Okta multi-factor authentication with PSM — an overview

June 19, 2018

Abstract

An overview about the benefits of using Okta 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 multi-factor authentication provider *Okta* 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.

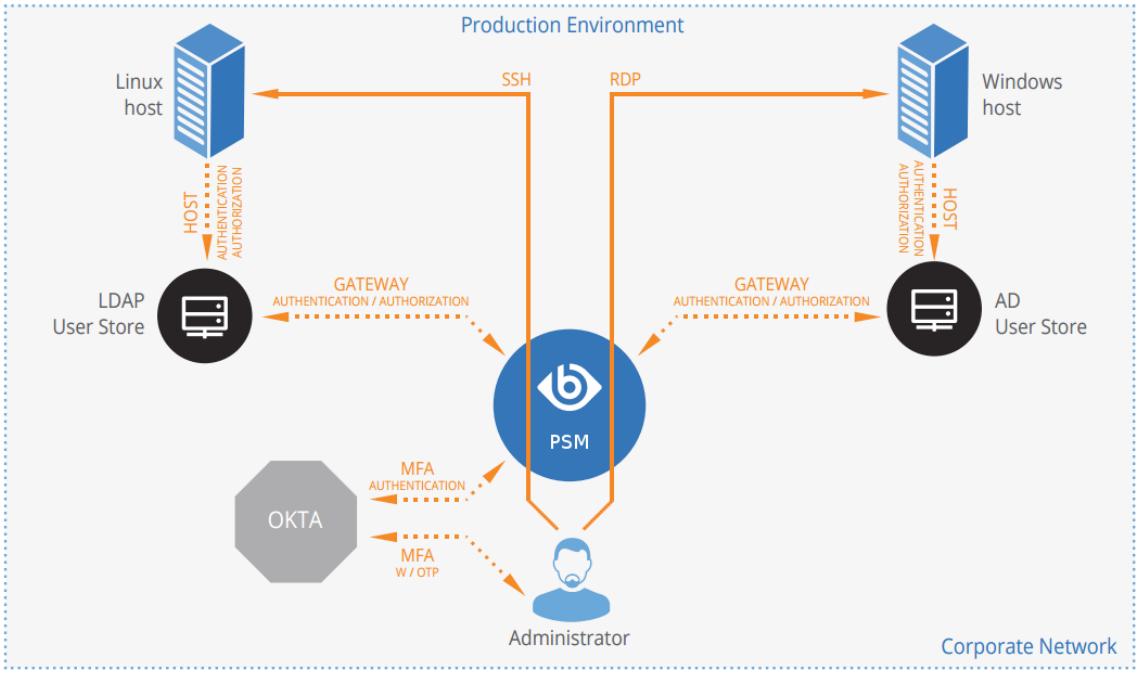
PSM acts as a central authentication gateway, enforcing strong authentication before users access sensitive IT assets. PSM can integrate with remote user directories to resolve the group memberships of users who access nonpublic information. Credentials for accessing information systems can be retrieved 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 Okta (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.

Okta Adaptive Multi-factor Authentication:

To support multi-factor authentication, PSM integrates with the identity management service Okta. This enables you to leverage an additional out-of-band factor (typically through the user's registered smartphone) when authenticating the user. The additional factor is processed in-line with the connection, so users do not have to switch to an external application to process the additional factor. This results in an efficient user experience that is readily accepted by the users.

The Balabit's Privileged Session Management can interact with your Okta account and can automatically request multi-factor authentication for your privileged users who are accessing the servers and services protected by PSM.

Figure 1. How PSM and Okta work together



Solution benefits

> Balabit Privileged Session Management helps us meet a portion of our compliance and internal security requirements related to access management.
>
> —Matt Magleby, Sr. Computer Scientist at Adobe

Using PSM together with Okta provides the following benefits.

