Stand: 12.11.2017

OSSOS - Netzwerk-Hilfen

BPass: Lehrer ändern NDS-Passworte von Schülern, Passwortmanagement für Administratoren/Netzwerkberater

Labs

Zur OSSOS - Homepage

Kurzbeschreibung: **(Aktuelle Version: BPass 4.20)** für ML-3 und ML-4 freigegeben

- BPass erlaubt bestimmten Benutzern, Passworte anderer Benutzer zu ändern.
  (Z.B. Lehrer können Schülerpassworte ändern.)
  Dem Netzwerkberater/Administrator steht ein Passwort-Management zur Verfügung.
  (ZufallspassworteMultipassworte setzen, Login-Status wählen, Passwort prüfen.)
- Voraussetzung: Diese besonders berechtigten Benutzer erhalten dazu bestimmte Trustee-Rechte an anderen Benutzern.
- Neuerungen gegenüber der Vorgängerversion:
  - siehe bpass_history.txt und BPass3Neuerungen.pdf
- BPass ist für diejenigen Schulen in Baden-Württemberg, die das Nutzungsrecht für die sogenannte "paedML Novell 3 " oder "paedML Novell 4 " für Novell-Netzwerke des Landes Baden-Württemberg, Deutschland, besitzen, kostenlos in der jeweils mit der "Musterlösung" ausgelieferten Version bzw. in der für die Musterlösung freigegebenen Version nutzbar.
  (Einzelheiten siehe Registrierung und Nutzungsbestimmung.)
  BPass wurde optimiert für die Verwendung bei der Novell Musterlösung der Zentralen Planungsgruppe Netze des Kultusministeriums bzw. der Zentralen Expertengruppe Netze des Landesmedienzentrums Baden-Württemberg (ist aber auch in anderen Netware-Umgebungen von Nutzen. ->Einzelheiten der Lizenzdatenvergabe.

Registrierung und Nutzungsbestimmung

(Achtung: Auch Schulen, die BPass kostenlos nutzen dürfen, benötigen Lizendaten. Diese liegen der ML bzw. dem Update der ML ab Version 3.0 bei. Falls Sie diese Lizenzdaten nicht über das LMZ beziehen können, können Sie sich an den Programmautor wenden.)
Beim Update von BPass-Version 3 auf Version 4 werden neue Lizenzdaten benötigt!

Entwicklung der Versionen von BPASS: bpass_history.txt

Update auf Version 4.x: bpass_update.txt

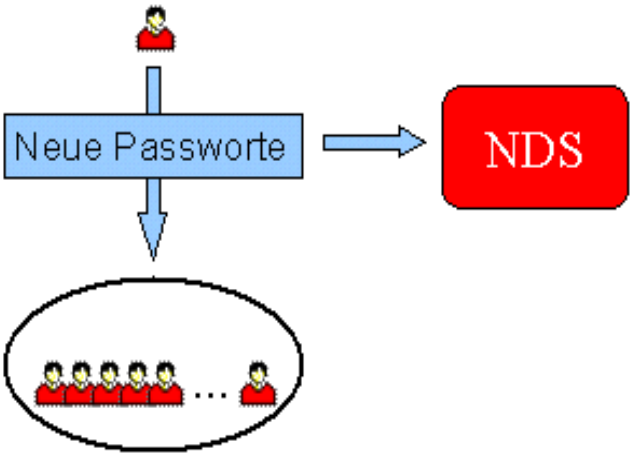
BPASS.EXE

Das Programm BPASS können Sie über die OSSOS-Homepage und dort über die Download-Links herunterladen.

Diese Seite als PDF.

Achtung: Die Version 4.x erfordert neue Lizenzdaten! Nutzer der paedML-Novell-3.x können BPass 3.x weiter nutzen.

