



One Identity Safeguard for Privileged Sessions 6.0

YubiKey Multi-Factor Authentication - Overview

Copyright 2020 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.

Contents

Introduction	4
How SPS and YubiKey MFA work together	6
Technical requirements	8
About us	10
Contacting us	10
Technical support resources	10

Introduction

i 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 [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 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 PSM. When used together with YubiKey, SPS directs all connections to the YubiKey tool, 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 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.
- The General Data Protection Regulation (GDPR) goes 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.

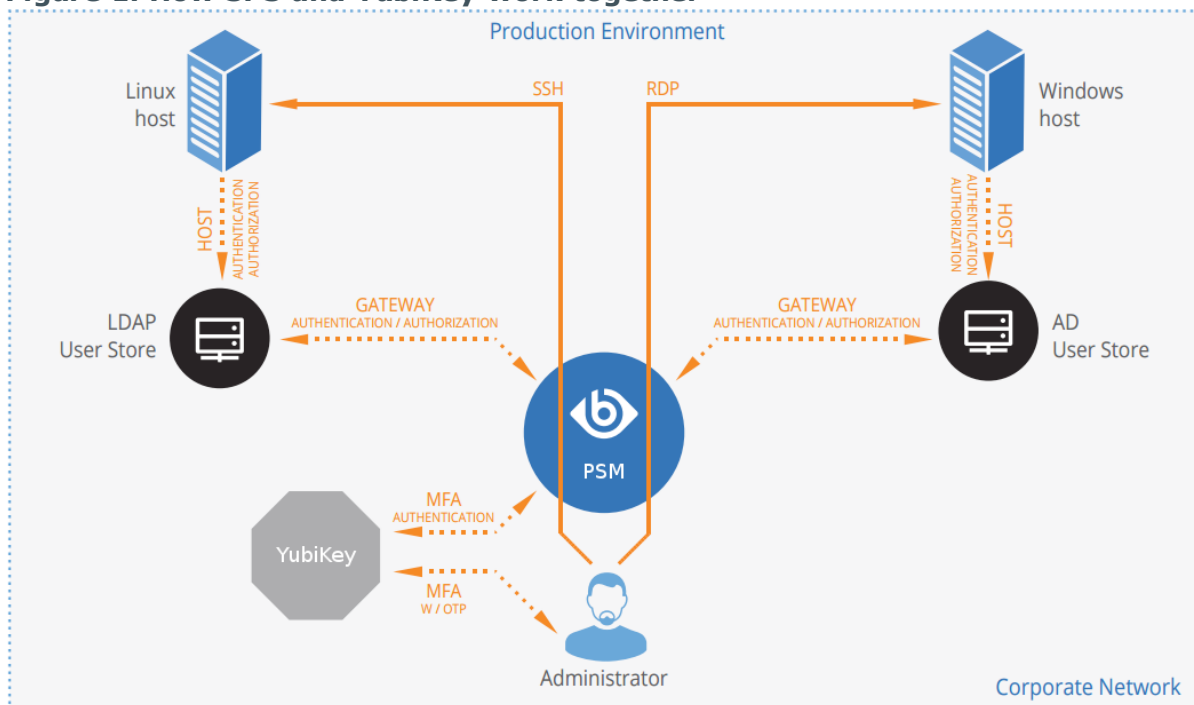
The multi-protocol YubiKey meets DFARS requirements for strong authentication, and is the only hardware authentication solution to meet DoD contractor security requirements.

- 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 MFA work together

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. 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. SPS supports authentication factors that are based on keyboard interaction such as Yubico-OTP, OATH-OTP, OATH-HOTP, and OATH-TOTP. For details on these authentication factors, see [What is OATH?](#)

For OTP-like authentication factors, SPS requests the one-time password (OTP) from the user, and sends it to the YubiKey Validation Service for verification either running on premise or using the YubiCloud Validation 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 YubiKey, 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 [YubiKey Multi-Factor Authentication - Tutorial](#) and [YubiKey Multi-Factor Authentication - Tutorial](#).
- The YubiKey Client ID and API Key.

For details on generating your Client ID and API Key, see [How do I get 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 **cccjggkhcbb** are the Public ID, and the remaining characters are the passcode.

```
cccjggkhcbbirdrfdnlnghhfgrtnnlgedjlftrbdeut
```

- 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 5 F1.
- A copy of the SPS YubiKey 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 Key.

- 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 YubiKey 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](#).

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