



# Privileged Account Manager User Guide

December 2020

## **Legal Notice**

For information about Micro Focus legal notices, see <https://www.microfocus.com/about/legal>.

© Copyright 2020. Micro Focus or one of its affiliates.

<b>1</b>	<b>Welcome to Privileged Account Manager</b>	<b>5</b>
<b>2</b>	<b>Accessing Resources</b>	<b>7</b>
	Windows .....	7
	SSO to Windows Session Using Privileged Account Manager Proxy .....	7
	SSO to Windows Session Using Privileged Account Manager Credential Provider .....	8
	Direct Access to Windows Machine .....	9
	Linux, UNIX, Mainframes, and Network Devices .....	9
	Using SSH Relay .....	9
	Using Privileged Shell .....	10
	Database .....	11
	Application SSO .....	11
	Launch from User Console .....	11
	Launch Using Remote Desktop Connection .....	11
	Applications, Shared Keys, and Cloud Services .....	12
	Checking Out Credentials .....	12
	Checking In Credentials .....	13
	Viewing Credential Checkout History .....	13
<b>3</b>	<b>Understanding Tags</b>	<b>15</b>
	Tagging Resource Accesses .....	15
	Create and Apply Tag .....	16
	Apply Existing Tag .....	16
	Remove Tag .....	16
<b>4</b>	<b>Creating an Emergency Access Request</b>	<b>17</b>
<b>5</b>	<b>Viewing Emergency Access Request History</b>	<b>19</b>
<b>6</b>	<b>Managing API Tokens</b>	<b>21</b>
	Generating and Using API Tokens .....	21
	Using API Tokens .....	22
<b>7</b>	<b>Importing and Exporting Configuration</b>	<b>25</b>
<b>8</b>	<b>Viewing Alerts and Notifications</b>	<b>27</b>



# 1 Welcome to Privileged Account Manager

Privileged Account Manager (PAM) helps an organization to protect its critical assets and maintain the compliance requirements by securing, managing, and monitoring privileged accounts for privileged access. It is capable of managing the shared accounts and also auditing those accounts. You can monitor all the actions performed in the servers for Windows, Linux, database, or any application such as, LDAP.

For more information about this software, see the [Privileged Account Manager documentation](#).



# 2 Accessing Resources

The **Home** page displays all the resource accesses that are granted to you through Privileged Account Manager policies or by creating a request. You can access the resources in the following ways based on the type of policy configured by the administrator:

- ◆ Launch the session from the user console and Privileged Account Manager does a single sign on to the resource.
- ◆ Check out the credentials from the user console and use them to connect to the resource.
- ◆ Directly access the resource using the server credentials or user console credentials based on the policy defined. These resource accesses are not displayed in the user console as you cannot launch these sessions from the user console. However, you can create an emergency access request for these type of accesses.

In all the above scenarios, if the administrator has enabled secondary authentication, then you must pass secondary authentication.

---

**NOTE:** When you are accessing the resource, if a risky or a suspicious activity is detected, your session will be disconnected automatically based on the policy defined by the administrator.

---

The following sections explain how to access the sessions of various resources:

- ◆ [Windows](#)
- ◆ [Linux, UNIX, Mainframes, and Network Devices](#)
- ◆ [Database](#)
- ◆ [Application SSO](#)
- ◆ [Applications, Shared Keys, and Cloud Services](#)

## Windows


You can start the Windows session in the following ways based on the type of access granted to you by the administrator:

- ◆ [“SSO to Windows Session Using Privileged Account Manager Proxy” on page 7](#)
- ◆ [“SSO to Windows Session Using Privileged Account Manager Credential Provider” on page 8](#)
- ◆ [“Direct Access to Windows Machine” on page 9](#)

### SSO to Windows Session Using Privileged Account Manager Proxy

These are remote desktop sessions to target computers through Privileged Account Manager proxy where Privileged Account Manager does a single sign on as a privileged user.

