Wie werden Benutzer aus einem LDAP Verzeichnis in KentixONE importiert?

Benutzerdaten sind ein wesentlicher Bestandteil einer Zutrittssteuerung. In Benutzerprofilen werden Kontaktdaten hinterlegt und Identitätsdaten wie PINs, Passwörter und die Daten der RFID-Karten oder Chips hinterlegt. Diese Daten werden zur Identifizierung des Benutzers an der Tür verwendet und deren Zutrittserlaubnis in Kombination mit Zutrittsprofilen und den damit gesteuerten Türen geprüft.

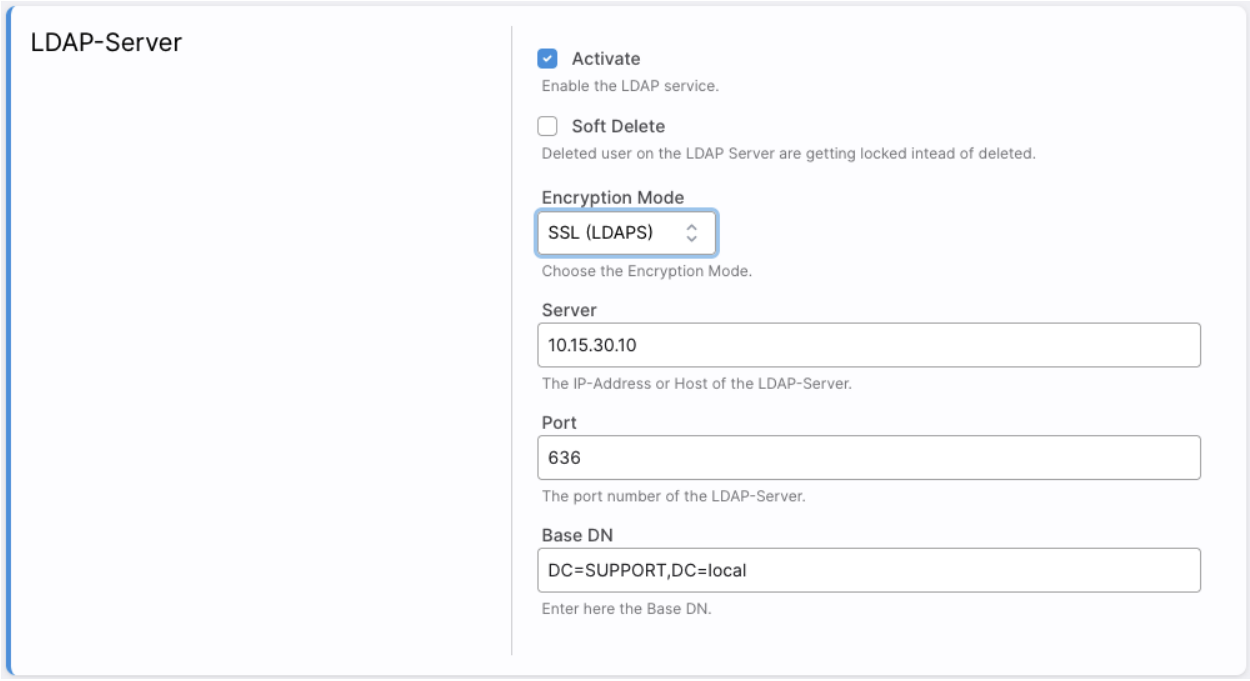
Benutzer werden in KentixONE entweder manuell angelegt oder aus vorhandenen Datenbanken Importiert. Zum Import kann eine kommaseparierte Tabelle (.csv) verwendet werden. Eine weitere Möglichkeit besteht aus dem Abgleich von Benutzerdaten aus einer LDAP Struktur (z. B.: Active Directory). Diese Daten können in Intervallen automatisch abgeglichen werden. Somit stehen Änderungen in der Personalstruktur bei Neueinstellungen oder Abteilungswechseln zum Beispiel nach wenigen Augenblicken auch der Zutrittskontrolle zur Verfügung.

Der Zugriff von KentixONE auf das LDAP Verzeichnis erfolgt ausschließlich lesend. Es werden keine Änderungen oder Löschungen an den Daten vorgenommen.

