One Identity Safeguard On Demand Hosted

Quick Start

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 - 13 April 2022, 12:14
Version - Hosted

Contents

Overview: What is Safeguard On Demand?

This product is a complete Safeguard (One Identity Safeguard for Privileged Passwords (SPP) and One Identity Safeguard for Privileged Sessions (SPS)) installation, provisioned in the One Identity cloud and connected to your network through a virtual private network (VPN) to manage your on-premises assets. One Identity will operate and monitor the runtime environment for you.

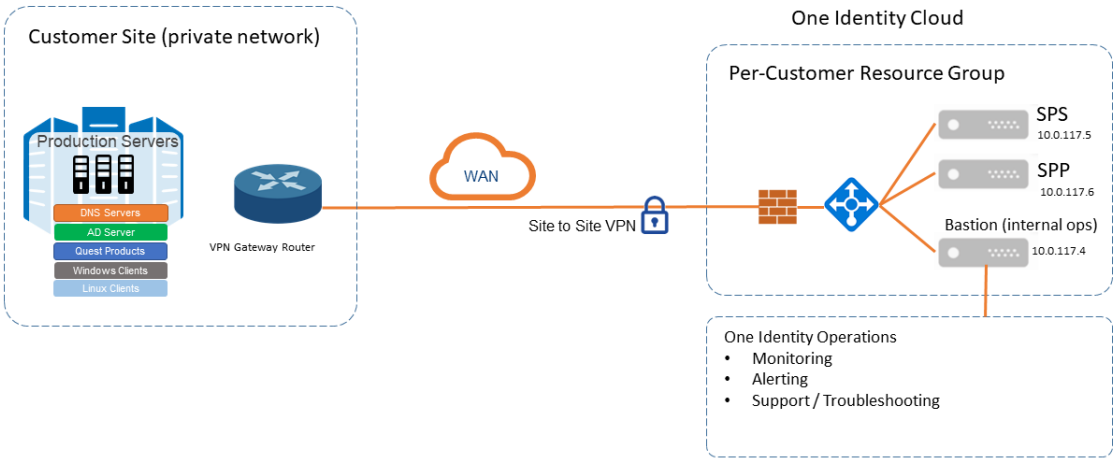
Safeguard On Demand is available both in a limited-time trial mode and in a subscription-based licensing model. Once One Identity enables Safeguard On Demand for your organization, you must send a set of required configuration information to the One Identity Cloud Operations Team via the One Identity Starling portal. For more information on providing the requested information, see Sending required information to One Identity.

One Identity will provision your environment after providing the requested 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 One Identity is provisioning this deployment in an address that is private to your VPN, One Identity will provide the IP addresses for SPS and SPP, and default credentials.

Architectural Overview

The following describes the components and architectural overview of your deployment.



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

SPS: One Identity 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 Operations Team to provide maintenance and support.

Sending required information to One Identity

Before the One Identity Cloud Operations Team can configure and provision your Safeguard On Demand environment, you must send a set of configuration information via the One Identity Starling portal (https://www.cloud.oneidentity.com).