### To launch the Windows SSO session:

- 1 You can launch a Windows session by clicking either of the following:
  - ◆ **Resource Name:** Allows you to select the display resolution of the RDP session to the target machine and add session notes before launching the session.
  - ◆ **The  Icon:** Allows you to download launch the session.


An RDP file is downloaded after you click either of the above.

- 2 Save and open the RDP file to launch the session.

The downloaded RDP file is valid only for 1 minute. After 1 minute, repeat the above steps to download a new RDP file. These RDP files are not deleted automatically. Hence, after using delete these files manually.

## Launching Live Session Using RDP Web Relay

Privileged Account Manager now allows administrators to provision privilege access without a need for an agent on the target host, which the provisioned users can access without the need of any

client application, from within their browsers. You can launch the session using the  icon which allows you to launch the live session for RDP web relay. You can now monitor all the live sessions using **Active Sessions**.

## SSO to Windows Session Using Privileged Account Manager Credential Provider

These are remote desktop sessions to target computers that can be accessed using your user console credentials. These resource accesses are not displayed in the user console as you cannot launch these sessions from the user console.

To start a remote desktop connection by using credential provider, you must save the Remote Desktop Connection to a separate file, which creates a shortcut for the remote desktop session. You can directly launch the Remote Desktop Connection from the shortcut you created.

### Perform the following steps to save the Remote Desktop Connection to a separate file:

- 1 Open the Remote Desktop Connection client.
- 2 Specify the IP address of the target computer.
- 3 Click **Options** and then click **Save As** to save the Remote Desktop connection as a separate file.
- 4 Add the following to the saved Remote Desktop Connection file by using a text editor and save the file:

```
enablecredsspssupport:i:0
```
- 5 Click the saved Remote Desktop Connection file.

For subsequent sessions you can just click the saved **Remote Desktop Connection** icon.
- 6 Click the Credential Provider tile.
- 7 Specify your user console credentials to log in to the computer.



---

**NOTE:** Ensure that you provide the user name in uppercase.

---

## Direct Access to Windows Machine

These are direct sessions to the computer using the respective server credentials where Privileged Account Manager authorizes the access. This type of resource accesses are not displayed in the user console, as you cannot launch these sessions from the user console.

## Linux, UNIX, Mainframes, and Network Devices

You can access resources such as, UNIX or Linux machines, Mainframes, or network devices in the following ways based on the policies defined by administrator:

- ◆ [Using SSH Relay](#)
- ◆ [Using Privileged Shell](#)

### Using SSH Relay

SSH Relay allows you to access the target computer through Privileged Account Manager proxy where the Privileged Account Manager does a single sign on as a privileged user. You can launch the SSH relay sessions in the following ways:


- ◆ [“Launch from User Console” on page 9](#)
- ◆ [“Launching Live Session Using SSH Web Relay” on page 10](#)
- ◆ [“Launch Using SSH Client” on page 10](#)

### Launch from User Console

#### Prerequisites:

You must have JRE installed for the JNLP file to launch. For information about the supported JRE versions, see the [Technical Information for Privileged Account Manager](#).

#### To launch an SSH or a Telnet session:


- 1 You can launch the SSH session by clicking either of the following:
  - ◆ **Resource Name:** Allows you to add session notes before launching the session.
  - ◆ **The  icon:** Allows you to download the session without adding notes. A JNLP file is downloaded.
- 2 Save and open the JNLP file to launch the Java user interface.

In Edge browser, modify the default program for launching the JNLP file to `javaws.exe`.
- 3 Specify your user console credentials to start the session.

The downloaded JNLP file is valid only for 1 minute. After 1 minute, repeat the above steps to download a new JNLP file. These files are not deleted automatically. Hence, after using delete these files manually.

