How are users imported from an LDAP directory into KentixONE?

User data is an essential component of an access control system. Contact data is stored in user profiles, and identity data such as PINs, passwords, and RFID card or chip data is stored. This data is used to identify the user at the door and check their access authorization in combination with access profiles and the doors controlled by them.

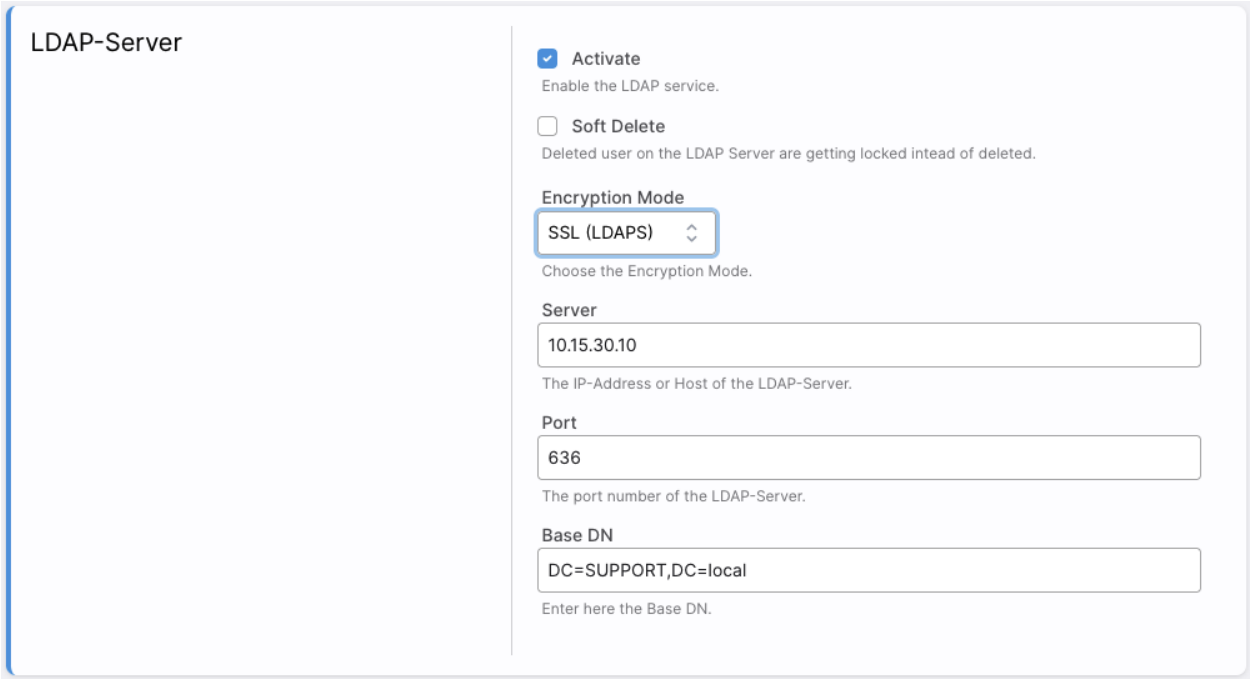
Users are either created manually in KentixONE or imported from existing databases. A comma-separated table (.csv) can be used for import. Another possibility consists of matching user data from an LDAP structure (e.g.: Active Directory). This data can be automatically reconciled at intervals. This means that changes to the personnel structure in the case of new hires or department changes, for example, are also available to the access control system after just a few moments.

KentixONE access to the LDAP directory is read-only. No changes or deletions are made to the data.

The following data is required for this type of import:

1. IP address of the LDAP server.
2. The security mode used there. KentixONE supports “SSL (LDAPS)” and communication with LDAP without encryption.
3. The port of the LDAP service (default: 636)
4. The base service name (Base DN) of the Active Directory. In the following example: SUPPORT.local.
5. Attributes for the users
6. Access profiles in KentixONE

