One Identity Safeguard for Privileged Sessions 6.0

Starling Two-Factor Authentication - Overview

SPS Starling Two-Factor Authentication - Overview
Updated - November 2019
Version - 6.0

Contents

1

Introduction

NOTE:

This tutorial describes the deprecated version of the plugin.

To upgrade your deprecated plugin for One Identity Safeguard for Privileged Sessions 6.0, see Upgrading plugins for One Identity Safeguard for Privileged Sessions version 6.0.

This document describes how you can use the services of One Identity Starling 2FA to authenticate the sessions of your privileged users with One Identity Safeguard for Privileged Sessions (SPS).

One Identity Safeguard for Privileged Sessions:

One Identity Safeguard for Privileged Sessions (SPS) controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. SPS is a quickly deployable enterprise device, completely independent from clients and servers — integrating seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill down for forensic investigations.

SPS acts as a central authentication gateway, enforcing strong authentication before users access sensitive IT assets. SPS can integrate with remote user directories to resolve the group memberships of users who access nonpublic information. Credentials for accessing information systems can be retrieved transparently from SPS's local credential store or a third-party password management system. This method protects the confidentiality of passwords as users can never access them. When used together with Starling (or another multi-factor authentication provider), SPS directs all connections to the authentication tool, and upon successful authentication, it permits the user to access the information system.

Integrating One Identity Starling 2FA with SPS:

SPS can interact with your Starling account and can automatically request strong multi-factor authentication for your privileged users who are accessing the servers and services protected by PSM. When used together with One Identity Starling 2FA, SPS prompts the user for a second factor authentication, and upon successful authentication, it permits the user to access the information system.

The integration adds an additional security layer to the gateway authentication performed on SPS. If the Starling 2FA App is installed on the user's device (smartphone, tablet, and so on), the user can generate a one-time password on the device. This will be used for the authentication to the One Identity platform. This way, the device turns into a two-factor authentication token for the user. The one-time password is changed after a few seconds.