## Launching Live Session Using SSH Web Relay

Privileged Account Manager now allows administrators to provision privilege access without a need for an agent on the target host, which the provisioned users can access without the need of any

client application, from within their browsers. You can launch the session using the  icon, which allows you to launch the live session for SSH web relay. You can now monitor all the live sessions using [Active Sessions](#).

## Launch Using SSH Client

To launch the SSH Relay session using SSH client:

- 1 Open the SSH client.
- 2 (conditional) If you know the target hostname and the target user as whom you want to access the computer, use the following command:

To initialize an SSH session:

```
ssh -t -p2222 <PAMuser@PAMsshrelayhost> <targetuser@targethostname>
```

To initialize an SSH relay session with X11 forwarding, use the command:

```
ssh -X -t -p2222 <PAMuser@PAMsshrelayhost> <targetuser@targethostname>
```

- 3 (Conditional) If you do not know the target host name, perform the following:

**3a** To initialize an SSH session, use the command:

```
ssh -t -p2222 <PAMuser@PAMsshrelayhost>
```

To initialize an SSH relay session with X11 forwarding, use the command:

```
ssh -X -t -p2222 <PAMuser@PAMsshrelayhost>
```

A list of all the available SSH sessions are displayed.

- 3b** Enter the appropriate option to start the respective SSH session and provide your user console credentials.

---

**NOTE:** When you exit from the SSH session, all the available SSH Relay sessions are displayed again that enables you to connect to a different target system.

---

## Using Privileged Shell

Using privileged shell you can gain elevated access to the Linux or Unix machine. These resource accesses are not displayed in the user console as you cannot launch these sessions from the user console.

To access privileged sessions on Linux or UNIX systems, perform the following:

- 1 Log in to the required system using the SSH client as a non-privileged user.
- 2 Specify `usrun pcksh` or `usrun shell`.
- 3 Execute the commands that require privileged access.

# Database

You can access a database through Privileged Account Manager proxy in the following ways:

- ♦ **Using Checked Out Credentials:** If you do not know the database credentials, you can check out the credential from the user console and use them on any database client along with the proxy IP address and port to connect to the database. For more information about checking out the database credentials, see [Checking Out Credentials](#).

You can also generate API tokens for checking out and checking in the credentials through REST API. For more information about API tokens, see [Managing API Tokens](#).

- ♦ **Using Database Credentials:** If you know the database credentials, use the proxy IP address, port number, and the database credentials on any client to connect to the database. This type of database accesses are not displayed in the user console.

For the Privileged Account Manager proxy IP address and port number, contact the administrator.

## Application SSO


You can do a single sign on to applications that are configured for you in the following ways based on the policies defined by the administrator:

- ♦ [“Launch from User Console” on page 11](#)
- ♦ [“Launch Using Remote Desktop Connection” on page 11](#)

### Launch from User Console

You can launch the application from the user console and Privileged Account Manager does a single sign on to the application.

**To launch the application from user console, perform the following:**

- 1 You can launch the application by clicking either of the following:
  - ♦ **Resource Name:** Allows you to add session notes before launching the session.
  - ♦ **The  icon:** Allows you to launch the session without adding notes.

An RDP file is downloaded, when you click either of the above.

- 2 Save and open the downloaded RDP file.

Application launches and Privileged Account Manager does a single sign on for you to use the application.

### Launch Using Remote Desktop Connection

You can start a remote connection to a Windows server and Privileged Account Manager does a single sign on when you launch the application. This types of resource accesses are not displayed in the user console as you cannot launch these sessions from the user console.

### To launch the application:

- 1 Open the Remote Desktop Connection client.
- 2 Specify the IP address of the target machine that has the application installed.
- 3 Specify your user console credentials.
- 4 Right-click the application you want to access and select **Run as privileged user**.

Application launches and Privileged Account Manager does a single sign on as a privileged user for you to use the application.

## Applications, Shared Keys, and Cloud Services

For accessing resources such as, applications, shared keys, and cloud services, you must check out the credentials from the user console and use the appropriate client to access the resource. You can use these credentials until the access duration expires.