- Easy-to-use multi-factor authentication to secure your privileged users who access your business-critical servers. The enforcement of a second-factor authentication and the availability of session recordings make the access of high-risk users more secure.
- Out-of-band authentication to protect against privileged identity theft
- Logs and audits administrative network traffic
- Integrates with existing LDAP user directory
- Easy and fast deployment and implementation: a network-level solution that does not require installing agents on clients or servers
- Can forward user logs into Splunk for long-term storage and analysis
- Supports SSH and RDP protocols to access both Linux and Windows servers, without disrupting the daily workflow of your system administrators and other privileged users
- Supports strong authentication methods, including SSH keys and certificates

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

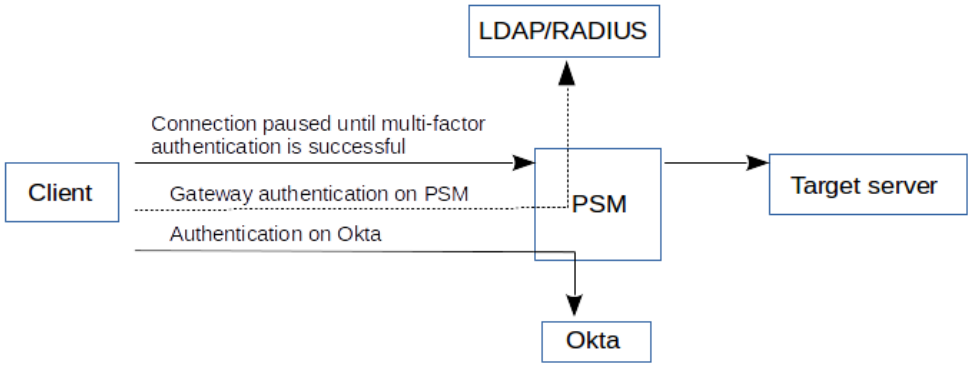
of all administrative sessions. In addition to other requirements, using PSM and Okta helps you comply with the following requirements:

- PCI DSS 8.3: Secure all individual non-console administrative access and all 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

To read about the experiences of Adobe Experience Cloud business unit using PSM and Okta, *download our case study*.

2. Procedure – How PSM and Okta MFA work together

Figure 2. How PSM and Okta 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 Okta.**
If gateway authentication is successful, PSM connects the Okta server to check which authentication factors are available for the user. Then PSM requests the second authentication factor from the user.

- For OTP-like authentication factors, PSM requests the one-time password (OTP) from the user, and sends it to the Okta server for verification.
- For the Okta push notification factor, PSM asks the Okta server to check if the user successfully authenticated on the Okta server.

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 Okta, you need the following components.

In Okta:

- A valid Okta subscription that permits multi-factor authentication.
- An Okta API key. You will need it to configure the PSM plugin.
- Your users must be available in Okta.
- The users must activate their Okta accounts, and be able to perform the authentication required for the factor (for example, install the Okta mobile app, possess the required hardware token, and so on).
- A factor that the PSM plugin supports must be enabled in Okta. Note that this is a global setting, you cannot selectively enable factors. For a list of factors that PSM supports, see *Section 4, Supported factors and scenarios (p. 8)*.

In PSM:

- A Balabit's Privileged Session Management appliance (virtual or physical), at least version 5 F1.
- A copy of the PSM Okta plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the Okta multi-factor authentication service.
- PSM must be able to access the Internet (at least the services on *https://www.okta.com*). Since Okta is a cloud-based service provider, PSM must be able to access its web services to authorize the user.
- Depending on the factor you use to authenticate your users, your users might need Internet access as well, for example, to use the Okta Verify Push Notification factor. Note that the Okta app generates one-time passwords (OTPs) offline.
- 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 Okta 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 F3 and later. If you need to use the plugin on PSM 5 LTS, *contact professionalservices@balabit.com*.

4. Supported factors and scenarios

The PSM Okta plugin can provide multi-factor authentication in the Remote Desktop (RDP), Secure Shell (SSH), and TELNET protocols. In RDP, using push notifications (when the user authenticates using the Okta mobil app) is the most convenient method. You can use another factor, but in this case the user must encode the OTP password into the username used in the connection, before trying to connect to the server.

Okta supports several different authentication backends ("factor types" in Okta terminology). When using one-time passwords (OTP-like factors), your users can specify which factor they use (from the ones available for them in Okta).

You can also set a default factor in the Okta configuration, it defaults to Okta Verify (One-Time Password).

The PSM Okta plugin supports the following authentication factors:

- Google Authenticator (One-Time Password)
- Okta Push Authentication
- Okta Verify (One-Time Password)
- RSA token
- Symantec token (One-Time Password)
- YubiKey token (One-Time Password)

You can also configure PSM to require multi-factor authentication only from selected users or usergroups. You can also specify exceptions, that is, require multi-factor authentication from everyone except the specified users. This allows you to have emergency or break-glass users who can access your servers even if the Okta services are not available. For details, see *Section whitelist* in *Tutorial — How to use Okta multi-factor authentication with PSM*.

5. Learn more

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

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

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

5.1. 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/*