CloudSOC (Audit, CASB for SaaS, CASB for IaaS, CASB Gateway)

Service Description

August 25, 2017

This Service Description describes Symantec's CloudSOC Audit, CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS), CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS), and CloudSOC CASB Gateway services (each, a "Service"). All capitalized terms in this description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Conditions (hereinafter refered to as the "Agreement").

Table of Contents

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

Symantec CloudSOC is a Cloud Access Security Broker (CASB) platform that provides multiple services, including CloudSOC Audit, CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS), CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS), and CloudSOC CASB Gateway services (each, a "Service"). The Service will be provided in accordance with the terms of the Agreement and the documentation available at the Portal.

Service Features

- Customer can access the Service through a self-service online portal ("Portal"). Customer may configure and manage the Service, access reports, and view data and statistics, through the Portal, when available as part of the Service.

Service Level Agreement

- Symantec provides the availability service level agreement ("SLA") for the Service as specified in Exhibit A.

Service Enabling Software

- This Service may include enabling software, which should be used only in connection with Customer's use of the Service during the Subscription Term. Use of the enabling software is subject to the license agreement accompanying such software ("Software License Agreement"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove enabling software upon expiration or termination of the Service.

2. CUSTOMER RESPONSIBILITIES

Symantec can only perform the Service if Customer provides required information or performs required actions, otherwise Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Order Confirmation within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Subscription Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Symantec is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- Customer must comply with all applicable laws with respect to use of the Service.
- Customer must use the Service in accordance with the documentation available at the Portal.

- Customer is responsible for obtaining all approvals and consents required by any third parties in order for Symantec to provide the Service. Symantec is not in default of its obligations to the extent it cannot provide the Service either because such approvals or consents have not been obtained or any third party otherwise prevents Symantec from providing the Service.
- Customer is responsible for maintaining current, valid agreements with its cloud application providers and complying with all terms and conditions of such agreements (including, but not limited to, acceptable use policies and usage restrictions), which Customer understands may be more restrictive than the terms and conditions of this Agreement.
- Customer is responsible for its data, and Symantec does not endorse and has no control over what users submit through the Service. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.
- Customer is responsible for its account information, password, or other login credentials. Customer agrees to use reasonable means to protect the credentials, and will notify Symantec immediately of any known unauthorized use of Customer's account.

Acceptable Use Policy

- Customer is responsible for complying with the Symantec Online Services Acceptable Use Policy.

Customer Service-Specific Warranties

- Customer warrants that all information it provides related to usage for calculating the applicable Meter and/or applicable Fees is accurate and complete.

3. SUBSCRIPTION INFORMATION

Customer may use the Service only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the applicable Order Confirmation; and (ii) as defined in this Service Description or the Agreement. Service-related documentation is available in the Portal and at: https://elastica.zendesk.com/hc/en-us.

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

- "**User**" has the meanings set forth in the descriptions for CloudSOC Audit, CloudSOC CASB for SaaS, CloudSOC CASB for IaaS, and CloudSOC CASB Gateway in the "Subscription Information" section of the Service Description.
- **"Usage"** means GB/day usage for processed data for IaaS applications as set forth in the description for CloudSOC CASB for IaaS in the Service Description.

CloudSOC Audit

CloudSOC Audit is a cloud-based service that provides visibility into usage of cloud applications, and the security risk of the applications based on a business reading rating (BRR) model.

CloudSOC Audit may be used for no more than the number of licensed Users. A "User" is defined as a uniquely identifiable user in the proxy or firewall logs as identified by username or user ID. In the absence of either, client IP addresses are used for user identification.

• Subscription to CloudSOC Audit includes access to functionality within the SpanVA virtual appliance to collect, compress and/or tokenize proxy or firewall logs before transferring to CloudSOC Audit for processing.

• Customers can create up to twenty (20) unique log data sources from CloudSOC Audit app.

• Customers can define data retention for CloudSOC Audit results from a minimum of two (2) and up to twelve (12) months.

