One Identity Safeguard for Privileged Sessions 6.9.4

YubiKey Multi-Factor Authentication - Overview

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.

SPS YubiKey Multi-Factor Authentication - Overview
Updated - 08 February 2022, 12:40
Version - 6.9.4

Contents

Introduction

This document describes how you can use the services of Yubico (YubiKey) 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 YubiKey (or another Multi-Factor Authentication (MFA) provider), SPS directs all connections to the authentication tool, and upon successful authentication, it permits the user to access the information system.

Integrating YubiKey with SPS:

SPS can interact with your YubiKey account and can automatically request strong Multi-Factor Authentication for your privileged users who are accessing the servers and services protected by SPS. When used together with YubiKey, 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. YubiKey 4, YubiKey 4 Nano, and YubiKey NEO devices are pre-configured with the Yubico one-time password (OTP) (all other YubiKeys, except for the FIDO U2F Security Key by Yubico, also support Yubico OTP). The OTP will be used for 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 every authentication and is generated using dynamic keys.

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 YubiKey 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 MFA.
- PART 500.12 Multi-Factor Authentication: Covered entities are required to apply MFA 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 MFA for network access to privileged accounts.
- The General Data Protection Regulation (GDPR) went into effect on May 25, 2018, and is applicable to organizations keeping Personally identifiable information (PII) and offering goods or services to individuals based in the EU.

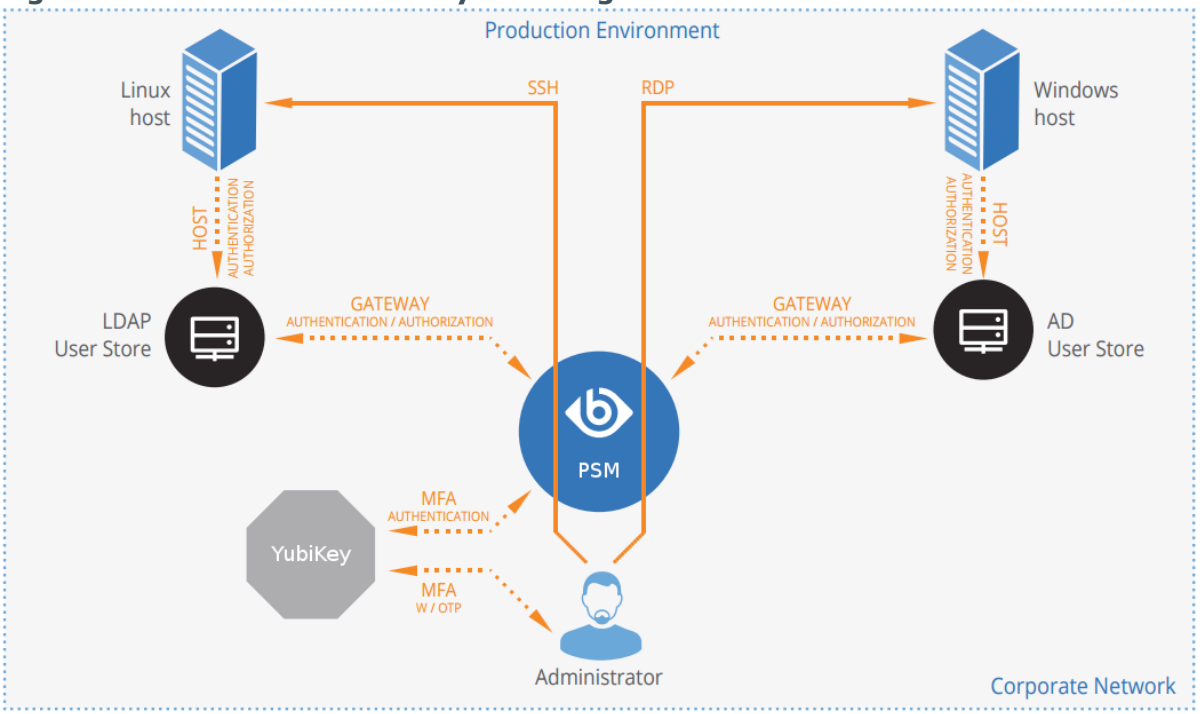
  YubiKey provides strong authentication to secure access to PII and comply with GDPR.
- The Defense FAR Supplement (DFARS) clause went into effect on December 31, 2017, and is applicable to US Department of Defense (DoD) contractors to protect unclassified DoD information and minimize loss of information.

