EKRAN®

Ekran System

Password Management (PAM)

Table of Contents

About

Ekran System Password Management allows you to securely store and manage credentials of shared privileged accounts. This feature is available if you have the Enterprise license for Ekran System and the Terminal license for Clients (Jump Servers) from which users will get access to critical endpoints.

Using Password Management

To use the Password Management feature, do the following:

1. Make sure that you have Enterprise license activated.
2. Configure the Client that will be used as a jump server.
3. Optionally, when you are using the Active Directory Account Secret, configure the LDAP Target.
4. Add the Secret.
5. Now, the user with the corresponding permission can work with the protected computers using the Secret.

Jump Server Configuration

Make sure the Client machine that is used as a jump server meets the following requirements:

- .Net Framework 4.5.2 or higher
- Microsoft Visual C++ 2015 Redistributable: https://www.microsoft.com/en-gb/download/details.aspx?id=48145

To configure the Client that will be used as a jump server, do the following:

1. Log in to the Management Tool as a user with the Client configuration management permission.
2. Click the **Client Management** navigation link to the left.
3. On the **Client Management** page, select the Client that will be used as a jump server, and click **Edit Client**. To find a specific Client, enter its name in the **Contains** box and click  .
4. On the **Editing Client** page, on the **Properties** tab, in the **Client Properties** group, make sure the Terminal Server license is assigned to the Client.
5. In the **Client mode** group, select the **Enable jump server mode** option. Optionally, select the **Replace Windows Shell to Ekran System Connection Manager** option to display only the **Ekran System Connection Manager** window.
6. If you want to share the Secret with the internal users, on the **Authentication options** tab, select the **Enable secondary user authentication on log-in** option.
7. Click **Finish**.

LDAP Target Configuration

Active Directory user credentials are required to use the Active Directory Account Secret.

To define the Active Directory user 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 Active Directory user login and password.
4. Click **Finish**. The credentials are saved.

Secret Management

About

Credentials of shared privileged accounts are stored in Secrets. There are four types of accounts that can be accessed using a Secret: Active Directory account, Windows account, Unix account (SSH), Unix account (Telnet).

To protect sensitive information, the Secrets are encrypted with AES-256.

Viewing Secrets

The Secrets are displayed on the **Password Management** page in the Management Tool. A list of Secrets is displayed in the form of grid. The grid includes the following information:

- **Secret Name:** Displays the name of a Secret.
- **Secret Type:** Displays the type of a Secret (Active Directory account, Windows account, Unix account (SSH), Unix account (Telnet)).
- **Added By:** Displays the name of the user who added the Secret.
- **Description:** Displays the description of the Secret.
- **Delete All:** Allows deleting information about Secrets.

You can search for required Secret using a search expression (keyword).

On the **Password Management** page, you can add new Secrets or edit and delete existing Secrets.

You can filter and sort the information about the Secrets in the grid.

By default, the following filters are displayed:

- **Secret Name**: Allows filtering Secrets by their names.
- **Secret Type:** Allows filtering Secrets by a specific type.
- **Expiration Date**: Allows filtering Secrets by the expiration date. The result Secrets list includes all Secrets that expires during the set time period.
  To set the time period, select one of the following and click Apply:
  - Define the number of latest hours, days, weeks, or months.

- Define the start date and the end date of the time period.

To sort Secrets on the **Password Management** page, click the required column header. You can change the column sort order from ascending to descending, and vice versa. To do this, click the **Sort** arrow near the column header.

If data is not sorted by this column, the **Sort** arrow is hidden.

Adding Secret

Adding Active Directory Account Secret

To add the Active Directory Account Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. On the **Secrets** tab, click **Add Secret**.
4. In the **General** group, do the following:
   - Enter a unique name for a Secret.
   - Select the **Active Directory account** Secret type.
   - Optionally, enter the Secret description.
5. In the **Account** group, define a computer which user will access using the Ekran System Connection Manager:
   - Select the domain a computer belongs to.
   - Define the user login and password under which the connection will be established.
6. In the **Permissions** group, click **Add** and in the opened drop-down list select the check boxes next to the users or user groups you want to grant permissions to, and then click **Add**. Next to each user, select the permission to be granted to them.
7. Click **Save**.