Für diese Art des Import werden folgende Daten benötigt:

1. IP-Adresse des LDAP Servers.
2. Der dort verwendete Sicherheitsmodus. KentixONE unterstützt „SSL (LDAPS)“ und die Kommunikation mit LDAP ohne Verschlüsselung.
3. Der Port des LDAP Dienstes (Standard: 636)
4. Den Basis Dienstnamen (Base DN) der Active Directory. Im folgenden Beispiel: SUPPORT.local.
5. Attribute für die Benutzer
6. Zutrittsprofile in KentixONE

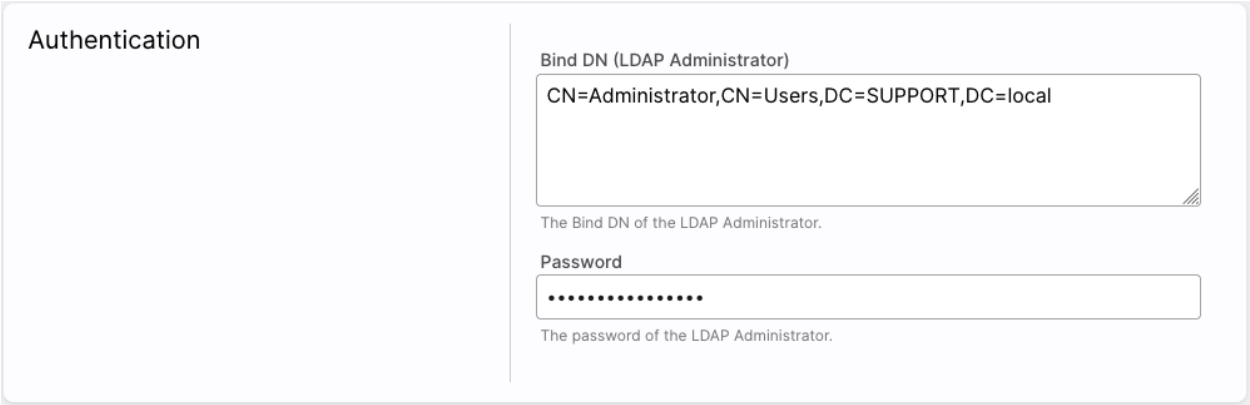
In den Einstellungen zu „Kommunikation“->“LDAP“ auf dem KentixONE Main Gerät werden diese Daten eingegeben.



LDAP Daten

Die Option „Soft Delete“ verhindert das Löschen von Benutzern in KentixONE, wenn diese in der LDAP-Struktur gelöscht wurden. Diese Benutzer werden stattdessen in den Status „Inaktiv“ gesetzt und erhalten weder weiteren Zutritt durch die Zutrittskontrolle noch Zugriff auf KentixONE.

Zusätzlich werden die Zugriffsdaten eines Administrators im LDAP Verzeichnis benötigt:



Administrator Konto für LDAP

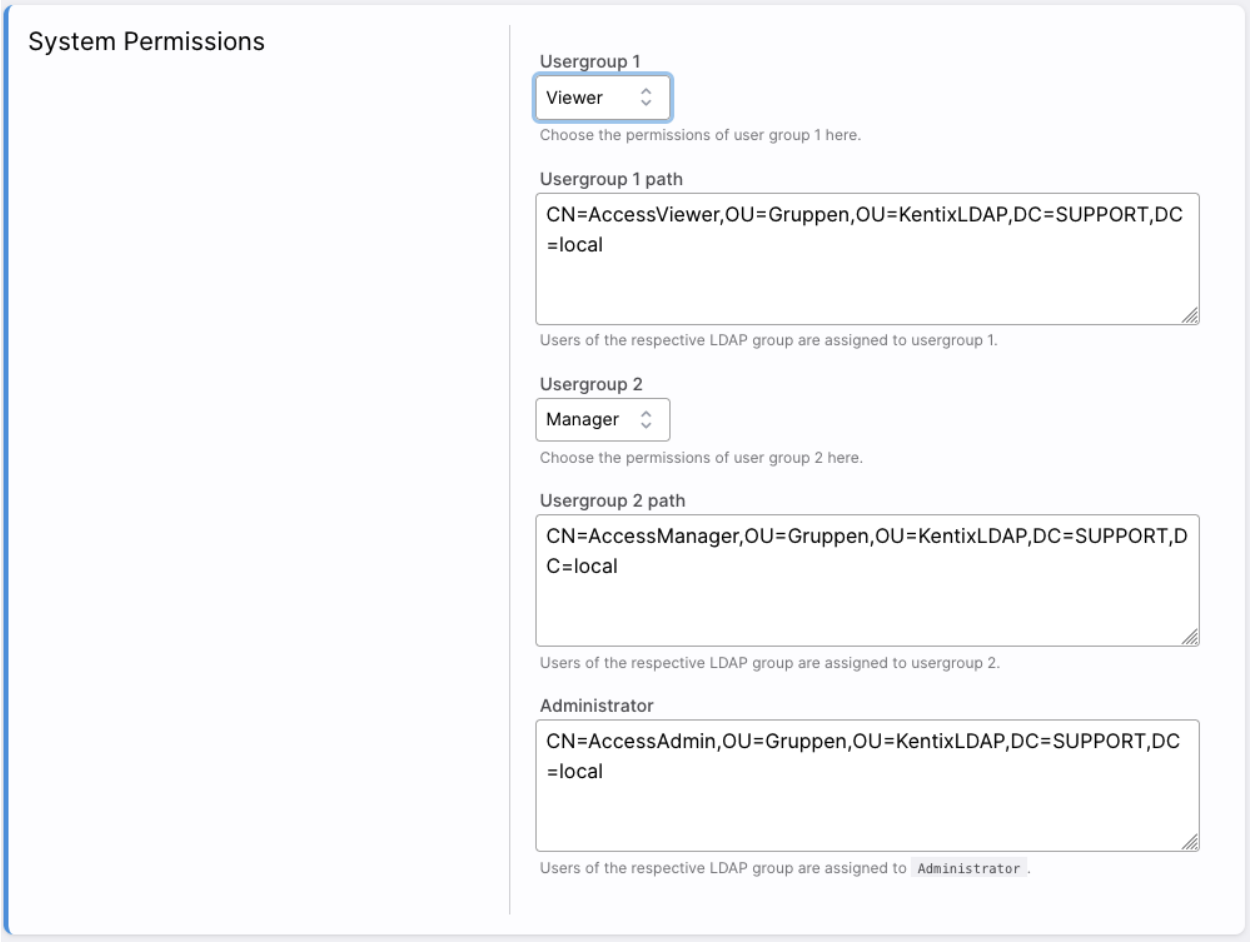
Gruppen

KentixONE kann drei Gruppen aus LDAP exportieren. Diese Gruppen dienen der Kontrolle des Zugriffs auf die KentixONE Oberfläche. Kentix Verwendet hierzu die Gruppen „Administratoren“, „Manager“ und „Viewer“. Jeder Benutzer in KentixONE muss einer dieser Gruppen zugeordnet werden, auch wenn keiner der Benutzer den Zugriff auf KentixONE erhalten soll. Für diese Gruppen

können sie entsprechende Gruppen in LDAP bestimmen.

Im Beispiel werden für die Kentix Gruppen „Viewer“, „Manager“ und „Administrator“ die Werte der LDAP Eigenschaften von CN=AccessViewer, CN=AccessManger und CN=AccessAdmin importiert. Diese Gruppen wurden zuvor in LDAP erstellt und die Benutzer diesen zugewiesen.

Der Import in KentixONE ist für 3 Gruppen insgesamt möglich.
Verschachtelte Gruppen können nicht importiert werden.

