One Identity Safeguard for Privileged Sessions 6.0

How to connect One Identity Safeguard for Privileged Passwords with One Identity Safeguard for Privileged Sessions

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.

SPS How to connect One Identity Safeguard for Privileged Passwords with One Identity Safeguard for Privileged Sessions
Updated - April 2020
Version - 6.0

Contents

1

Introduction

This tutorial describes how you can connect One Identity Safeguard for Privileged Sessions (SPS) and your One Identity Safeguard with a Credential Store Plugin.

SPS can interact with the One Identity Safeguard and can automatically retrieve the password of the target host to form a comprehensive Privileged Access Management solution to protect critical assets and meet compliance requirements.

2

Technical requirements

To successfully connect SPS with One Identity Safeguard, you need the following components:

- A valid, working One Identity Safeguard server or cluster of servers with the following configuration:
  - Access request policy configured for auto-approval, because the plugin does not wait for manual approval, rather immediately checks out the password.
  - Simultaneous access for the access request policy to enable multiple sessions.
  - In case of explicit authentication:
    - A proxy user must be created on the Safeguard vault that has access to start access request the accounts/assets. The plugin will be using this "proxy user" to access Safeguard Vault.
  - In case of gateway-based authentication:
    - SPS reuses the username/password from the gateway authentication to authenticate on the Safeguard Vault. This requires password-based gateway authentication on SPS and that the same user is available on the Safeguard Vault with the same password. The best way is to use an LDAP/AD-based authentication backend.
- A SPS appliance (virtual or physical), at least version 4 F3.
- A Credential Store plugin for One Identity Safeguard.

  SPS uses plugins to interact with third-party credential stores and password vaults. One Identity provides the sample One Identity Safeguard plugin free of charge, and provides help to customize it for your environment.

How SPS and One Identity Safeguard work together

Starting access request

The Credential Store plugin can start a new access request and can checkout and checkin passwords. Right now, one access request is used for each session, access requests are not reused. The access request policy must be configured for auto-approval, because the plugin does not wait for any manual approval, rather immediately checks out the password. It is recommended to allow simultaneous access (for the access request policy) to enable multiple sessions (at least as long as access request reuse is not implemented).

Authentication

The plugin can use either explicit or gateway-based credentials.

- *Explicit authentication:*

  A proxy user must be created on the Safeguard Vault that has access to start access request the accounts/assets. The plugin will be using this "proxy user" to access Safeguard Vault.

- *Gateway-based authentication:*

  SPS reuses the username/password from the gateway authentication to authenticate on the Safeguard Vault. This requires password-based gateway authentication on SPS and that the same user is available on the Safeguard Vault with the same password. The best way is to use an LDAP/AD-based authentication backend.

Asset and account lookup

Depending on settings and runtime environment, the plugin does one or more asset-account pair lookups. If the asset-account pair exists, the plugin does not check if the account has a password or if the user can check out a password, it rather tries to check out the password directly. If the user does not have permission to start an access request for a password or if the account is not found, autologin fails. Autologin also fails if the account has already been checked out (either by the same or any other user).

The account is always taken to be the remote server username, and it is compared to the Safeguard account name in a case insensitive manner. The list of assets for the account is generated according to the following sequence:

1. The IP address of the remote server.
2. If the IP resolving option is turned on, then the hostnames returned by the built-in DNS reverse lookup on SPS.
3. The remote server domain name if it is present in the connection (for example, when using RDP). This domain name is potentially expanded with a configurable suffix.

NOTE:

Once a checkout with one pair is successful, the sequence is stopped and not restarted even if the password was unusable in the end.

Safeguard cluster

When there are multiple Safeguard addresses, the plugin will try every checkout-checkin operation on the first specified address and will fail over to the next address(es) if the address was unreachable.

4

Configuring SPS

This section provides detailed instructions as to what to configure on SPS:

Using a custom Credential Store plugin to authenticate on the target hosts

The following describes how to configure One Identity Safeguard for Privileged Sessions (SPS) to retrieve the credentials used to login to the target host using a custom plugin.