Benutzer-Passworte ändern mit BPASS



Inhaltsverzeichnis

1 Konzept und Voraussetzungen

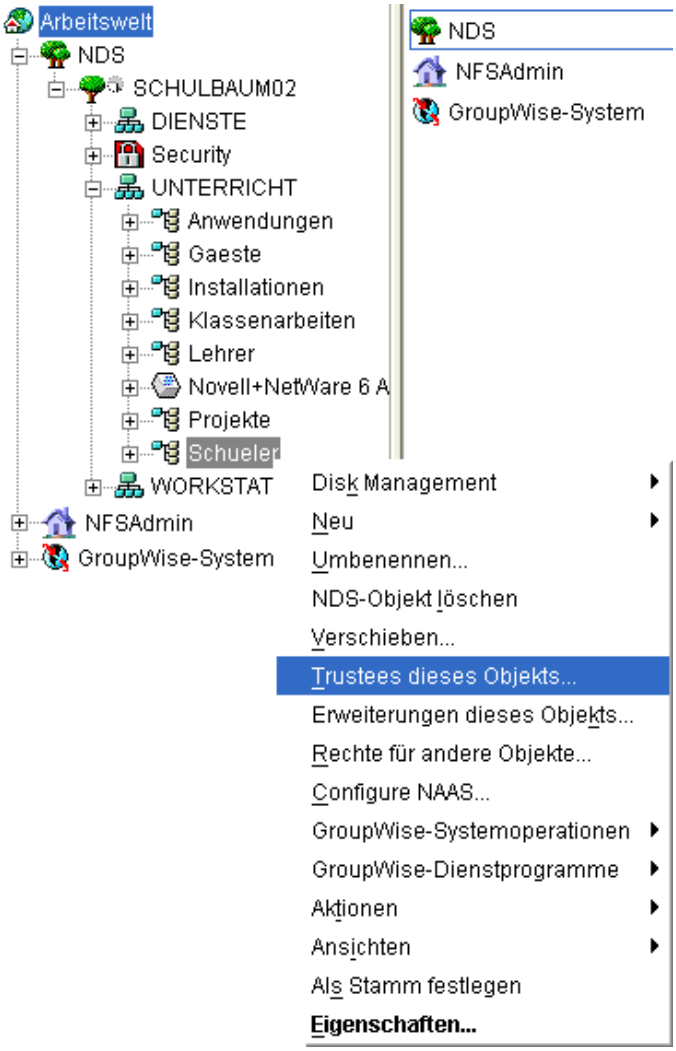
Außer dem Administrator kann normalerweise kein Benutzer ein Passwort eines anderen Benutzers ändern. Neben dem Ändern des eigenen Passwortes wäre es jedoch oft wünschenswert, wenn eine Gruppe bestimmter Benutzer (z.B. Lehrer), die Passworte einer anderen Benutzergruppe (z.B. Schüler) ändern könnte. In diesem Fall käme man dem Problem vergessener Passworte auf elegante Weise bei.

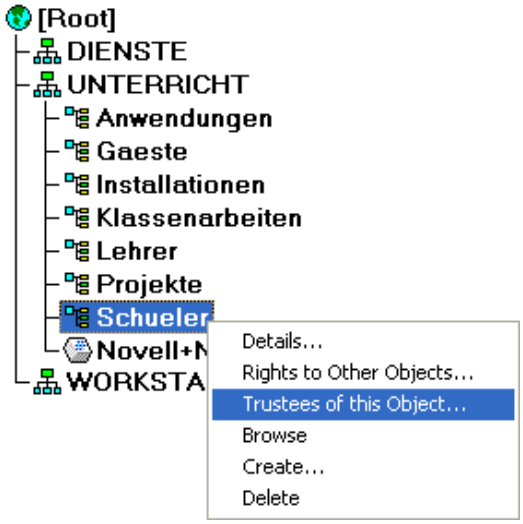
Wir gehen von zwei Benutzergruppen aus, die folgende Rechte haben sollen:

Recht	**Gruppe 1 (Lehrer)**	**Gruppe 2 (Schüler)**
darf eigenes Passwort ändern	ja	ja
darf Passworte der anderen Gruppe ändern	ja	nein

Die beiden Benutzergruppen sollten in Form von OUs (Organizational Units) organisiert sein. In der baden-württemberischen Musterlösung 2 (Novell) sieht das so aus (in der ML-3 ähnlich):

ConsoleOne-Ansicht: NWAdmin-Ansicht:





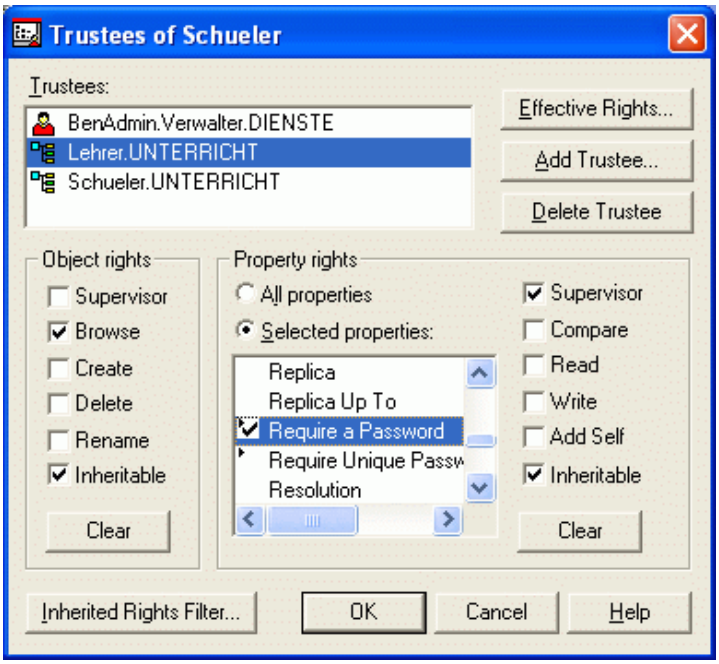
Damit die Lehrer nun Passworte der Schüler ändern können, muss die OU der Lehrer Trustee der OU Schueler sein, wobei drei Rechte bearbeitet werden müssen (ab ML 2 schon gesetzt):

Mit "Add Trustee" wird zuerst die OU Lehrer in die Trustee-Liste eingefügt.

Unter "Property Rights" wird der Button "Selected Properties" gedrückt, in der Liste der Eintrag "Password Management" gesucht und mit der linken Maustaste darauf geklickt.