Adding Windows Account Secret

To add the Windows Account Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. On the **Secrets** tab, click **Add Secret**.
4. In the **General** group, do the following:
   - Enter a unique name for a Secret.
   - Select the **Windows account** Secret type.
   - Optionally, enter the Secret description.
5. In the **Account** group, define a computer which user will access using the Ekran System Connection Manager:
   - Enter the computer name.
   - Define the user login and password under which the connection will be established.

6. In the **Permissions** group, click **Add** and in the opened drop-down list select the check boxes next to the users or user groups you want to grant permissions to, and then click **Add**. Next to each user, select the permission to be granted to them.
7. Click **Save**.

Adding Unix Account (SSH) Secret

To add the Unix Account (SSH) Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. On the **Secrets** tab, click **Add Secret**.
4. In the **General** group, do the following:
   - Enter a unique name for a Secret.
   - Select the **Unix account (SSH)** Secret type.
   - Optionally, enter the Secret description.
5. In the **Account** group, define a computer which user will access using the Ekran System Connection Manager in one of the following ways:
   - Using login credentials:
     - Select the Linux computer name.
     - Define the user login and password under which the connection will be established.
   - Using private key:
     - Select the Linux computer name and define the user login under which the connection will be established.
     - Click **Choose file** to add the Private Key.
     - Enter the passphrase for the chosen Private Key.
6. In the **Permissions** group, click **Add** and in the opened drop-down list select the check boxes next to the users or user groups you want to grant permissions to, and then click **Add**. Next to each user, select the permission to be granted to them.
7. Click **Save**.
   NOTE: Putty must be installed on the Jump Server from which the connection to the Linux Client machine will be established.

Adding Unix Account (Telnet) Secret

To add the Unix Account (Telnet) Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. On the **Secrets** tab, click **Add Secret**.
4. In the **General** group, do the following:
   - Enter a unique name for a Secret.
   - Select the **Unix account (Telnet)** Secret type.
   - Optionally, enter the Secret description.
5. In the **Account** group, define a computer which user will access using the Ekran System Connection Manager:

- Select the Linux computer name.
- Define the user login and password under which the connection will be established.

6. In the **Permissions** group, click **Add** and in the opened drop-down list select the check boxes next to the users or user groups you want to grant permissions to, and then click **Add**. Next to each user, select the permission to be granted to them.
7. Click **Save**.

Editing Secret

Editing Secrets is available for the users with the Owner or Editor permissions.

To edit a Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. Click the required Secret in the **Secrets** grid.
4. Edit Secret data in the same way as when adding a new Secret and click **Save**.
5. The Secret is edited.

Deleting Secret

Deleting Secrets is available for the users with the Owner permission.

To delete a Secret, do the following:

1. Log in to the Management Tool.
2. Click the **Password Management** navigation link to the left.
3. On the **Secret** tab, click **Delete** for the required Secret.
4. In the confirmation message, click **Delete.**
5. The Secret is deleted.

Permissions

About

The permissions allow you to define which functions a user will be able to perform with the Secret. There are three types of permissions:

- **Owner:** Allows a user to grant any permissions, view the Secret data including the credentials of shared privileged accounts, delete, edit, and use the Secret.
- **Editor:** Allows a user to grant the Editor or PAM User permissions, view the Secret data, edit, and use the Secret.
- **PAM user:** Allows a user to use the Secret.

If you define permissions for the group, any user belonging to this group inherits these permissions. Apart from the permissions inherited from the group, you can assign a user their own permissions.

