



One Identity Safeguard for Privileged Sessions 5.7

Okta Multi-Factor Authentication -  
Overview

## Copyright 2018 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](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

### Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

# Contents

<b>Introduction</b> .....	<b>4</b>
<b>How Safeguard for Privileged Sessions and Okta MFA work together</b> .....	<b>7</b>
<b>Technical requirements</b> .....	<b>9</b>
<b>Supported factors and scenarios</b> .....	<b>11</b>
<b>Learn more</b> .....	<b>12</b>
<b>About us</b> .....	<b>13</b>
Contacting us .....	13
Technical support resources .....	13

## 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 One Identity Safeguard for Privileged Sessions (Safeguard for Privileged Sessions).

### **One Identity Safeguard for Privileged Sessions:**

One Identity Safeguard for Privileged Sessions (Safeguard for Privileged Sessions) controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. Safeguard for Privileged Sessions 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.

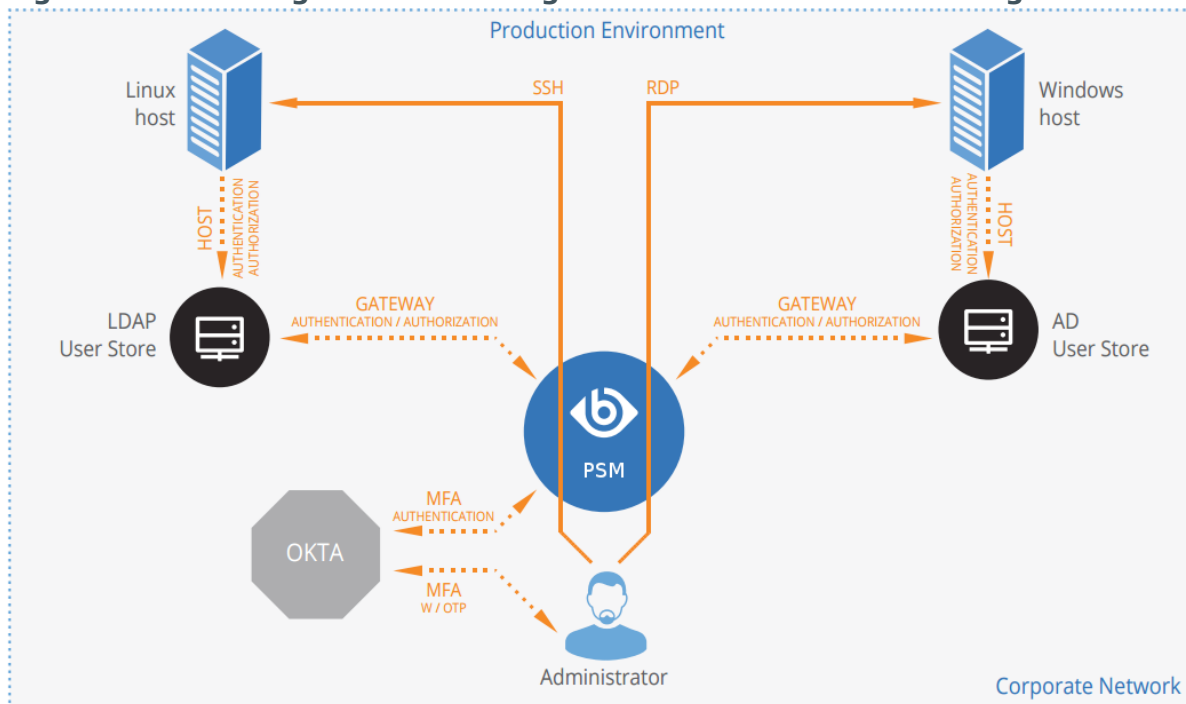
Safeguard for Privileged Sessions acts as a central authentication gateway, enforcing strong authentication before users access sensitive IT assets. Safeguard for Privileged Sessions can integrate with remote user directories to resolve the group memberships of users who access nonpublic information. Credentials for accessing information systems can be retrieved transparently from Safeguard for Privileged Sessions'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), Safeguard for Privileged Sessions 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, Safeguard for Privileged Sessions 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 One Identity Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions.

**Figure 1: How Safeguard for Privileged Sessions and Okta work together**



## Solution benefits

Matt Magleby, Sr. Computer Scientist at Adobe

One Identity Safeguard for Privileged Sessions helps us meet a portion of our compliance and internal security requirements related to access management.