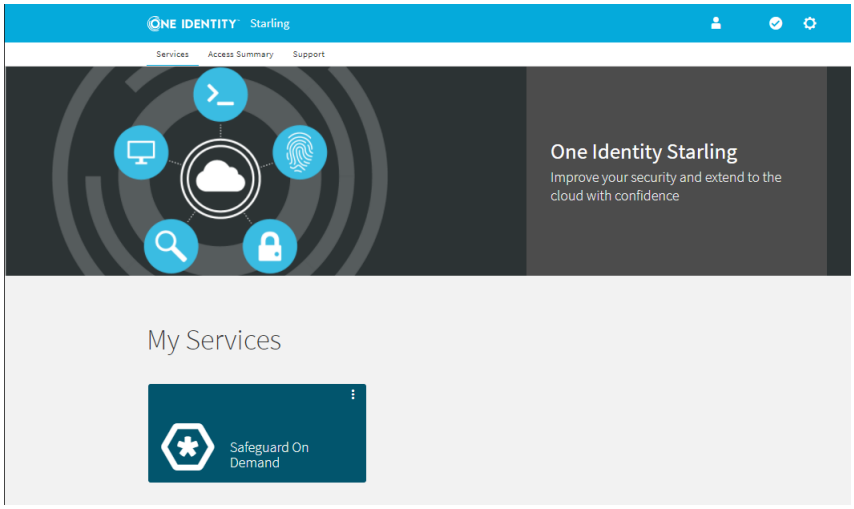
Prerequisites

Before collecting and sending the required information, make sure that the following conditions are met:

- Your organization is already registered on the One Identity Starling portal.
- If you configure a product trial, your One Identity representative notified your organization that the product trial has been added to your organization account.
- If you configure a subscribed product, your organization received a subscription confirmation email from One Identity.

To send product configuration information to the One Identity Cloud Operations Team

1. To open the list of product services available for your organization, in the One Identity Starling portal, click **Services**.

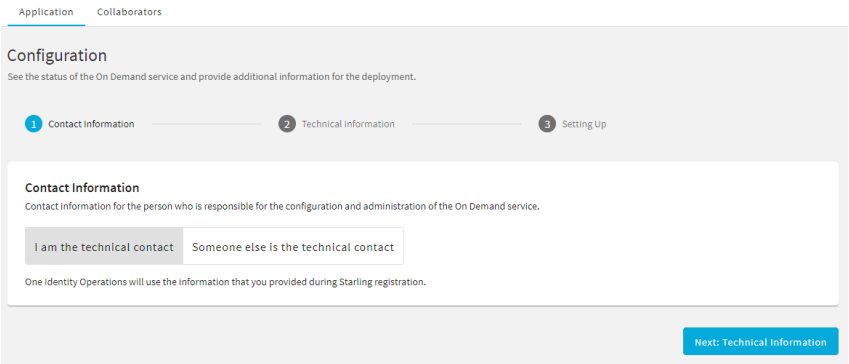


2. To start configuring the product, open the **Application** page of Safeguard On Demand.
    - To configure a product trial, open the **View On Demand services** ribbon at the bottom of the page and click **Safeguard On Demand** > **Trial**. This will create the trial subscription for you. Continue configuring the trial subscription

as described in the next bullet point.

- To configure a subscribed product (or an active product trial), click **My Services** > **Safeguard On Demand**.

3. In the **Contact Information** step, specify whether you are the technical contact for the One Identity Cloud Operations Team in your organization.



   - If you are the technical contact (that is you have all the technical information required by One Identity to configure and provision Safeguard On Demand), select **I am the technical contact** and click **Next: Technical information**.
   - If you are not the technical contact, then invite the contact who can provide the required configuration information. This is typically required if the initial On Demand invitation email was sent to you due to organizational policies, even if you are not the technical contact of the On Demand product. To invite the actual technical collaborator:
     a. Select **Someone else is the technical contact**, then click **Invite Collaborator**.
     b. In the **Invite Collaborator** dialog, provide the name and email address of the technical contact.
     c. To send an invitation to the specified contact, click **Invite**.

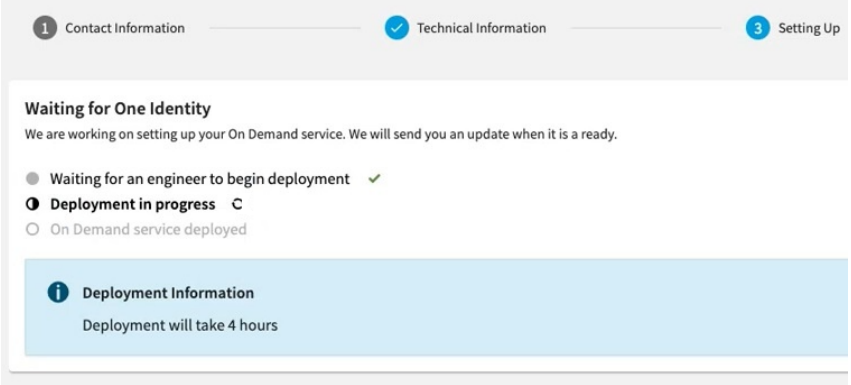
        TIP: You can also invite a technical contact by clicking **Collaborators** on the top left corner of the One Identity Starling web interface.

