



One Identity Safeguard for Privileged Sessions 6.4

inWebo 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 inWebo work together in detail	6
Technical requirements	8
About us	10
Contacting us	10
Technical support resources	10

Introduction

This document describes how you can use the services of [inWebo](#) 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 inWebo (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 inWebo with SPS:

SPS 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 SPS. When used together with inWebo, 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. If the inWebo Authenticator App is installed on the user's device (smartphone, notebook, smartwatch, and so on), the user can generate a One-Time Password (OTP) using the device. This will be used for the authentication to the One Identity platform. The one-time password is changed after 60 seconds.

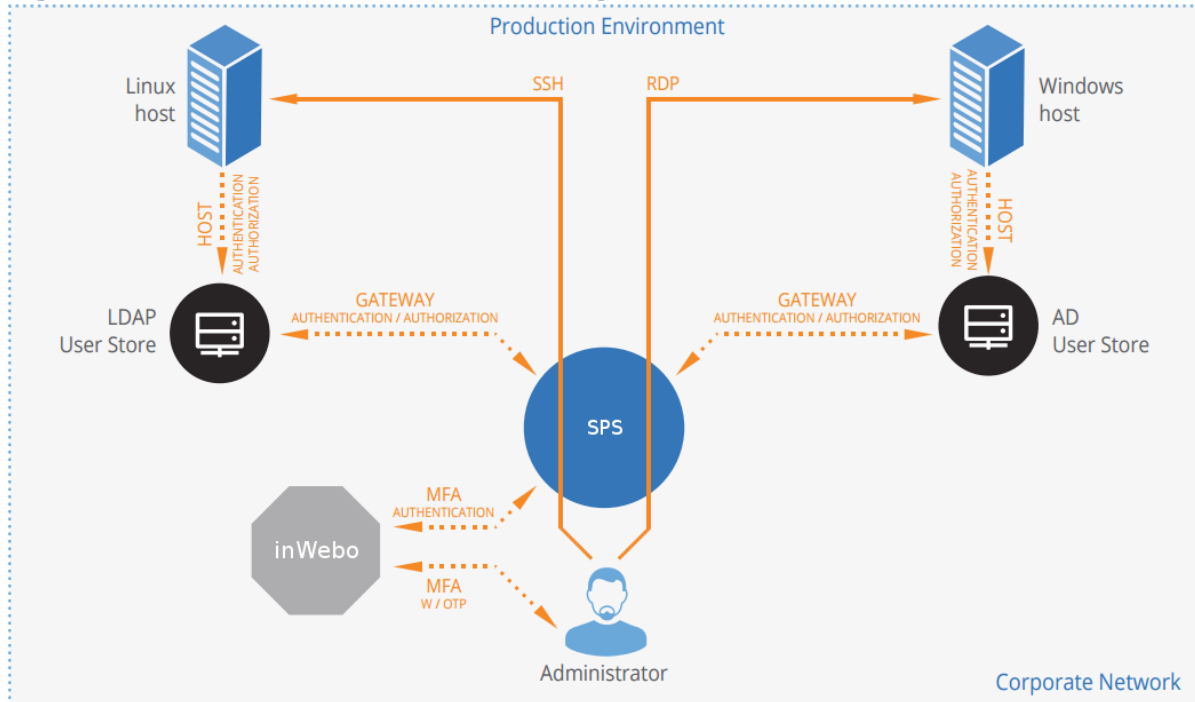
Meet compliance requirements

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 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 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.

How SPS and inWebo work together in detail

Figure 1: How SPS and inWebo 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 [inWebo Multi-Factor Authentication - Tutorial](#).

4. **Determining the external inWebo identity**

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

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 [inWebo Multi-Factor Authentication - Tutorial](#).

5. **Outband authentication on inWebo**

If gateway authentication is successful, SPS connects the inWebo 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 inWebo server for verification.
 - For the inWebo push notification factor, SPS asks the inWebo server to check if the user successfully authenticated on the inWebo server.
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 [inWebo Multi-Factor Authentication - Tutorial](#).

Technical requirements

In order to successfully connect SPS with RADIUS server, 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 SPS:

- A One Identity Safeguard for Privileged Sessions appliance (virtual or physical), at least version SPS 5.11.0.
- A copy of the SPS inWebo Multi-Factor Authentication plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the inWebo multi-factor authentication service.
- SPS must be able to access the Internet (at least the services on api.myinwebo.com). Since inWebo is a cloud-based service provider, SPS 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>.cert**. 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>.cert 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.
 - 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 inWebo Multi-Factor Authentication plugin is available for download as-is, free of charge to every SPS customer from the [InWebo 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.

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