Viewing Permissions

The assigned permissions are displayed on the **Permissions** tab on the **Password Management** page in the Management Tool. A list of permissions is displayed in the form of grid. The grid includes the following information:

- **User/Group Name:** Displays the name of the user or user group to whom the permission is granted.
- **Secret Name:** Displays the name of the Secret for which the permission is granted.
- **Secret Type:** Displays the type of a corresponding Secret (Active Directory account, Windows account, Unix account (SSH), Unix account (Telnet)).
- **Permission:** Displays the type of a permission (Owner, Editor, PAM User).
- **Description:** Displays the description of the corresponding Secret.

You can search for required permission using a search expression (keyword).

You can filter and sort the information about the permissions in the grid.

By default, the following filters are displayed:

- **Who**: Allows filtering permissions by a specific user or user group to whom the permission is granted.
- **Secret Name:** Allows filtering permissions by a specific name of the Secret for which the permission is granted.

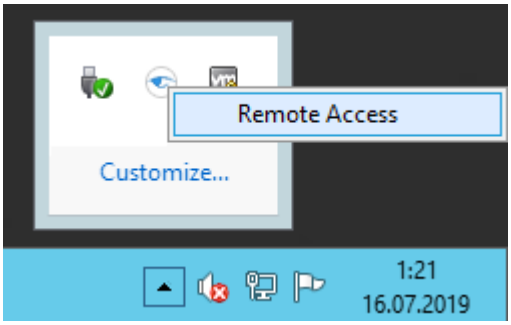
To sort permissions on the **Permissions** tab on the **Password Management** page, click the required column header. You can change the column sort order from ascending to descending, and vice versa. To do this, click the **Sort** arrow near the column header.

If data is not sorted by this column, the **Sort** arrow is hidden.