     Once you sent the invitation to the technical contact, make sure that they perform the remaining steps.

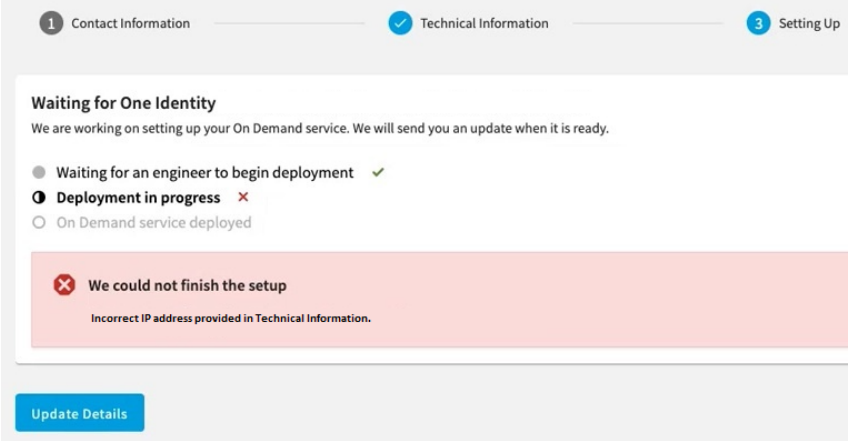
4. In the **Technical Information** step, provide the required configuration information as instructed on-screen.
5. To confirm the information you entered, click **Submit Details**. This opens the **Confirm Details** dialog, where you can either send the information to the One Identity Cloud Operations Team (**Submit Details**), or return to the **Technical Information** step and make any final changes (**Edit Details**).

   NOTE: Once you submit the specified information, you cannot make any further changes, unless One Identity rejects the provided configuration information for some reason.

6. Once you sent the configuration information, the **Setting Up** step will indicate the status of provisioning and configuring Safeguard On Demand. One Identity will also send you an email notification each time the status of deployment changes.



The **Setting Up** step will also indicate if configuration fails for any reason (for example, because of incorrect data provided in the **Technical Information** step).



To open the **Technical Information** step and fix the provided information as requested by the One Identity Cloud Team, click **Update Details**. Once you updated the configuration details, resend them to the One Identity Cloud Operations Team by clicking **Submit Details** again in the **Technical Information** step.

Once Safeguard On Demand is configured for your organization, the **Application** page of Safeguard On Demand will display the connection and configuration data of your On Demand deployment.

Operational Guidelines

The following list describes the operational guidelines for your deployment.

- 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-configures the bootstrap password and the administrator password. Use the administrator 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 Operations Team will proactively monitor your installation. Therefore, do not shut it down explicitly because that will be considered an outage.
- The One Identity Cloud Operations Team will back up the system periodically and retain the backup 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 following describes details regarding your VPN connection and configuration. Make sure that you read and understand these guidelines.

- 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.

  CAUTION: If you are planning to change your VPN settings or other aspects of network configuration (for example, firewall rules), contact One Identity Support in advance to ensure that the One Identity Cloud Operations 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.

  For more information, see About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections in the *Microsoft VPN Gateway documentation*.

  For additional troubleshooting and configuration information, see the Microsoft VPN Gateway documentation.

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.
- The delivery of your system will be based on 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 One Identity Safeguard for Privileged Passwords, one for One Identity Safeguard for Privileged Sessions). 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