You can perform credential check out for the following:

- ♦ **Shared Keys:** Key for any application, such as license key to install an application.
- ♦ **Applications:** Credentials to access any application. The application can be LDAP, eDirectory, ESXi Server, SAP, Linux, AIX and Windows.
- ♦ **Cloud Services:** Credentials to access cloud platforms such as, AWS, Openstack and Microsoft Azure.

You can also generate API tokens for checking out and checking in the credentials through REST API. For more information about API tokens, see [Managing API Tokens](#).


The following sections explain the credential check in and check out process in detail:

- ♦ [Checking Out Credentials](#)
- ♦ [Checking In Credentials](#)
- ♦ [Viewing Credential Checkout History](#)

## Checking Out Credentials

When you check out the credentials, the credentials are valid only for the requested access duration. To access the resource after the access duration expiry, you must check out the credentials again if it is an access granted through Privileged Account Manager policy. If it is an emergency access, you must create a new request. For shared keys, there is no expiry.

### To check out the credentials, perform the following:

- 1 Select the appropriate resource type such as database, application, cloud services, and so on.
- 2 You can check out the credentials by clicking either of the following:
  - ♦ **Resource Name:** Allows you to add notes before checking out the resource credentials.
  - ♦ **The  icon:** Allows you to check out the resource credentials without adding notes.
- 3 Specify the access duration, email address, and reason for credential check out.
- 4 Click **Check Out**.


- 5 The credentials are visible only for 10 seconds. After 10 seconds, click **Show Credentials** to view the credentials.

You can also copy the password by clicking **Copy to Clipboard**.

After you check out the credentials, the resources for which the credential is checked out can be viewed from **Home > Checked Outs**.

## Checking In Credentials

You must check in the checked out credentials after the access duration expiry for Privileged Account Manager to reset the credentials. If you do not check in the credentials, Privileged Account Manager automatically checks in the credentials. After every check in, Privileged Account Manager resets the credentials for all resource types except shared keys.

To check in the credentials quickly, click  of the appropriate resource. If you want to view the credentials before checking in, perform the following:

- 1 Click the appropriate resource name.
- 2 Click **Show Credentials** and complete the authentication process to view the credentials.
- 3 Click **Check In**.

## Viewing Credential Checkout History

Go to **Home > Checkouts** to view the history and current status of credential checkouts.



# 3 Understanding Tags

Tags are customized labels given to the resource access groups to help you identify, organize, and search the resource accesses easily. The tags are categorized into the following:

- ♦ **Predefined Tags:** Predefine set of resource access groups which you cannot edit or delete.

This group is further categorized as follows:

- ♦ **Emergency Access:** Emergency access requests that are in approved or pending state. When you do not have access to a resource, you can create an emergency access request to a resource for a limited time period. These emergency access requests are sent to the administrator and are approved or denied based on the administrator's discretion. When the request is approved, you can access the resource for the requested duration.
- ♦ **Checked Out Credentials:** Resources for which the credentials are checked out. These resources can be a database, shared key, application, or cloud service for which the credentials are checked out.
- ♦ **Groups based on the resource or connection type:** For example, Windows, SSH/Telnet, Applications, and so on, where **Windows** group lists all the Windows servers you can access and so on.
- ♦ **User Defined Tags:** Resource access groups created by you. For more information about creating custom groups and tagging resource accesses to these groups, see [Tagging Resource Accesses](#).

## Tagging Resource Accesses

You can create a tag and add one or more resource accesses to a tag. You can also add the same resource access to multiple tags. The tags created by you are displayed in **Home > My Access > User Defined Tags**.

The tags created by you are stored in the browser cache. If you switch browsers or clear cache, the tag configuration will be deleted. To reuse tags, you must export and import the tag configuration wherever required. For more information about exporting and importing tags, see [Importing and Exporting Configuration](#).