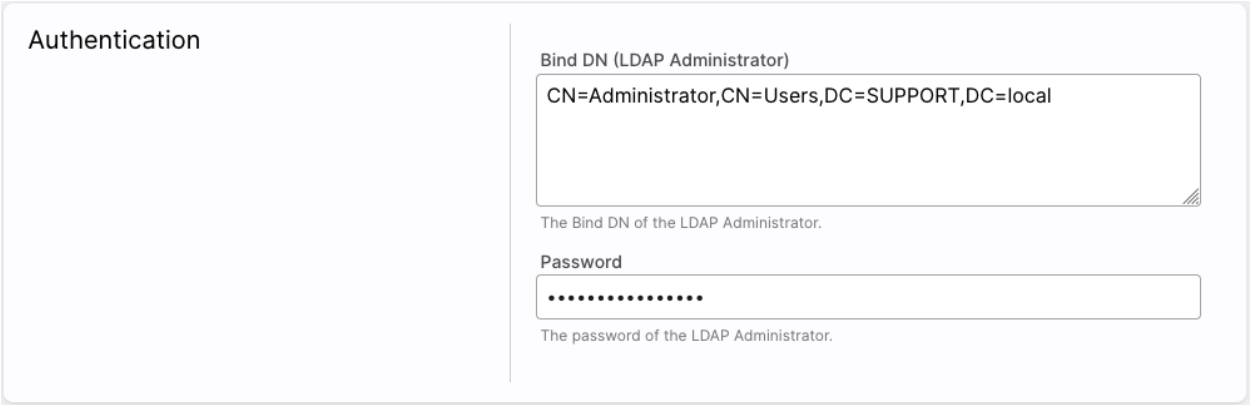
This data is entered in the settings for “Communication”–>”LDAP” on the KentixONE Main device.



LDAP data

The “Soft Delete” option prevents users from being deleted in KentixONE if they have been deleted in the LDAP structure. Instead, these users will be set to the “Inactive” status and will not be granted further access by the access control system or access to KentixONE.

Additionally, the access data of an administrator in the LDAP directory is required:



Administrator account for LDAP

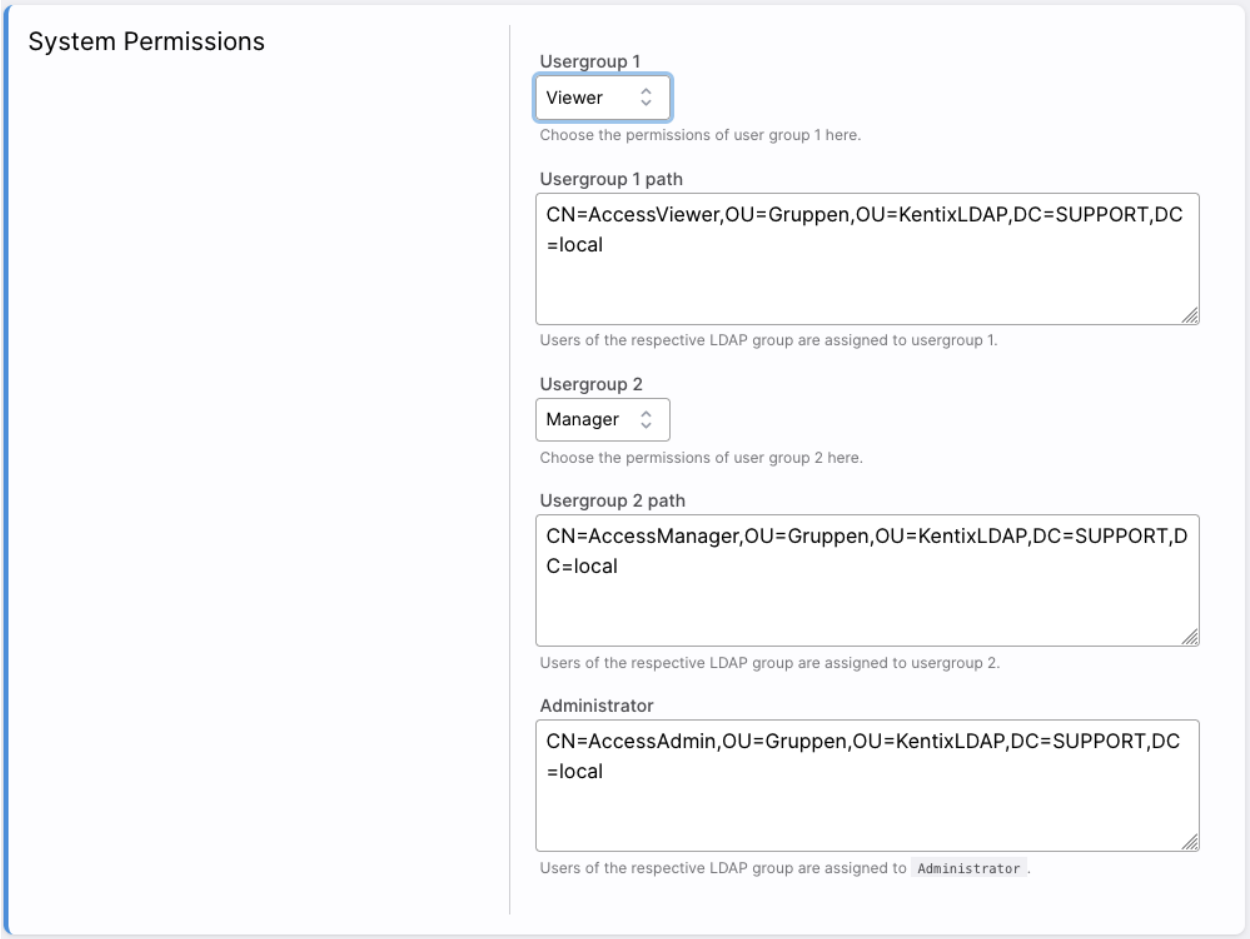
Groups

KentixONE can export three groups from LDAP. These groups are used to control access to the KentixONE interface. Kentix Uses the groups “Administrators”, “Managers” and “Viewers” for this purpose. Each user in KentixONE must be assigned to one of these groups, even if none of the users are to be given access to KentixONE. For these groups, they can determine corresponding groups in

LDAP.