  The multi-protocol YubiKey meets DFARS requirements for strong authentication, and is the only hardware authentication solution to meet DoD contractor security requirements.
- The revised Directive on Payment Services (PSD2) provides recommendations on standardized access to customer data and banking infrastructure, including draft regulatory technical standards specifying the requirements of strong customer authentication (SCA).

  Yubico and FIDO are playing active roles in the PSD2 framework with proven technology.

How SPS and YubiKey work together in detail

Figure 1: How SPS and YubiKey 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. **Check if the user is exempt from multi-factor authentication**

   You can configure SPS using whitelists and blacklists to selectively require multi-factor authentication for your users, (for example, to create break-glass access for specific users).

   - If multi-factor authentication is not required, the user can start working, while SPS records the user's activities. The procedure ends here.
   - If multi-factor authentication is required, SPS continues the procedure with the next step.

For details on creating exemption lists, see "[WHITELIST]" in the YubiKey Multi-Factor Authentication - Tutorial.

4. **Determining the external YubiKey identity**

   The gateway usernames are different from the external YubiKey identities, you must configure the SPS YubiKey plugin to map the gateway usernames to the external YubiKey identities.

   The external identity is the YubiKey Public ID, which is 12 lowercase letters.

   The mapping can be as simple as appending a domain name to the gateway username, or you can query an LDAP or Microsoft Active Directory server.

   For details, see "[USERMAPPING]" in the YubiKey Multi-Factor Authentication - Tutorial.

5. **Outband authentication on YubiKey**

   If gateway authentication is successful, SPS connects the YubiKey server to check which authentication factors are available for the user. Then SPS requests the second authentication factor from the user.

   - For OTP-like authentication factors, SPS requests the OTP from the user, and sends it to the YubiKey server for verification.

6. 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.)
7. If the user opens a new session within a short period, they can do so without having to perform multi-factor authentication again. After this configurable grace period expires, the user must perform multi-factor authentication to open the next session.

   For details, see "[authentication_cache]" in the YubiKey Multi-Factor Authentication - Tutorial.

Technical requirements

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

In YubiKey:

- The users must have a YubiKey device and a means to map usernames to YubiKey Public IDs. For details, see "[USERMAPPING]" in the YubiKey Multi-Factor Authentication - Tutorial.
- The YubiKey Client ID and API Key.

  For details on generating your Client ID and API Key, see Obtaining an API Key for YubiKey Development.

  To generate your Client ID and API Key, authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference at Yubico get API key.

  A Yubico OTP is a 44-character, one-use, secure, 128-bit encrypted Public ID and Password. The OTP is comprised of two major parts: the first 12 characters remain constant and represent the Public ID of the YubiKey device itself. The remaining 32 characters make up a unique passcode for each OTP generated.

  For example, in the following Yubico OTP, the characters `cccjgjgkhcbb` are the Public ID, and the remaining characters are the passcode.

  ```
  cccjgjgkhcbbirdrfdnlnghhfgrtnnlgedjlftrbdeut
  ```

- YubiKey does not require network connectivity or access to a mobile phone device. Just touch or tap the YubiKey device to authenticate.

In SPS:

- A One Identity Safeguard for Privileged Sessions appliance (virtual or physical), at least version SPS 5.11.05.11.0.
- A copy of the SPS YubiKey Multi-Factor Authentication plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the YubiKey multi-factor authentication service.
- SPS must be able to access the validation service.

  The connection also requires the Client ID and API Ke.
- SPS supports AA plugins in the MSSQL, 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.

- 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 YubiKey Multi-Factor Authentication plugin is available for download as-is, free of charge to every SPS customer from the YubiKey Multi-Factor Authentication plugin for Safeguard for Privileged Sessions page. In case you need any customizations or additional features, contact our Support Team.

CAUTION:

Using custom plugins in SPS is recommended only if you are familiar with both Python and SPS. Product support applies only to SPS: that is, until the entry point of the Python code and passing the specified arguments to the Python code. One Identity is not responsible for the quality, resource requirements, or any bugs in the Python code, nor any crashes, service outages, or any other damage caused by the improper use of this feature, unless explicitly stated in a contract with One Identity. If you want to create a custom plugin, contact our Support Team for details and instructions.

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