You can select one or more resource accesses and perform one of the following:

- ♦ [“Create and Apply Tag” on page 16](#)
- ♦ [“Apply Existing Tag” on page 16](#)
- ♦ [“Remove Tag” on page 16](#)

## Create and Apply Tag

To create and add the resource accesses to the tags, perform the following:

You can also apply multiple tags to each privileged access.

- 1 Select one or more resources.
- 2 Click **Tag**.
- 3 (Conditional) If there are no tags, perform the following:
  - 3a Specify the tag name.
  - 3b Click **Create Tag and Apply**.
- 4 (Conditional) If there are tags and you want to add a new tag, perform the following:
  - 4a Click **Create Tag**.
  - 4b Specify the tag name.
  - 4c Click **Create Tag and Apply**.

## Apply Existing Tag

- 1 Select one or more resources.
- 2 Click **Tag**.
- 3 Select a tag from the list or search for the tag.
- 4 Click **Choose Existing** of the appropriate tag name.

All the selected tags are displayed above the Search text box.
- 5 Click **Apply Changes**.

## Remove Tag

To remove a tag from a resource, perform the following:

- 1 Select one or more resources.
- 2 Click **Tag**.
- 3 (Conditional) To remove specific tags, click **X** on the appropriate tag name.
- 4 (Conditional) To remove all the tags added to the selected resource, click **Clear Selection**.
- 5 Click **Apply Changes**.



# 4 Creating an Emergency Access Request

Emergency access request is a request to access a resource for a limited time period. You can create an emergency access request in the following scenarios:

- ◆ When you do not have access to the resource.
- ◆ When you have access to the resource, but it is not active because the access is granted only for a specific time interval. For example, you are granted access to a Windows server from 10.00 a.m. to 5.00 p.m. After 5.p.m. though it is displayed in the user console, you cannot access the resource. In this scenario, you can create a request.

You can create an emergency access request for any type of resource except shared keys.

When you create a request,

1. The request is sent to the administrator and it is approved or denied based on the administrator's discretion.

You can view the pending requests at [Home > My Access > Predefined Tags > Emergency Access > Pending](#).

2. When the request is approved, you are authorized to access the respective resource.

After approval, you can access the request from [Home > My Access > Predefined Tags > Emergency Accesses > Approved](#).

3. When the request is denied or revoked by the administrator, you will receive an alert. You can click the Bell icon on the top-right corner of the page to view the alerts.

**To create an emergency access request, perform the following:**

- 1 Click [My Access > New Request](#).
- 2 Select the **Target** you want to access.
- 3 Based on the selected target configure the following:

Target	Fields
Windows	<p><b>Connection Type:</b></p> <p>Select <b>SSO</b> when you need privileged single sign on access to Windows. When you select this option you get single sign on access through Privileged Account Manager proxy as well as Privileged Account Manager credential provider.</p> <p>Select <b>Direct Access</b> when you want to access the Windows directly using the server credentials.</p>

Target	Fields
SSH/Telnet	<p><b>Connection Type:</b> Select <b>SSH</b> or <b>Telnet</b> based on the connection method the target system supports.</p> <p><b>Enable X11:</b> Select this option to get X11 application access through SSH.</p>
Database	<p><b>Database:</b> Select the database you want to access.</p> <p><b>Password Checkout:</b> Select this option to check out credentials to access the database.</p> <p><b>Database Access:</b> Select this option when you know the credentials to access the database but you need access to the database through Privileged Account Manager proxy.</p>
Privileged Shell	Choose this option to get elevated access to the UNIX/Linux workstation using your local credentials.
Application SSO	<b>Application:</b> Select the application or computer you want to access.
Application Credential	<b>Application:</b> Select the application for which you want to get the credentials.
SSH Web Access	<p><b>Connection Type:</b> Select <b>SSH</b> or <b>Telnet</b> based on the connection method the target system supports.</p> <p>All the current running sessions can be seen in <b>Active Sessions</b>.</p>
Windows Web Access	<p><b>Connection Type:</b> Select the Windows resource you want to access.</p> <p>All the current running sessions can be seen in <b>Active Sessions</b>.</p>

**4** Specify the following details common to all the target resources:

**Hostname/IP Address:** Specify the hostname or IP address of the target resource which you want to access, wherever applicable.

