Ekran System v.6.0
Privileged User Accounts and Sessions (PASM)
# Table of Contents

About ................................................................................................................................. 3  
Using Privileged User Accounts ..................................................................................... 4  
Password Vault Configuration ......................................................................................... 5  
Defining Domain Administrator Credentials .................................................................. 6  
Adding Privileged User .................................................................................................. 7  
Editing Privileged Account ............................................................................................ 8  
Deactivating Privileged Account ..................................................................................... 8  
Using Privileged Accounts .............................................................................................. 9  
Viewing Privileged Sessions .......................................................................................... 10
About

If you want to provide users temporary access to the particular computer or computer group without revealing credentials, you can add a privileged user. This feature is available if you have the Enterprise license for Ekran System and the Terminal Server license for Clients from which users will get access to protected computers (Jump Servers).

Account credentials of shared privileged accounts are automatically generated and stored in a password vault. The passwords are encrypted with the RSA key stored in the Certificate Storage on the Server and auto-changed every 24 hours until the account is not deactivated. The passwords are also reset every time after the account expiration. It allows enhancing data access security.
Using Privileged User Accounts

To use the Privileged Accounts feature, do the following:

1. Make sure that you have Enterprise license activated.

2. Configure the password vault.  
   NOTE: You can use MS SQL Express for a password vault.

3. On the Configuration page, LDAP Target tab, define the administrator credentials for the domain in which shared accounts will be created. These credentials will be encrypted and saved to the password vault.

4. Select the Enable jump server mode option for the Client with the assigned Terminal Server license.

5. Add a privileged user.

6. The shared account for access to the defined computer/computer group will be automatically created in the selected domain. Its credentials will be stored in the password vault in the encrypted format.

7. Now, the user can work with the protected computers using the remote desktop connection under the created privileged user account.
Password Vault Configuration

**Password vault** is an SQL database for storing encrypted credentials of the shared accounts used for privileged access.

**To configure a password vault, do the following:**

1. Log in to the Management Tool as a user with the administrative **Database Management** permission.
2. Click the **Database Management** navigation link to the left.
3. On the **Password Vault** tab, select **Use password vault**.
4. Define the instance, database name, user, and password of the SQL database to be used as a password vault.
5. Click **Save**.
Defining Domain Administrator Credentials

Domain Administrator credentials are required for creation of shared accounts used for privileged access.

To define the domain administrator credentials, do the following:

1. Click the Configuration navigation link to the left.
2. On the LDAP Targets tab, select the LDAP target for which you want to edit the configuration, and click Edit.
3. Define the domain administrator login and password.

4. Click Finish. Domain administrator credentials are saved.
Adding Privileged User

To add a new privileged user, do the following:

1. Log in to the Management Tool as a user with the administrative User Management permission.
2. Click the Access Management navigation link to the left.
3. On the Privileged Accounts tab, click Add User.
4. The Privileged Accounts window appears.

5. Select the user you give access to the computer or computer group.
   - For the Active Directory user, select a user and domain. You can select a user group to give access to all users belonging to it.
   - For the Local computer user, select the user login and computer name.
   - For the Ekran System user for secondary authentication, select the user login. These credentials will be checked if the Forced user authentication is enabled on the target computer.

6. Select a computer or computer group to which user will access using the remote desktop connection (target computers). To do this, select the domain and computer or computer group from the corresponding lists.

   NOTE: The administrator’s credentials for the selected domain must be defined.
7. Select a domain group from which the privileged account will inherit permissions (target computers). This must be a user group whose members are allowed to login to the target computers remotely.
8. Define the date when privileged account will be deactivated.
9. Add comment, if necessary.
10. Click **Grant Access**.
11. The privileged account is generated in the selected domain user group. Its credentials are stored in the password vault and the user can access the selected computers via Ekran System remote access application.

**Access Management**

<table>
<thead>
<tr>
<th>User/Group</th>
<th>User Type</th>
<th>Computer Group</th>
<th>Computer Group</th>
<th>Domain Group</th>
<th>Shared Account</th>
<th>Expiration Date</th>
<th>Status</th>
<th>Time Added</th>
<th>Added By</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>ekransystem_guest</td>
<td>ActiveDirectory</td>
<td>SRV-APP</td>
<td>RDP_Users</td>
<td>ES_User_FYD462</td>
<td>11/05/2018 10:55:00</td>
<td>Active</td>
<td>admin</td>
<td>10:04:58</td>
<td>10:04:58</td>
<td>Privileged access to the server</td>
<td>Delete</td>
</tr>
<tr>
<td>admin</td>
<td>Internal</td>
<td>at_e brittle</td>
<td>Domain Computers</td>
<td>ES_User_CC0841CF</td>
<td>10/05/2018 14:47:00</td>
<td>Disabled</td>
<td>admin</td>
<td>10:04:58</td>
<td>10:04:58</td>
<td>Privileged access to the server</td>
<td>Delete</td>
</tr>
<tr>
<td>ekransystem_guest</td>
<td>ActiveDirectory</td>
<td>BA-W0006R2</td>
<td>Domain Computers</td>
<td>ES_User_FYD462</td>
<td>10/05/2018 14:43:00</td>
<td>Disabled</td>
<td>admin</td>
<td>10:04:58</td>
<td>10:04:58</td>
<td>Privileged access to the server</td>
<td>Delete</td>
</tr>
</tbody>
</table>

**NOTE:** If you select a domain user group as a privileged user, then a separate shared account will be created for each member of this group.

**Editing Privileged Account**

Once you created the shared account for the privileged user, there is no way to edit it. You have to delete the record deactivating the account and then create a new one with the edited parameters. Please note that if you created the shared account for the user once, then it will not be re-created but only re-activated with a new password.

**Deactivating Privileged Account**

To deactivate the privileged account, do the following:
1. Log in to the Management Tool as a user with the administrative **User Management** permission.
2. Click the **Access Management** navigation link to the left.
3. On the **Privileged Accounts** page, click **Delete** in the selected user row.
4. Click **Delete** in the confirmation window.
5. The privileged account of the selected user is deactivated. It can be deleted via Active Directory.

**Using Privileged Accounts**

To access remote computer via Ekran System remote access application, do the following:

1. Login to the Jump Server as a user for whom the shared privileged account has been created. Please note that if the forced user authentication is enabled on the Jump Server, then credentials of the secondary user will be checked.
2. Click Remote Access in the Client tray menu.
3. The Ekran System Remote Access application opens. The drop-down list contains the list of computers to which you have been granted access. If you have been granted access to the computer group, the drop-down list will be empty and you will have to enter the name of the computer or its IP manually.
4. Select the computer from the drop-down list or enter its name/IP, click **Connect**.

4. The auto-logged remote desktop session under the shared privileged account starts.
Viewing Privileged Sessions

If the Ekran System is installed only on the jump server, you can view a privileged session as a part of the original Jump Server session.

If the Client is installed on the protected target computer, you can view the privileged session as a session of the shared account.