Handbuch

Unterstützung für LDAP

WeLearn Release 2.3.0

Oktober 2005

Das WeLearn-Team wünscht Ihnen viel Spaß und Erfolg im Arbeiten mit WeLearn. Bei Fragen und Anregungen können Sie uns unter info@welearn.at erreichen.

Unter http://www.welearn.at finden Sie ebenfalls Unterstützung und eine Zusammenstellung häufig gestellter Fragen.

© 2000- 2005 DI Dr. Susanne Loidl (loidl@fim.uni-linz.ac.at), o.Prof. Dr. Jörg R. Mühlbacher, ALLE RECHTE VORBEHALTEN

Inhaltsverzeichnis

1 WAS IST LDAP?

Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll, welches die Abfrage von Informationen eines Verzeichnisdienstes erlaubt. Die aktuelle Version ist in RFC 2251 (http://www.rfc-editor.org/rfc/rfc2251.txt) spezifiziert.

LDAP wurde 1995 an der Universität von Michigan entwickelt und stellt eine vereinfachte Form des so genannten DAP-Protokolls dar, welches im X.500-Standard definiert ist. Der X.500-Standard ist sehr umfangreich und setzt auf einem vollständigen ISO/OSI-Stack auf, was die Implementierung schwierig machte und damit einen Erfolg verhinderte.

2 WAS ERMÖGLICHT DIE „LDAP UNTERSTÜTZUNG“ BEI WELEARN?

In WeLearn kann LDAP für zwei unterschiedliche Aufgaben verwendet werden. Zum einen unterstützt die LDAP Implementierung von WeLearn das Importieren von Benutzerdaten von einem LDAP Server. D. h., dass Benutzer, die bereits im LDAP Verzeichnisdienst angelegt sind, direkt in WeLearn importiert werden können. Mit den importierten Benutzerdaten werden vom System „normale“, lokale WeLearn Benutzer erstellt, die aber im weiteren Verlauf keine weitere Besonderheit mehr aufweisen.

Zum anderen kann ein LDAP Server verwendet werden, um die Benutzerauthentifizierung für WeLearn-Benutzer durchzuführen. Das heißt, dass die Zugangsdaten eines Benutzers zentral auf dem LDAP Server (bzw. im Active Directory) verwaltet werden. Jedes Mal, wenn sich ein Benutzer einloggt, wird das eingegebene Passwort nicht gegen das lokale WeLearn Passwort überprüft. Vielmehr wird das aktuelle Passwort vom LDAP Server übermittelt, bzw. führt dies der LDAP Server selbst die Authentifizierung durch, wie es beispielsweise beim Microsoft Active Directory (bei Windows Server) der Fall ist.

Die Vorteile einer zentralen Accountverwaltung sind bekannt und werden an dieser Stelle nicht weiter erörtert. Für WeLearn sind die Argumente ausschlaggebend, dass Accounts zentral aktiviert und deaktiviert werden können und weiters, dass die Benutzer nur ein

einziges Passwort für die Benutzung mehrerer System benötigen. Im Fall einer Änderung muss dieses nur an einer einzigen Stelle (nämlich in der Datenbasis des LDAP-Servers) geändert werden.

3 GRUNDLEGENDES

Um eine LDAP Verbindung herstellen zu können, sind einige grundlegende Kenntnisse über LDAP notwendig. Generell wird vor Beginn der Konfiguration des WeLearn Systems für den LDAP Einsatz empfohlen, mittels eines „LDAP Browsers“ das LDAP-Verzeichnis zu erkunden. Ein kostenloses Produkt, welches sich hervorragend für diese Aufgabe eignet, ist etwa der LDAP Browser von der Firma Softerra (www.softerra.com). Aus lizenzrechtlichen Gründen kann dieser leider nicht auf der WeLearn.System CD mitgeliefert werden, sondern muss individuell heruntergeladen werden.

Im Weiteren wird hauptsächlich davon ausgegangen, dass Sie als Verzeichnisdienst das Microsoft Active Directory verwenden, welches bei Windows Servern von zentraler Bedeutung ist. Eine derartige Infrastruktur ist in der Praxis sehr häufig anzutreffen. Das Microsoft Active Directory bietet eine LDAP-Schnittstelle, d. h., dass mit LDAP-Client Produkten auf die darin gespeicherten Daten zugegriffen werden kann.

3.1 Binding-Benutzer

Wie bereits erwähnt kann mittels der LDAP Funktionalität in WeLearn auch auf Windows-Server zugegriffen werden. Das Microsoft Active Directory bietet eine LDAP Schnittstelle an, welche von WeLearn verwendet werden kann. Voraussetzung ist, dass diese Funktionalität nicht deaktiviert oder durch eine Firewall blockiert wurde (Port 389).

Zunächst muss auf dem LDAP Server ein Benutzer eingerichtet werden, welcher berechtigt ist, auf das Active Directory und somit auf den LDAP Server zuzugreifen und dort Daten auszulesen. Unter Windows hat jeder Benutzer im Active Directory (sofern der Account nicht deaktiviert wurde, der Account abgelaufen ist, etc.) das Recht, sich mittels eines LDAP-Clients auf den Server zu verbinden und dort Verzeichnis-Daten einzusehen. Dieser neu angelegte Benutzer wird im weiteren Verlauf als „*Binding-Benutzer*“ bezeichnet (weil dieser verwendet wird, um sich zum Server zu ver-“binden“).

Es sollte sich um einen dedizierten Benutzeraccount handeln, der ausschließlich für diese Aufgabe erstellt wird.

3.1.1 Binding-Benutzerdaten für Active Directory ermitteln

Zu beachten ist, dass unter Windows der zum Verbinden benötigte Benutzername des Binding-Benutzers nicht derselbe ist, mit welchem man sich an der Domäne anmeldet. Den Benutzernamen des Binding-Benutzers in Erfahrung zu bringen, ist eine erste kleine Hürde für LDAP-Neulinge. Zuerst ist es notwendig, das Benutzeradministrations-werkzeug des Active Directories, welches als Snap-In für die MMC (Microsoft Management Console) geliefert wird, zu öffnen. Dort müssen die Eigenschaften des angelegten Binding-Benutzers im Kontextmenü desselbigen aufgerufen werden.