- A CloudSOC Audit subscription provides access to CloudSOC CASB Audit AppFeed that allows cloud application discovery and controls from the ProxySG, Secure Web Gateway VA, Advanced Secure Gateway, or Web Security Service.

CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS) and CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS)

CloudSOC CASB for SaaS and CloudSOC CASB for IaaS are cloud-based services that provide visibility and control over activities of Users in cloud applications, as well as monitoring and protection of data that is transferred, stored, and/or shared.

Available for SaaS or IaaS applications, a complete list of cloud applications supported by the CloudSOC CASB offerings can be found in the CloudSOC online store, and includes, but is not limited to:

- Microsoft Office365
- Google Suite
- Box
- Dropbox
- Salesforce.com
- DocuSign
- Jive
- ServiceNow
- GitHub
- Amazon Web Services (AWS)
- Yammer
- Microsoft Azure

The licenses are available on a per User basis in multiple user bands for SaaS applications, and on a GB/day total aggregate usage basis in multiple processed-data-volume tiers for IaaS applications. A "User" is defined as a uniquely identifiable user in each cloud application that has a name and email address. Unless noted below, CloudSOC CASB may be used for no more than the number of licensed users for that cloud application or total across all cloud applications, as applicable. If supported, API connectivity and scanning content within cloud applications is limited to all documents and last thirty (30) days of messages, posts, emails and attachments. Retention of data for CloudSOC CASB offerings is limited to a maximum of three (3) full calendar months for use with the Service. During the first week of each calendar month, one (1) calendar month of older data will be archived and made available for download for one (1) calendar year after the date that the data was archived. For example, for a subscription term that begins on January 15, the data from January 15 through April 30 will be available for active use until the first week of May. During the first week of May, the data from January 15-31 will be archived for one (1) calendar year, and data from February, March and April will continue to be available for active use during the month of May. During the first week of June, data for the calendar month of February will be archived for one (1) calendar year, and data from March, April and May will continue to be available for use during the month of June.

In the event that Symantec discontinues the Service for a cloud application before the end of the applicable Subscription Term, Symantec shall provide to Customer directly or through the reseller, where applicable, a refund for the pro-rata portion of the service fees paid in advance and not yet used in the form of a credit toward a new Symantec product purchase to be used within a set period of time.

CloudSOC CASB for SaaS and CloudSOC CASB for IaaS is offered in two editions:

- Advanced/E10: includes the Securlet module for API based monitoring and protection for one (1) or more specific cloud applications; Protect feature for policies and content inspection; Detect feature for User behavior analytics; and Investigate feature for forensic analysis of User activities.

- Premium/E20: includes all elements of the Advanced edition and the Gatelet module for one (1) or more specific cloud applications on the CloudSOC CASB Gateway. A "User" for the Gatelet module is defined in the CloudSOC CASB Gateway section below.

CloudSOC CASB Gateway

CloudSOC CASB Gateway is a cloud-based transparent gateway service that provides visibility and control of user activities through inline inspection of traffic.

CloudSOC CASB Gateway is offered as a subscription license on a per User basis in multiple user bands. A "User" is defined as a uniquely identifiable user who has authenticated with the CloudSOC environment (either directly, via Single Sign On, or by other means) in order to access supported cloud applications. Retention of data for the CloudSOC CASB Gateway service is limited to a maximum of three (3) full calendar months for use with the Service. During the first week of each calendar month, one (1) calendar month of older data will be archived and made available for download for one (1) calendar year after the date that the data was archived. For example, for a subscription term that begins on January 15, the data from January 15 through April 30 will be available for active use until the first week of May. During the first week of May, the data from January 15-31 will be archived for one (1) calendar year, and data from February, March and April will continue to be available for active use during the month of May. During the first week of June, data for the calendar month of February will be archived for one (1) calendar year, and data from March, April and May will continue to be available for use during the month of June.

• CloudSOC CASB Gateway (E30) subscription includes access to all Gatelets (supported cloud applications are listed in the 'Cloud applications supported on Gateway' technical note located at: https://elastica.zendesk.com/hc/en-us).

• CloudSOC CASB Gateway (E30) subscription includes access to CloudSOC Reach Agent.