Using Safeguard for Privileged Sessions 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

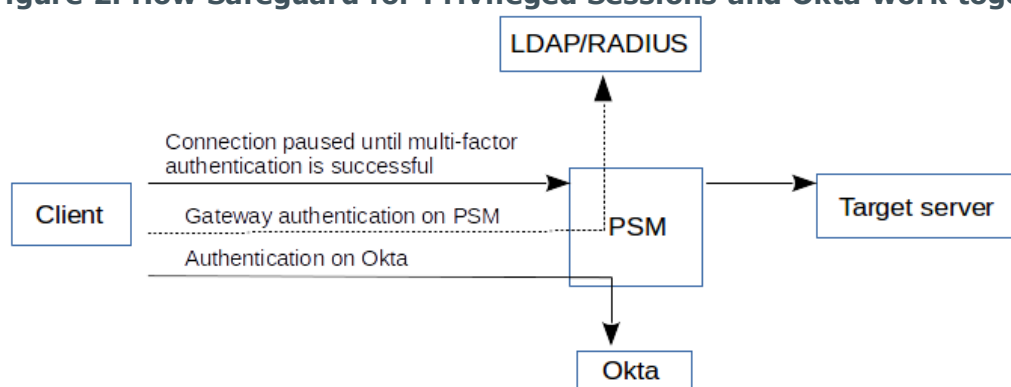
ISO 27001, ISO 27018, SOC 2, and other regulations and industry standards include authentication-related requirements, for example, multi-factor authentication (MFA) for accessing production systems, and the logging of all administrative sessions. In addition to other requirements, using Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions and Okta, [download our case study](#).

## How Safeguard for Privileged Sessions and Okta MFA work together

Figure 2: How Safeguard for Privileged Sessions and Okta work together



1. A user attempts to log in to a protected server.
2. **Gateway authentication on Safeguard for Privileged Sessions**

Safeguard for Privileged Sessions receives the connection request and authenticates the user. Safeguard for Privileged Sessions 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 Okta**

If gateway authentication is successful, Safeguard for Privileged Sessions connects the Okta server to check which authentication factors are available for the user. Then Safeguard for Privileged Sessions requests the second authentication factor from the user.

- For OTP-like authentication factors, Safeguard for Privileged Sessions requests the one-time password (OTP) from the user, and sends it to the Okta server for

verification.

- For the Okta push notification factor, Safeguard for Privileged Sessions asks the Okta server to check if the user successfully authenticated on the Okta server.
4. If multi-factor authentication is successful, the user can start working, while Safeguard for Privileged Sessions records the user's activities. (Optionally, Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions supports, see [Supported factors and scenarios](#).

### In Safeguard for Privileged Sessions:

- A One Identity Safeguard for Privileged Sessions appliance (virtual or physical), at least version 5 F1.
- A copy of the Safeguard for Privileged Sessions Okta plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with the Okta multi-factor authentication service.
- Safeguard for Privileged Sessions must be able to access the Internet (at least the services on <https://www.okta.com>). Since Okta is a cloud-based service provider, Safeguard for Privileged Sessions 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.

- Safeguard for Privileged Sessions 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 "[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 Safeguard for Privileged Sessions Okta plugin is available as-is, free of charge to every Safeguard for Privileged Sessions customer from the [Plugin Page](#). In case you need any customizations or additional features, [contact professionalservices@balabit.com](mailto:professionalservices@balabit.com).

You can use the plugin on Safeguard for Privileged Sessions 5 F3 and later. If you need to use the plugin on Safeguard for Privileged Sessions 5 LTS, [contact professionalservices@balabit.com](mailto:professionalservices@balabit.com).

## Supported factors and scenarios

The Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions 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 [Okta Multi-Factor Authentication - Tutorial](#).

## Learn more

To find out more about Safeguard for Privileged Sessions, visit the [One Identity page](#).

For a detailed tutorial about how to connect your Okta account with Safeguard for Privileged Sessions, see [Okta Multi-Factor Authentication - Tutorial](#).

If you need help in connecting your Okta account with One Identity Safeguard for Privileged Sessions, [contact our Sales Team](#) or [contact professionalservices@balabit.com](mailto:professionalservices@balabit.com).

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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

## 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product