Seamless authentication

The password authentication process is redesigned to allow users to connect to Soffid LDAP using their internally stored password, or a password trusted by Soffid.

1. The first attempt is to check the password against the **local userPassword attribute**. If it fails, Soffid LDAP will connect any of the configured sync servers, and will let the sync server validate the password.
2. Then, the sync server will check the password against **Soffid internal tables**.
3. If the password is not accepted according to Soffid internal tables, the authentication request will be forwarded to any **trusted target systems**. The trusted flag is enabled or disabled on a per-agent basis, at the agents configuration page
4. If everything fails, the login is rejected

Anyway, whenever a password change is detected by Soffid, the attribute userPassword can be updated. This is done by means of the LDAP connector.

The opposite way also works for password changes. Whenever the user attribute userPassword is updated, SoffidLDAP does:

1. Generates a secure hash using SSHA-256, and replaces the provided value for the corresponding hash
2. Notifies Soffid sync server the password has been changed
3. Adds an additional value {SOFFID} to the userPassword attribute. Now, the userPassword attribute has two values: the SSHA hash and the Soffid marker
4. Soffid sync server, in turn, validates the received passwords and stores it in Soffid database and other target systems. This only happens if the trusted flag is enabled for the Soffid LDAP agent

---

Revision #3
Created 7 June 2022 12:55:55 by pgarcia@soffid.com
Updated 17 October 2024 09:29:21 by pgarcia@soffid.com