

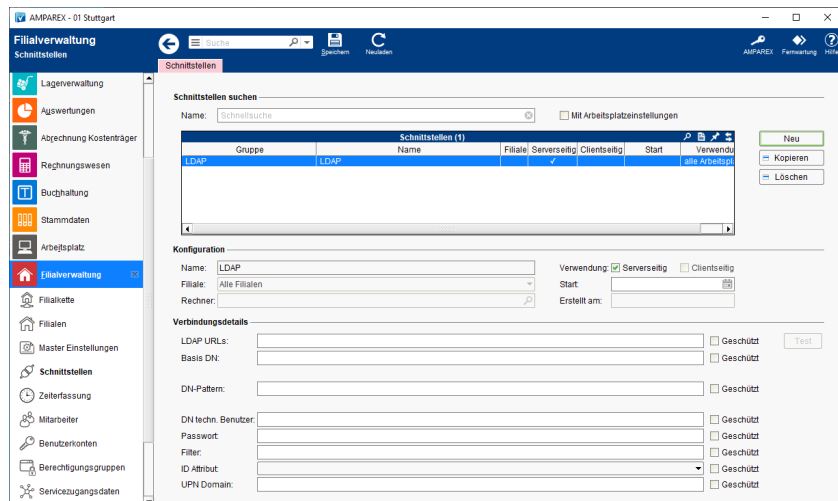
# LDAP | Schnittstelle

Bei der Anmeldung in AMPAREX wird der Benutzername und das Passwort gegenüber den konfigurierten Anmeldedaten in der AMPAREX-Datenbank geprüft. Als alternative Möglichkeit kann das Benutzerpasswort gegen die Daten in einem Active Directory/LDAP geprüft werden.



## Hinweis

Bei Nutzung der LDAP-Schnittstelle sollte die Einstellung 'Filialverwaltung Filialkette Sicherheit Passwort beim Benutzerwechsel immer abfragen' gesetzt sein. Zudem funktioniert das direkte Ummelden nicht. Ein Anwender muss sich immer zuerst abmelden, bevor sich ein anderer anmelden kann.



In der Filialverwaltung kann die Schnittstelle LDAP (ausschließlich für die gesamte Filialkette) angelegt werden.



## Achtung

Es wird lediglich das Passwort gegen LDAP/AD geprüft. Die Benutzer müssen wie bisher auch immer in AMPAREX angelegt sein und die Anmeldedaten übereinstimmen (siehe auch [Benutzerkonto | Filialverwaltung](#)).

**Die Konfiguration setzt detaillierte Kenntnisse des eingesetzten LDAP/AD voraus.** Wird die Konfiguration falsch durchgeführt, dann sind **keine normalen Benutzeranmeldungen** mehr möglich. In diesem Fall kann sich nur noch der ausgezeichnete 'Administrator'-Benutzer anmelden, dessen Passwort generell gegen die AMPAREX-Datenbank geprüft wird.

## Verschiedene Konfigurationsmöglichkeiten

1. Liegen die Benutzer alle in einer flachen Hierarchie und sind die eindeutigen Benutzernamen Teil des *DistinguishedName* (DN), dann kann über die Konfiguration eines *DN-Pattern* direkt auf die DNs zugegriffen werden.
2. Ist der Benutzername nicht Teil des DNs, dann muss der DN zuerst gesucht werden, bevor die Passwortprüfung ('BIND') erfolgt. In diesem Fall kann kein *DN-Pattern* konfiguriert werden und es muss neben dem technischen Benutzer auch noch das ID-Attribut und ggf. ein Filter angegeben werden.

## Schnittstellen suchen

| Feld                                                    | Beschreibung                                                                                                                           |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Mit Arbeitsplatz Einstellungen | Zeigt nur über Arbeitsplatz Einstellungen konfigurierte Schnittstellen an (siehe auch <a href="#">Schnittstellen   Arbeitsplatz</a> ). |

## Konfiguration

| Feld    | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filiale | Sie können über den Punkt Filiale den Service so einschränken, dass nur eine Filiale diesen Service nutzen darf - ist keine ausgewählt, darf jede Filiale den Service nutzen.                                                                                                                                                                                                                                          |
| Rechner | Mit der oben genannten Option 'Mit Arbeitsplatz Einstellungen' wird der Name des Arbeitsplatzrechners angezeigt, wenn die Schnittstelle über die Arbeitsplatz Einstellungen an einem gewünschten Computer eingerichtet wurde (siehe auch <a href="#">Schnittstellen   Arbeitsplatz</a> ). Wird die Schnittstelle über die Filialverwaltung eingerichtet, darf jeder Computer der Filialkette die Schnittstelle nutzen. |