• Customers can deploy any number of CloudSOC Reach Agents for the express purpose of device management and traffic steering to CloudSOC CASB Gateways on Windows, Mac OS X, and Android endpoints and VPN profiles on iOS devices.

• Customers can forward traffic for supported cloud applications from other web gateways that support proxy chaining rules to the CloudSOC CASB Gateway.

• Access to Detect feature for User behavior analytics, Investigate feature for forensics, Protect feature for policies and content inspection.

<u>CloudSOC SpanVA</u>

Subscription to any CloudSOC product includes access to up to ten SpanVAs - a virtual appliance that can be installed and run by Customers inside their network for log collection, tokenization, and directory integration. SpanVA can be hosted on supported platforms including but not limited to VirtualBox, VMWare Fusion, VMware ESX/ESXi, VMWare Workstation, or VMPlayer.

<u>CloudSOC Reach Agent</u>

Subscription to any CloudSOC product includes access to CloudSOC Reach Agents for Windows, Mac OS X, and Android endpoints and VPN profiles on iOS devices.

Changes to Subscription

If Customer has received Customer's Subscription directly from Symantec, communication regarding permitted changes of Customer's Subscription must be sent to the following address (or replacement address as published by Symantec): support@elastica.co, unless otherwise noted in Customer's agreement with Symantec. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's Subscription through a Symantec reseller, please contact the reseller.

4. ASSISTANCE AND TECHNICAL SUPPORT

Technical Support

If Customer is entitled to receive technical support ("Support") from Symantec, the Support as specified in Exhibit B is included with the Service. If Customer is entitled to receive Support from a Symantec reseller, please refer to Customer's agreement with that reseller for details regarding such Support, and the Support described in Exhibit B will not apply to Customer.

5. ADDITIONAL TERMS

- Customer may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.

- The Service may be accessed and used globally unless otherwise set forth in Customer's signed agreement with Symantec, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- Customer acknowledges and agrees that Symantec reserves the right to update this Service Description at any time during the Subscription Term to accurately reflect the Service being provided, and the updated Service Description will become effective upon posting.
- Additional terms and conditions that may apply to the Service are available at: https://www.symantec.com/content/dam/symantec/docs/eulas/third-party-notice/blue-coat-products-third-party-en.pdf.
- Excessive Consumption. If Symantec determines that Customer's aggregate activity on the Service imposes an unreasonable load on bandwidth, infrastructure, or otherwise, Symantec may impose controls to keep the usage below excessive levels. For Inline Service, defined as the processing or effecting data in transit to and from the end-user to the internet, the expected average weekly usage is 6 kilobits per second per user (approximately 2GB per month per user). Upon receiving notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. If the parties are not able to establish a resolution within ten (10) days after the initial notification, then Symantec may institute controls on the Service or terminate the Service and this Agreement, without liability. In addition, if Symantec determines that the excessive usage may present a risk to the Service, Symantec may implement technical and business measures to bring usage into compliance.
- User/Usage Count. In the event that Customer exceeds its licensed Users or Usage amount (as measured in Symantec's reporting system or as otherwise calculated by Symantec), Customer agrees to promptly pay the amounts invoiced for the excess usage and/or submit a new order for the excess use. In addition, the parties agree to meet in good faith to determine the number of new User/Usage amount subscriptions required by Customer for the remainder of the Subscription Term.
- Optional add-on services may be available with the Service and will be provided in accordance with their documentation.

6. DEFINITIONS

For the purposes of this Service, the definition of **"Network Data"** includes Cloud Application Data.

"Cloud Application Data" means cloud application data that Symantec may receive, store, and/or process to configure and provide the Online Service, and/or to provide any included support for the Online Service, including but not limited to time of transaction, User IP address, username, URL, URL category, status (success or error), file type, filter result (allowed or denied), virus ID, files, records, Customer selected account names and activity types, and other metadata (e.g. browser software used), and any other network traffic (and data related thereto) sent to or received from You through use of the Online Service, in detail and/or in an aggregated form.