**Access As:** Select **Normal User** when you want access to the resource without any privileges. Select **Super User** when you want privileged access to the resource.

**Access Duration:** Specify how long you want access to the resource.

**Email:** Specify the email address for receiving notification about the status of the request.

**Reason:** Specify the reason for this request.

**5** Click **Create**.


When the request is created, an email notification is sent to you. Whenever the state of the request changes, you will receive a notification in the user console and also through an email.

# 5 Viewing Emergency Access Request History

Select **Home > Requests** to view the history and current status of your emergency access requests. The status can be one of the following:

- ♦ **Pending:** These are the requests that are pending actions from the administrator. You can cancel the requests in pending state.

**To cancel a pending request, perform the following:**

1. Select **Home > Predefined Tags > Emergency Access > Pending**.
  2. (Conditional) To cancel multiple requests, perform the following:
    - a. Select one or more requests.
    - b. Click **Cancel Request**.
  3. (Conditional) To cancel one specific request, perform the following:
    - a. Click  of the appropriate request.
    - b. Click **Cancel Request**.
- ♦ **Approved:** These are the requests approved by the administrator. You can access the approved requests from **Home > Predefined Tags > Emergency Access**. For more information about how to access the different types of resources, see [Accessing Resources](#).
  - ♦ **Denied:** These are the requests denied by the administrator due to a specific reason, which is specified in the request. You can access the approved requests from **Home > Requests**.
  - ♦ **Revoked:** These are requests approved by the administrator and revoked later due to a specific reason, which is specified in the request.
  - ♦ **Expiring:** These are the requests about to expire in 15 minutes.
  - ♦ **Expired:** These are the requests which have already expire.







# 6 Managing API Tokens

API token is a method used for REST API authentication. You can generate API token from Privileged Account Manager and include them in the Privileged Account Manager REST API request for authentication. This REST API request can then be included in scripts, configuration files, applications, processes, and so on as required.

For example, you may have several scripts, applications, processes, and so on to perform some automated task in any application. They must be authenticated before performing any operation on the application. These authentication credentials are usually included in clear text, which is a security issue. To overcome this issue, Privileged Account Manager enables you to use API tokens in REST API requests for checking out the credentials of an application. In this way, the privileged account credentials are not exposed.

For information about how to generate and use API tokens, see [Generating and Using API Tokens](#). After generating the token, you can perform the following operations on the token:

- ◆ **Copy Token to Clipboard:** Click  to copy the token to the clipboard. You can use this copied token on the appropriate REST API request for authentication.
- ◆ **Modify Token:** Click  to modify the token details, such as extending the expiry time of the token, adding or removing host in the hosts list from which the token can be used, and so on.
- ◆ **Revoke Token:** Click  to revoke a token, if you identify that the token is compromised.  
The administrator can also revoke a token. You will receive a notification, if your token is revoked by the administrator.  
Whenever a token is revoked, you must replace the revoked token with a new token wherever the revoked token is used.
- ◆ **Check In Credentials:** Click  to check in the credentials checked out using the token.

## Generating and Using API Tokens

You can generate an API token for an application and use the token in the required REST API request. You can generate multiple tokens for one application. You can generate tokens for all the resources for which you can check out credentials from the user console.

To generate an API token, perform the following:

- 1 Select the appropriate resource for which you need to generate a token.  
For example, if you want to generate a token for a database, select **Predefined Tags > Databases** and then select the required database.
- 2 Click **API Token > Generate Token**.
- 3 Specify the following details:

**Token Expiry:** Duration for which the token is valid.

Select **Set Expiry** if you want the token to be disabled after a specific duration and select the appropriate expiry date and time. These tokens expire after the configured duration. If you want to use the token after expiry, you can edit the token and modify the expiry duration.

