One Identity Safeguard for Privileged Sessions 6.9.5

ServiceNow - Overview

Copyright 2023 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/trademark-information.aspx. 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.

SPSServiceNow - Overview
Updated - 08 March 2023, 10:07

For the most recent documents and product information, see Online product documentation.

Contents

Introduction 4

How SPS and ServiceNow work together in detail 6

Technical requirements 8

About us 9

Contacting us 10

Technical support resources 11

Introduction

This document describes how you can use the services of ServiceNow to authenticate and authorize 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 ServiceNow (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 ServiceNow with SPS:

SPS integrates with ServiceNow by enabling ticket ID request and validation during authentication and authorization on target servers.

The integration adds an additional security layer to the gateway authentication performed on SPS by verifying that the user has a valid reason to access the server. SPS prompts the user for a valid ServiceNow ticket ID, and upon successful authorization, it permits the user to access the information system.

Meet compliance requirements

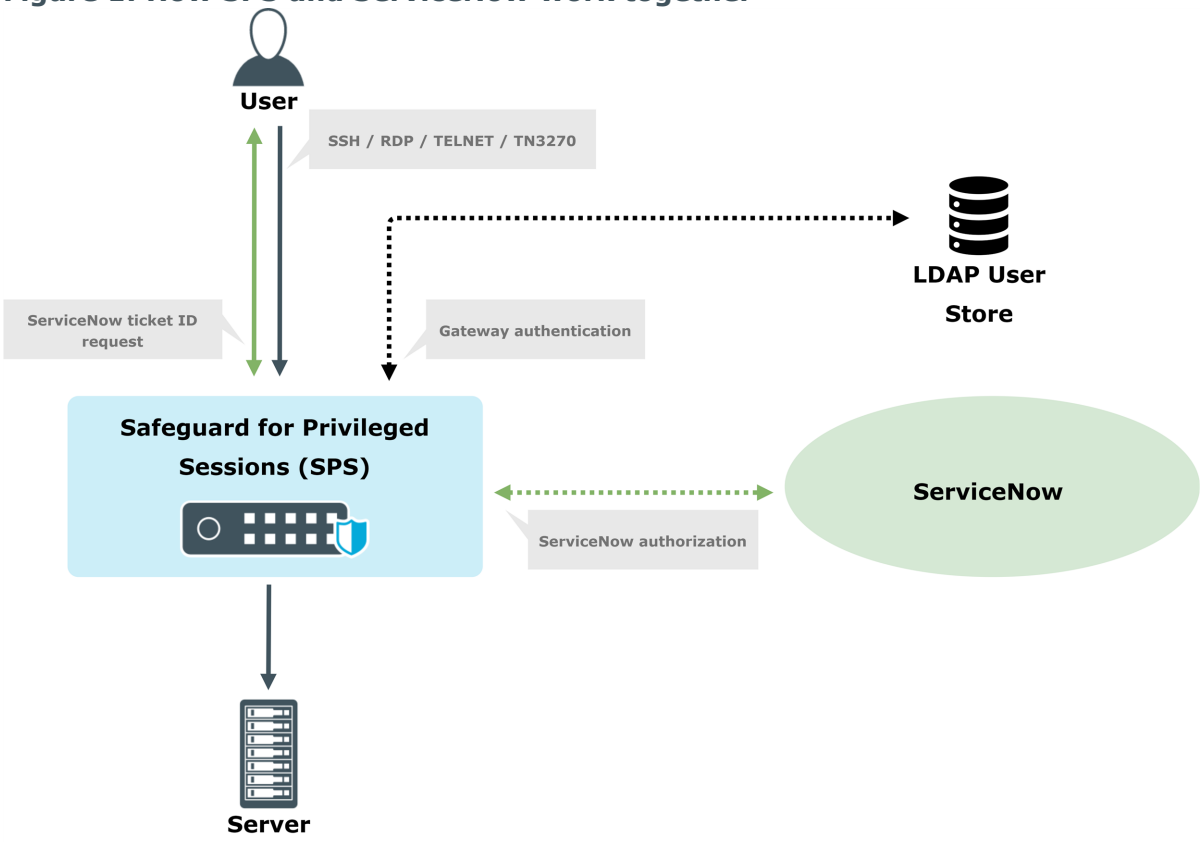
ISO 27001, ISO 27018, SOC 2, and other regulations and industry standards include authentication-related requirements, (for example, Multi-Factor Authentication (MFA) for accessing production systems, and the logging of all administrative sessions). In addition to other requirements, using SPS and ServiceNow 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 ServiceNow work together in detail

Figure 1: How SPS and ServiceNow 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 and authorization**

   You can configure SPS using whitelists and blacklists to selectively require multi-factor authentication and authorization for your users, (for example, to create break-glass access for specific users).

- If multi-factor authentication and authorization is not required, the user can start working, while SPS records the user's activities. The procedure ends here.
- If multi-factor authentication and authorization is required, SPS continues the procedure with the next step.

For details on creating exemption lists, see "[WHITELIST]" in the ServiceNow - Tutorial.

4. **Determining the external ServiceNow identity**

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

5. **Outband authorization on ServiceNow**

   If gateway authentication is successful, SPS prompts the user for a valid ServiceNow ticket ID. Then SPS connects to the ServiceNow server and runs a predefined query, and upon successful authorization, it permits the user to access the information system.

6. If multi-factor authentication and authorization 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 ServiceNow - Tutorial.

Technical requirements

In order to successfully connect SPS with RADIUS server, you need the following components.

In ServiceNow:

- An active ServiceNow instance.
- A technical user who has access to the ServiceNow REST API.

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 ServiceNow plugin. This plugin is an Authentication and Authorization (AA) plugin customized to work with ServiceNow.
- SPS must be able to access the Internet (at least the API services). Since ServiceNow is a cloud-based service provider, SPS must be able to access its web services to authorize the user.

  The connection also requires the ServiceNow ticket ID.
- SPS supports AA plugins in the MSSQL, 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.
- 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 ServiceNow plugin is available for download as-is, free of charge to every SPS customer from the ServiceNow 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.

About us

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