Service.
- Hardware or software configuration changes made by the Customer without the prior written consent of LevelBlue.

SLA-1.4. SLA Claims Limitations

Section Effective Date: 27-Apr-2021

Customer may receive only a maximum total combined Service Credits equivalent to 7 days of one (1) month's service. Service Credits do not include installation charges, monthly recurring charges for services not included in the Service Level Agreement for which a Service Credit is paid, or charges related to additional services. Any SLA credit paid to Customer shall constitute the sole and exclusive remedy available to Customer for a failure by LevelBlue to meet a performance objective.

SLA-1.5. Service Availability

Section Effective Date: 8-Aug-2025

Service levels for Service Availability, Latency, and Virus Capture Rate are provided directly by Zscaler and as such, Zscaler's commitments regarding those metrics are passed through LevelBlue to the customer. Those details can be found at: Zscaler SLA Support | Service Level Agreement Documentation.

SLA-1.6. General Provisions for Service Level Agreements

Section Effective Date: 27-Apr-2021

LevelBlue will provide access to the Zscaler Portal where Customer can view service reports. LevelBlue SSE with Zscaler service status, real time service status/health will be directly accessible to the Customer from the Zscaler portal. The Service will scan as much of the traffic as technically possible; however, it may not be possible to scan items that (i) are encrypted, encapsulated, tunneled, compressed, modified from their original form for distribution, (ii) have product license protection, or (iii) are protected by the sender in ways that the Service cannot inspect (e.g., password protected). Items (i) through (iii) are excluded from the Service Level Agreements.

In order for any of the Service Level Agreements to apply Customer's network must be properly configured and Service activated.

- The Service Credits set forth in the Service Level Agreements shall be Customer's sole and exclusive remedy for failing to meet the applicable Service Level Agreement. In order to be eligible for a Service Credit, Customer cannot be past due on any payments owed.

- The aggregate maximum Service Credit that LevelBlue will issue for failing to meet any Service Level Agreements in a single calendar month will not exceed seven (7) calendar days' worth of Service.

SLA-1.7. Chronic Failure

Section Effective Date: 27-Apr-2021

Subject to the exclusions and limitations stated in this Service Level Agreement section, if the Service is not available, for reasons other than an Excused Outage, and such non-availability is attributable solely to LevelBlue and not to Customer, in whole or in part, for more than thirty-six (36) hours in any calendar quarter, Customer may terminate the Service upon thirty (30) days' written notice to LevelBlue. In the event that LevelBlue validates the conditions of the termination under this Section, LevelBlue shall refund to Customer a pro-rata portion of the Service fees paid in advance and not yet used within forty-five (45) days from termination.

Service Level Objective (SLO)

SLO-1. Incident Response Objectives

Section Effective Date: 21-Jan-2023

Incident Response is defined as the duration, in minutes, between the time an incident is created in the incident management tool and a first response is communicated by LevelBlue to the Customer. The response time listed will be on hold until the fault resolution is completed.

Incident Response Objectives			
Ticket Classification	Definition	Target Response Time	Target Resolution Time
1	Service is not available	Within 15 minutes	Within 4 hours
2	Service is available, but performance or some features are severely degraded, materially affecting normal use if the service.	Within 2 hours	Within 48 hours
3	Service is available and critical functions are usable, but there is a non-critical malfunction.	Within 24 hours	Within 10 business days
4	Cosmetic or feature requests (Service is functioning as expected).	N/A	Next release, subject to acceptance

Bill credits are not available if a SLO is not satisfied.

Pricing (P)

P-1. LevelBlue Secure Service Edge Pricing

Section Effective Date: 27-Apr-2021

Applicable rates, prices, discounts, and other terms for LevelBlue SSE are set forth in a customer's Service Agreement.

P-1.1. General Charges and Fees

Section Effective Date: 27-Apr-2021

There is a Monthly Recurring Charge (MRC) associated with each Service Components as applicable per the Service Agreement. The quantity purchased by Customer from LevelBlue will be reflected on each Order submitted by LevelBlue. If Customer wishes to add additional Seats, Users, or additional optional features as applicable, LevelBlue will submit an additional Order.

P-1.2. Discounts

Section Effective Date: 27-Apr-2021

Discounts for each of the Service Components are specified in the Service Agreement. The discount will be applied against the charges contained in the Service Agreement.

Where a Service Agreement does not list a discount for a Service Component (including optional features), or if Customer adds additional or new Service Components to Customer's account after execution of a Service Agreement and no discount is listed for the new Service Component or feature on the Pricing Schedule, no discount applies.

P-2. Billing

Section Effective Date: 27-Apr-2021

Billing commences upon Service Activation. LevelBlue invoices will be presented on a monthly basis and will cover charges for Services performed during the previous calendar month. Invoices will be offered in electronic format only unless a paper invoice is explicitly requested by the customer.

Cross References

SD-3. Service Activation

P-3. Bandwidth Surcharge – Middle East and Rest of World for LevelBlue SSE with Zscaler

Section Effective Date: 27-Apr-2021

This surcharge is applied if Customer needs to forward traffic to the Service from certain countries or regions. Bandwidth Surcharge – Middle East applies if Customer is forwarding traffic to enforcement nodes in the Middle East. Bandwidth Surcharge –

Rest of World (ROW) applies if Customer is forwarding traffic to enforcement nodes in Australia, Central and Latin America, Africa, mainland China, New Zealand, and Korea.

Forwarding traffic to enforcement nodes in the regions above requires approval from LevelBlue before ordering. Upon approval, the Bandwidth Surcharges will apply.

Country Specific Provisions (CSP)

CSP-1. Country Availability

Section Effective Date: 27-Apr-2021

LevelBlue Secure Service Edge is available inside and outside the United States.