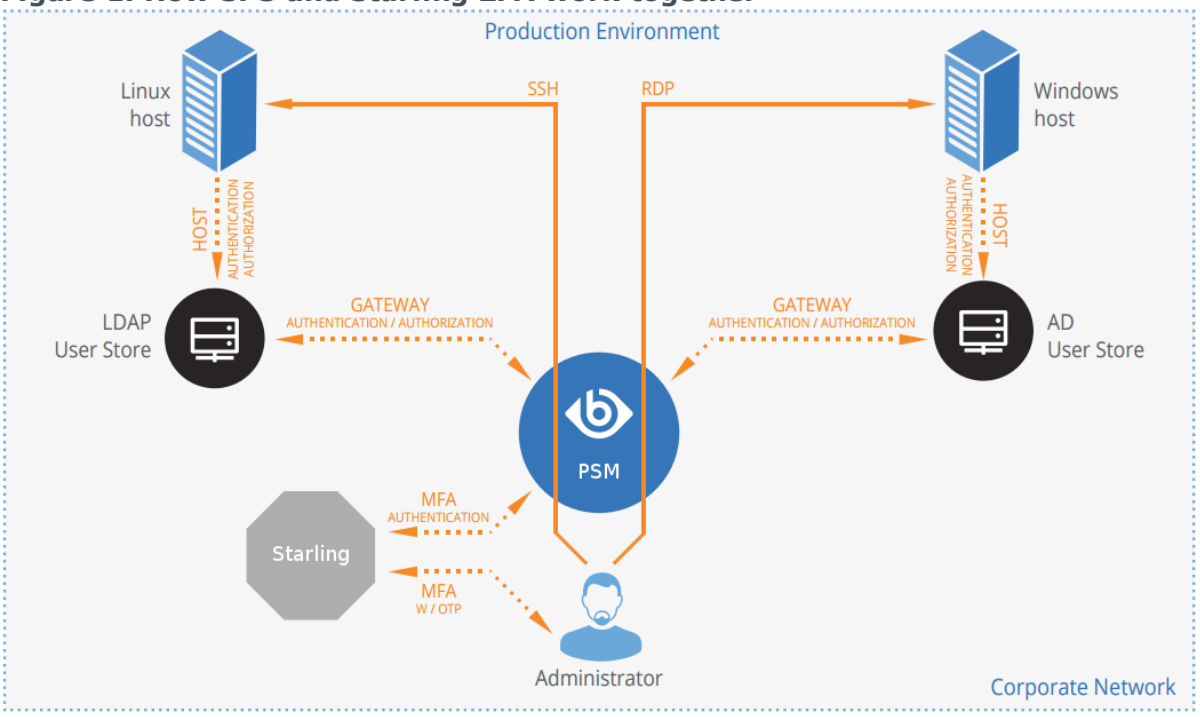
Meet compliance requirements

ISO 27001, ISO 27018, SOC 2, and other regulations and industry standards include authentication-related requirements, for example, multi-factor authentication (MFA) for accessing production systems, and the logging of all administrative sessions. In addition to other requirements, using SPS and Starling helps you comply with the following requirements:

- PCI DSS 8.3: Secure all individual non-console administrative access and all remote access to the cardholder data environment (CDE) using multi-factor authentication.
- PART 500.12 Multi-Factor Authentication: Covered entities are required to apply multi-factor authentication for:
    - Each individual accessing the covered entity’s internal systems.
    - Authorized access to database servers that allow access to nonpublic information.
    - Third parties accessing nonpublic information.
- NIST 800-53 IA-2, Identification and Authentication, network access to privileged accounts: The information system implements multi-factor authentication for network access to privileged accounts.

How SPS and Starling 2FA work together

Figure 1: How SPS and Starling 2FA work together



1. A user attempts to log in to a protected server.

2. **Gateway authentication on SPS**

   SPS receives the connection request and authenticates the user. SPS can authenticate the user to a number of external user directories, for example, LDAP, Microsoft Active Directory, or RADIUS. This authentication is the first factor.

3. **Outband authentication on Starling**

   If gateway authentication is successful, SPS connects the Starling service to check which authentication methods are available for the user. Then SPS requests the second authentication factor from the user.

   - For OTP-like authentication methods, SPS requests the one-time password (OTP) from the user, and sends it to the Starling service for verification.
   - For the Starling push notification method, SPS asks the Starling service to check if the user successfully authenticated on the Starling service.

4. If multi-factor authentication is successful, the user can start working, while SPS records the user's activities. (Optionally, SPS can retrieve credentials from a local or external credential store or password vault, and perform authentication on the server with credentials that are not known to the user.)

Technical requirements

In order to successfully connect SPS with Starling, you need the following components.

In Starling:

- A valid Starling subscription that permits multi-factor authentication.
- Your users must be enrolled in Starling and their access must be activated. To create a new user account, log on to Starling, navigate to the **Users** tab and click **Add**.
- The users must install the Starling mobile app.
- To configure Starling 2FA Authentication in your product, you have to provide the Subscription Key that is available on the Starling 2FA Dashboard. To do this, log on to your Starling account. Navigate to **Dashboard**and click **Subscription Key**.

In SPS:

- A One Identity Safeguard for Privileged Sessions appliance (virtual or physical), at least version 5 F1.
- A copy of the SPS Starling plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the Starling multi-factor authentication service.
- SPS must be able to access the Internet (at least the API services). Since Starling is a cloud-based service provider, SPS must be able to access its web services to authorize the user.

  The connection also requires the API Key.
- Depending on the method you use to authenticate your users, your users might need Internet access on their cellphones.
- SPS supports AA plugins in the RDP, SSH, and Telnet protocols.
- In RDP, using an **AA plugin** together with Network Level Authentication in a Connection Policy has the same limitations as using Network Level Authentication without domain membership. For details, see "Network Level Authentication without domain membership" in the Administration Guide.
- In RDP, using an **AA plugin** requires TLS-encrypted RDP connections. For details, see "Enabling TLS-encryption for RDP connections" in the Administration Guide.

Availability and support of the plugin

The SPS Starling plugin is available as-is, free of charge to every SPS customer from the Plugin Page. In case you need any customizations or additional features, contact our Professional Services Team.

You can use the plugin on SPS 5 F5 and later. If you need to use the plugin on SPS 5 LTS, contact our Professional Services Team.

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