"Symantec Online Services Terms and Conditions" means the terms and conditions located at or accessed through https://www.symantec.com/content/dam/symantec/docs/eulas/service-agreement/symantec-online-services-agreement-2016-12-en.pdf or https://www.symantec.com/about/legal/service-agreements.jsp.

EXHIBIT A

SERVICE LEVEL AGREEMENT

The following service levels are applicable to the Service during the Subscription Term.

1. Availability of the Service.

a. Availability. Availability of the Service is distinguished between Inline Service and Non-Inline Service. Inline Service is defined as the processing or effecting data in transit to and from the end-user to the internet. CloudSOC CASB Gateway is an Inline Service. Non-inline Service is any service that does not process or effect data in transit to and from the end-user to the internet (e.g., reporting tools used by the administrator). CloudSOC CASB for SaaS and IaaS (Securlets), CloudSOC Audit, and the CloudSOC portal with multi-page UI are Non-inline Services. Inline Service will be generally available 99.999% of the time. Non-inline Service will be available 99.5% of the time. Availability is calculated per calendar month as follows:

$$\frac{\text{Total} - \text{Non-excluded}}{\text{Total} - \text{Excused Outages}} \text{ X } 100 > \text{availability target}$$

• Service unavailability for Non-inline services is assessed if the CloudSOC portal or UI pages are unavailable.
• Service unavailability for Inline services is assessed when End Users are unable to access a supported cloud application via any of the CloudSOC CASB global gateway locations.
• Service unavailability will not be assessed due to: (i) a failure of Customer to correctly configure the service in accordance with applicable service documentation or adherence to the Agreement; (ii) the unavailability of a specific web page or a third party's cloud application(s); (iii) individual data center outage; or (iv) unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
• "Total" means the number of minutes for the calendar month.
• "Non-excluded" means unplanned downtime.
• "Excused Outages" include:

o Planned downtime. With respect to planned downtime, Symantec shall provide Customer with as much notice as practical under the circumstances and strives for a minimum of 72 hours or more of advance notice. Symantec shall make commercially reasonable efforts to schedule planned downtime in off peak hours (local datacenter time).

o Emergency maintenance. Customer acknowledges that Symantec may, in certain situations, need to perform emergency maintenance (unplanned downtime) on less than 24 hours advance notice.

o Any unavailability caused by circumstances beyond Symantec's reasonable control, including, without limitation, acts of God, acts of government, flood, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (excluding those involving Symantec employees), failures or delays involving hardware, software, network intrusions or denial of service attacks not within Symantec's possession or reasonable control.

For any partial calendar month during which Customer subscribes to the Service, general availability will be calculated based on the entire calendar month, not just the portion for which Customer subscribed.

b. Remedies. In the event that any particular feature within the Service is not Available for reasons other than an Excused Outage and subject to the requirements of Section 4 below, Symantec will provide an extension of the current term of the subscribed service at no charge to Customer in an amount equal to two (2) days of additional service for each 1 hour or part thereof that the service is not available, subject to a maximum of a one (1) additional week of service per incident of un-availability and subject to the maximum of four (4) service extensions for any one year of subscribed service.

In the event that the Service is licensed as a bundled offering with the Symantec DLP Cloud Detection Service (the "DLP Detection"):

- any extension of the current term pursuant to this Section 1(b) will also include extended access to the DLP Detection for the same period; and
- any failure to meet the Service Availability as described in the DLP Detection service description will extend the current term pursuant to this Section 1(b) as if the failure were for the Service, as well as the DLP Detection for the same period.

c. Chronic Failure. Subject to the requirements of Section 4 below, if the subscribed service is not Available, for reasons other than an Excused Outage, and such non-availability is attributable solely to Symantec and not to Customer, in whole or in part, for more than thirty-six (36) non-consecutive hours in any calendar quarter or where Symantec has provided three (3) or more service extensions for any one year of subscribed service, Customer may terminate the effected service upon thirty (30) days' written notice to Symantec. In the event that Symantec validates the conditions of the termination under this Section, Symantec shall refund to Customer directly or through the reseller, where applicable, a pro-rata portion of the service fees paid in advance and not yet used within forty-five (45) days from termination, or, upon Customer's request and at Symantec's sole option, offer a credit of the pro-rata refund amount toward a new Symantec product purchase to be used within a set period of time. In the event that the Service is licensed as a bundled offering with the DLP Detection, the same will apply to the DLP Detection.