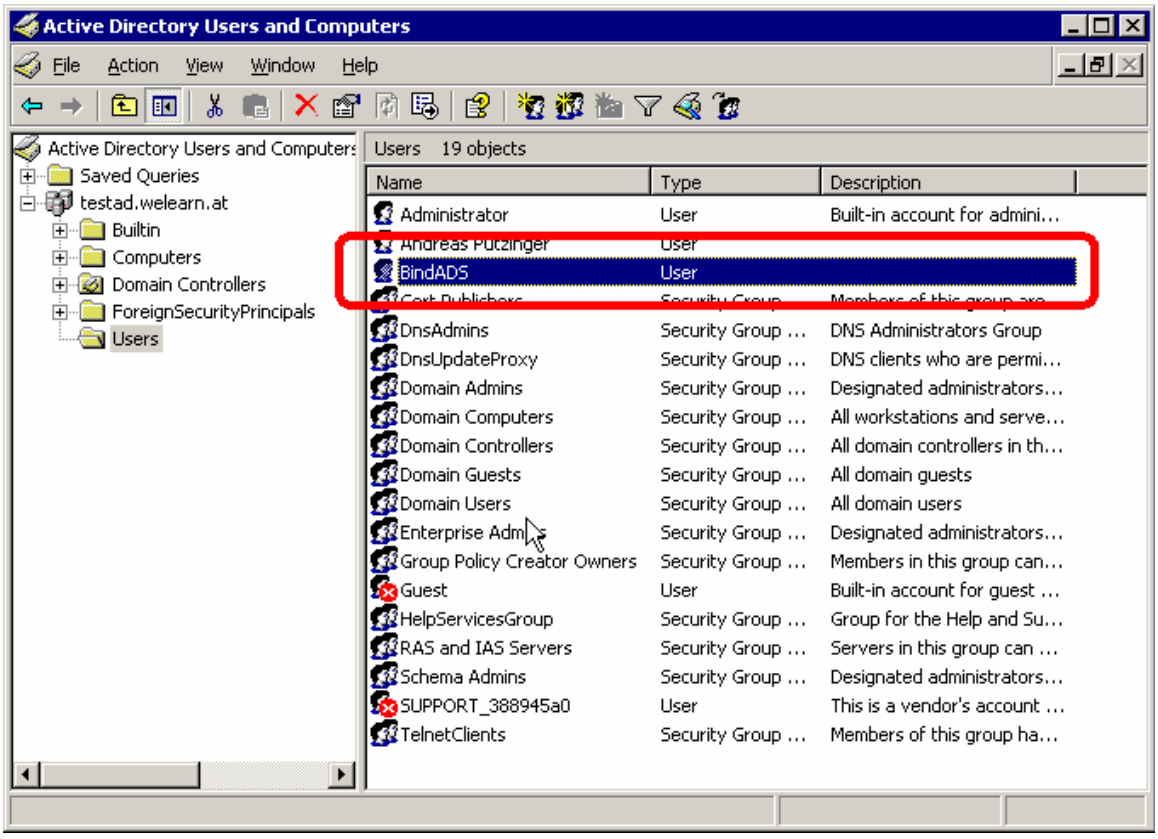

Abbildung 1: MMC Snap-In zur Benutzerverwaltung

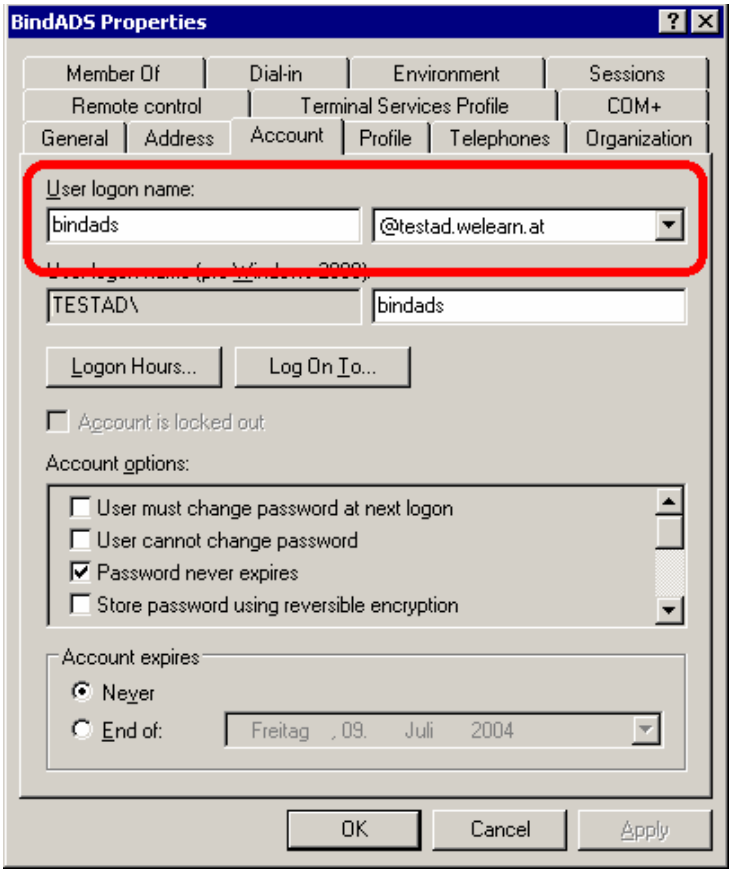

Abbildung 2: Eigenschaften des Binding-Benutzers

Der in der Abbildung markierte Teil besteht aus zwei Abschnitten. Der linke Abschnitt entspricht dem Benutzernamen des Binding-Benutzers zur Anmeldung an der Domäne. Der rechte Teil besteht aus den verwendeten Domänen-Komponenten. Dieser rechte Teil ohne dem Klammeraffen („@“) wird nun benötigt (im Beispiel: testad.welearn.at).

Die Wörter zwischen den Punkten werden als „Domänenkomponenten“ bezeichnet.

testad.welearn.at wird in LDAP Notation wie folgt angeschrieben:

`dc=testad,dc=welearn,dc=at` (wobei dc für Domain Component steht).

Im nächsten Schritt muss ermittelt werden, in welchem Verzeichnispfad des Active Directories der Binding-Benutzer liegt.

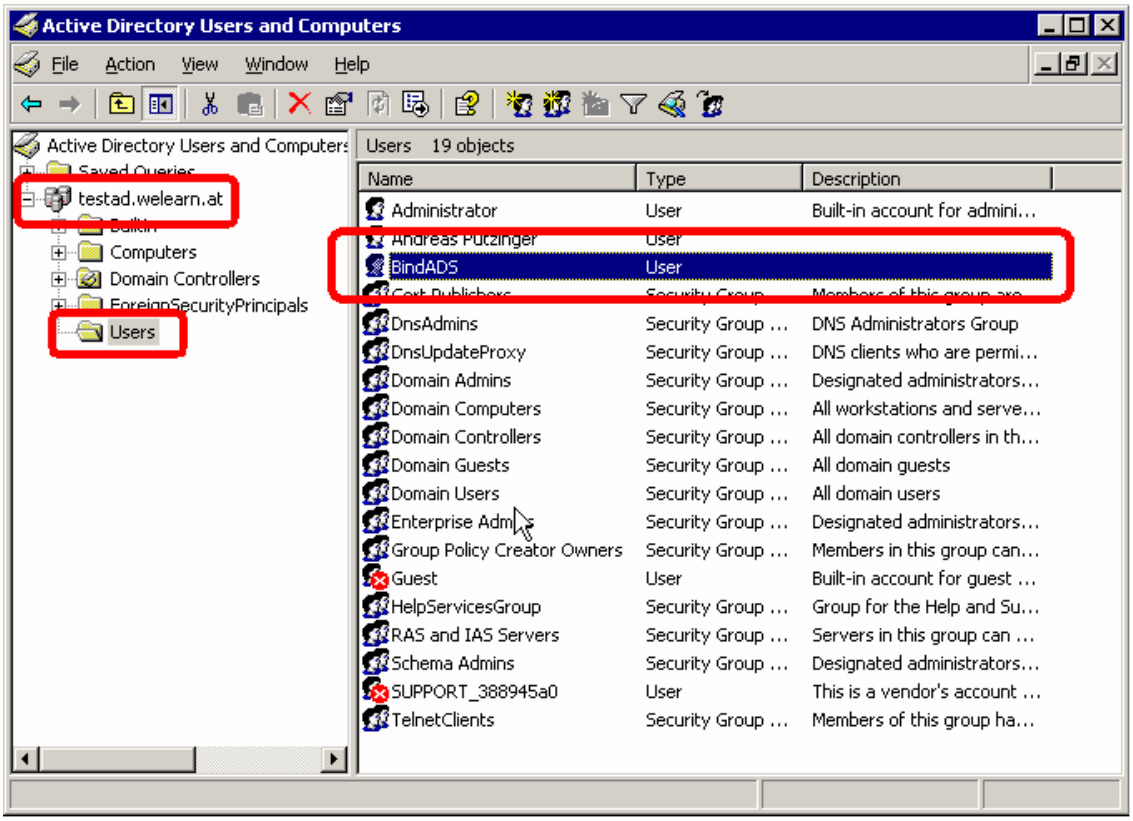

Abbildung 3: Verzeichnispfad zum Binding-Benutzer

Wie in der Abbildung ersichtlich liegt der Benutzer BindADS innerhalb der Domäne „testad.welearn.at“ (bereits im vorigen Schritt festgestellt) und dort innerhalb der Gruppe Users. Übersetzt in LDAP Notation heißt dieser Pfad

`cn=Users,dc=testad,dc=welearn,dc=at` (cn = CommonName)

Dass Users ein CommonName ist, ist deshalb ersichtlich, weil der Ordner auf der linken Seite mit einem „normalen“ Ordnersymbol dargestellt ist. Würde es sich um ein Symbol wie bei „Domain Controllers“ handeln, würde man von einer ou = Organizational Unit sprechen. Der entsprechende LDAP Pfad würde dann

`ou=Users,dc=testad,dc=welearn,dc=at` (ou = Organizational Unit)

lauten.

Als letzte Komponente für den Binding-Benutzer ist der eigentliche Benutzername notwendig. Dazu muss abermals ein Blick in die Eigenschaften des Benutzers im Active Directory geworfen werden.

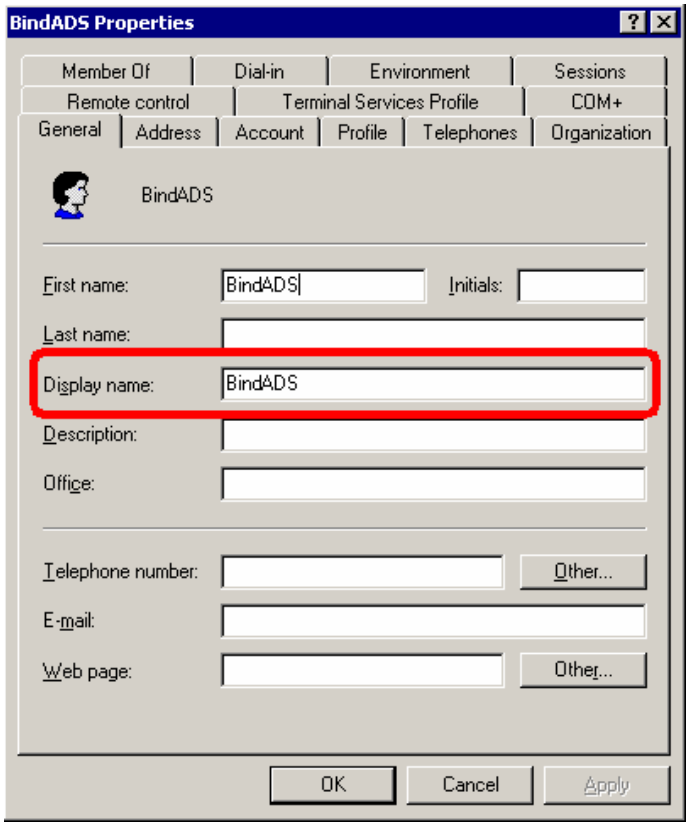

Abbildung 4: Display-Name des Binding-Benutzers

Der Benutzername entspricht dem Display-Namen. Dieser wird als Common-Name dem Pfad vorangestellt (der Display-Name kann auch Leerzeichen enthalten, welche ebenfalls 1:1 übernommen werden müssen). Der vollständige LDAP Benutzername für den Binding-Benutzer lautet hiermit:

```
cn=BindADS,cn=Users,dc=testad,dc=welearn,dc=at
```

Das Passwort für den Binding-Benutzer entspricht dem im Active Directory gesetzten Passwort des Benutzers.

Bitte beachten Sie, dass, wenn Sie den Binding-Benutzer in einen anderes Verzeichnis im Active-Directory verschieben, sich auch der LDAP-Benutzername des Binding-Benutzers ändert!

3.1.2 Benutzerverwaltung im Active-Directory

Sofern die Benutzer für WeLearn im Active-Directory noch nicht existieren, wird empfohlen, diese in einer neuen Organizational Unit (oder in einem normalen Ordner) anzulegen, wie dies in den folgenden Abbildungen dargestellt wird. Zwei Benutzer „wluser1“ und „wluser2“ werden in der Organizational Unit „wlusers“ erstellt.