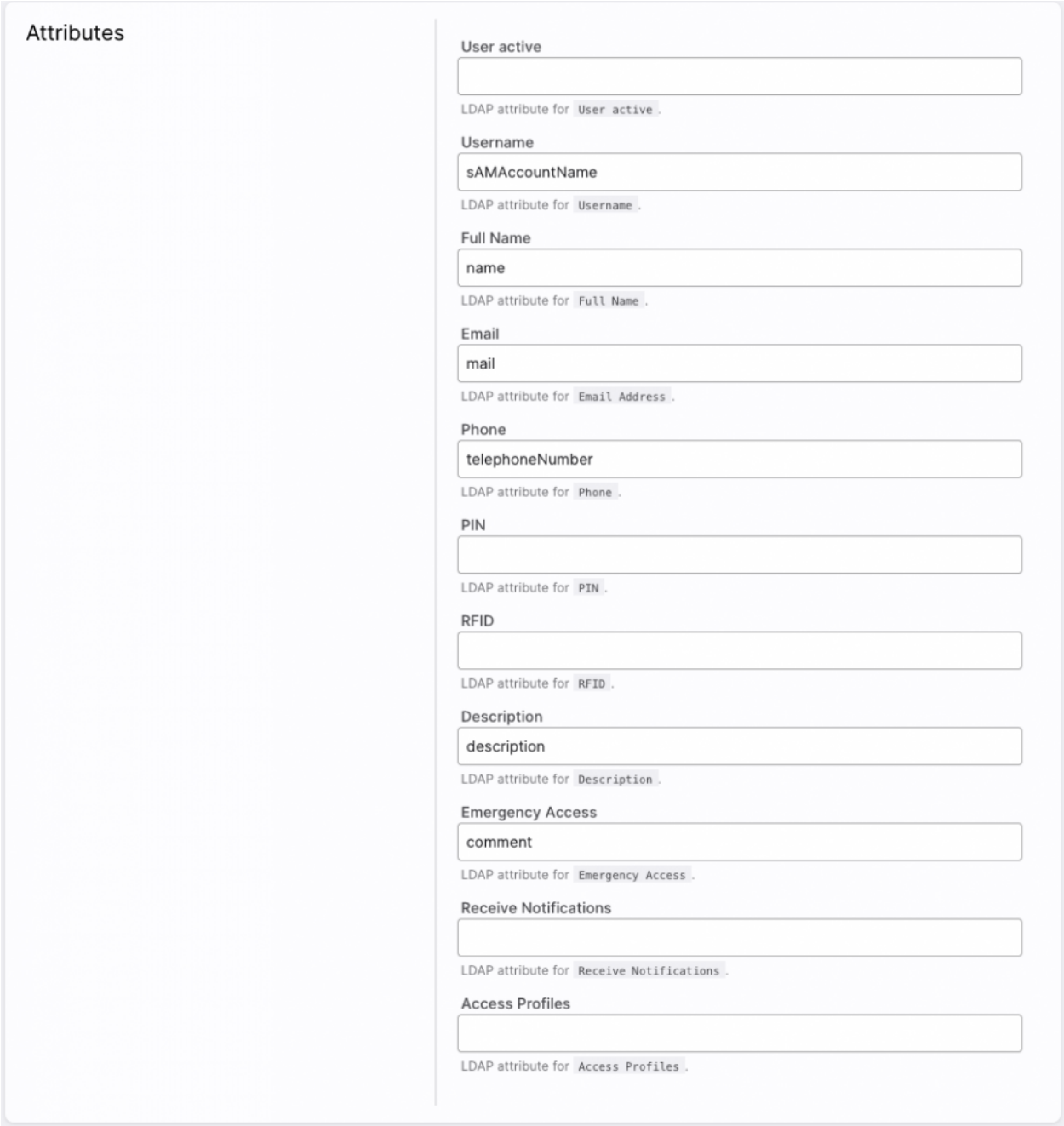


Gruppen Import

Benutzerdaten

Beim Import steht die Synchronisierung verschiedener Stammdaten der Benutzer zur Verfügung. Die Daten für die in KentixONE verwendeten Felder haben anderslautende Entsprechungen in LDAP. Deshalb werden im nächsten Schritt die zu übernehmenden Attribute der Benutzer mit den LDAP Attributen verknüpft.

Der KentixONE „Benutzername“ wird hier zum Beispiel mit dem LDAP Attribut „sAMAccountName“ verknüpft.



Zutritt

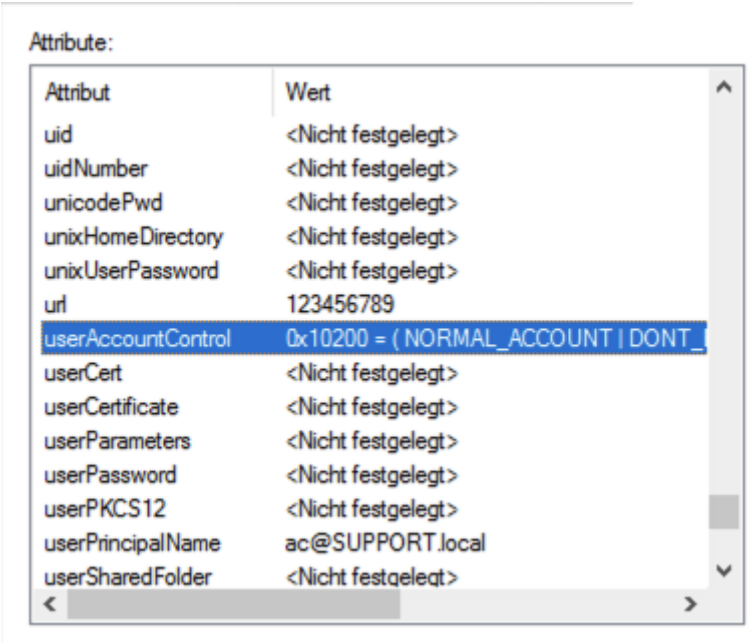
Der Zutritt von Benutzern kann somit aus der LDAP Struktur gesteuert werden. Ein Anwendungsfall ist zum Beispiel die Pflege der Daten inklusive der RFID-Tokens durch die Personalabteilung. Die dort verwendete Software überträgt die Daten in eine LDAP Struktur. KentixONE aktualisiert seine Benutzerdaten regelmäßig und erhält somit immer den aktuellen Stand der Personalsoftware.

