One Identity Safeguard On Demand

Quick Start

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Safeguard On Demand Quick Start
Updated - 09 February 2022, 08:35

Contents

Overview: What is Safeguard On Demand? **4**

Architectural Overview **5**

Operational Guidelines **6**

VPN Notes **7**

General Notes **8**

About us **9**

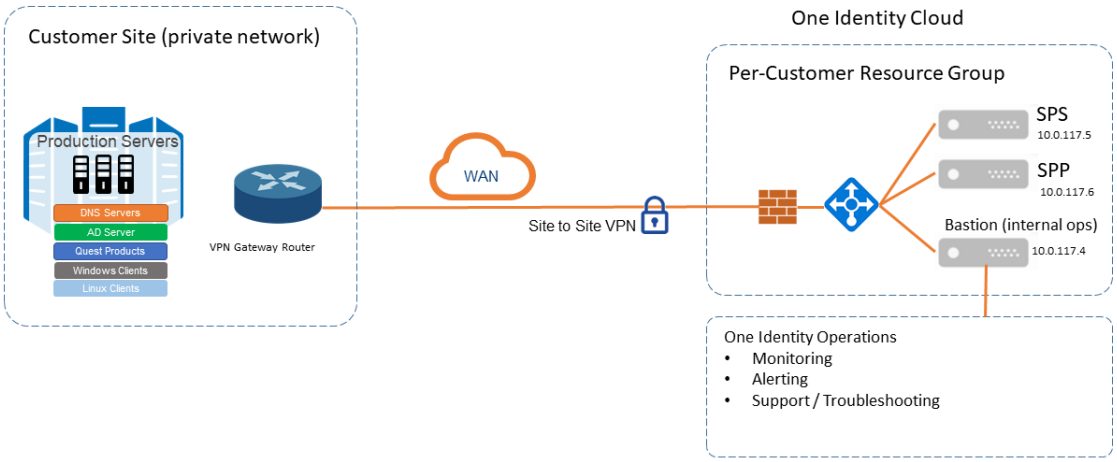
Contacting us 9

Technical support resources 9

Overview: What is Safeguard On Demand?

This product is a complete Safeguard installation (Safeguard for Privileged Passwords (SPP) and Safeguard for Privileged Sessions (SPS)), provisioned and connected to your virtual private network configuration (VPN) to manage your on-premises assets. One Identity will operate and monitor the runtime environment for you. When you purchase Safeguard On Demand, our team will provision your environment after collecting your specific network and VPN connection information. This provisioning can take up to 24 hours to complete, and some additional VPN configuration may be required to adjust your VPN gateway device to connect to the VPN gateway hosted on your behalf. Because we are provisioning this in an address that is private to your VPN, One Identity will provide IP addresses for SPS and SPP, and default credentials.

Architectural Overview



SPP: Safeguard for Privileged Passwords (SPP) automates, controls, and secures the process of granting privileged credentials with role-based access management and automated workflows.

SPS: Safeguard for Privileged Sessions (SPS) is a privileged session management solution, which provides industry-leading access control, as well as session monitoring and recording to prevent privileged account misuse, facilitate compliance, and accelerate forensics investigations.

Bastion: The bastion host is intended for the One Identity Cloud Ops team to provide maintenance and support.

Operational Guidelines

- For security reasons, Safeguard On Demand as deployed within the One Identity Cloud, will never have a public IP address. You must provide your site's VPN connection information to connect to Safeguard On Demand so that you can configure and use Safeguard On Demand from within your company network.
- The One Identity Cloud operations team pre-sets the bootstrap password and the admin password. Use the admin account and password to configure Safeguard On Demand for your environment. The One Identity Cloud operations team will retain the bootstrap password for maintenance and emergency use only.
- The One Identity Cloud ops team will pro-actively monitor your installation, so please do not shut it down explicitly because that will be considered an outage.
- The One Identity Cloud ops team will back up the system periodically and retain it for a period of 7 days in case an emergency restoration is required. Contact One Identity Support if an explicit restore is required.

VPN Notes

- The parameters collected to set up your VPN initially are used to provision explicit network routes in Azure to connect your Safeguard On Demand instance to your own network. If you are going to change your VPN settings or other aspects of network configuration (for example, firewall rules), please contact One Identity Support to ensure that the One Identity Cloud Ops team can make suitable changes to keep your network connected.
- As part of the provisioning process, you should receive a "VPN Configuration Bundle" which is created by the One Identity Cloud Operations team to connect to your VPN device. Apply this script to your VPN configuration to set up the connection between your on-premises network and the VPN Gateway the One Identity Cloud operations provisions for you.
- One Identity monitors the VPN connection and raises an alarm condition if the VPN appears to be disconnected for approximately 15 minutes.
- One Identity uses the Azure Gateway product which supports several common on-premises VPN devices. These are outlined here, and additional troubleshooting and configuration information can be found here.

General Notes

- To avoid HTTPS certificate warnings when visiting the web interface, you must provide and install a certificate to your instance of Safeguard On Demand. Configure the server name in your corporate DNS space, then create and upload a suitable certificate for your instance of Safeguard On Demand.
- Delivery of your system will be a direct result of the data provided to One Identity at setup time. For example, your Safeguard On Demand instance will reside in the One Identity Cloud at distinct IP addresses (one for Safeguard for Privileged Passwords, one for Safeguard for Privileged Sessions), and these are the systems you will connect to configure and use the system. These IP addresses will be inside the pre-selected subnet of your network address space because of the VPN.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product