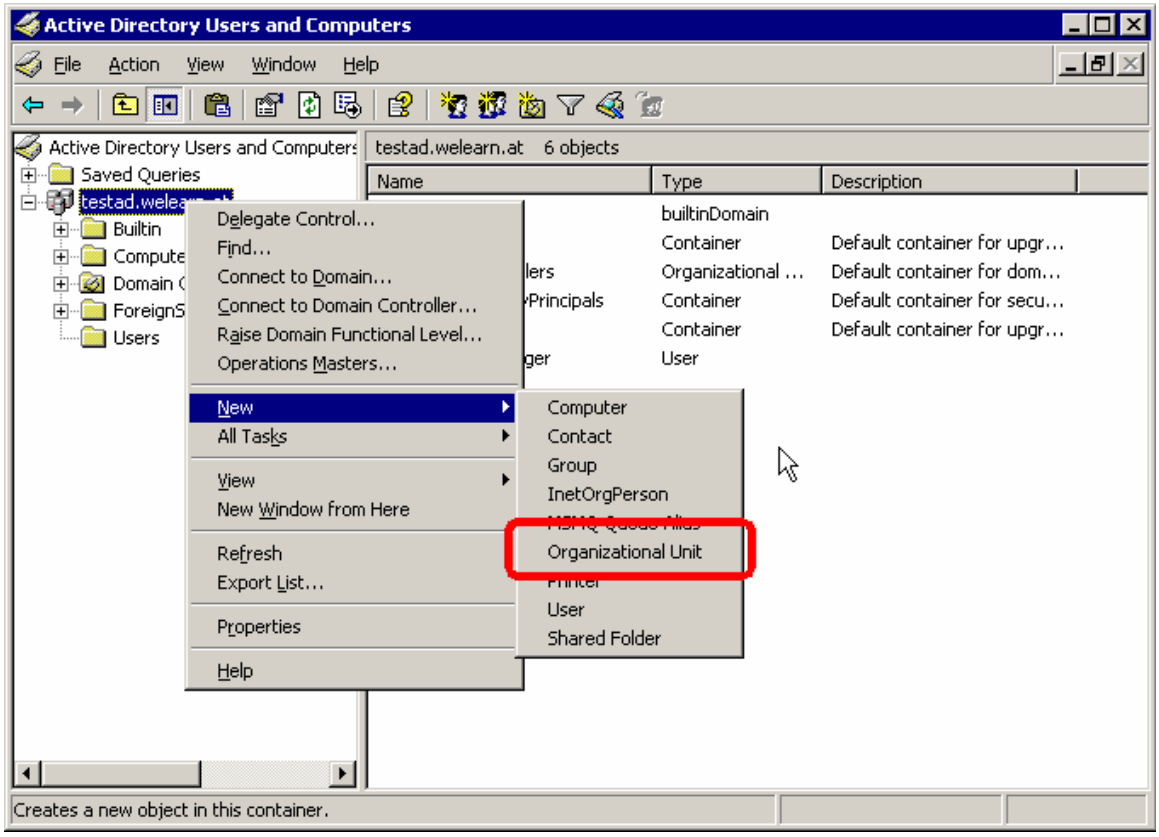

Abbildung 5: Erzeugen einer Organizational Unit für die WeLearn Benutzer

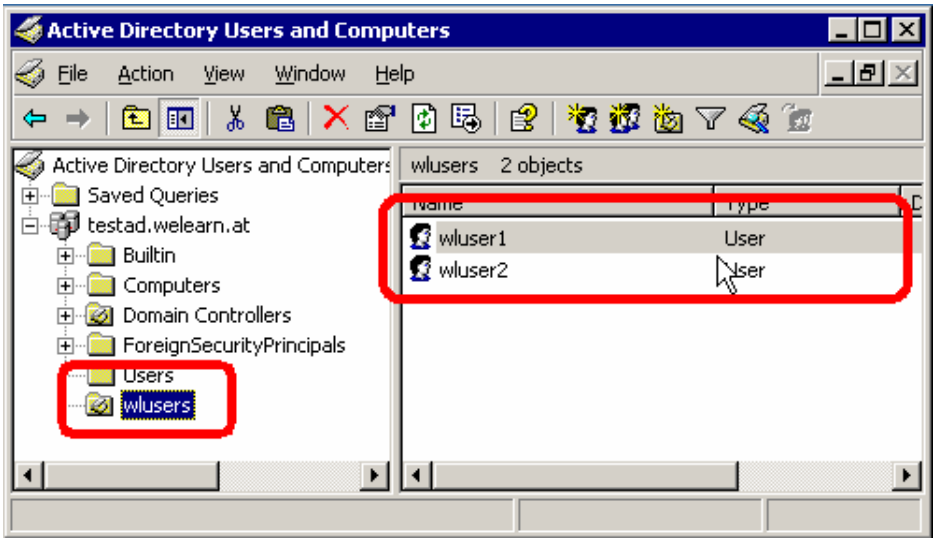

Abbildung 6: Zwei Benutzer in der OU „wlusers“

3.1.3 Binding-Benutzer testen

Im nächsten Schritt soll versucht werden, ob man sich mit den ermittelten Binding-Benutzer-Daten zum LDAP-Server verbinden kann. Dazu wird der erwähnte LDAP Browser der Firma Softerra verwendet und eine neue LDAP Verbindung eingerichtet.

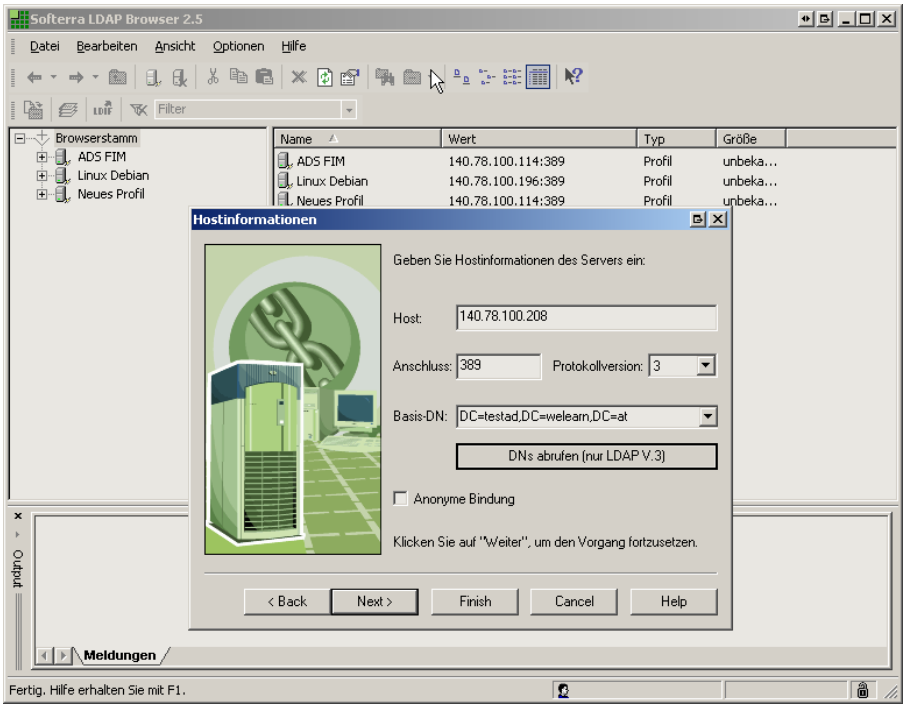

Abbildung 7: Anlegen einer neuen Verbindung im LDAP-Browser - Serverdaten

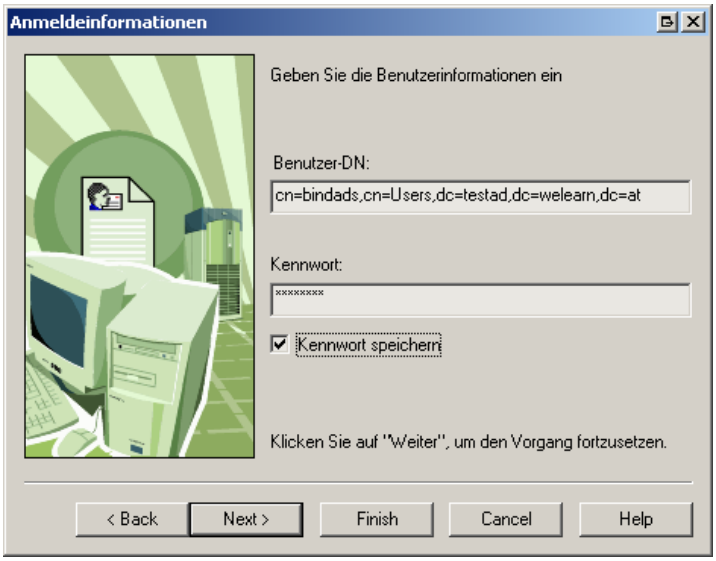

Abbildung 8: Daten des Binding-Benutzers eingeben

Kommt an dieser Stelle eine Verbindung nicht zustande und erscheint die Meldung „Invalid Credentials“ (oder eine ähnliche), so sollten folgende Punkte überprüft werden:

- Korrekte Zusammensetzung des Benutzernamens des Binding-Benutzers
- Korrektes Passwort für den Binding-Benutzer
- Firewall dazwischen (Port 389)?
- Binding-Benutzer aktiviert?

Nach einem erfolgreichen Verbinden bekommt man eine ähnliche Struktur wie in der folgenden Abbildung:

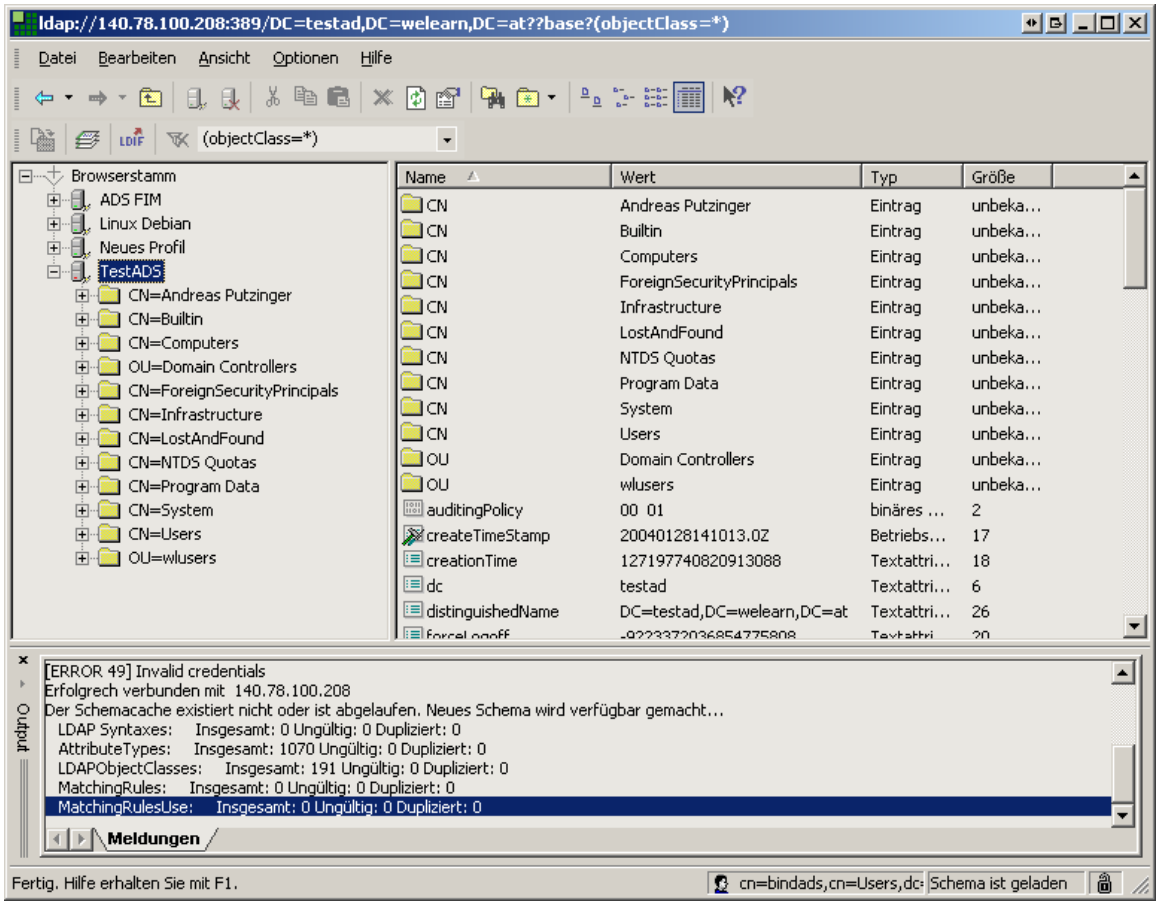

Abbildung 9: Ansicht nach erfolgreichem Verbinden zum Active Directory

Sobald eine Verbindung erfolgreich hergestellt wurde, hat man die Gewissheit, dass die Daten für den Binding-Benutzer korrekt sind.

3.2 Startcontext

Als Startcontext wird derjenige Pfad bezeichnet, der das Verzeichnis beschreibt, in welchem die Benutzer zu finden sind, die von WeLearn gefunden werden sollen. Im obigen Beispiel wäre dies

```
ou=wlusers,dc=testad,dc=welearn,dc=at
```

da sich in der Organizational Unit „wlusers“ die Benutzer befinden, welche grundsätzlich von WeLearn als Benutzer importiert werden können. Wurde im Active Directory keine separate Strukturierung eingeführt und alle Benutzer im Ordner „Users“ angelegt, könnte der Startcontext beispielsweise wie folgt aussehen:

```
cn=Users,dc=testad,dc=welearn,dc=at
```

Würden die Benutzer wluser1 und wluser2 in einen anderen Ordner verschoben, könnten sich diese Benutzer nicht mehr einloggen, da nur im Startcontext Verzeichnis nach diesen gesucht wird.

Zu erwähnen ist auch, dass WeLearn standardmäßig auch die Unterordner des Start-contexts nach Benutzern durchsucht.

Wichtig: Ein Context muss immer mit einem „ou=…“ oder mit einem „cn=…“ beginnen!

4 BENUTZER IMPORTIEREN UND GEGEN LDAP AUTHENTIFIZIEREN

4.1 WeLearn-Konfiguration für die Benutzung eines Active Directories

Um WeLearn für die Authentifizierung gegen ein Active Directory vorzubereiten, muss die WeLearn Konfiguration mittels des mitgelieferten Konfigurations-Programms angepasst werden. Die Bedienung des Konfigurations-Programms kann in einem eigenen Handbuch nachgelesen werden. Nachfolgend wird nur die Konfiguration der LDAP-Einstellungen besprochen.

Vor einer Konfigurations-Änderung muss Tomcat (und somit WeLearn) gestoppt werden (Systemsteuerung → Verwaltung → Dienste→Apache Tomcat→stoppen). Starten Sie dann das Konfigurationsprogramm und wechseln Sie auf die LDAP-Seite.

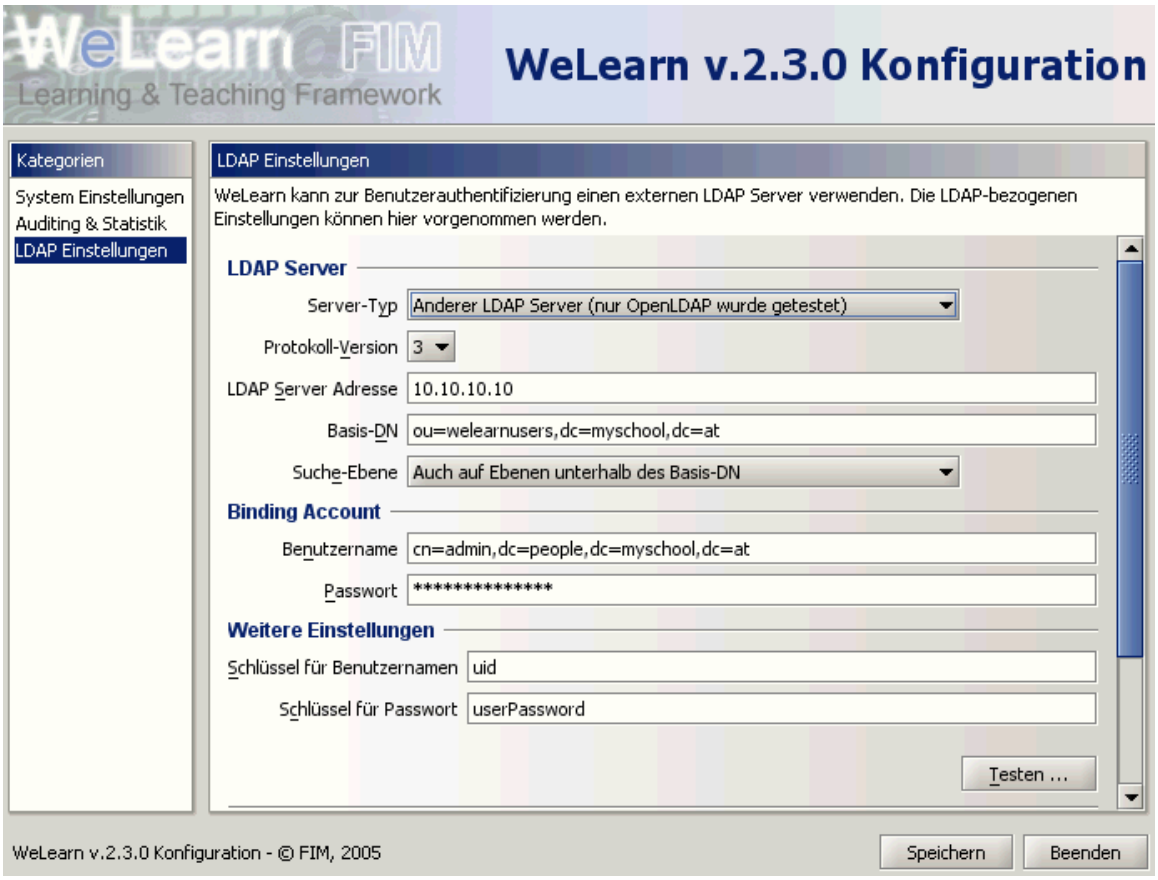

Abbildung 10: LDAP Konfigurationsseite

Stellen Sie unter „Server-Typ“ „Microsoft Active Directory“ ein und fügen Sie die bereits besprochenen Einstellungen in die vorgesehenen Felder ein.

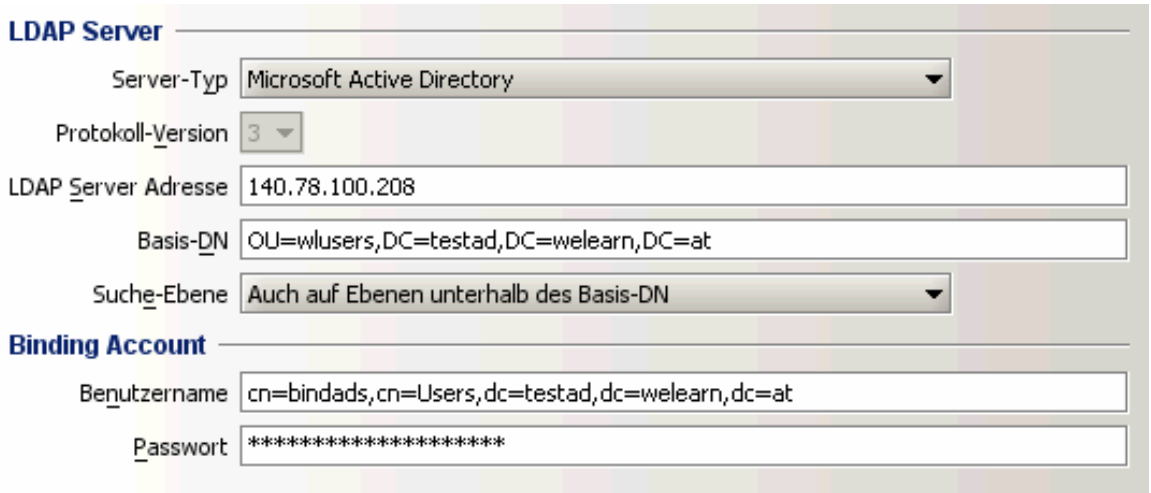

Abbildung 11: Active Directory konfigurieren

Im Feld „Suche-Ebene“ können Sie einstellen, ob ausschließlich auf Ebene des Basis-DN Benutzer gesucht werden sollen, oder auch in Unterebenen, was die stdm. Einstellung darstellt.

4.2 WeLearn-Konfiguration für die Benutzung eines OpenLDAP Servers

Um WeLearn für die Authentifizierung gegen einen OpenLDAP vorzubereiten, muss die WeLearn Konfiguration mittels des mitgelieferten Konfigurations-Programms angepasst werden. Die Bedienung des Konfigurations-Programms kann in einem eigenen Handbuch nachgelesen werden. Nachfolgend wird nur die Konfiguration der LDAP-Einstellungen besprochen.

