Symantec™ Identity: Access Manager

Service Description

November 2014

Service Overview

The Symantec™ Identity: Access Manager Service ("**Service**") is a hosted security platform that offers single sign-on with strong authentication, access control, and user management in a unified solution. Additionally, this solution allows Customer to extend internal security policies to public and private cloud services in support of compliance and auditing requirements.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Symantec.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

Single Sign-On with Strong Authentication

- The Access Control Gateway ("**Gateway**") is a virtual software appliance, including the Single Sign-On ("**SSO**") portal and the Administrator portal, that is responsible for enforcing access policies for the Service. The Gateway enables Customer to authenticate against a single or multiple user stores.
- The Service supports strong authentication and is compatible with the Symantec™ Validation & ID Protection ("**Symantec VIP**") service. This enables second-factor authentication to the SSO portal and Web based applications. Symantec VIP is available under separate terms and conditions and for an additional fee. A complete list of supported strong authentication products is available in the installation guide.
- The Service also supports strong authentication through the use of digital certificates and is compatible with the Symantec™ Managed Public Key Infrastructure ("**PKI**") service which enables primary authentication to the SSO portal
- The Service supports Customer user stores as defined in the installation guide, including, but not limited to Microsoft Active Directory, LDAP, and third-party identity providers, which are SAML enabled.
- A list of all Administrator approved SaaS and Intranet Web applications will display after the End User is authenticated to the Service via the SSO portal, some of which may only be accessible through a browser add-on.

Access Management

- Administrators can control which cloud applications an End User may access by defining policies, based on End User's identity and session context, which are enforced by the Service.
- Administrators can also control which cloud application an End User may access by enforcing strong authentication.
- The Service includes a Generic Connector Template to allow integration with an application not currently supported or published in the Application catalog.

User Management

- Administrators may invite or enable End Users to self-register for a personal profile and credential in the built-in user directory whereby that credential can be used to access authorized applications.
- Administrators may enable End Users to manage their profile and password through self-service in the SSO Portal.

Production Environment

- Includes management of four (4) Gateways where 1 primary Gateway and 3 secondary Gateways make up a single cluster.
- High Availability for logical cluster that contain multiple gateways in different locations. High Availability is available for the SSO portal and other hosted components only, and may perform with reduced capability until the primary node is restored.
- Disaster Recovery for multiple clusters of gateways and internal data replication across logical clusters. Disaster Recovery is available for the SSO portal and the Administrator portal.

Sandbox Option

- A pre-production environment ("**Sandbox**") option is available to allow Customer to test product functionality with the Service. Customers may leverage the Sandbox instance to stage new deployments to a limited set of End Users, or assess the stability of the new deployment before rolling out to the rest of the End Users or the production environment. The Sandbox may only be hosted by Symantec. The following restrictions will apply whether Customer purchases a Sandbox in addition to a production Service, or a Sandbox-only instance for testing.

- The Sandbox is limited to fifty (50) users and for use up to twelve (12) months. Only one (1) primary Gateway will be assigned to the Sandbox. The Sandbox option may not be renewed without purchase of the Service.
- A Sandbox instance is eligible for Technical Support, however such support does not include Severity 1 or Severity 2 response and resolution commitments.
- High Availability and Disaster Recovery do not apply to the Sandbox. Sandbox environments are not eligible for service level commitments.

General Features

- Available updates to the Service will be communicated to Administrators via email alerts or made visible via the Administrator dashboard.
- Symantec will make additional relevant Service documentation available online through the Administrator portal.
- Basic reporting for the Service is available through the Administrator portal.
- The Service records important security events to create audit trails that can be transmitted to a log management and SIEM solution. Customer can archive the logs according to its requirements and internal policies.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Symantec also offers professional services to assist Customer with the Services under separate terms and conditions and for an additional fee.

Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Objective benefits may be voided, as noted below.

- Customer must provide information required for Symantec to begin providing the Service.
- Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec. See the online help for more information on each required role.
  - An Administrator must install the Bridge, as defined below, as instructed in the License Certificate email and confirm that it is joined to the cluster.
- An Administrator must update to the most current version of the Bridge. Technical Support is only available for the most-current version and the immediate prior version of the Bridge.
- Customer must communicate if it is their preference for an Administrator to perform updates to the Gateway, otherwise Symantec will perform such updates as they become available.
- Customer must configure the Service to begin use with supported applications.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Administrator portal, if applicable, or default settings will apply. Configuration and use of the Service(s) are entirely in Customer's control.

Supported Platforms and Technical Requirements

- Supported platforms for the Service are defined in the Service documentation.

Hosted Service Software Components

The Service includes the following software Service Components, upon Service Activation, as defined below:

- The Bridge Service Software is used to enable connectivity across network firewalls and authentication between the Gateway and a customer's user store such as AD/LDAP. The Bridge is available for Customer download per the instructions provided in License Certificate email.