Folgende Attribute sind für die Zutrittsteuerung relevant:

User Active

Verknüpfen sie dieses Attribut mit einem LDAP Attribut. Im Beispiel „userAccountControl“.

Wird der Benutzer in LDAP deaktiviert, wird er in KentixONE ebenfalls deaktiviert.



UserAccountControl

Alternativ ist auch ein eigenes LDAP Attribut mit „0“ oder „1“ (aktiv) möglich.

PIN und RFID

Daten für die Identifizierung von Benutzern im System. Werden diese bei der Anlage von Benutzern bereits in LDAP erfasst, können sie übernommen werden.

Die Gesamtlänge der PINs stellen sie systemweit in „Sicherheit“ ein.
Werden Rackhebel RA4 mit PINs für Zutritt und Schaltung der Alarmgruppen verwendet, beachten Sie:
Dort stehen lediglich die Zahlen 1-4 zur Eingabe bereit. Erstellen sie für Benutzer der Rackhebel deshalb nur PINs in diesem Zahlenbereich.

Notfallzutritt

Ermöglicht ausgewählten Benutzern den Zutritt, wenn der DoorLock keine Verbindung zum AccessManager aufbauen kann. Die Daten des Benutzers wird mit dieser Berechtigung lokal im DoorLock gespeichert. Verwenden sie hierzu ein Attribut mit „0“ oder „1“ (Notfallzutritt aktiv).

Der Notfallzutritt steht nicht sofort nach der Zuweisung an einen Benutzer zur Verfügung.
Die Benutzerdaten für den Notfallzutritt werden bei Buchungen an DoorLocks übertragen. Um jeden

Notfallbenutzer lokal im DoorLock zu speichern ist deshalb die gleiche Anzahl von Zutrittsbuchungen nötig, wie Notfallbenutzer erstellt wurden.

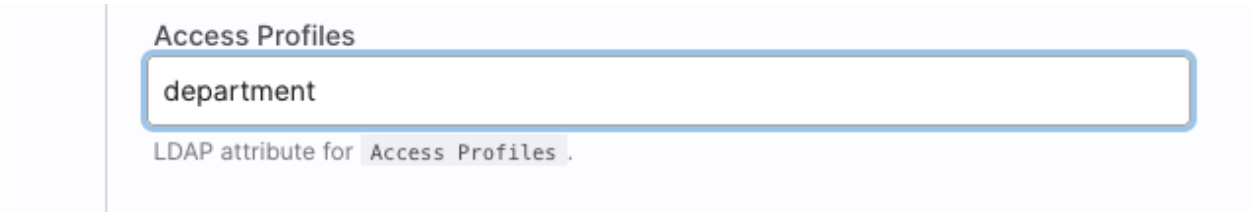
Zutrittsprofile

Sind in KentixONE und in der LDAP Struktur gleinnamige Profile vorhanden, können Zutrittsprofile mit den Benutzern übertragen werden. Diese Profile werden auf Benutzerebene von KentixONE verknüpft. Mehrere Zutrittsprofile können in LDAP als Aufzählung angelegt werden. Dabei gilt die Schreibweise: Profil1, Profil2, Profil3 usw.

Gruppen werden in KentixONE für die Zutrittsteuerung Importiert. Die Berechtigungen für den Zugriff auf das KentixONE System können dort für die Gruppen konfiguriert werden werden.

Im Beispiel hier wurde als Attribut „department“ in LDAP verknüpft. Es enthält eine Liste von Zutrittsprofilen für den Benutzer.

Zutrittsprofile als Liste in LDAP



Verknüpfung in KentixONE