Vor einer Konfigurations-Änderung muss Tomcat (und somit WeLearn) gestoppt werden (Systemsteuerung → Verwaltung → Dienste→Apache Tomcat→stoppen). Starten Sie dann das Konfigurationsprogramm und wechseln Sie auf die LDAP-Seite.

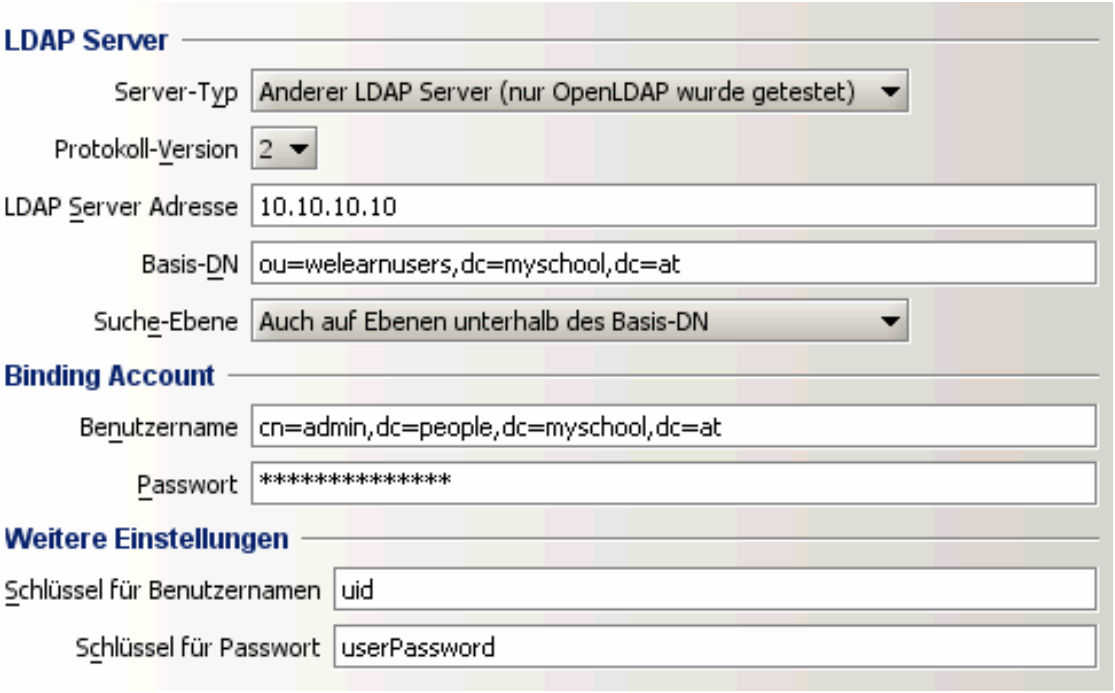

Abbildung 12: OpenLDAP konfigurieren

Stellen Sie im Feld für „Server-Typ“ „Anderer LDAP Server“ ein und setzen Sie die Daten Ihres LDAP Servers in den restlichen Feldern ein.

4.3 Importvorgang in WeLearn

Zunächst als Administrator in WeLearn einloggen. Nachdem im Control Panel „Users“ geöffnet wurde, kann man die Option „Import users from LDAP“ auswählen.

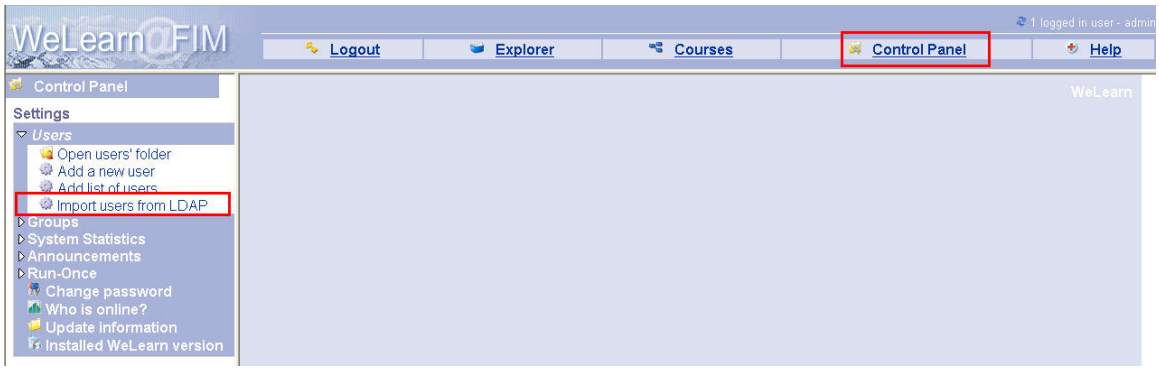

Abbildung 13: LDAP users auswählen

Danach die Möglichkeit zwei auswählen und auf den „Next“ Button drücken.

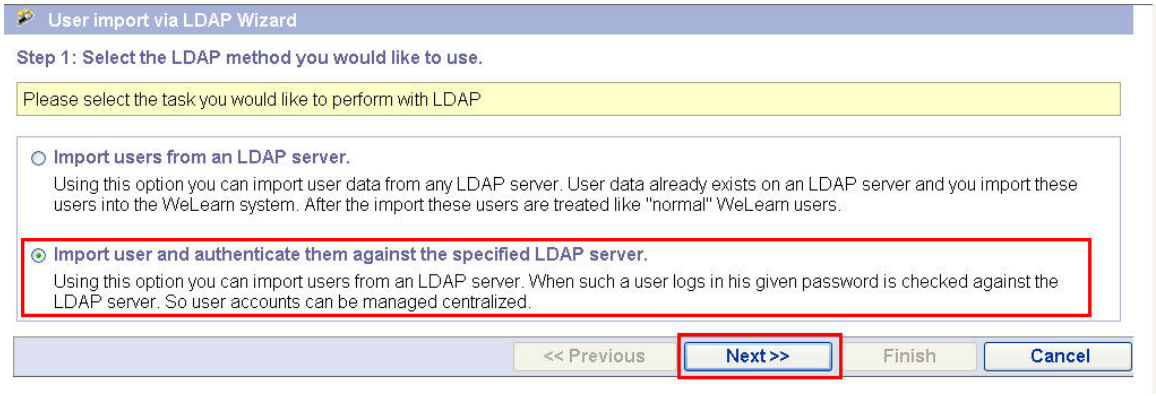

Abbildung 14: Möglichkeit zwei auswählen

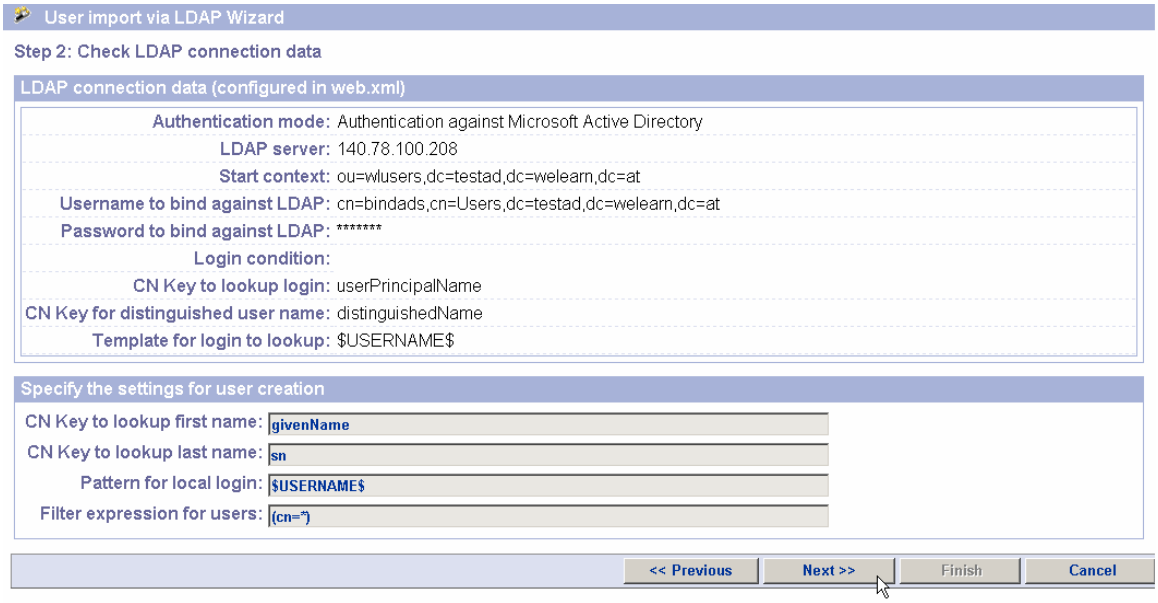

Abbildung 15: Übersicht der LDAP Konfiguration

Auf dieser Seite wird eine Zusammenfassung der in der „web.xml“ getätigten Einstellungen (inklusive den nicht explizit spezifizierten Standard-Einstellungen) angezeigt. Im Beispiel wurde eine Authentifizierung gegen ein Active Directory konfiguriert. Die Standard-Einstellungen reichen für die gängigsten Fälle aus und müssen deshalb meist nicht mehr verändert werden.

Ist als „Pattern for local login“ `$USERNAME$` eingestellt (ebenfalls standardmäßig), wird der WeLearn-Benutzername derselbe sein, der auch für den Login an der Domäne verwendet wird. Sollten die Benutzernamen anders gestaltet werden, wie z. B. mit vorname.nachname, dann ist dies durch Eingabe von `$FIRSTNAME$.$LASTNAME$` möglich.

