Security recommendations

Backup accounts

Solutions of Privileged Access Management class are a combination of hardware, software and organizational tools that protect privileged accounts from unauthorised use.

One of the Indeed Identity PAM protection mechanisms is isolation of account passwords in the Indeed Identity PAM Core storage, encryption of those, as well as change of passwords to random or user-specified values on schedule or upon request.

The Indeed Identity PAM Core storage is a critical element. If it is damaged, then all the resources become inaccessible, since account passwords are unknown either to administrators or users.

It is highly recommended to assign a backup account for every resource. This account must possess local administrator privileges (Windows) or have privileges to execute SUDO command (Unix\Linux). This would allow to restore resource accessibility in case the data storage of Indeed Identity PAM Core fails. Therefore, you should assign an employee who is responsible for storing the backup accounts and passwords.

Access to Indeed Identity PAM

To provide for security of Indeed Identity PAM components, it is recommended to install the system according to Basic deployment. In this case, the following components are installed on a single server:

- Indeed Identity PAM Core
- Indeed Identity IdP
- Indeed Identity PAM Management Console
- Indeed Identity PAM User Console
- Indeed Identity Log Server
- Indeed Identity Pam EventLog
- Microsoft SQL Server or PostgreSQL

Placing the key components of Indeed Identity PAM and data storage to a single server allows to reduce risk of their unauthorized use. The following ports must be open to provide for correct operation:

Protocol	Port	Description
Inbound and outbound		
TCP/UDP	53	DNS
TCP/UDP	389/636	LDAP/SSL
TCP	3268/3269	Microsoft Global Catalog/SSL
TCP/UDP	88	Kerberos
TCP/UDP	464	Kerberos
Inbound		
TCP	80/443	PAM Core/SSL PAM Management Console/SSL PAM User Console/SSL IdP/SSL Log Server/SSL