Symantec Certificate Intelligence Center

Service Description

November 2016

Service Overview

The Symantec Certificate Intelligence Center Service ("Service") allows Customer to automate digital certificate discovery tasks, set-up alerts to notify administrators, automate certificate signing request (CSR) generation, certificate issuance and subsequent installation on supported applications when digital certificates require renewal or maintenance. This Service is only available to a Customer who also uses the Symantec Managed PKI for SSL Certificates ("MSSL") Service.

This Service Description, with any attachments included by reference, is part of: (i) any signed agreement between Symantec and Customer that is intended to govern this Service Description; or (ii) if no such signed agreement exists, the Symantec Hosted Services Terms. If you already have a Service Agreement in connection with MSSL (the "MSSL Service Agreement"), then this Service Description for Symantec Certificate Intelligence Center Service supplements the MSSL Service Agreement. In the event of a conflict between the terms and conditions contained in this Service Description and the MSSL Service Agreement, the terms and conditions of the MSSL Service Agreement shall control.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES
Service Features

- Web-based Console to perform and maintain configurations and actions, including, but not limited to, rich reporting, data sorting and customization, tagging, user notations, audit logging and other tools.
- Discovery of SSL certificates and related attributes through Sensors, which are managed through the Console.
- Configurable discovery scan to create inventory of SSL certificates.
- Configurable notifications and alerts for status and actions required to maintain SSL certificate lifecycle.
- Automated CSR generation and SSL certificate issuance.
- Automated installation of SSL certificates.
- Central inventory of SSL certificates filtered by various values (e.g. CA, key length, algorithm, organization, server type, etc.)
- Customer may: (i) delegate deployment and management responsibilities to one or more individuals within the organization; (ii) set up and manage users with pre-determined roles; and (iii) customize new roles using the permissions settings, all within the Console.
- Using the License Keys supplied by Symantec, Customer can configure the Sensor and/or Agent to identify networks to scan, schedule the frequency of the scans, determine how the scans are performed across Customer's network(s), identify which servers to automate and configure applications for automation.
- Automation licenses can be reclaimed and reused by voiding the applicable Sensor or Agent within the Console.
- Scan using domain names. Customer may scan using domain names in addition to IP address.
- Transport Layer Security (TLS) v1.2 support: Customer may discover SSL certificates on servers with TLS v1.2.
- Hardware requirements, options, and other information related to the Service are specified in the Installation Guide.

Customer Use and Responsibilities

Customer may use the Service only in accordance with the use meter or model under which Customer has obtained use of the Service as defined in this Service Description. Customer may use the Service for up to the number of Nodes/IP that Customer has purchased for the Service.

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, 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 must keep the "Technical Contact" information in the account up to date at all times to ensure that Customer receives provisioning emails and other time sensitive information from Symantec that affect the account.
- Maintain accurate email addresses for each administrative user of the Service.
- Download at least one (1) Sensor and run a scan to use discovery feature of Service.
- Obtain unique License Keys for each Sensor as required through the Console.
- Configure alerts and notifications, download and install Agents, and configure desired automation of tasks.
- If Customer downloads the Sensor as a virtual appliance, Customer may only install and run the virtual appliance image of the Sensor on the virtualization platform Symantec specifies when the Sensor is downloaded.
- Customer must purchase a separate license for each server IP that is under automation, using the Sensor and/or the Agent.

- If Customer delegates deployment and management responsibilities, any action taken by such delegate on behalf of Customer shall be deemed as an action taken by Customer.
- Prior to downloading and installing the Sensor(s) and/or Agent(s), Customer must ensure that each device receiving the Sensor and/or Agent meet the requirements set forth in the documentation.
- Sensors must be able to communicate with the Console over the Internet, through Customer's infrastructure and through Customer's network firewalls, if applicable, in order to obtain its configuration data and event/action details from the Console. Agents must be able to communicate with one or more Sensors on Customer's network.
- Customer affirms that: (i) Customer authorizes Symantec to scan, gather, and collect data pertinent to the Service and to automate certificate renewal and upgrade; (ii) Customer will use the Service to scan and automate only the domains, IP addresses, or assets that Customer owns or controls; (iii) Customer will use the Service only for its intended purpose as described and marketed by Symantec.
- Customer may not: (i) modify, reverse engineer, or create derivative works of, or otherwise make any attempt to build a competitive product or service using the Service; (ii) decompile, disassemble or attempt to obtain the source code for any software provided; (iii) use the Service for or on behalf of any organization other than your own, unless you have that organization's express consent to do so; and (iv) use the Service for competitive benchmarking or comparing the Service with competitor products.
- Reseller represents and warrants to Symantec that: (i) Reseller has obtained the authority of its customer to enter into the MSSL Service Agreement on behalf of its customer and/or to bind its customer to the MSSL Service Agreement; (ii) Reseller shall comply with and procure its customer's compliance with the MSSL Service Agreement.