Mit einem Klick auf „Next“ versucht WeLearn.System, sich zum LDAP Server zu verbinden und die gewünschten Daten zu ermitteln. Ist dieser Vorgang erfolgreich, erscheint eine Maske, die im Beispiel wie folgt aussieht:

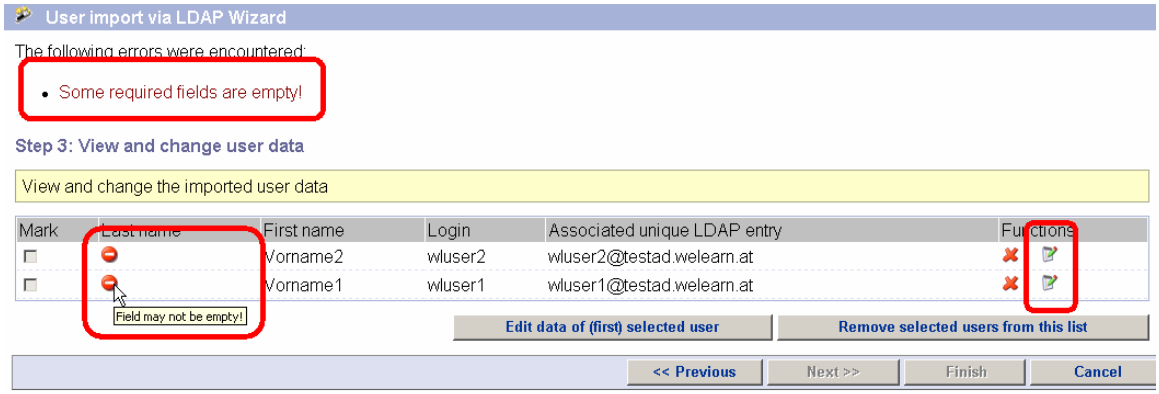

Abbildung 16: Vorgang erfolgreich

In den Account-Daten der Active-Directory Benutzer wurden keine Nachnamen eingetragen. Jeder WeLearn Benutzer benötigt jedoch einen solchen. Deshalb können an dieser Stelle die importierten Daten noch modifiziert werden (Klick auf das „Bearbeiten“-Symbol neben den Datensätzen).

Die Spalte mit dem Titel „Associated unique LDAP entry“ dient lediglich zur Information, welches Datum verwendet wird, um am LDAP-Server die eindeutige Identifizierung vornehmen zu können. Die Daten in dieser Spalte sollen nicht geändert werden. Ist kein Eintrag in der Spalte vorhanden, kann der Benutzer nicht über LDAP authentifiziert werden.

Wenn alle Datensätze in der Liste korrekt vorliegen, wird der „Next“-Button freigeschaltet.

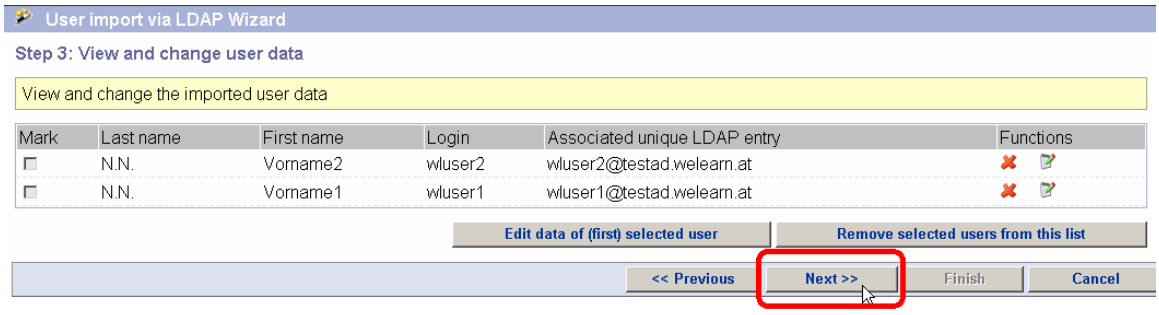

Abbildung 17: Übersicht der zu importierenden Benutzer, fehlerbereinigt

Mit einem Klick auf „Next“ gelangt man zur nächsten Seite, wo Einstellungen zum Anlegen der Benutzer getroffen werden können (siehe auch „Add list of users“ im Handbuch für Administratoren und Kursleiter).

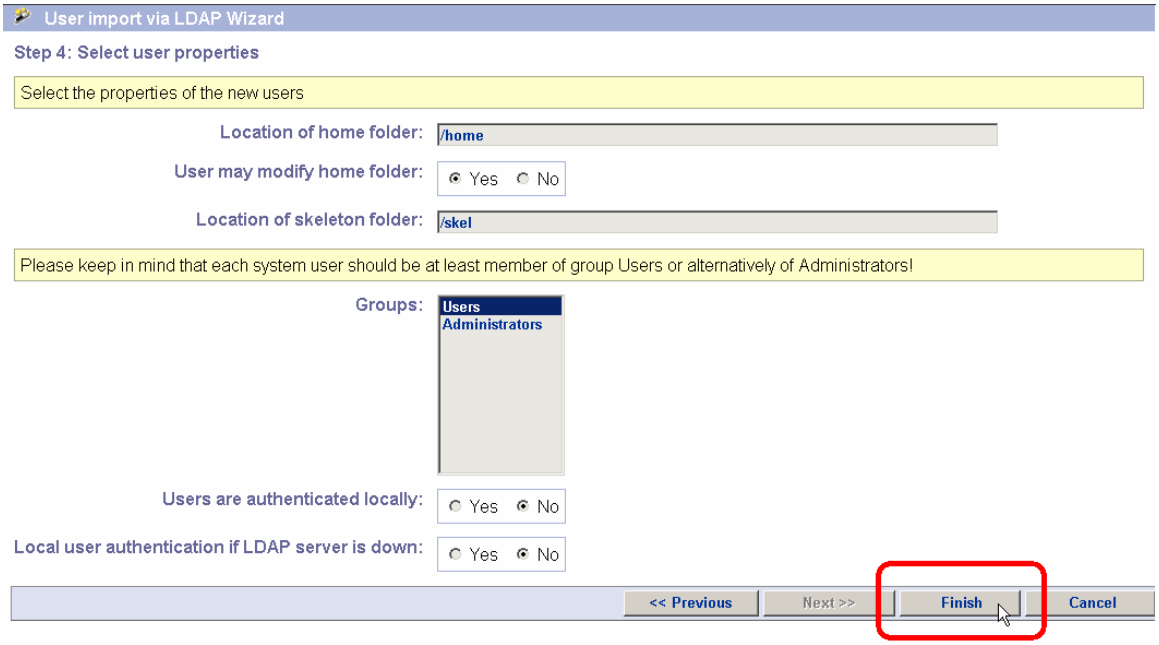

Abbildung 18: Einstellungen zum Anlegen der Benutzer

Wird „Users are authenticated locally“ auf „Yes“ gestellt, wird der Benutzer lokal authentifiziert. Jeder WeLearn Benutzer (auch diejenigen, die von einem LDAP Server importiert wurden) hat ein WeLearn Passwort (das sich vom Passwort am LDAP Server unterscheidet). Bei der lokalen Authentifizierung wird das eingegebene Passwort gegen dieses geprüft. Wird die Option also gesetzt, besteht im Weiteren kein Unterschied mehr zu „normal“ angelegten Benutzern. Der LDAP Server wird zum späteren Betrieb nicht mehr benötigt.

Wird die Option „Local user authentication if LDAP server is down“ gewählt, wird das vom Benutzer eingegebene Passwort zum LDAP Server geschickt und überprüft. Ist die Authentifizierung erfolgreich, ist der Benutzer eingeloggt. Ist die Authentifizierung nicht erfolgreich (z. B. falsches Passwort, deaktivierter Account, etc.), bekommt der Benutzer eine Fehlermeldung. Ist der LDAP Server jedoch nicht erreichbar, wird das eingegebene Passwort bei gesetzter Option zusätzlich noch gegen das lokale WeLearn Passwort des Benutzers überprüft (welches vom Passwort am LDAP-Server abweicht).

Ist letztgenannte Option gesetzt, muss der Administrator den neu angelegten Benutzern auch noch das auf der nächsten Seite des Wizards erzeugte, zufällige Passwort mitteilen, welches die Benutzer verwenden können, wenn eine LDAP Authentifizierung nicht möglich ist, weil der LDAP Server nicht erreichbar ist.

Ein Klick auf Finish liefert folgendes Ergebnis:

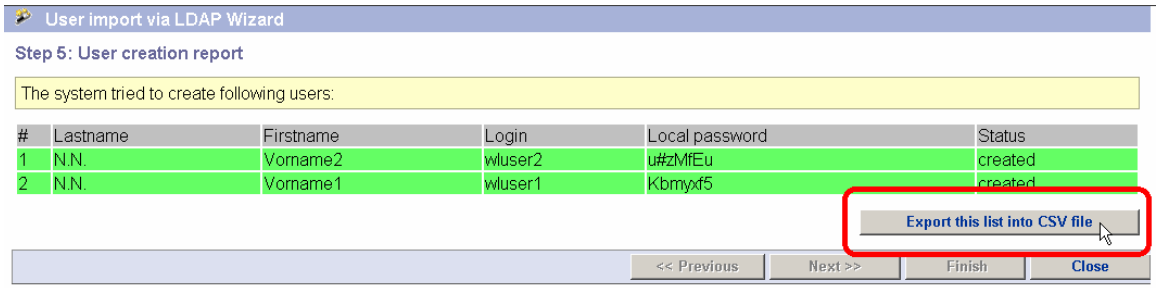

Abbildung 19: Angelegte Benutzer

Das Ergebnis kann mit einem Klick auf „Export this list into CSV file“ in eine Datei exportiert werden.

