inWebo multi-factor authentication with PSM — an overview

June 19, 2018

Abstract

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

ONE IDENTITY™

Table of Contents

1. Introduction

This document describes how you can use the services of _inWebo_ 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 inWebo (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 inWebo with PSM:

PSM can interact with your inWebo 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 inWebo, PSM directs all connections to the inWebo 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. If the inWebo Authenticator App is installed on the user's device (smartphone, notebook, and so on), the user can generate a one-time password on the device. This 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 inWebo 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.

2. Procedure – How PSM and inWebo MFA work together

Figure 1. How PSM and inWebo work together
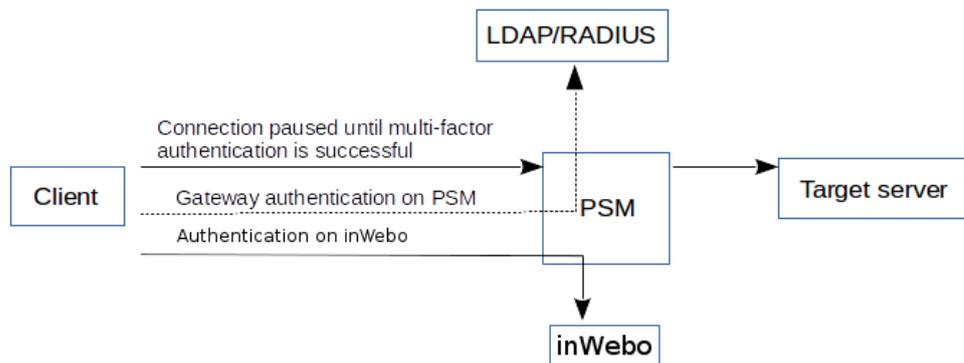
Step 1.   A user attempts to log in to a protected server.

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 inWebo.**
If gateway authentication is successful, PSM connects the inWebo 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 inWebo server for verification.

■ For the inWebo push notification factor, PSM asks the inWebo server to check if the user successfully authenticated on the inWebo 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 inWebo, you need the following components.

In inWebo:

- A valid inWebo subscription that permits multi-factor authentication.
- Your users must be enrolled in inWebo and their access must be activated.
- The users must install the inWebo mobile app.

In PSM:

- A Balabit's Privileged Session Management appliance (virtual or physical), at least version 5 F1.
- A copy of the PSM inWebo plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the inWebo multi-factor authentication service.
- PSM must be able to access the Internet (at least the services on api.myinwebo.com). Since inWebo is a cloud-based service provider, PSM must be able to access its web services to authorize the user. The connection also requires the Service ID that is displayed on the inWebo Administration interface under the **Service Users** tab.

  Generate and download an X.509 certificate and store it in the credential store:

  1. In the inWebo Administration interface, navigate to **Secure Sites** and click **Download a new certificate for the API**. Configure the parameters (**Authentication**: `Yes`, **Provisioning**: `No`) and click **Download**.

  2. Decrypt the downloaded X.509 certificate with the following command: `openssl rsa -in <certificate-file-name>.crt`. Enter the required passphrase. The decrypted part of the certificate is displayed on the console screen.

  3. Copy the decrypted part from `-----BEGIN RSA PRIVATE KEY-----` to `-----END RSA PRIVATE KEY-----`, open the `<certificate-file-name>.crt` and replace the encrypted part with the copied decrypted part from `-----BEGIN ENCRYPTED PRIVATE KEY-----` to `-----END ENCRYPTED PRIVATE KEY-----`.

- Depending on the factor you use to authenticate your users, your users might need Internet access on their cellphones.
- 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 inWebo 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 F4 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 inWebo account with PSM, see *Tutorial — How to use inWebo multi-factor authentication with PSM*.

If you need help in connecting your inWebo 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*.