2. Average Latency Specific to Services.

a. CloudSOC CASB Gateway. Average latency for transactions passing through the CloudSOC CASB Gateway service is based on end-user performance and will not exceed the greater of: one second or two times the Direct Response Time (defined below). The CloudSOC CASB Gateway average latency is assessed on the difference between: (a) The completion time for a cloud application transaction when its traffic is sent to a cloud service via an CloudSOC CASB Gateway; and (b) the completion time for an identical cloud application transaction from the same end-point device and location when its traffic is sent directly to the cloud service, without using an CloudSOC CASB Gateway ("Direct Response Time"). Average latency is determined by the monthly average among samples taken by Symantec in a given month. Average Latency excludes file transfer activities requiring content inspection and/or encryption.

b. CloudSOC Audit. The average latency for processed data to be available in CloudSOC Audit will be no later than six (6) hours after periodic uncorrupted data batch in formats supported by Symantec is completely streamed/uploaded by the end device. Average latency is determined by the monthly average among samples taken by Symantec in a given month. Maximum daily streaming exceeding one day's worth of logs will be excluded from average latency calculations.

c. CloudSOC CASB for SaaS and IaaS (Securlets). The average latency to process an event and associated data within the CloudSOC CASB monitored SaaS application will take no more than six (6) hours after the occurrence of that event. Average latency is determined by the monthly average among samples taken by Symantec in a given month. Initial processing of events and associated data triggered by the activation or re-activation of a Securlet is excluded from average latency calculations.

d. Malware Analysis. Not subject to average latency calculation.

e. Data Loss Prevention. Not subject to average latency calculation.

f. Remedies. Subject to the requirements of Section 4 below, in the event that a particular average latency is not met in any month for reasons other than an Excused Outage (as defined in Section 1a above) or any actions attributable to Customer, Symantec will provide an extension of the current term of the specific subscribed service at no charge to Customer in an amount equal to an additional one (1) week of such service per commitment failure incident, subject to the maximum of four (4) weeks of additional service for any one year term of the subscribed service.

In the event that the Service is licensed as a bundled offering with the DLP Detection:

- any extension of the current term pursuant to this Section 2(f) will also include extended access to the DLP Detection for the same period; and
- any failure to meet the Service Availability as described in the DLP Detection service description will extend the current term pursuant to this Section 2(f) as if the failure were for the Service, as well as the DLP Detection for the same period.

3. Exclusions.

Notwithstanding any other clause herein, no commitment is made under this policy with respect to: (i) the Service being used in conjunction with hardware or software other than as specified in Symantec's published Documentation; (ii) alterations or modifications to the Service, unless altered or modified by Symantec (or at the direction of or as approved by Symantec); (iii) defects in the Service due to abuse or use other than in accordance with Symantec's published documentation (unless caused by Symantec 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.

4. Reporting and Claims.

a. 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.

b. 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 10 days of the end of a calendar quarter.

c. All claims will be verified against Symantec's system records. Should any claim submitted by Customer be disputed, Symantec 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 Symantec shall be definitive. Symantec will provide records of service availability in response to valid Customer claims upon Customer's request. Symantec shall respond to a Customer claim within 10 days of claim submission.

d. All remedies referred to in this Service Level Agreement are subject to Customer having paid all applicable fees and fulfilled all of its obligations under the Agreement.

e. Notwithstanding any other clause herein, the remedies in this Service Level Agreement do not apply to any matters arising due to any of the following:
(i) Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
(ii) Excused Outages.
(iii) Hardware, software or other data center equipment or services not in the control of Symantec or within the scope of the Service.
(iv) Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.