Die Benutzer wurden tatsächlich angelegt, wie aus einem Blick in das Users-Verzeichnis ersichtlich ist:

Abbildung 20: Users-Verzeichnis nach dem Importieren der Benutzer

In den Eigenschaften der neu angelegten Benutzer können noch diverse LDAP-Einstellungen vorgenommen werden, die im Detail bereits erläutert wurden:

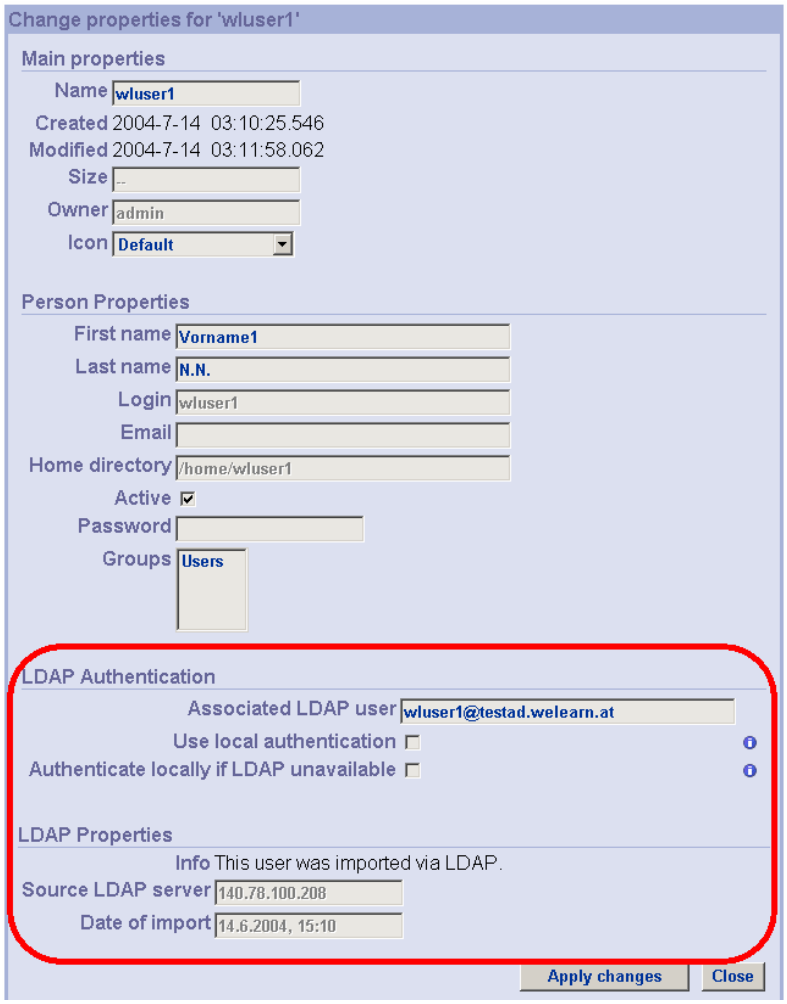

Abbildung 21: Eigenschaften eines importierten Benutzers

Die angelegten Benutzer können sich ab sofort mit LDAP-Benutzernamen und Passwort am WeLearn System anmelden.

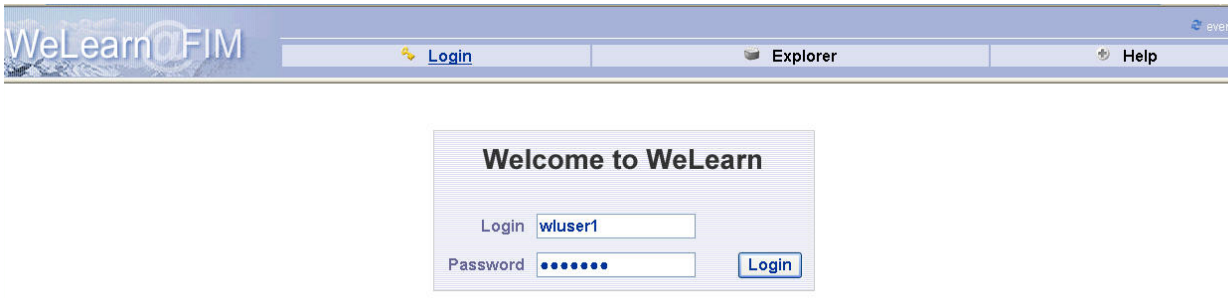

Abbildung 22: Login-Screen

Sollen neue Benutzer importiert werden, so wird bei den bereits in WeLearn importierten Benutzern (nochmals) versucht diese zu importieren.

Die mit (EXISTS) markierten Benutzer (hier: wluser1 und wluser2) wurden bereits früher vom LDAP Server übernommen. Mit einem Klick auf „Remove already imported users from list“ werden diese von der Liste entfernt, und nur der neue Benutzer wluser3 bleibt übrig.

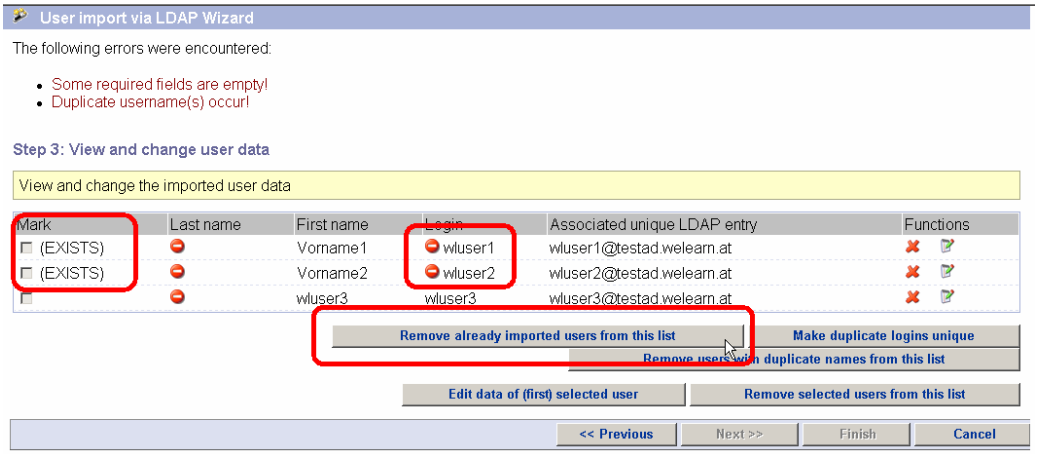

Abbildung 23: Erneutes Importieren von Benutzern

Mit einem Klick auf „Make duplicate logins unique“ könnten die Benutzer ein zweites Mal in WeLearn importiert werden, allerdings ändert sich der Login, da dieser eindeutig sein muss.

Das Passwort am LDAP Server kann nicht in WeLearn geändert werden. In WeLearn kann ausschließlich das lokale WeLearn Passwort geändert werden.

5 BENUTZER IMPORTIEREN UND LOKAL AUTHENTIFIZIEREN

Eine weitere Funktionalität der LDAP Implementierung von WeLearn ist, Benutzerdaten von einem LDAP Server zu importieren, ohne dass in weiterer Folge die Passwörter der importierten Benutzer vom LDAP Server überprüft werden.

Diese Möglichkeit hat den Vorteil, dass man die gesamten LDAP-Konfigurationsdaten interaktiv eingeben kann.

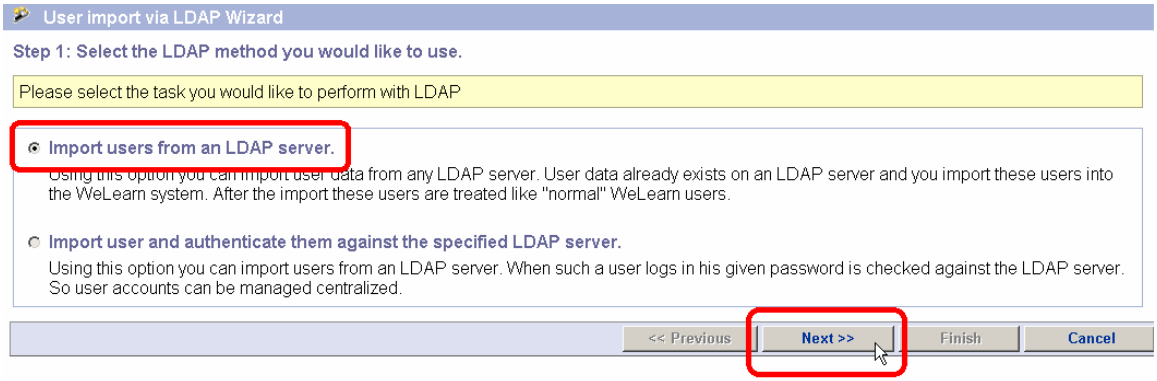

Abbildung 24: Möglichkeit 1, Benutzer nur importieren

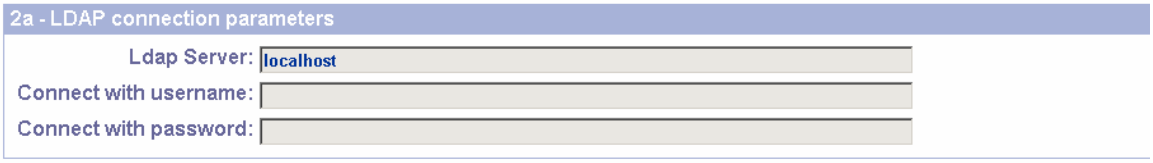

Abbildung 25: Konfiguration der LDAP-Verbindung (LDAP-Server, Binding-Benutzer)

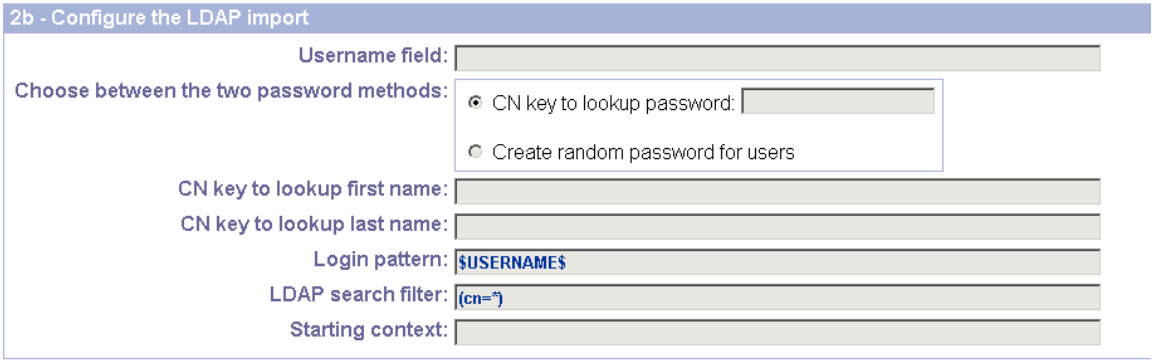

Abbildung 26: Import-Parameter

In das „Username field“ wird eingegeben, von welchem Feld der Login importiert werden soll.