In the example, the values of the LDAP properties of CN=AccessViewer, CN=AccessManger and CN=AccessAdmin are imported for the Kentix groups “Viewer”, “Manager” and “Administrator”. These groups were previously created in LDAP and the users assigned to them.

Import into KentixONE is possible for 3 groups in total.
Nested groups cannot be imported.

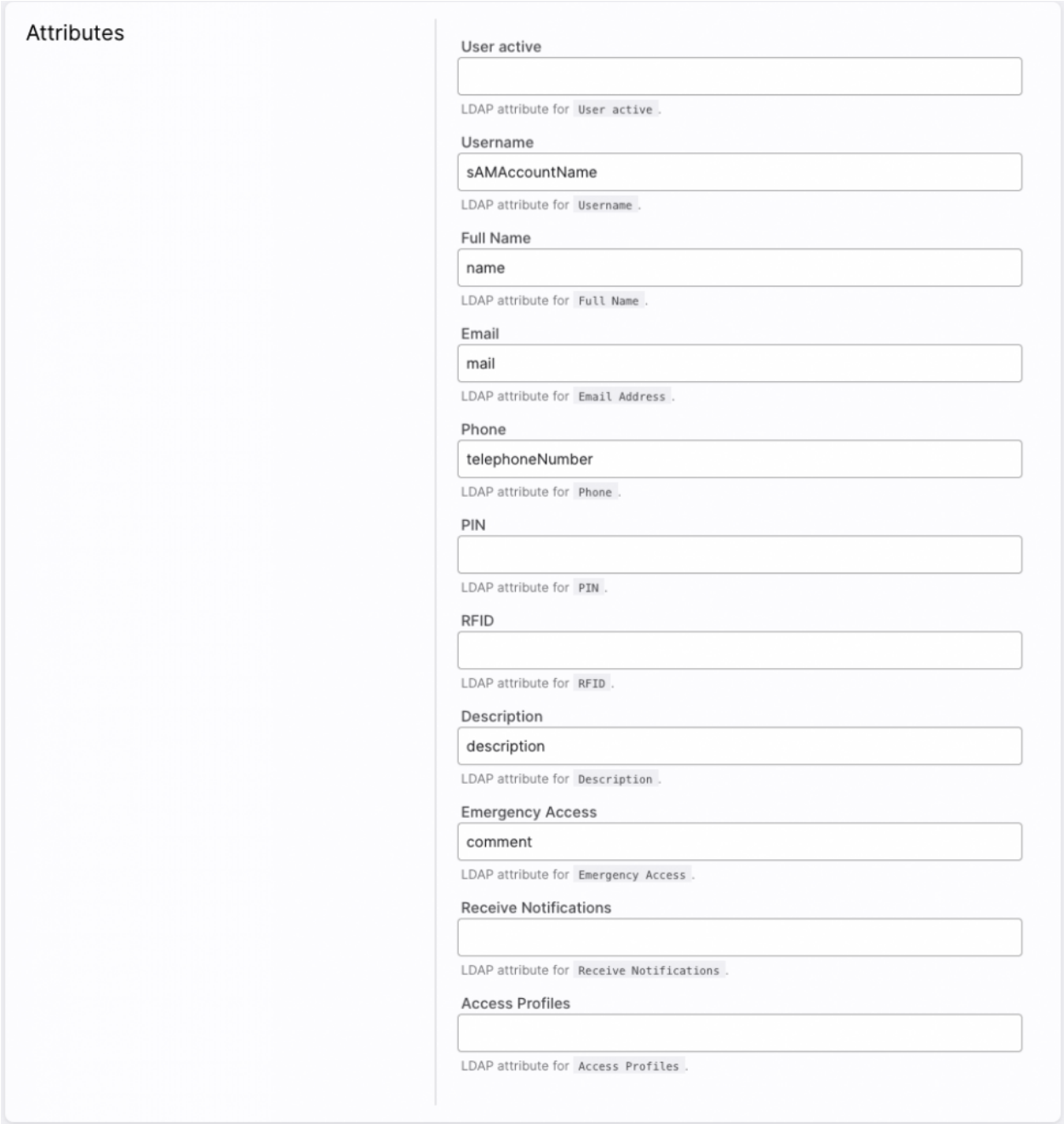


Groups import

User data

When importing, synchronization of various master data of users is available. The data for the fields used in KentixONE have different equivalents in LDAP. Therefore, in the next step, the attributes of the users to be transferred are linked to the LDAP attributes.