Anschließend sind die Häkchen "Supervisor" und "Inheritable" zu setzen.

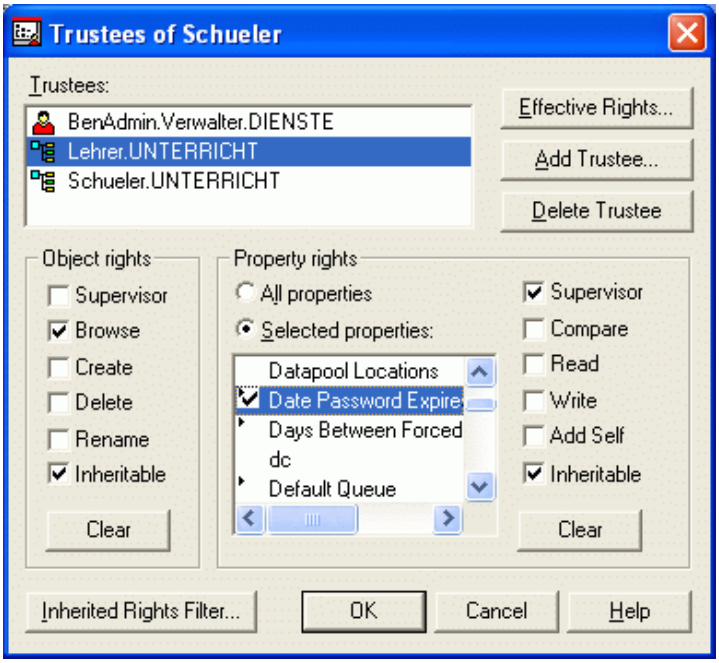
Damit Passworte nicht nur geändert, sondern auch gelöscht werden können (in diesem Fall kann sich anschließend der Schüler wieder selber ein Passwort vergeben), muss an gleicher Stelle in der Auswahlliste ein weitere Punkt bearbeitet werden:



In der Liste wird außerdem der Eintrag "Require a Password" gesucht und mit der linken Maustaste darauf geklickt.

Anschließend sind die Häkchen "Supervisor" und "Inheritable" zu setzen.

Unter Umständen muss BPass auch das Passwort-Ablaufdatum bearbeiten:



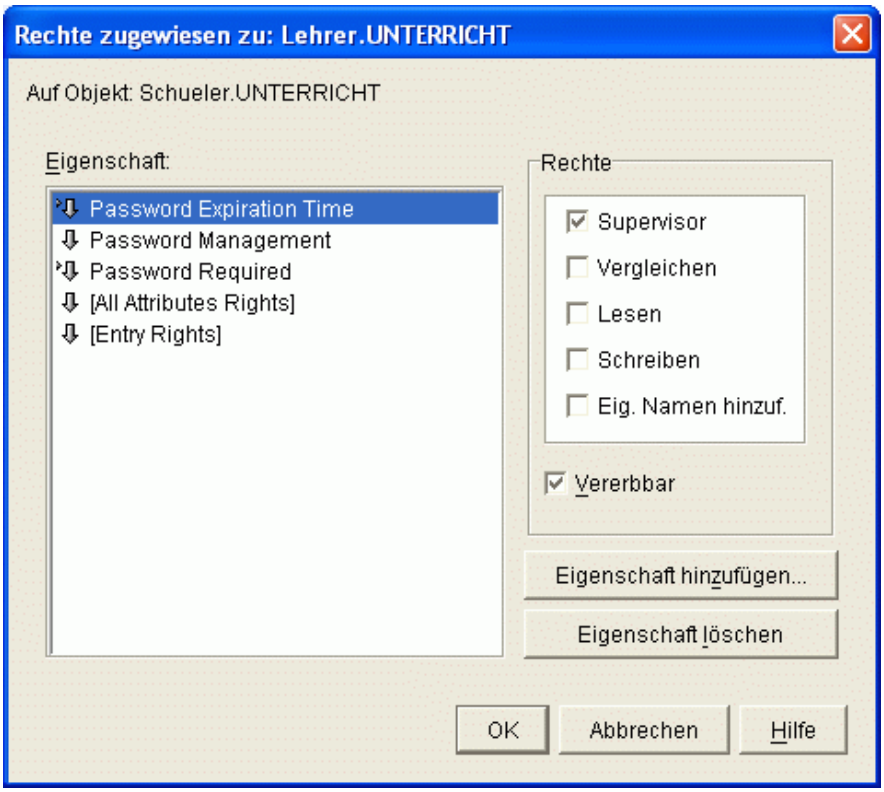
In der Liste wird außerdem der Eintrag "Date Password Expires" gesucht und mit der linken Maustaste darauf geklickt.

Anschließend sind die Häkchen "Supervisor" und "Inheritable" zu setzen.