Wenn die Option „CN key to lookup password“ ausgewählt wird, muss ein Feldname eingegeben werden, von welchem das (Plaintext-)Passwort importiert werden kann. Soll für die Benutzer ein zufälliges Passwort erzeugt werden, kann die Option „Create random password for users“ gewählt werden.

Bei „CN key to lookup firstname/surname“ gibt man die Felder ein, von welchen der Vorname bzw. der Nachname übernommen werden kann.

Ist „Login pattern“ auf `$USERNAME$` gesetzt, wird der lokale Login aus dem Feld erzeugt, welches unter „Username field“ spezifiziert wurde. Sollte der Login aus vorname.nachname bestehen, kann z. B. `$FIRSTNAME$.$LASTNAME$` verwendet werden.

Im „Starting context“ Feld muss noch ein Startcontext für den Benutzerimport angegeben werden.

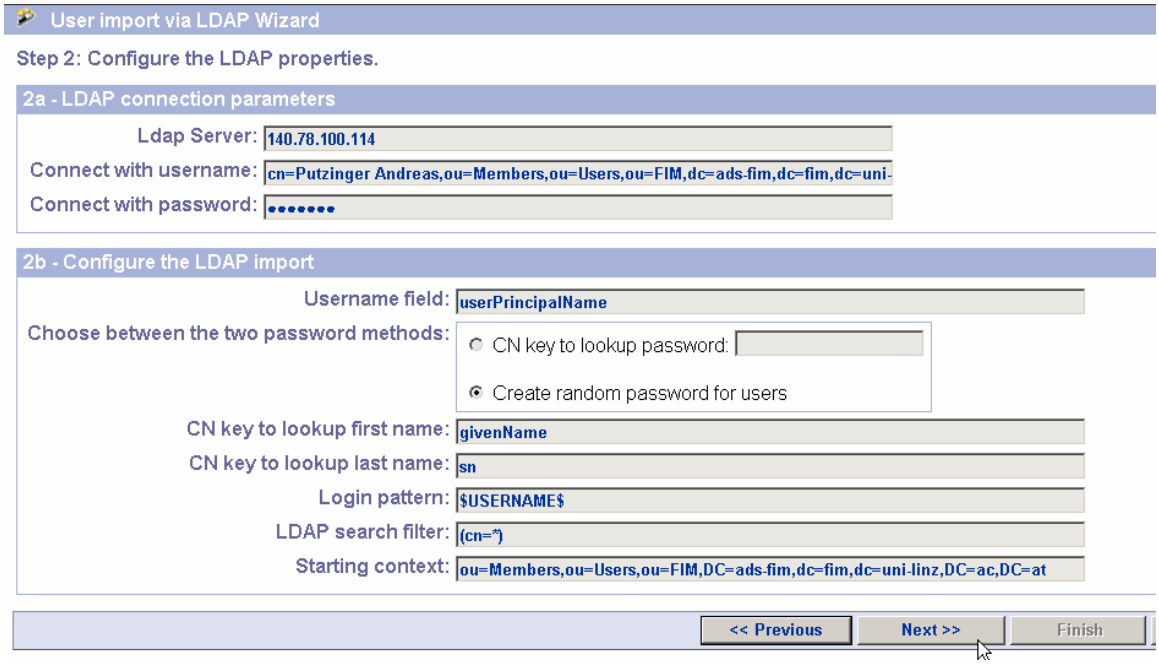

Abbildung 27: Beispielkonfiguration für Active Directory

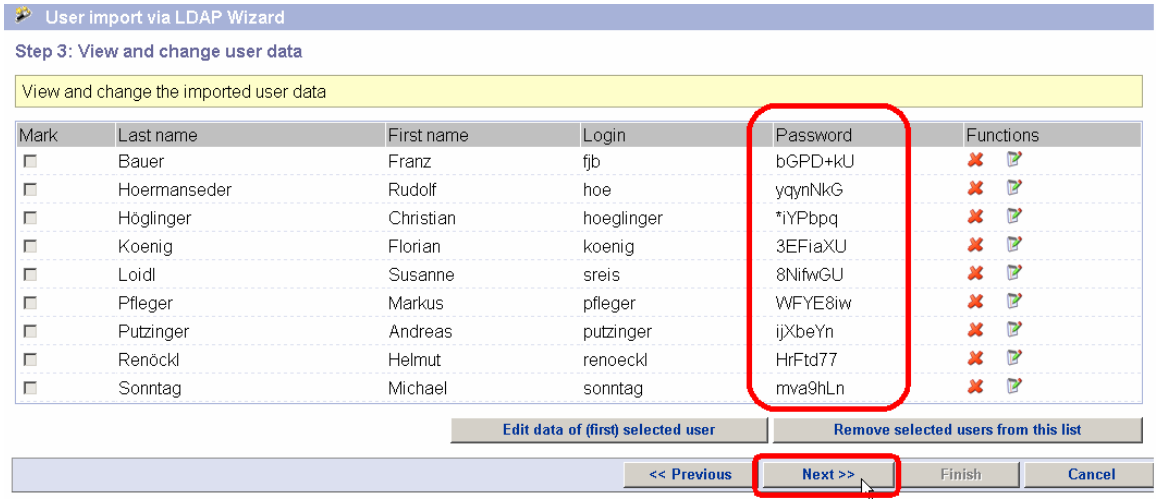

Abbildung 28: Importierte Benutzer mit zufällig erzeugten Passwörtern

Die Optionen und Schaltflächen für diese Maske sind unter „List of users“ im Handbuch für Administratoren und Kursleiter im Detail erklärt.

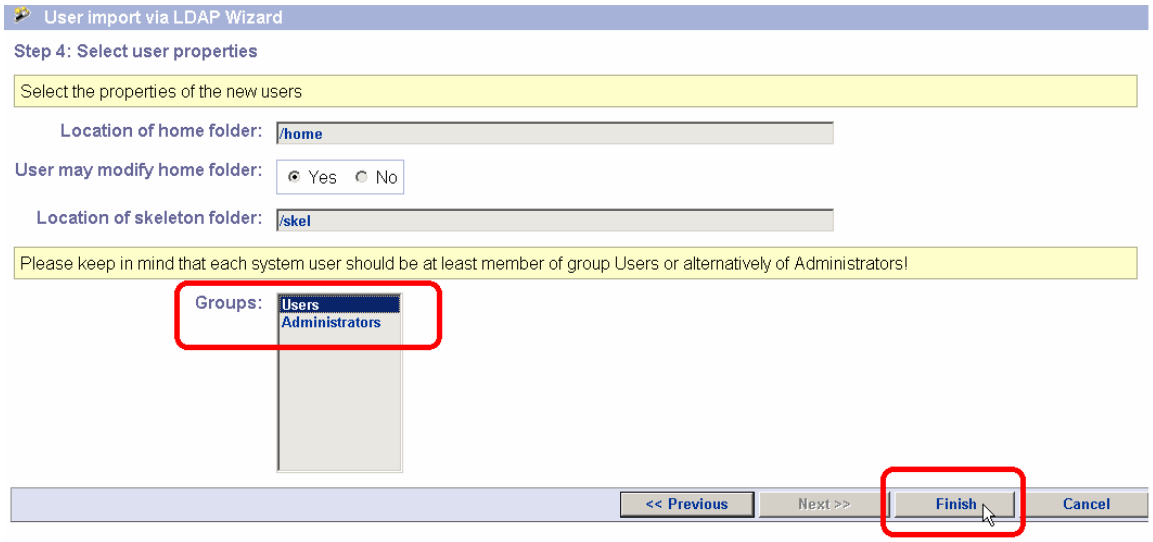

Abbildung 29: Optionen für die neuen Benutzer

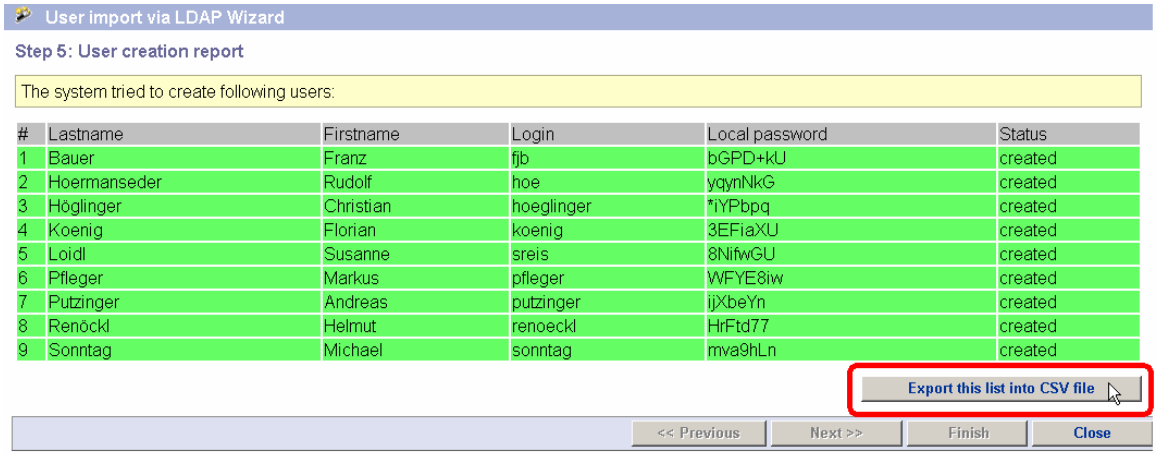

Abbildung 30: Status-Report der angelegten Benutzer

Mit einem Klick auf „Export this list into CSV file“ wird eine Datei erzeugt, welche die präsentierte Übersicht enthält und beispielsweise mit Microsoft Excel weiterverarbeitet werden kann.

Mit „Close“ wird der Dialog geschlossen und die Benutzer sind gemäß der Angaben angelegt.

Das WeLearn-Team wünscht Ihnen viel Spaß und Erfolg im Arbeiten mit WeLearn. Bei Fragen und Anregungen können Sie uns unter info@welearn.at erreichen.

Unter http://www.welearn.at (deutsche Version/FAQ) finden

Sie ebenfalls Unterstützung und eine Zusammenstellung häufig gestellter Fragen.