Select **Never** if you do not want the token to expire.

**Token Name:** Name to identify the token.

**Access From:** Represents the host from which the token can be authenticated.


Select **Any Host** to allow token access from any host.

Specify the **Host IP / Host Name** to allow the token access only from those hosts. To specify multiple hosts, use comma as a separator.

**Notes:** Any additional information about this token.

4 Click **Generate Token**.

The generated token is added to the API Tokens list.

5 Click  to copy the appropriate token and use it as required. For more information about how to use tokens, see [Using API Tokens](#).

## Using API Tokens

After generating the tokens, copy the token and add it to the appropriate REST API request as needed to authenticate the request.

### Usage Scenario:

For example, if you have a script that performs some operation on the database, the script must be authenticated for valid authorization. To enable the script for authentication, perform the following:

1. Generate the token for the specific database from the user console.
2. Copy and paste the generated token to the credential check-in and checkout REST API requests as described in the following sample:

### Sample REST API for Credential Check Out Using Tokens

◆ **Request:**

```
curl --insecure -X POST -H "Authorization:Token token=<API_Token>" -
H "Cache-Control: no-cache" -H "Content-Type:application/json" -d '{
  "Request": {
    "type": "PasswordCheckout",
    "runHost": "<Specify the target resource for
which you want the credentials.>",
    "reason": "<Reason for credential checkout.>",
    "duration" : "<Specify the credential expiry
duration in minutes. >",
    "emailid": "<Specify your email address to get
notifications. >"
  }
}' "https://<PAM_SERVER>/rest/cmdctrl/Request"
```

◆ **Response:**

```
{
  "CheckOut": {
    "Request": {
      "id": "<Request Id>"
    },
    "account": "<username>",
    "passwd": "<password>"
  },
  "message": "OK",
  "status": 200,
  "vrm": "3.5.0"
}
```

**Sample REST API for Credential Check In Using Tokens**

◆ **Request:**

```
curl --insecure -X PUT -H "Authorization:Token token=<API-Token>" -H "Cache-Control: no-cache" -H "Content-Type:application/json" -d '{
  "Request": {
    "type": "PasswordCheckin",
    "runHost": "<Specify the target resource whose
credentials must be checked in.>"
  }
}' "https://<PAM_SERVER>/rest/cmdctrl/Request/<Request Id>"
```

◆ **Response:**

```
{
  "message": "OK",
  "status": 200,
  "vrm": "3.5.0"
}
```

3. Include the credential check out and the check in REST API requests with the token in the script.

The database authentication credentials are received as a response of the REST API request, which must be used by the script for logging in to the target application.

Ensure that you call the REST API for credential check out and check in at the beginning and end of the script respectively.





# 7 Importing and Exporting Configuration

Select the logged in user name at the top right corner and select **Import Configuration** or **Export Configuration** to import and export configurations respectively.


Privileged Account Manager stores some of your user console configurations in the browser cache. These configurations are:

- ◆ **User Defined Tags:** Customized groups of resource accesses granted to you.
- ◆ **Notes:** Personalized notes that you have added on any resource accesses issued to you.

You will lose these configurations when you switch browsers or clear browser cache. To reuse these configurations, export and import them when accessing a different browser or after clearing the browser cache.



# 8 Viewing Alerts and Notifications

Click  at the top-right corner to view alerts and notifications.

Privileged Account Manager displays alerts or notifications in the following scenarios:

- ◆ When the status of the request changes to approved, revoked, or denied.
- ◆ When the credentials are forcefully checked in by administrator.
- ◆ When the credentials are checked in automatically after expiry.
- ◆ When the API tokens are revoked by the administrator.
- ◆ When the API tokens are added to you and when your tokens are transferred to another user.