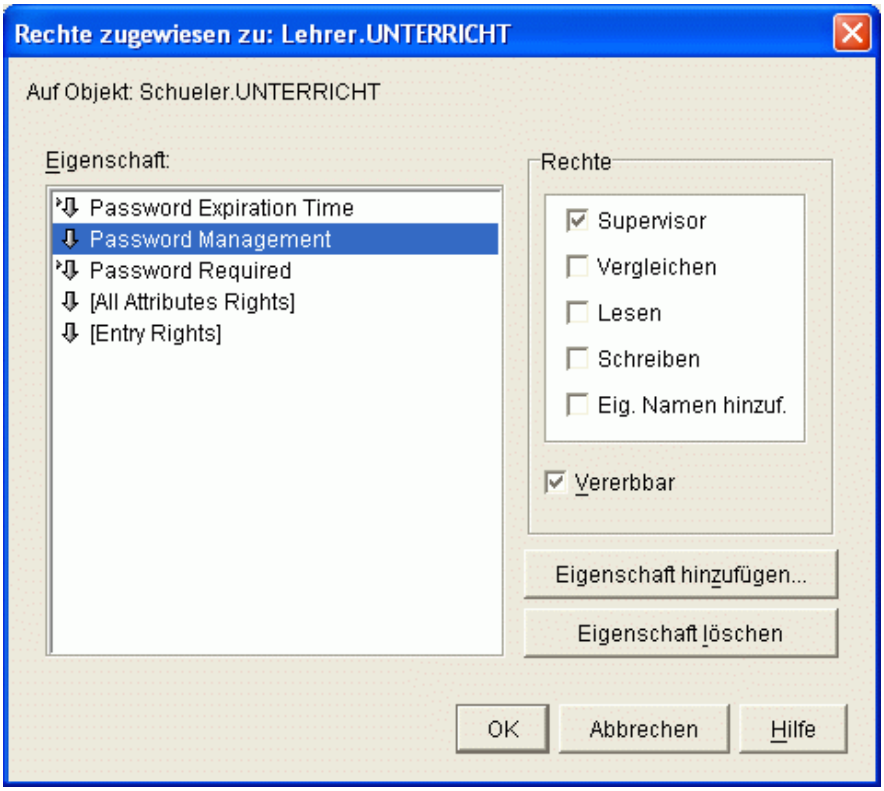
Damit ein Benutzer auch sein eigenes Passwort ändern kann, muss natürlich bei den "Details" jedes Benutzers unter "Password Restrictions" ein Häkchen bei "Allow user to change password" gesetzt sein, ein Eintrag, der üblicherweise beim Erzeugen eines Benutzers per Template so voreingestellt wird.

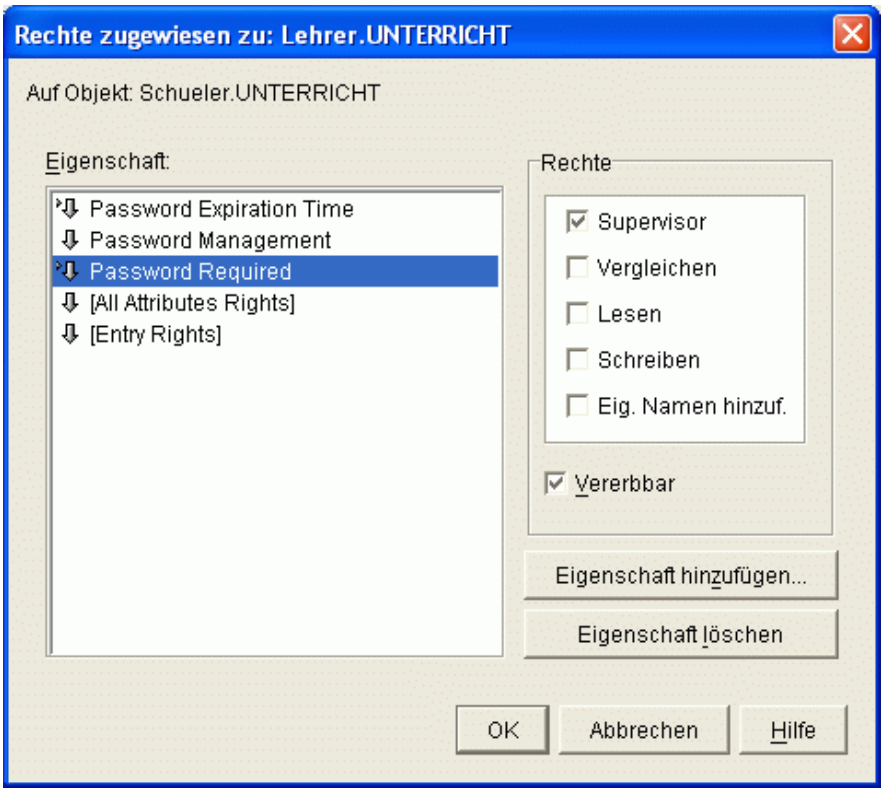
Für Benutzer der ConsoleOne sieht das Ganze so aus:

ConsoleOne: Rechte
Maustaste auf Schueler,
Trustees dieses Objekts, die
"OU Lehrer" hinzufügen.
Lehrer.Unterricht markieren,
Zugewiesene Rechte klicken.
Eigenschaft hinzufügen
klicken und die Eigenschaften
(Properties)
"Password Expiration Time",
"Password Management" und
"Password required"



hinzufügen. Alle bekommen die Rechte: "Supervisor", "Vererbbar" (entsprechende Häkchen setzen).