5. Exclusive Remedies.

Notwithstanding any other clause in the Agreement, the remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort or otherwise in respect of service affecting events.

END OF EXHIBIT A

EXHIBIT B

TECHNICAL SUPPORT

Technical Support for the Service is provided in accordance with the following terms and conditions and the “Elastica Support Quick Reference Guide” (attached).

DEFINITIONS

“BlueTouch Support Provider” or “Secure One Services Provider” means a Symantec partner authorized by Symantec to provide Technical Support for the Service.

“Customer Support Portal” or “Support Portal” means that portion of Symantec’s website URL where Customer may access Service Documentation, software downloads, active tracking of service requests and such other information as Symantec may provide to Customer as part of the Technical Support.

“Error” means a failure of the Service to conform to the applicable Service Description.

“Service Request” means the specific case number assigned to the Customer by Symantec at the time Customer makes a verified request under a valid Support Contract or Warranty.

“Service Software Update” means a formal or informal software release for a Service which incorporates functionality changes to the Software, but is not treated as a new Service by Symantec. Symantec shall make Software Updates available to Customer via electronic download from the Customer Support Portal for so long as the Service is in effect. The content of all Software Updates shall be determined by Symantec in its sole discretion.

1. TECHNICAL SUPPORT SERVICES

1.1 Coverage Generally. Symantec will use commercially reasonable efforts to provide assistance with the diagnosis of, and resolution of, basic Service configuration issues and failures specific to Services in production. All Technical Support will be provided “as is” and in accordance with the processes set forth on the Customer Portal, including, without limitation, the proper initiation of Service Requests, priority rules, information and assistance required, escalation paths, and work arounds. Symantec does not offer support for any software provided by application vendors and will not provide software fixes, patches, maintenance releases, updates or new feature releases for any third party applications, and such support is expressly excluded from Technical Support.

1.2 Service Software Support. In the event that Customer demonstrates a non-conformance with Service Software specifications that can be duplicated by Symantec and that is not addressed by an Update, Symantec will use commercially reasonable efforts to remedy such non-conformance. Such remedy may include a work around or other temporary or permanent fix. Symantec does not represent or warrant that all non-conformities of the Service Software will be corrected. Symantec reserves the right to incorporate any remedies provided to Customer into future software revisions, in its sole discretion.

2. CUSTOMER OBLIGATIONS

Technical Data. Customer shall provide reasonable assistance to Symantec when providing Technical Support, which may include the Customer providing required data from the Service to implement a work around to minimize Customer impact, or such other information as may be required by Symantec in order to perform the Technical Support.

3. SERVICE EXCLUSIONS

Technical Support covered by a Service Level Agreement will include only those items expressly defined in the Service Level Agreement, and no other services shall be implied. Without limiting the foregoing, the following services are specifically excluded from Technical Support, but may be provided by Symantec at the request of Customer for an additional charge under a Professional Services Agreement:

(a) Any work at Customer's site, other than as mutually agreed as necessary to perform a specific Service Request;
(c) Support for any modifications of the Services by anyone other than Symantec;
(d) Services purchased through a non-authorized source; or maintenance or repair by anyone other than Symantec personnel or authorized Symantec representatives;
(e) Support for any software provided by application vendors; Symantec does not provide software fixes, patches, maintenance releases, updates or new feature releases for any third party applications;
(f) Support for any non-Symantec equipment, including, without limitation, electrical or network cabling external to the Services; accessories, attachments or any other devices not furnished by Symantec;
(g) Failure to notify Symantec of the Service defect during the term of Service; and
(h) Any Services to the extent Customer ordered such Service through a BlueTouch Support Provider, in which case Customer shall obtain Support Services from that BlueTouch Support Provider.

4. EXCLUSIVE REMEDIES

Notwithstanding any other clause in the Agreement, the remedies set out in the Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort or otherwise for claims arising under these Technical Support terms and conditions.