For example, the KentixONE “user name” is linked here with the LDAP attribute “sAMAccountName”.



Access

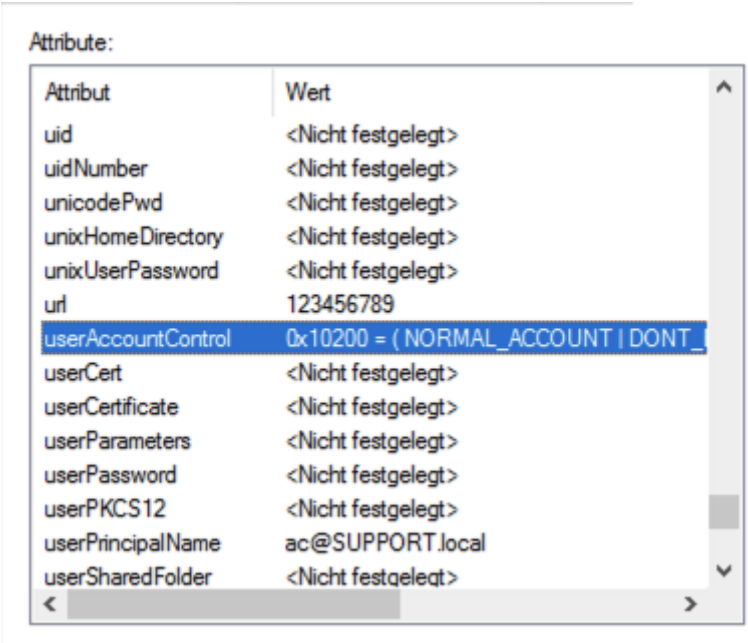
The access of users can thus be controlled from the LDAP structure. One use case, for example, is the maintenance of data including RFID tokens by the HR department. The software used there transfers the data into an LDAP structure. KentixONE regularly updates its user data and thus always maintains the current status of the HR software.

The following attributes are relevant for access control:

User Active

Link this attribute to an LDAP attribute. In the example “userAccountControl”.

If the user is deactivated in LDAP, it will also be deactivated in KentixONE.



UserAccountControl

Alternatively, an own LDAP attribute with “0” or “1” (active) is also possible.

PIN and RFID

Data for the identification of users in the system. If these are already recorded in LDAP when users are created, they can be adopted.

They set the total length of the PINs system-wide in “Security”.
If RA4 rack levers with PINs for access and switching of alarm groups are used, note:
Only the numbers 1-4 are available for input there. Therefore, only create PINs in this number range for users of the rack levers.

Emergency access

Allows selected users access if the DoorLock cannot establish a connection to the AccessManager. The user’s data is stored locally in DoorLock with this authorization. Use an attribute with “0” or “1” (emergency access active).

Emergency access is not available immediately after assignment to a user.
User data for emergency access is transferred to DoorLocks when bookings are made. Therefore, to store each emergency user locally in DoorLock, the same number of access bookings is required as

emergency users were created.

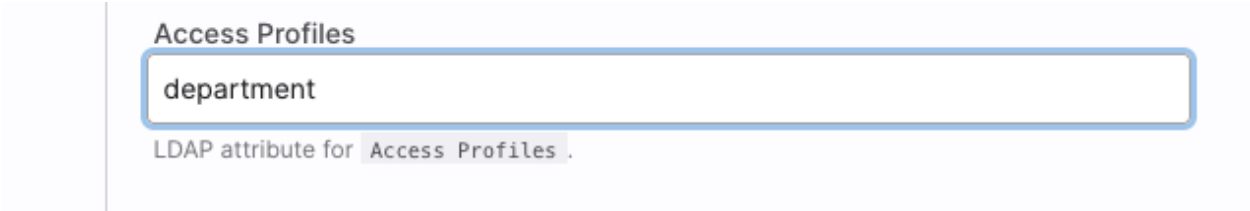
Access profiles

If there are identical profiles in KentixONE and in the LDAP structure, access profiles can be transferred with the users. These profiles are linked at the KentixONE user level. Multiple access profiles can be created in LDAP as an enumeration. The following notation applies: Profile1, Profile2, Profile3, etc.

Groups are imported into KentixONE for access control. The permissions for access to the KentixONE system can be configured there for the groups.

In the example here, “department” was linked as an attribute in LDAP. It contains a list of access profiles for the user.

Access profiles as list in LDAP



Linking in KentixONE