Für den Administrator/Netzwerkberater oder einem speziellen Benutzer-Administrator müssen ebenfalls die oben genannten Rechte gesetzt werden, wenn sie nicht sowieso schon vorhanden sind. Damit ist dieser Gruppe ein umfangreiches Passwortmanagement zugänglich.

Passwort-Management:

Herzstück ist ein konfigurierbarer Passwortgenerator, der es gestattet, Benutzern sogenannte sichere Zufallspassworte zuzuweisen. Ein Mini-NDS-Browser dient dabei zur Auswahl derjenigen Benutzer, die ein individuelles Passwort erhalten sollen.

Ein weiteres Highlight ist eine Reportfunktion, die für die BPass-Aufgaben Ausgabelisten und –seiten in HTML erstellt, die auf Basis von HTML-Schablonenseiten völlig frei gestaltbar sind. So lassen sich z.B. nach Ausdruck der Liste der Zufallspassworte Schüler und Lehrer bequem über ihr neues bzw. vorläufiges Zufallspasswort benachrichtigen.

Auch lässt sich mit BPass leicht überprüfen, ob Benutzer ihr vorläufiges oder gar leeres Passwort geändert haben. Die oben beschriebene HTML-Reportfunktion kann auch hierzu für den Administrator/Netzwerkberater/BenutzerAdmin Ausgabelisten erstellen, mit denen er leicht den Überblick behält und Gegenmaßnahmen einleiten kann.
Z.B. kann er mit BPass derartige Accounts sperren bzw. wieder freigeben. Für den zugehörigen Login-Status helfen natürlich auch wieder die HTML-Reportlisten.

Für die Passwortvergabe von BPass ist eine genaue Konfiguration vorhanden. So lässt sich z.B. festlegen, was beim Setzen oder Löschen eines Schülerpasswortes durch den Lehrer mit dem Ablaufdatum des Accounts und den Kulanzanmeldungen geschehen soll. Damit ist in dieser Sache eine Abhängigkeit des Netware/NDS-Defaults aufgehoben.
Ebenso lässt sich diese Festlegung auch für Multipassworte und Zufallspassworte vorwählen.

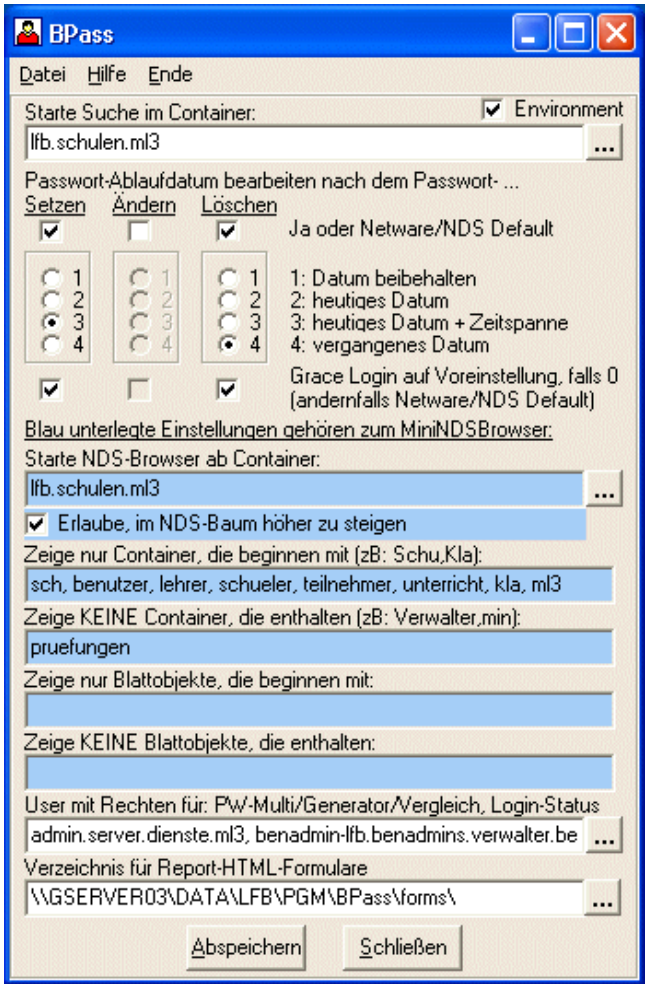
2 Installation

(BPass benötigt Lizenzdaten, falls es nicht nur als Demoversion getestet werden soll.)

BPass.exe und (falls vorhanden bpass.ini) wird vom Administratopr am besten in ein schreibgeschütztes Verzeichnis auf dem Server kopiert, z.B. in ein neues Unterverzeichnis von SYS:PUBLIC bzw. in der Musterlösung nach DATA:Pgm\BPass oder in der Musterlösung 3 nach DATA:zentral\pgm\bpass bzw. DATA:<schule>\pgm\bpass, wobei <schule> durch das korrekte Schulkürzel zu ersetzen ist. (In der gezippten

Datei bpass.zip befinden sich zwei INI-Dateien. bpass.ini passt gut für die Musterlösung. Für andere Umgebungen sollte bpass1.ini auf bpass.ini kopiert werden.)