Customer Service-Specific Warranties

- Customer warrants that all information material to the issuance of a Certificate Customer provides to Company in its Certificate Application is accurate and complete.

Assistance and Technical Support

Technical Support**.** The following technical support ("Support") is included with the Service.

- Technical Support is available on a twenty-four (24) hours/day by seven (7) days/week basis by telephone and email through the Console to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Also, Customer has access to self-service assistance through the Console. Support levels and service level commitments for Customer's selection for MSSL shall apply to Customer's use of the Service. No service level commitments will apply with respect to the Service unless a Gold or Platinum Service Fee obligation is in effect.

Maintenance. Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on the SMC. Symantec will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service. "**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance by posting an alert on the applicable SMC no less than one (1) hour prior to the start of the Emergency Maintenance. "**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.
- *Routine Maintenance (SMC).* Symantec will use commercially reasonable efforts to perform routine maintenance of SMCs at times when collective Customer activity is low to minimize disruption to the availability of the SMC. Customer will not receive prior notification for these routine maintenance activities.

SERVICE-SPECIFIC TERMS

Service Conditions

- 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/.
- Customer shall comply with all applicable laws with respect to use of the Service. In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service is 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.
- Symantec shall be entitled to rely upon the correctness of the information and accuracy of the settings Customer provides (including proper installation of the Sensors and/or Agents by Customer) to deliver the Service.
- Notice of Creative Commons Software: If Customer opts to download Sensor(s) containing Community ENTerprise Operating System (CentOS), an Enterprise-class Linux distribution, such software is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported, a copy of which is provided with the Sensor. If Customer chooses to download and use CentOS, the Creative Commons license will govern its use and the terms of the MSSL Service Agreement shall not apply to such use.
- The Service is enabled to interoperate with Citrix's NetScaler products and includes a license for Citrix nitro.jar software that is licensed for use only in conjunction with Citrix NetScaler products. Use of the Citrix nitro.jar software in conjunction with non-Citrix products is not licensed hereunder. CITRIX NITRO.JAR SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND AND CITRIX EXPRESSLY DISCLAIMS THE IMPLIED WARRRANTIES OF TITLE, MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PUROSE. Symantec

or Citrix do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links, or other items contained within the nitro.jar software.

- The Service contains Java open source from Oracle Corporation. Customer's use of the Java portion of the Service ("Java Software") is subject to the following additional terms: Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.

Customer's Use of Service Automation Toolkit

- **Development License to Service Automation Toolkit.** Along with Customer's purchased entitlement to use the Service, Customer is entitled under this Service Description to use the Service Automation Toolkit, solely for the purposes of designing, developing, testing, and using Customer's own scripts to facilitate the integration of the Service with Customer's existing systems. This Service Automation Toolkit license shall be in addition to any licenses for the other portions of the Service acquired by Customer under this Service Description. Customer shall have no right to modify or alter the Service Automation Toolkit.
- **No Redistributable Code.** The Service Automation Toolkit shall only be used by Customer for Customer's internal use, and may be not be distributed, alone or as integrated with any other code or product, by Customer in any manner whatsoever to any third party (except as explicitly set forth below under "Third Party Consultants").
- **Open Source Code.** Customer's license rights to the Service Automation Toolkit are conditioned upon Customer not creating derivative works of the Service Automation Toolkit in any manner that would cause the Service Automation Toolkit in whole or in part to become Open Source Code. "Open Source Code" means a software program that is licensed under terms that require disclosure to parties other than the licensor of the source materials of the software program or modifications thereof, or any source materials of any other software program with which the Open Source Code software program is intended to operate, or that create obligations to distribute any portions of any software program with which the Open Source Code software program is used. Open Source Code includes, without limitation, any software licensed under the GNU General Public License.
- **Third Party Consultants.** Customer may allow third party consultants to exercise the rights granted herein to use the Service Automation Toolkit on Customer's behalf provided that: (a) Customer ensures that such consultants adhere to the applicable terms and conditions of this Service Description; and (b) Customer indemnifies Symantec for any breach of the Service Description by such consultants.
- **Support/Maintenance for Service Automation Toolkit.** Any maintenance/support provided by Symantec in conjunction with Customer's authorized use of the Service under this Service Description shall apply to Customerr use of the Service Automation Toolkit as described herein.
- **No Use of Symantec Trademarks.** Customer acknowledge that Symantec, the Symantec logo, the Checkmark logo and other related marks are trademarks or registered trademarks of Symantec or its affiliates in the U.S. or other countries (the "Symantec Marks"). Except as specifically granted herein, nothing in this Service Description creates any ownership or license in and to Symantec Marks. Customer's use of the Service Automation Toolkit under this Service Description does not include any right for Customer to use any Symantec Marks in any form without prior written approval by Symantec. Any use of the Symantec Marks is subject to the Symantec Trademark Usage Guidelines at http://www.symantec.com/about/profile/policies/trademarks.jsp.
- **Warranty Disclaimer. THE SERVICE AUTOMATION TOOLKIT IS PROVIDED "AS IS," EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. FURTHERMORE, SYMANTEC SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY CUSTOMER OR ANY USER OF THE SERVICE**