[ELASTICA SUPPORT QUICK REFERENCE GUIDE FOLLOWS]

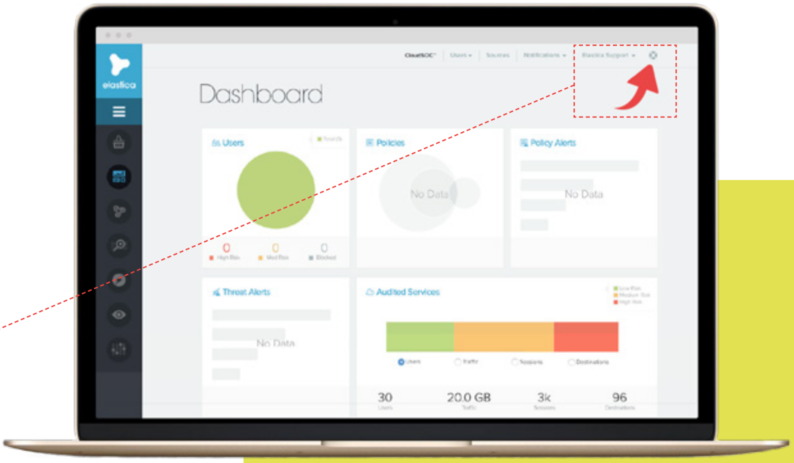
Elastica Support

Quick Reference Guide

you’ve got options

how to engage support

elastica



1

SUBMIT A TICKET

Log in at https://app.elastica.net

Click on the SUPPORT icon

You will be directed to the Support portal to submit a ticket.

2

GIVE US A CALL

If you need immediate assistance you can reach us at any of the numbers listed here

☎

US	+1	888 510-1225
EMEA	+44	(20) 37433295
APAC	+61	284172620

SUPPORT HOURS

BY REGION

US	9 AM – 5 PM*
EMEA	1 AM – 9 PM*
APAC	5 PM – 1 AM*

*NORTH AMERICA PT TIME

3

EMAIL US

Send an email to support@elastica.co

If email method has been selected the following information is required for case processing

before you contact us... get ready!

Be as specific as possible. No amount of detail is too much! The more information our Support Engineers have about your particular issue, symptoms and contextual conditions, the faster they will get you back on track.

HAVE ON HAND

- Detailed description of the issue
- Steps to reproduce
- What browser and version
- Screenshots of any errors (to email if necessary)

fast and reliable

elastica

call response times

ISSUE SEVERITY	INITIAL CONTACT	STATUS UPDATE
CRITICAL **SEV 1** Product is down. No workaround available	1hr	2hr
HIGH **SEV 2** End-User can access the Elastica service, but one or more significant features are unavailable	4hr	12hr
MED **SEV 3** Issues that do not prevent the End-User from accessing a significant feature of the service	8hr	2 business days
LOW **SEV 4** Product function is not impaired and no impact to customer business. > General Questions	24hr	7 business days

ONLINE HELPFUL TOOLS

- Knowledge Base
- User Guides
- Community

All of these can be accessed once logged into the Support portal. The Elastica Support Portal provides support where and when you need it. You can access your cases and the online helpful tools 24x7. Our support engineers are excellent problem solvers. As and when they encounter unique issues, they document the resolutions. These resolutions along with the common issues are available in the knowledge base accessible through the support portal.

elastica

enhancement requests

Our products go through a variety of quality assurance tests before release. In the event that our product fails to meet your expectation of a certain function, we will be more than happy to file an enhancement request on your behalf. We conduct regular reviews on the enhancements and potential bugs filed on behalf of the customers. The engineering team will evaluate the issue and provide a feasibility and potential schedule for the request.

Have a thought to share? Help us improve your experience.

SUPPORT TIPS

before you reach us for technical support

Being able to articulate the problem and symptoms before contacting software support will expedite the problem solving process. It is very important that you are as specific as possible in explaining a problem or question to our support engineers. Our engineers want to be sure that they provide you with exactly the right solution so, the better they understand your specific problem scenario, and the better they are able to resolve it.

define the problem

In order to understand and resolve your software support service request in the most expedient way possible it is important that you take the following steps before you contact us. You will need to gather information about the problem and have it on hand when discussing the situation with our support engineer.

elastica.net