Prerequisites

To use a custom Credential Store plugin, you have to upload a working Credential Store plugin to SPS. This plugin is a script that can be used to access an external Credential Store or Password Manager. If you want to create such a custom Credential Store plugin, contact our Support Team or see or see the documentation about custom Credential Store plugins.

NOTE:

Users accessing connections that use Credential Stores to authenticate on the target server must authenticate on SPS using gateway authentication. Therefore, gateway authentication must be configured for these connections. For details, see "Configuring gateway authentication" in the Administration Guide.

To upload the custom Credential Store plugin you received, navigate to **Basic Settings > Plugins > Upload/Update Plugins**, browse for the file and click **Upload**.

NOTE:

It is not possible to upload or delete Credential Store plugins if SPS is in sealed mode.

Your plugin `.zip` file may contain an optional sample configuration file. This file serves to provide an example configuration that you can use as a basis for customization if you wish to adapt the plugin to your site's needs.

To configure SPS to retrieve the credentials used to login to the target host using a custom plugin

1. Navigate to **Policies > Credential Stores**.
2. Click + and enter a name for the Credential Store.
3. Select **External Plugin**, then select the plugin to use from the **Plugin** list.
4. If your plugin supports configuration, then you can create multiple customized configuration instances of the plugin for your site. The **Configuration** textbox displays the example configuration of the plugin you selected. If you wish to create a customized configuration instance of the plugin for your site, then edit the configuration here.

   NOTE:

   Plugins created and issued before the release of SPS 5 F1 do not support configuration. If you create a configuration for a plugin that does not support this, the affected connection will stop with an error message.

5. Click 

.
6. Navigate to the Connection policy where you want to use the Credential Store (for example, to **SSH Control > Connections**), select the Credential Store configuration instance to use in the **Credential Store** field, then click 

.

Configuring other related parameters

Steps:

To configure other related parameters

1. Navigate to **Policies > Usermapping Policies** and configure a usermapping policy. For details, see "Configuring usermapping policies" in the Administration Guide.
2. Depending on your requirements, configure an LDAP policy, or a Local User Database for gateway authentication.
   - To configure an LDAP policy, navigate to **Policies > LDAP Servers**. For details, see "Authenticating users to an LDAP server" in the Administration Guide.
   - To configure a Local User Database, navigate to **Policies > Local User Databases**. For details, see "Creating a Local User Database" in the Administration Guide.

3. Navigate to **SSH Control > Authentication Policies** and configure the authentication policy with gateway authentication. For details, see "Authentication Policies" in the Administration Guide.
4. Navigate to the Connection policy where you want to use the Credential Store (for example, to **SSH Control > Connections**), select the Credential Store configuration instance to use in the **Credential Store** field. Select the Authentication Policy that you have configured in **Authentication policy** field, and the Usermapping Policy in the **Usermapping policy** field.

SPS One Identity Safeguard Credential Store plugin parameter reference

To configure the plugin, you must edit the parameters in the `config_local.py` file.

The following is a sample configuration file for gateway authentication:

```
[safeguard]
address=<address-of-the-safeguard>
ca=<optional-ca-certificate-for-ssl-verification>
check_host_name=1

[auth]
use_credential=gateway
# provider=<provider-for-explicit-or-gateway>
# username=<username-only-for-explicit>
# password=<provider-only-for-explicit>
```

[safeguard]

address

Type: string

Description: The IPv4 address(es) or hostname(s) of the One Identity Safeguard machine or cluster. Use a comma (,) to separate multiple IP addresses/hostnames, ensuring that there is no space inserted around commas.

For example:

`address=10.0.0.5,10.0.0.6`

ca

Type: string

Description: Optional. The certificate authority (CA) certificate to use for validating the server certificate of Safeguard Vault server(s). The certificate must be in the PEM format. Multi-line values must be specified in the following way:

- Starting from the second line, each line must begin with a space character.
- There must be an empty line after the certificate value.

