Secure Access Cloud

Service Description

April 2019

This Service Description describes Symantec's Secure Access Cloud ("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, Online Services Terms and Conditions published at www.symantec.com/about/legal/repository (hereinafter referred to as the "Agreement").

Table of Contents

Secure Access Cloud

Service Description

April 2019

1: Technical/Business Functionality and Capabilities

Service Overview

Secure Access Cloud ("Service") is designed to enable enterprise IT and security teams to create Zero Trust application access architecture, replacing traditional Virtual Private Network (VPN) and other remote access technologies. The Service assists in connecting Users from devices across the globe to specific corporate applications, services or workloads located either on-premises or in the public cloud, while leaving all other corporate resources cloaked.

Service Features

- Customer can configure the Service through either an Administration Portal ("Portal") or a management REST API by:
    - Configuring integration with Corporate Identity Providers;
    - Defining sites where the corporate IT resources are located;
    - Deploying connectors (that provide connectivity brokerage);
    - Configuring assets, and
    - Defining access entitlements and governance policies.
- The Service supports various access scenarios, such as, but not limited to:
    - Access to user-interactive Web Portals or Web Applications
    - Access to REST / SOAP services
    - Access to SSH Servers, including SCP, SFTP, X11, GIT and other SSH-based protocols
    - Access to Microsoft RDP Servers
    - Access to Databases and other specific servers via TCP-based protocols
- The Service can perform authentication of interactive User sessions via external IdP Providers using SAML, OpenID Connect, LDAP or other protocols. Additionally, the Service supports out-of-the-box integration with Identity-as-a-Service Providers, such as Okta, Microsoft Azure AD, OneLogin, Google Apps and more.
- The Service includes a customizable health check mechanism for all the resources that are exposed to the Users. The mechanism can alert the resource owners when these become unavailable, prior to User complaint.
- The Service includes a built-in dynamic DNS subsystem allowing remote Users to access corporate resources by name, as well as an ability to create dedicated URLs under the Customer's DNS zone.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for availability, performance and capacity, as well as User experience. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Reporting for the Service is available through the Portal or a management API. Reporting may include activity logs and/or statistics.

Supported Platforms and Technical Requirements

- Supported platforms for the Service include any supported Docker runtime engine.

Service Software Components

- This Service may require the use of software components which should be used only in connection with Customer's use of the Service during the Subscription Term ("Service Software"). The use of any software component is governed by the Agreement and, if applicable, any license published with this Service Description on www.symantec.com/about/legal/repository.

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.
- 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 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 account.
- 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.

3: Entitlement and Subscription Information

Charge Metrics

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

- "**User**" means an individual person authorized to use and/or benefit from the use of the Service, or that actually uses any portion of the Service. A User may access the Service from no more than three (3) endpoint devices. In addition, a "User" may be calculated by Symantec at its sole discretion through counting the number of endpoint devices or measuring equivalent activity/expected data consumption for an individual person where usage by individuals cannot be determined.

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): CustomerCare@symantec.com, 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 to request any permitted change.

4: Customer Assistance and Technical Support

Customer Assistance

Symantec will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If Symantec is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published terms and conditions and technical support policies published at https://support.symantec.com/en_US/article.TECH236428.html.
- Once a severity level is assigned to a Customer submission for Support, Symantec will make every reasonable effort to respond per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

Problem Severity	Support (24x7) Response Targets*
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	Within 30 minutes
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	Within 2 hours
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**
Severity 4: A problem has occurred where Customer's business operations have not been adversely affected.	Within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

The above Support Response Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.

** Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request).*

*** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business hours" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.*

Maintenance to the Service and/or supporting Service Infrastructure

Symantec must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.symantec.com/ and subscribe to Symantec Status email service to receive the latest updates. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Symantec will provide seven (7) calendar days' notification posted on Symantec Status Page. Customers can also receive notifications via SMS, email or Twitter by subscribing to Symantec Status Page.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec will provide a minimum of one (1) calendar day notification posted on the Symantec Status Page. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Symantec

will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.

- **Note:** For Management Console Maintenance, Symantec will provide fourteen (14) calendar days' notification posted on Symantec Status Page. Symantec may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

Symantec may modify the Online Services and/or the corresponding Service Descriptions at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Online Services during the Subscription Term.

- Any templates or policies supplied by Symantec as part of the Service are for use solely as a guide to enable Customer to create its own customized policies and templates.
- Excessive Consumption. If Symantec determines that Customer's aggregate activity on the Service imposes an unreasonable load (Customer's average per User usage is greater than the average per User usage generated by 95% of Users of the Service on a monthly basis) on bandwidth, infrastructure, or otherwise, Symantec may impose controls to keep the usage below excessive levels. Upon receiving Service 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. Symantec reserves the right to manage bandwidth and route traffic in a commercially optimal way.

6: Definitions

"**Administrator**" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

"Connector" means the Luminate connector docker container, as available on the docker hub at https://hub.docker.com/r/luminate/connector/, and is deployed on the Customer's datacenter environment. The Connector may be deployed in any type of datacenter (cloud, hosted or on-premises).

"**Service Credit**" means the number of days that are added to Customer's current Subscription Term.

"**Symantec Online Service Terms and Conditions**" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository.

Exhibit-A

Service Level Agreement(s)

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this Service Description only. If Symantec does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are Symantec's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit between the end-user to and from the connectors deployed in the customers environment (and to the customer's resources, via the connectors), leveraging the secure access cloud DNS names.

Inline Service Availability	**99.95%**

- **Non-inline Service Availability** is access to the controls that govern the features of the Service that do not impact data in transit between the end-user to and from the connectors deployed in the customers environment (e.g., administration portal, reporting tools used by the administrator, etc.).

Non-Inline Service Availability	**99.5%**

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\text{Total Minutes in Calendar Month} - \text{Excused Outages} - \text{Non-Excused Outages*}}{\text{Total} - \text{Excused Outages}} \times 100 > \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

Symantec will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other Symantec Online Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to Symantec Customer Support at ServiceCredit_Request@symantec.com. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for Symantec to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this Service Description, including any relevant calculations.

All claims will be verified against Symantec's system records. Should any claim be disputed, Symantec will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the Service Description.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-Symantec branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of Symantec or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this Service Description.
- Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by Symantec (or at the direction of or as approved by Symantec
- 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.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

Service-specific exclusions: For Secure Access Cloud, SLAs will not operate: (i) in respect of the Connector which is hosted in the Customer's datacenter as such datacenter's health and availability is maintained by the Customer.