Assistance and Technical Support

Technical Support**.** The Service includes Symantec technical support as described in the License Instrument confirming customer's purchase of the Service. Symantec technical support is provided and performed subject to Symantec's then-current terms, policies and processes ("**Support Terms**"). All references to "Software" in the Support Terms shall be deemed references to the Service, as applicable, provided, however, that any terms or deliverables in the Support Terms specific to software only shall not apply to support for the Service.

- Customer's technical assistance may be limited if Customer is using or working on an application that is not identified by Symantec as a supported application in the Application catalog or if Customer is using an implementation of the Service that was not installed or configured using recommended practices.
- Symantec Technical Support personnel may need to access Customer's Gateway to examine Customer's deployment configurations in order to fulfill support obligations.
- Symantec Technical Support may require Customer to provide certain log data in order to fulfill support obligations.

SERVICE-SPECIFIC TERMS

No Auto-Renewal.

- Notwithstanding anything to the contrary in the Agreement, there is no automatic renewal of the Service. Before the Service expires, Customer must contact Symantec or a Symantec reseller to renew the Service.

Service Conditions

- If Customer purchases directly from Symantec, the Symantec Quote Ordering Terms found on the Repository will apply. If Customer purchases through a Symantec reseller, the Additional Services Order Terms found on the Repository will apply.

- Customer will be invoiced from the date on which the Service is available for use by the Customer ("**Service Activation**"). Symantec will use commercially reasonable efforts to activate the Service within thirty (30) days from the date that Symantec can reasonably begin provisioning the Service.

- If the Service is terminated or expires, for any reason, Customer will have sixty (60) days to extract any information that may have been stored in the Service from the date of Service termination or expiration, then such information will be deleted.

- Upon Service Activation, Customer shall be responsible for all activities that occur under its Administrator accounts including, but not limited to, implementing the configuration options in line with Customer's internal policies, safeguarding the Software and related systems to protect against unauthorized access to the Service, and retaining any data and/or event logs generated by the Service.

- Customer may make the Service Software and the Service accessible to its authorized IT contractors, provided that Customer shall be responsible for such third party's compliance with the terms and conditions of the Agreement, and any breach thereof by such third party shall be deemed to be a breach by Customer.

- 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 use of any Service Component in the form of Software shall be governed by the license agreement accompanying the Software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.
- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.
- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.

SERVICE LEVEL OBJECTIVE

99.5% Service Availability

- Service Availability for the Service, not including the Administrator Portal, for any ninety (90) day period, shall be no less than ninety-nine and one half percent (99.5%). Service Availability is calculated on a rolling ninety (90) day basis as a percentage equal to (a) the total number of minutes in any such period that the Service is available and capable of receiving and processing data from customers, divided by (b) the total number of minutes in such period.
- Log-in pages for the Gateway are subject to the Service Availability objective, subject to the exceptions below.

Maintenance. Symantec must perform maintenance from time to time. Symantec will utilize planned maintenance windows to perform infrastructure changes to the system that will require impact to the production service. Symantec will give customers advance notice via email of the date and nature of such update, identifying any impacts to the Service and the duration of those impacts.

Service Level Exceptions

For purposes of calculating the Service Availability, the Services shall not be considered unavailable, even if inaccessible, if due to:

- Customer's failure to apply required updates received through Service alerts;
- Maintenance windows that are communicated to customers in writing (including by Email) at least seventy-two (72) hours in advance;
- Acts or omissions of Customer or third parties, including but not limited to, individual applications and application adapters;
- Customer's Internet connectivity being unavailable;
- Internet traffic problems not under Symantec's reasonable control;
- Customer's failure to meet minimum hardware and/or software requirements set forth in the Agreement;
- Customer's failure to use current, or immediately prior version, of updates to Service Software;
- Customer's infrastructure or other equipment failure;
- Failure of any hardware, software, service or other equipment used by an individual user to access the services; or
- Failure of services provided by customer (or a third party under contract to provide services to customer) that are incorporated into the Service in the absence of any fault attributable to Symantec.
- Customer's maintenance activity.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

- "**Administrator**" means an End 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.
- **"Agreement"** means the Master Services Agreement or such other agreement entered into between Symantec and Customer under which the ordering terms applicable to this Service Description are issued.
- **"Customer"** means the entity that purchased the Service, including any agents and/or contractors it authorizes to install and use the Service on its behalf.
- "**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).
- **"End User" or "User"** means Customer's employees, contractors and external users who are authorized by Customer to use the Services on behalf of Customer.
- **"Gateway"** means gateway in the form of a virtual software appliance installed on a virtual machine for use by Customer as part of the Service.
- **"Repository"** means the Web site where Customer may view the most current terms and conditions applicable to the Service, namely http://www.symantec.com/about/profile/policies/cloud-services-agreements.jsp or it successor Website.
- **"SaaS"** means software-as-a-service.
- "**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.
- "**Service Software**" means Software (defined below), as may be required by a Service, which must be installed on each Customer computer, in order to receive the Service. Service Software includes the Software and associated documentation that may be separately provided by Symantec as part of the Service.
- "**Software**" means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, or this Service Description, as applicable, including without limitation new releases or updates as provided hereunder.
- "**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

END OF SERVICE DESCRIPTION