Der Administrator startet BPass und wählt im Menü "Datei" den Punkt "Bearbeite INI-Datei".



BPass.exe und (falls vorhanden bpass.ini) wird vom Administrator für Nicht-Musterlösungsumgebungen am besten in ein schreibgeschütztes Verzeichnis auf dem Server kopiert, z.B. in ein Unterverzeichnis von SYS:PUBLIC bzw. in der Musterlösung nach DATA:Pgm\BPass oder in der Musterlösung 3 nach DATA:zentral\pgm\bpass bzw. DATA:<schule>\pgm\bpass, wobei <schule> durch das korrekte Schulkürzel zu ersetzen ist. Der Administrator startet BPass und wählt im Menü "Datei" den Punkt "Bearbeite INI-Datei".

BPass kann die von Ihnen gemachten Vorgaben in einer INI-Datei (bpass.ini) speichern. Über das Menü "Datei" und dann "Bearbeite INI-Datei" erhält man das oben stehende Bild.

Starte Suche im Container: Geben Sie hier den Such-Container ein, ab dem ein User gesucht werden soll. (Falls die gesamte NDS durchsucht werden soll, wird [root] eingegeben).
In der Musterlösung ist dies **`SCHUELER.UNTERRICHT`**. (Default: [root])

Environment: Wenn dieses Häkchen gesetzt ist und auf der Arbeitsstation die Environment-Variablen SCHULE und SCHULSERVER gesetzt ist, so wie dies in der ML3 durch das Loginskript erzeugt wird, werden beim Abspeichern der INI-Datei alle Verweise auf die Schule bzw. den Schulserver durch die Platzhalter %schule% bzw. %schulserver% ersetzt. Beim Start von BPass findet das Umgekehre statt: %schule% bzw. %schulserver% wird durch die Werte der Environment-Variablen SCHULE bzw. SCHULSERVER ersetzt. Ist das Häkchen nicht gesetzt, so wird genauso abgespeichert, wie die Eintrage in den Eingabefeldern zu sehen sind.

Passwort-Ablauf-Datum und Kulanzanmeldungen bearbeiten:

Schaut man mit ConsoleOne auf die Eigenschaftsseite „Beschränkungen/Passwortbeschränkungen“ (*Password Restrictions*) eines Benutzers, so finden sich dort u.a. folgende Attribute:

- Periodische Passwortänderungen erzwingen (*Force periodic password changes*)
  Tage zwischen erzwungenen Änderungen (*Days between forced changes*)

- Kulanzanmeldungen beschränken (*Limit grace logins*)
  Zulässige Kulanzanmeldungen (*Grace logins allowed*)
  Verbleibende Kulanzanmeldungen (*Remaining grace logins*)

Sind diese Attribute gesetzt (Musterlösungsstandard), so gilt folgendes für das Setzen, Ändern und Löschen eines Passwortes unter den Netware/NDS-Defaults, also unter Anwendung der netware-eigenen Funktionen oder unter BPass ohne Verwendung der BPass-Funktionen:

Netware-Defaults:

Setzen eines Passwortes
Fremdes nichtleeres Passwort (z.B. Lehrer setzt Schülerpasswort)
Das Passwortablaufdatum wird auf ein vergangenes Datum gesetzt i.d.R. auf 2.1.1992 01:00:00 oder 1.1.1970 01:00:00.
Die verbleibenden Kulanzanmeldungen (*Remaining grace logins*) werden auf den Vorgabewert, also auf die zulässigen Kulanzanmeldungen (*Grace logins allowed*) gesetzt.

Eigenes nichtleeres Passwort
(Hier nicht möglich)

Ändern eines Passwortes
Fremdes nichtleeres Passwort (z.B. Lehrer setzt Schülerpasswort)
Das Passwortablaufdatum wird auf ein vergangenes Datum gesetzt i.d.R. auf 2.1.1992 01:00:00 oder 1.1.1970 01:00:00.
Die verbleibenden Kulanzanmeldungen (*Remaining grace logins*) werden auf den Vorgabewert, also auf die zulässigen Kulanzanmeldungen (*Grace logins allowed*) gesetzt.

Eigenes nichtleeres Passwort
Das Passwortablaufdatum wird auf das heutige Datum plus der Anzahl der Tage zwischen erzwungenen Änderungen (*Days between forced changes*) gesetzt.
Die verbleibenden Kulanzanmeldungen (*Remaining grace logins*) werden auf den Vorgabewert, also auf die zulässigen Kulanzanmeldungen (*Grace logins allowed*) gesetzt.

Löschen eines Passwortes
Fremdes Passwort löschen (z.B. Lehrer löscht Schülerpasswort)
Passwortablaufdatum und die zulässigen Kulanzanmeldungen (*Grace logins allowed*) bleiben unverändert.

Eigenes Passwort löschen
Nicht möglich, wenn die Mindestlänge des Passwortes (*Minimum password length*) in den Benutzerattributen gesetzt ist.

