Legal Notice

Copyright 2009 - 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/.
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.
Accessing Privileged Account Manager Console

You can access Privileged Account Manager console using an URL similar to the format https://<my-pam-server>/pam. If you have configured OAuth as authentication server, use the Privileged Account Manager using the URL similar to the format https://pam_ip_or_dns/sso.
Accessing Resources

There are a set of resources on which the privilege access needs to be controlled and secured. And depending on organizations needs there can be multiple resources having similar privilege access and security requirement, which might be based on their usage, location, criticality to business and many other similar factors. You can access the resources either from the Web console or from thick clients from respective sources.

The My Access page displays all the resource accesses that are granted to you through Privileged Account Manager policies or by creating a request.

The left pane displays all the resource accesses based on the resource and type.

**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 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:** 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 access the Web RDP session.
Accessing Resources

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 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
- Launch Using SSH Client

Launch from User Console

To launch an SSH or a Telnet session:

1. You can launch the SSH session by clicking either of the following:
   - Resource: Allows you to add session notes before launching the session.
   - The icon: Allows you to access the Web SSH session.

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 -p 2222 <PAMuser@PAMsshrelayhost> <targetuser@targethostname>
   - To initialize an SSH relay session with X11 forwarding, use the command:
     ssh -X -t -p 2222 <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 and provide your user console credentials:
     ssh -t -p 2222 <PAMuser@PAMsshrelayhost>
   - To initialize an SSH relay session with X11 forwarding, use the command:
     ssh -X -t -p 2222 <PAMuser@PAMsshrelayhost>
   - A list of all the available SSH sessions are displayed.
   - 3b Enter the appropriate option to start the respective SSH session.
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.

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.

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: Allows you to add session notes before launching the session.
   - The icon: Allows you to access Web Application SSO session.

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**: 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 ➔ > Checkouts.

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 ➔ > Checkouts to view the history and current status of credential checkouts.
Viewing Emergency Access Request History

Select Access Requests > Requests from the ★ icon 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 ★ > Requests > Access Requests > Pending > Delete.
  2. (Conditional) To cancel multiple requests, perform the following:
     a. Select one or more requests.
     b. Click Delete.

- **Approved**: These are the requests approved by the administrator. You can access the approved requests from ★ > Requests. Click ★ > Access Requests > Approved. 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 ★ > Requests. Click Access Requests > Denied.

- **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 expired.
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 5.00 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 > My Access > Requests > Pending.

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

   After approval, you can access the request from > My Access > Requests > 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 > Requests > New Request from the page of Privileged Account Manager.
2. Select the Resource you want to access.
3. Based on the selected target configure the following:

<table>
<thead>
<tr>
<th>Target</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td><strong>Connection Type:</strong></td>
</tr>
<tr>
<td></td>
<td>Select <strong>SSO</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Direct Access</strong> when you want to access the Windows directly using the server credentials.</td>
</tr>
<tr>
<td>Target</td>
<td>Fields</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows Web Access</td>
<td><strong>Connection Type:</strong> Select the application or computer you want to access.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Web Access</strong> when you want to access the Windows directly using the server credentials.</td>
</tr>
<tr>
<td></td>
<td>Select  ➔ Active Sessions to view the active sessions.</td>
</tr>
<tr>
<td>SSH/Telnet</td>
<td><strong>Connection Type:</strong> Select SSH or Telnet based on the connection method the target system supports.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable X11:</strong> Select this option to get X11 application access through SSH.</td>
</tr>
<tr>
<td>SSH Web Access</td>
<td><strong>Connection Type:</strong> Select SSH or Telnet based on the connection method the target system supports.</td>
</tr>
<tr>
<td></td>
<td>Select  ➔ Active Sessions to view the active session.</td>
</tr>
<tr>
<td>Privileged Shell</td>
<td>Choose this option to get elevated access to the UNIX/Linux workstation using your local credentials.</td>
</tr>
<tr>
<td>Database</td>
<td><strong>Database:</strong> Select the database you want to access.</td>
</tr>
<tr>
<td></td>
<td><strong>Password Checkout:</strong> Select this option to check out credentials to access the database.</td>
</tr>
<tr>
<td></td>
<td><strong>Database Access:</strong> Select this option when you know the credentials to access the database but you need access to the database through Privileged Account Manager proxy.</td>
</tr>
<tr>
<td>Application SSO</td>
<td><strong>Application:</strong> Select the application or computer you want to access.</td>
</tr>
<tr>
<td>Application SSO Web Access</td>
<td><strong>Connection Type:</strong> Select the application or computer you want to access.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Web Access</strong> when you want to access the Windows directly using the server credentials.</td>
</tr>
<tr>
<td></td>
<td>Select  ➔ Active Sessions to access the active session.</td>
</tr>
<tr>
<td>Application Credential</td>
<td><strong>Application:</strong> Select the application for which you want to get the credentials.</td>
</tr>
</tbody>
</table>

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

**Resource/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.
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. From Home > My Access, select the appropriate resource for which you need to generate a token.
   
   For example, if you want to generate a token for Shared Keys, select the resource Predefined Tags > Shared Keys.

2. Click API Token > Generate Token.

3. Specify the following details:
Managing API Tokens

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:

```
  "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"
```
Managing API Tokens

- **Response:**

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

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

  - **Request:**

    ```bash
        "Request": {
            "type": "PasswordCheckin",
            "runHost": "<Specify the target resource whose credentials must be checked in.>"
        }
    }'"https://<PAM_SERVER>/rest/cmdctrl/Request/<Request Id>"
    ```

  - **Response:**

    ```json
    {  
        "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 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.