For example:

```
ca=-----BEGIN CERTIFICATE-----
  MIIGxzCCBK+gAwIBAgITOgAABd9VJ2E4MStYlQAAAAAF3zANBgkqhkiG9w0BAQsF
  ...
  Qpdb3REB/BfQLbA=
  -----END CERTIFICATE-----
```

check_host_name

Type: boolean (`no` | `yes`)

Description: If set to `no`, there is no host name checking. The default value is `yes` for strict host name checking, only when the parameter `ca` has been configured too.

For example:

```
check_host_name=yes
```

ip_resolving

Type: boolean (`no` | `yes`)

Description: Used when the target servers are listed under their hostname in Safeguard Vault as assets.

If set to `no`, this parameter has no effect. If set to `yes`, the plugin will resolve the IP address of the remote server to hostname(s) and attempt the password checkout using the hostname(s) as well. See Asset and account lookup on page 6 for details on the order in which the attempts are made. DNS resolution uses the DNS server specified for SPS (in the **Basic Settings > Network > Naming > Primary DNS server** and **Secondary DNS server** fields on SPS's web interface).

For example:

```
ip_resolving=yes
```

domain_suffix

Type: string

Description: If users do not provide the full domain name in the connection, this option can be used to automatically expand the domain name with a suffix.

For example:

```
domain_suffix=acme.org
```

If the user provides the credentials "user\backoffice", then the domain part will be replaced with "backoffice.acme.org". Note the automatically added dot (.). See Asset and account lookup on page 6 for details on when and how the domain name is used in the attempts to check out the password.

[auth]

use_credential

Type: string (`explicit` | `gateway`)

Description: To determine whether the authentication method is explicit authentication or gateway authentication. The default value is `gateway`.

> NOTE:
>
> Gateway authentication towards One Identity Safeguard for Privileged Passwords is not possible with RDP, because the protocol does not transfer the gateway password.

For example:

```
use_credential=gateway
```

provider

Type: string

Description: Determines which provider should SPP use to authenticate the user.

The default value is `local`. This is used when the username and password have been added in Safeguard.

If the username and password come from Active Directory, specify a provider value. To find out your provider value, complete the following steps:

In case of Safeguard 2.4 or newer:

1. Access the Core Shell on SPS or use the terminal on any Linux machine.
2. Enter the following command: `curl -k 'https://<One Identity Safeguard for Privileged Passwords-IP-address-or-hostname>/service/core/v2/AuthenticationProviders' | jq`
3. In the response returned, look for the `RstsProviderId` parameter. The value is your provider value.

> **Example: Provider value in Safeguard 2.4 or newer**
>
> If you see the following in the response:
>
> ```
> "RstsProviderId": "ad4",
> ```
>
> In this example, the value of `provider` would look like the following:
>
> ```
> provider=ad4
> ```

In case of Safeguard 2.3 or earlier:

1. Access the Core Shell on SPS or use the terminal on any Linux machine.
2. Enter the following command: `curl -k 'https://<One Identity Safeguard for Privileged Passwords-IP-address-or-hostname>/RSTS/UserLogin/LoginController?response_type=token&redirect_uri=urn:InstalledApplication&loginRequestStep=1' | jq`
3. In the response returned, look for the `PrimaryProviderID` parameter. The value is your provider value.

> **Example: Provider value in Safeguard 2.3 or newer**
>
> If you see the following in the response:
>
> ```
> "PrimaryProviderID": "ad3",
> ```
>
> In this example, the value of `provider` would look like the following:
>
> ```
> provider=ad3
> ```

username

Type: string

Description: The username that SPS uses to log in to One Identity Safeguard. Only if the value of `use_credential` has been configured to `explicit`. For example:

```
username=<username>
```

password

Type:	string

Description: The password that SPS uses to log in to One Identity Safeguard. Only if the value of `use_credential` has been configured to `explicit`.

For example:

```
password=<password>
```

6

Learn more

To find out more about SPS, visit the SPS homepage.

If you need help connecting One Identity Safeguard with One Identity Safeguard for Privileged Sessions, request a callback or contact our Professional Services Team.

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