Die soeben beschriebenen Netware/NDS-Defaults beim Setzen/Ändern/Löschen von Passworten können unbefriedigend sein. Deshalb gibt es in BPass die Möglichkeit, für alle drei Fälle festzulegen, wie verfahren werden soll. Im Bild sind für die für die Musterlösung sinnvollen Standardeinstellungen zu sehen.

Alle weiteren blau unterlegten Felder beziehen sich auf den weiter unten beschriebenen Mini-NDS-Browser:

Starte NDS-Browser ab Container: Festlegung des Startpunktes für den Mini-NDS-Browser in der NDS. (Default: [root]; Default-ML: schueler.unterricht)

Häkchen: Mit dem Häkchen legen Sie fest, ob man in der NDS vom Startpunkt auch nach oben steigen darf oder vielleicht besser nicht. (Default: kein Häkchen)

BPass zeigt im Mini-NDS-Browser nur Container und User an. Um den Benutzer von BPass nicht zu verwirren (meist ist es ja nicht der Admin), lassen sich noch Einschränkungen der Anzeige festlegen. Diese Einstellungen gelten jedoch nicht für die Programmteile Passwort-Generator, Multipasswort, Login-Status, Passwort-Vergleich, da diese ja normalerweise nicht für den normalen Benutzer zugänglich sind.

Zeige nur Container, die beginnen mit: Komma-getrennte Liste von Namens-Anfängen von anzuzeigenden Containern.
Im obigen Beispiel werden also nur Container angezeigt, die mit den Worten "Lehrer", "Schueler", "Unterricht" und "Kla" beginnen. Also würde z.B. ein Container names "LehrerGYM" oder "Klasse8a" angezeigt, nicht aber der Container "Projekte". (Default: kein Eintrag; Default-ML: siehe Text)

Zeige KEINE Container, die enthalten: Komma-getrennte Liste von Namens-TEILEN von NICHT anzuzeigenden Containern.

Im obigen Beispiel werden also keine Container angezeit, die die Worte "Verwalter" oder "min" enthalten. Also würden z.B. die Container "Verwalter", "SchuelerVerwalterContainer", KlonAdminContainer... nicht angezeigt. (Default: kein Eintrag; Default-ML: Klassenarbeiten)

Zeige nur Blattobjekte, die beginnen mit: Analogon zu der entsprechenden Container-Option. (Default: kein Eintrag)

Zeige KEINE Blattobjekte, die enthalten: Analogon zu der entsprechenden Container-Option. Beispiel einer Anwendung dieser Option: Sie haben z.B. einige Test-User, die alle im Namen das Wort "Test" enthalten, also z.B. TestUser1, LehrerTestUser,... Diese Benutzer würden dann im Mini-NDS-Browser nicht angezeigt werden. (Default: kein Eintrag)

User, die Generierte/Multi-Passworte, Passwortvergleiche und Login-Status bearbeiten dürfen: Komma-getrennte Liste von speziellen Benutzern, die Multi- und Zufallspassworte setzen, Passwortvergleiche durchführen und den Login-Status bearbeiten dürfen, in der Regel z.B. Admin.
(Default: kein Eintrag; Default-ML: Admin,BenAdmin)

Verzeichnis für Report-HTML-Formulare:
Hier liegen die HTML-Schablonen für die HTML-Reportausgabe. (Leeres Feld bedeutet: BPass-Programmverzeichnis).

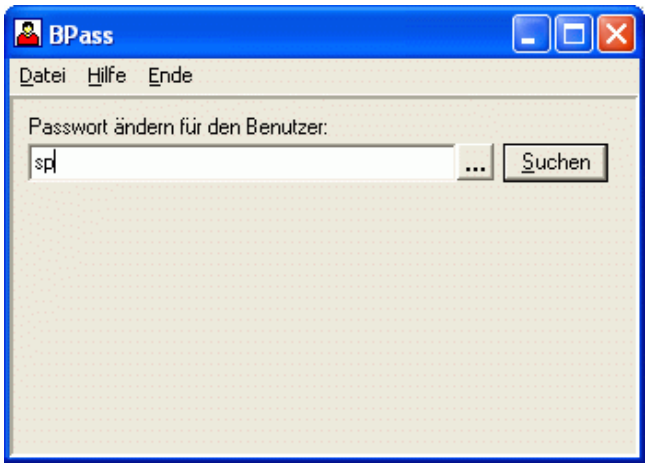
Anschließend wird gespeichert.

Durch diese Einstellungen lässt sich also für den nicht so kundigen Benutzer von BPass eine eingeschränkte und übersichtliche Sichtweise auf die NDS erzeugen.

