Accounts

The section is intended to work with local and domain accounts.

Account search

The search is performed in the **Accounts** section.

Quick search

Enter **Account name** in whole or in part in the search bar.

Extended search

Click **Extended search** and enter one or more criteria, **Account name** in whole or in part.
Select account state:

- Pending
- Ignored
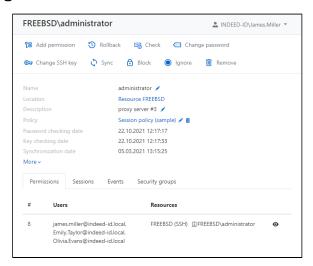- Managed
- Blocked
- Removed

Select account location:

1. **Local account**
   To search, enter the **Resource name** or **DNS name/IP address** in whole or in part.
2. **Domain account**
   To search, enter **NetBIOS name** or **DNS name** in whole or in part.

Account page

The profile displays the data specified while adding the account:

- **Name** - is the account name
- **Location** - the name of the resource or domain, where the account resides
- **Description** - this can be an arbitrary text
- **Policy** - is the set of rules applied to sessions started with the account
- **Password** (or a Key) **checking date** - is date and time when the account password or SSH key was last checked
- **Synchronization date** - date and time of the last data synchronization
- **Date added** - is the date and time when the account was added to Indeed PAM
- **Last change** - is the date and time when the account was last edited
- **Last password change date** - is the date and time when the account password was last changed in Indeed PAM database
- **Last password change date on resource/domain** - is the date and time when the account password was last changed at the Indeed PAM database and at the resource
- **Last SSH key change date** - the date and time of the SSH key change in the Indeed PAM database

- **Last SSH key change date on resource** - the date and time of the SSH key change in the Indeed PAM database and on the resource

Permissions

All permissions where the account is used are displayed in the **Permissions** tab. The following data is displayed for every permission:

- **#** - permission number.
- **User** - the Active Directory user, the permission is given to
- **Account** - the account used to start RDP, SSH or web session at the resources specified in the permission
- **Resources** - the resources that RDP, SSH or web session can be started at under the account specified in the permission

Sessions

All active and finished sessions for the account are available at the **Sessions** tab. The following data is displayed for every session:

- **User** - the Active Directory user who initiated the session
- **Account** - the account used to start RDP, SSH or web session
- **Resource** - the resource that RDP, SSH or web session is started at under the account
- **Connection address** - the actual address used when opening the session
- **Duration** - is the session duration
- **Connection** - remote connection type (RDP, SSH, user types)
- **Connected to PAM** - date and time when the session was started
- **Finished** - date and time when the session was finished
- **State** - this displays the current status of the session (active or finished)

To view detailed information about the session, click on it. To display all sessions for a given account, click **Show all**.

Events

The account events are displayed in the **Events** tab. The following data is displayed for every event:

- **Creation time** - date and time when the event was created
- **Code** - is the event code
- **Event** - is the event description
- **Component** - is the Indeed PAM component that generated the event. Initiator is the account that initiated the event generation
- **Initiator** - the account that initiated the generation of the event

To view detailed information about the event, click on it. To display all events for a given account, click the **Show all**.

Security groups

The **Security groups** tab displays a list of groups to which the account has been added.

> Built-in security groups are not displayed for domain accounts.