# LDAP | Schnittstelle

|            |                                                                                                                                                                       |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verwendung | <input type="checkbox"/>                                                                                                                                              |
| Start      | Angabe eines Startdatums, ab wann die Schnittstelle in AMPAREX automatisch freigegeben werden soll. Bleibt das Feld leer, ist die Schnittstelle sofort einsatzbereit. |

## Verbindungsdetails

| Feld               | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Beispiel                                                                                                                                                                                     |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP URLs          | <p>URL zum LDAP-Server im Format <code>ldaps://&lt;servername&gt;[:389 636]</code>. Es können mehrere Server (getrennt durch Semikolon, Leerzeichen, oder Komma) angegeben werden. Ist der erste Server nicht erreichbar, wird automatisch versucht, die alternativen Server aufzurufen.</p> <div>  <b>Wichtig</b><br/> Sind mehrere LDAP/AD-Server angegeben, müssen diese die gleiche Struktur haben (Basis-DN, DN-technischer Benutzer, ID-Attribut, ...) </div>                                                                                                                                                                                           | <p><code>ldaps://ldap1.example.com:636</code></p> <p><code>ldaps://ldap1.example.com:636; ldaps://ldap2.example.com:636</code></p>                                                           |
| Basis DN           | Hier wird das Basis-Verzeichnis angegeben, ab dem nach den Benutzern gesucht wird. Üblicherweise liegen die Benutzer neben anderen Daten in einem eigenen Verzeichniszweig.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <code>ou=users, dc=example, dc=com</code>                                                                                                                                                    |
| DN-Pattern         | Diese Konfigurationsmöglichkeit (s. o.) darf nur vorgenommen werden, wenn die Benutzer in einer flachen Hierarchie liegen und der Benutzername Teil des DN ist. Im Pattern muss als Platzhalter für den Benutzernamen die Zeichenkette <code>{0}</code> verwendet werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <code>uid={0},ou=users, dc=example, dc=com</code>                                                                                                                                            |
| DN techn. Benutzer | Zum Suchen der Benutzer-DNs ist eine Anmeldung mit einem technischen Benutzer notwendig. Hier wird der vollständige DN des technischen Benutzers angegeben.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <code>cn=techuser, ou=accounts, dc=example, dc=com</code>                                                                                                                                    |
| Passwort           | <p>Passwort des technischen Benutzers.</p> <div>  <b>Hinweis</b><br/> Mit der Filialkettenoption 'Administratoren dürfen gesetzte Passwörter einsehen' (siehe auch <a href="#">Sicherheit   Filialverwaltung</a>), wird das Passwortfeld, wenn es in einer Schnittstelle vorhanden ist, um eine Funktion erweitert. D. h. wenn ein Benutzer aus der 'Administratoren-Gruppe' angemeldet ist, kann sich dieser das Passwort an einer Schnittstelle anzeigen lassen. Dazu muss der Benutzer auf das 'Auge' im Feld klicken und zur Sicherheit sein Benutzerpasswort in einem Dialog eingeben. Danach wird das Passwort an der Schnittstelle angezeigt. </div> |                                                                                                                                                                                              |
| Filter             | Es kann ein Filter eingegeben werden, um die Suche nach den Benutzer-DNs einzuschränken. Üblicherweise wird ein Filter auf die 'objectclass' verwendet. Der Filter muss im syntaktisch korrektem LDAP-Filter-Format eingegeben werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <code>(objectclass=inetorgperson)</code>                                                                                                                                                     |
| ID Attribut        | Auswahl des verwendeten ID-Attributs der Benutzer (dessen Werte eindeutig/unique sein müssen). Es gibt verschiedene ID-Attribute (z. B. <code>uid</code> , <code>cn</code> , <code>userPrincipalName</code> , ...), es müssen dabei alle Benutzer im Verzeichnis das gleiche ID-Attribut verwenden. Dieses ID-Attribut ist für die Benutzersuche (bzw. den Suchfilter) wichtig.                                                                                                                                                                                                                                                                                                                                                                | <p><code>userPrincipalName</code></p> <p>(Eintrag mit DN: <code>cn=testbenutzer, ou=users, dc=example, dc=com</code> hat ein Attribut <code>userPrincipalName=tester@example.com</code>)</p> |

# LDAP | Schnittstelle

|            |                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UPN Domain | Hier kann die Domäne des LDAP/AD angegeben werden. Dieser Eintrag wird nur dann berücksichtigt, wenn das ID-Attribut ' <i>userPrincipalName</i> ' ausgewählt wurde und die übergebene Benutzerkennung nicht schon die Domäne-Kennung enthält. | <div>example.com</div> <div>übergebener Benutzer: 'tester@example.com' UPN Domain wird nicht weiter berücksichtigt</div> <div>übergebener Benutzer: 'tester' konfigurierte UPN Domain wird angehängt 'tester@example.com'</div> |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Siehe auch ...

- [Marktforschung | Schnittstellen](#)