YubiKey multi-factor authentication with PSM — an overview

June 19, 2018

Abstract
An overview about the benefits of using YubiKey multi-factor authentication with Balabit's Privileged Session Management (PSM)

Table of Contents

1. Introduction

This document describes how you can use the services of *Yubico (YubiKey)* to authenticate the sessions of your privileged users with Balabit's Privileged Session Management (PSM).

Balabit's Privileged Session Management:

Balabit's Privileged Session Management (PSM) controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. PSM 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.

PSM acts as a central authentication gateway, enforcing strong authentication before users access sensitive IT assets. PSM 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 PSM'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), PSM directs all connections to the authentication tool, and upon successful authentication, it permits the user to access the information system.

Integrating YubiKey with PSM:

PSM 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, PSM 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 PSM. 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 PSM 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.

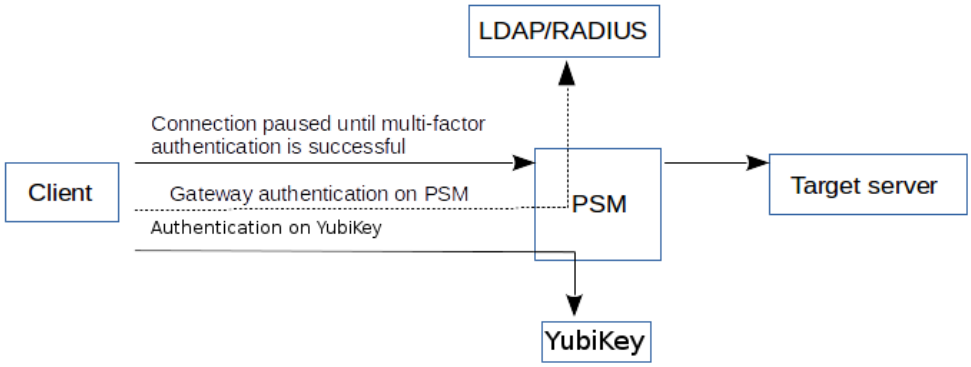
- NIST 800-53 IA-2, Identification and Authentication, network access to privileged accounts: The information system implements multi-factor authentication for network access to privileged accounts.
- The General Data Protection Regulation (GDPR) goes into effect on May 25, 2018, and is applicable to 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.

2. Procedure – How PSM and YubiKey MFA work together

Figure 1. How PSM and YubiKey work together



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

Step 2. **Gateway authentication on PSM.**
PSM receives the connection request and authenticates the user. PSM 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.

Step 3. **Outband authentication on YubiKey.**
If gateway authentication is successful, PSM connects the YubiKey server to check which authentication factors are available for the user. Then PSM requests the second authentication factor from the user. PSM 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, PSM 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.

Step 4. If multi-factor authentication is successful, the user can start working, while PSM records the user's activities. (Optionally, PSM 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.)

3. Technical requirements

In order to successfully connect PSM 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 *Section 9.2, [users]* in *Tutorial — How to use YubiKey multi-factor authentication with PSM* and *Section 9.6, [ldap]* in *Tutorial — How to use YubiKey multi-factor authentication with PSM*.
- 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 `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 PSM:

- A Balabit's Privileged Session Management appliance (virtual or physical), at least version 5 F1.
- A copy of the PSM YubiKey plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the YubiKey multi-factor authentication service.
- PSM must be able to access the validation service.
  The connection also requires the Client ID and API Key.

- PSM supports Authentication and Authorization 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 *Procedure 10.3.3, Network Level Authentication without domain membership* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- In RDP, using an **AA plugin** requires TLS-encrypted RDP connections. For details, see *Procedure 10.5, Enabling TLS-encryption for RDP connections* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

Availability and support of the plugin

The PSM YubiKey plugin is available as-is, free of charge to every PSM customer from the *Appstore*. In case you need any customizations or additional features, *contact professionalservices@balabit.com*.

You can use the plugin on PSM 5 F5 and later. If you need to use the plugin on PSM 5 LTS, *contact professionalservices@balabit.com*.

4. Learn more

To find out more about PSM, visit the *One Identity page*.

For a detailed tutorial about how to connect your YubiKey account with PSM, see *Tutorial — How to use YubiKey multi-factor authentication with PSM*.

If you need help in connecting your YubiKey account with Balabit's Privileged Session Management, *contact our Sales Team* or *contact professionalservices@balabit.com*.

4.1. About One Identity

One Identity LLC, is a leading provider of Privileged Access Management (PAM) and Log Management solutions. Founded in 2000, One Identity has a proven track record of helping businesses reduce the risk of data breaches associated with privileged accounts. With offices in the United States and Europe, and a global client list that includes 25 Fortune 100 companies, One Identity and its network of reseller partners serves more than 1,000,000 corporate users worldwide.

For more information, visit *www.balabit.com*, read the One Identity blog, or follow us on Twitter via @balabit, LinkedIn or Facebook.

To learn more about commercial and open source One Identity products, request an evaluation version, or find a reseller, visit the following links:

- *Privileged Session Management homepage*
- *One Identity Documentation page*
- To request an evaluation version, *contact our Sales Team*

About One Identity

One Identity helps organizations optimize identity and access management (IAM). Our combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, enables organizations to achieve their full potential — unimpeded by security, yet safeguarded against threats. For more information, visit *oneidentity.com*.

All questions, comments or inquiries should be directed to <info@balabit.com> or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*