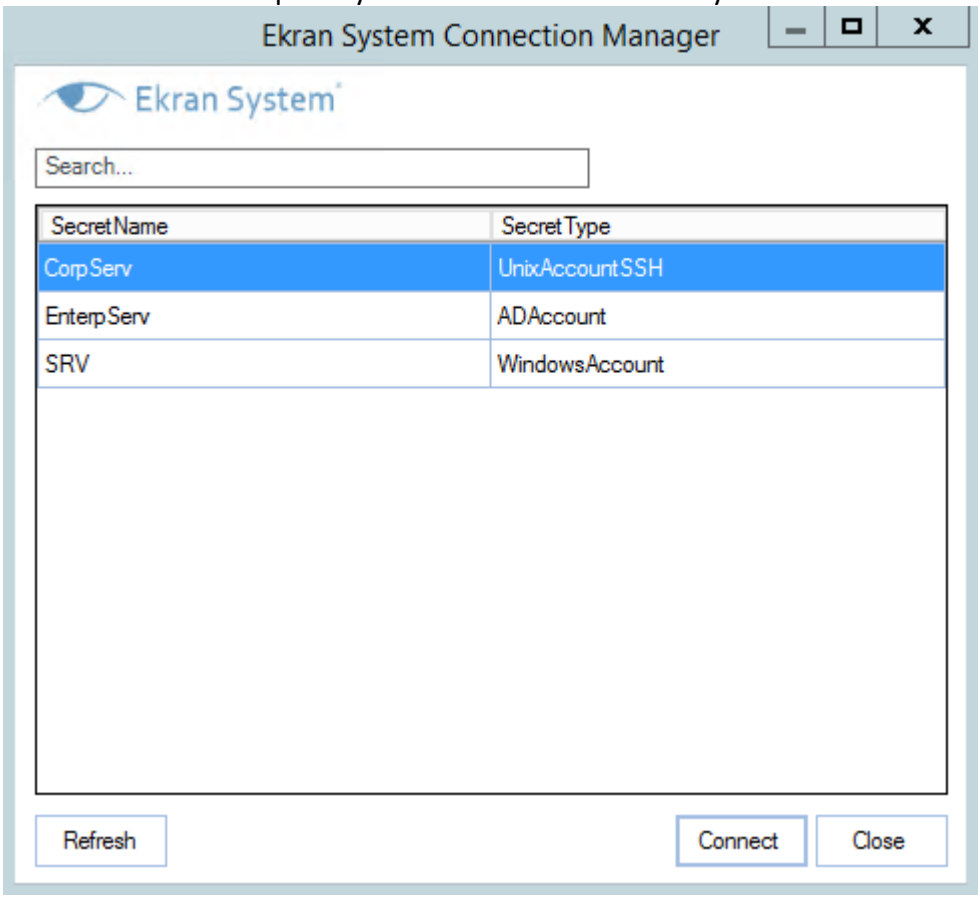
Using Secret

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

1. Log in to the Jump Server in a common way (locally or remotely). If the permission to use the corresponding Secret was granted to an Active Directory user, enter their credentials.
2. If the Forced User Authentication is enabled, enter the credentials of the secondary user to whom the permission to use the corresponding Secret was granted.
3. Right-click the **Tray** icon in the notification area and click **Remote Access.**



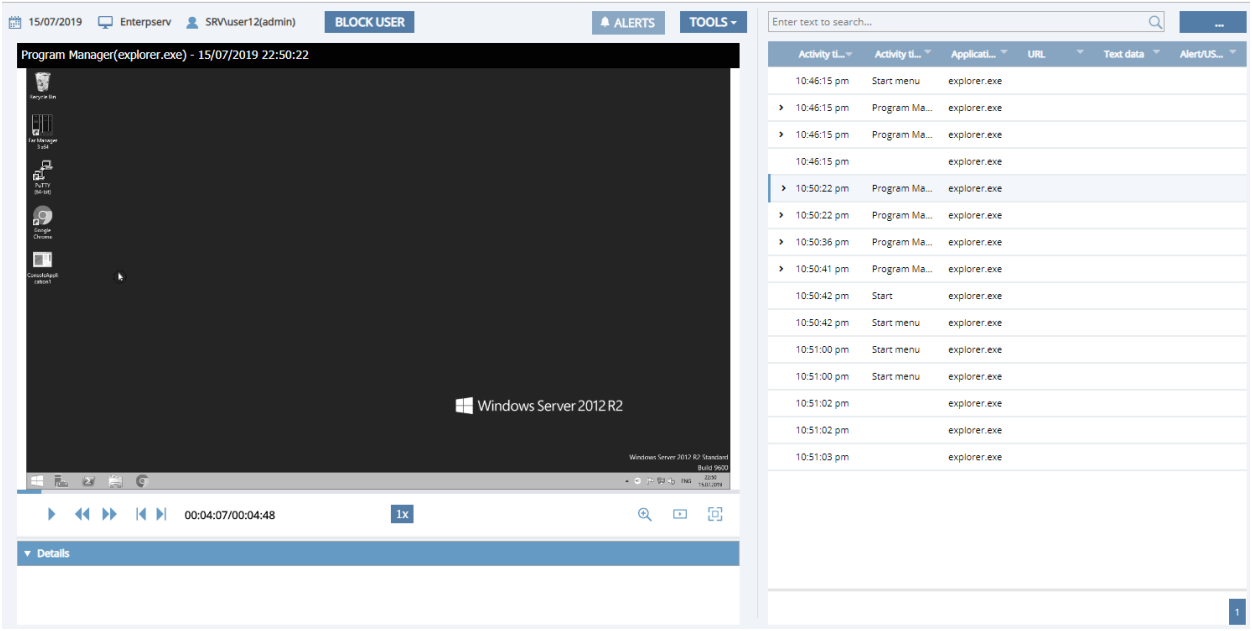
4. The **Ekran System Connection Manager** opens. The grid contains the list of Secrets for which you have been granted a corresponding permission. To update the list of Secrets, click **Refresh**.
5. Click the required Secret, and then click **Connect**. For the Active Directory account, enter the name of the computer you want to access manually and click **Connect**.



6. The remote connection is established according to the Secret type.

Viewing Privileged Session

If the Client 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.