AUTOMATION TOOLKIT OR ANY APPLICATIONS PROVIDED BY CUSTOMER WHICH WERE DEVELOPED USING THE SERVICE AUTOMATION TOOLKIT.

- **Development Disclaimer.** Notwithstanding any other provision of the License Agreement, the following terms shall be applicable to the Service Automation Toolkit: **THE SERVICE AUTOMATION TOOLKIT ALLOWS CUSTOMER TO INTEGRATE THE SERVICE WITH CUSTOMER'S EXISTING SYSTEMS, OTHER SYMANTEC PRODUCTS, AND/OR THIRD PARTY PRODUCTS, SUBJECT TO THE LIMITATIONS SET FORTH IN THIS SECTION. SYMANTEC SHALL NOT BE RESPONSIBLE FOR ANY SUCH INTEGRATION OR ANY DEVELOPMENT AND/OR PROGRAMMING ACTIVITIES UNDERTAKEN BY CUSTOMER, INCLUDING BUT NOT LIMITED TO USE OF THE SERVICE AUTOMATION TOOLKIT FOR ANYTHING OTHER THAN ITS INTENDED PURPOSE. UNLESS CUSTOMER USES THE APPROPRIATE DEGREE OF SKILL AND CARE IN CUSTOMER'S DEVELOPMENT AND PROGRAMMING ACTIVITIES, CUSTOMER'S INTEGRATION OF THE SERVICE WITH CUSTOMER'S EXISTING SYSTEMS, OTHER SYMANTEC PRODUCTS, OR THIRD PARTY PRODUCTS MAY CAUSE ERRORS OR PROBLEMS IN THE USE OR OPERATION OF THE SERVICE. CUSTOMER'S USE OF THE SERVICE AUTOMATION TOOLKIT TO INTEGRATE THE SERVICE WITH CUSTOMER'S EXISTING SYSTEMS, OTHER SYMANTEC PRODUCTS, AND/OR THIRD PARTY PRODUCTS SHALL BE AT CUSTOMER'S SOLE RISK. SYMANTEC SHALL HAVE NO LIABILITY FOR ANY USE OF THE SERVICE AUTOMATION TOOLKIT FOR ANY OTHER PURPOSES, OR FOR ANY FAILURE OF THE SERVICE AUTOMATION TOOLKIT AND/OR THE SERVICE BASED ON CUSTOMER'S FAILURE TO PROPERLY DEVELOP, PROGRAM, INSTALL, CONFIGURE AND/OR MONITOR CUSTOMER'S INTEGRATION OF THE SERVICE WITH CUSTOMER'S EXISTING SYSTEMS, OTHER SYMANTEC PRODUCTS, AND/OR THIRD PARTY PRODUCTS.**

DEFINITIONS

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

"Activation Key" means a unique, single use, numeric key used to activate a Sensor.

"Agent" means the Service-related Software (defined below) application that Customer must download from the Console in cases where the certificate lifecycle will be automated, on supported applications, chosen based on the target hardware architecture and operating system, installed in Customer's network at appropriate locations, and communicating with one of the installed Sensors to the Console.

"Console" means the web-based "Certificate Intelligence Center" application hosted by Symantec and accessed either directly through the provided URL, or through Customer's MSSL console. The Console provides Customer access to all of the configuration, user management, permissions, and application logic for the Service.

"**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).

"License Key" means a unique numeric key used to activate a single IP address for automation on the Sensor or Agent.

"Node/IP" means a unique network or machine addresses, such as an internet protocol or MAC address, that is monitored by the Service.

"Reseller" means an Internet service provider, a systems integrator, a Web host, a technical consultant, an application service provider, or other entity that obtains the Services for re-sale.

"Sensor" means the Service-related Software (defined below) application that Customer must download from the Console, install in Customer's network at appropriate locations, and configure within the Console for access, performance and activity based on Customer's requirements. Sensors act as a conduit between the Agent and the Console by facilitating all communications.

"Service Automation Toolkit" means publicly-supported Service interfaces, including web service APIs, and correlary user interfaces.

"**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.

"Symantec Hosted Service Terms" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

END OF SERVICE DESCRIPTION