Terms

User Directory

Active Directory container or organization unit (OU) from which Indeed Identity PAM receives employee data. It is possible to work with multiple Active Directory domains.

Users

Active Directory users that are members of container or Organization Unit defined as User Directory.

Accounts

Accounts of Windows OS, * nix OS, DBMS, Active Directory, web applications or client applications on behalf of which sessions will be opened in controlled systems.

Resources

Various systems that need to be accessed on behalf of the accounts.

Domains

Domains are intended for obtaining and automatically adding domain computers and domain accounts to Indeed Identity PAM.

Data storage

For data storage Indeed Identity PAM can use different DBMS:

- Microsoft SQL Server
- PostgreSQL
- PostgreSQL Pro
- Jatoba

Service connection

Service connection to a resource allows you to perform the following operations:

- Checking the connection to the resource
- Synchronizing accounts
- Account Security Groups synchronization
- Control of passwords and SSH keys of accounts
- Synchronizing resource OS version or DBMS version
- Synchronizing domain computers in Active Directory

Service connections are supported for the following resources:

- Windows
- *nix
- Microsoft SQL Server
- PostgreSQL
- MySQL
- OracleDB
- Cisco (IOS XE)
- Inspur BMC (IPMI)

User connection

The User connection allows you to open sessions on resources or run individual RemoteApp applications. The following types of connections are supported:

- RDP
- SSH
- Telnet
- RemoteApp

Permissions

Permissions are used to manage privileged access. Any Active Directory user can be given permission to access the resource.
Contents of the permission:

- **User** - an employee whose personal account is part of the User Directory.
- **Account** - local or domain account used by Active Directory user to start a session at the resource.
- **Resource** - the resource on which the session will be opened.

Permission cannot be modified while used. Revoked permissions cannot be restored.

Access account states

- **Pending** () – an account would have **Pending** state if added to Indeed Identity PAM using synchronization with resource or domain. This happens because the Indeed Identity PAM database contains no password for the account. As a result, the account is not managed by Indeed Identity PAM and cannot be a part of permission.
- **Managed** – the account has password in Indeed Identity PAM database. Therefore, the account is managed by Indeed Identity PAM and can be a part of permission.
- **Ignored** () – an account can be switched to **Ignored** if it has **Pending** or **Managed** state. In this case, the account is stored without password and is not managed by Indeed Identity PAM. The account cannot be a part of permission. Moreover, all permissions it was used in are revoked.
- **Blocked** () – an account can be switched to **Blocked** if it has **Managed** status. In this situation, the account cannot be a part of permission. And all permissions it was used in are suspended.
- **Removed** () – an account can be switched to **Removed** status from any other one. A removed account is not managed by Indeed Identity PAM and is hidden from the common list. All permissions it was used in are revoked. A removed account can be restored and switched to **Managed** status if required.

Resource states

- **Stand by** – means that the resource is added to Indeed Identity PAM
- **Blocked** () – means that resource has been blocked and, it cannot be a part of permission. All permissions it was used in are suspended.
- **Removed** () – a resource can be switched to **Removed** state from any other one. Removed resources are hidden from the common list. A removed resource can be restored and switched to **Stand by** state if required.

Domain states

- **Stand by** – means that the Domain is added to Indeed Identity PAM.
- **Removed** () – a domain can be switched to **Removed** state. Removed domains are hidden from the common list. A removed domain can be restored and switched to **Stand by** status if required.

Session states

- **Active** - if the user has permission to access the target resource from the specified account, which are not blocked and the permission is not revoked, then the server creates a session that becomes active.
- **Finished** - the session ends when the user ends the session with the target resource, for example, terminating the remote access session to the server, closing the window of the working application or web page.
- **Aborted** - the session becomes aborted when the PAM administrator forcibly terminates the active user session.

Policies

A policy is a set of settings that is propagated to multiple system objects. A single object can be assigned only one policy of the certain type.