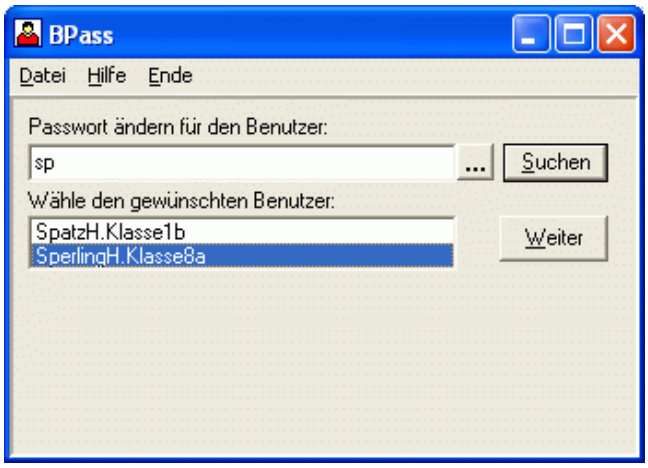
Tipp: Damit alle Lehrer BPass leicht finden, legt man eine Verknüpfung mit BPass auf dem Desktop der Arbeitsstation ab, dies am Besten mit Hilfe von ZenWorks (in dem man ein einfaches Applikationsobjekt ohne AOT-File erzeugt).

3 Benutzen von BPass

Wir studieren das Benutzen von BPass an einem Beispiel:
Der Lehrer B.Specht (Username **spechtb**) möchte das Passwort vom Schüler Hans Sperling (Username **sperlingh**) ändern. Vielleicht weiß Herr Specht den Namen des Schülers auch nicht mehr so genau. Er startet also BPass und gibt ein:



Ein Klick auf den Suchen-Button listet nun alle Schüler (in der OU **SCHUELER.UNTERRICHT**) auf, deren Namen mit "sp" beginnen:



Hier wählt Herr Specht nun den richtigen Schüler, in unserem Fall also SperlingH aus Klasse8a und klickt anschließend auf den Weiter-Button:

Jetzt kann Herr Specht ein neues Passwort vergeben, dass zur Sicherheit noch einmal wiederholt werden muss. Falls es sich Herr Specht anders überlegt, besteht auch die Möglichkeit abzubrechen und einen anderen Benutzer zu suchen. Klickt er aber auf den Weiter-Button, so erscheint (hoffentlich) die Erfolgsmeldung:

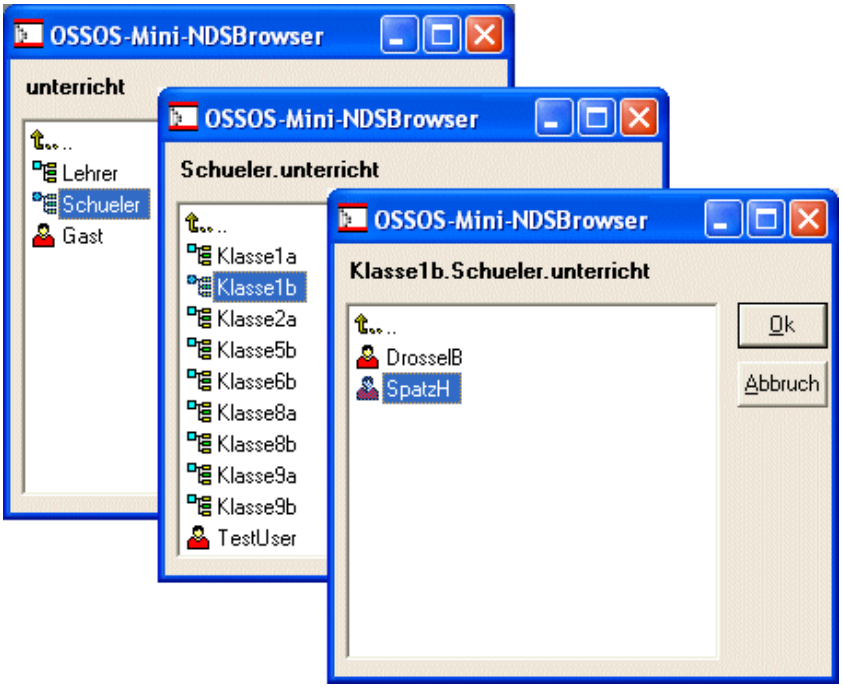
Jetzt führt der Weiter-Button wieder zur Möglichkeit, einen weiteren Schüler zu suchen.

Falls Herr Specht sich nicht selber ein Passwort ausdenken mag oder er ein besonders sicheres Passwort vergeben möchte, kann er auf den "Vorschlag"-Button klicken. Jetzt wird ein Zufallspasswort vorgeschlagen. Bei Nichtgefallen wird über den "Noch eins"-Button immer wieder ein neues Passwort vorgeschlagen. Selbstverständlich kann dieses Passwort nicht per Drag&Drop übernommen werden, sondern muss - gewissermaßen zum Eingewöhnen- abgetippt werden.

Bei der Passwort-Eingabe besteht auch die Möglichkeit kein Passwort einzugeben. In diesem Fall bleiben die Felder "Neues Passwort" und "Neues Passwort wiederholen" leer. Loggt sich dann später der Schüler SperlingH ein, wird er aufgefordert, sich selbst ein neues Passwort zu geben.

Bemerkung: Wollen Sie Ihr **eigenes** Password ändern, so erscheint zunächst ein Fenster, in dem Sie Ihr bisheriges Passwort eingeben müssen.

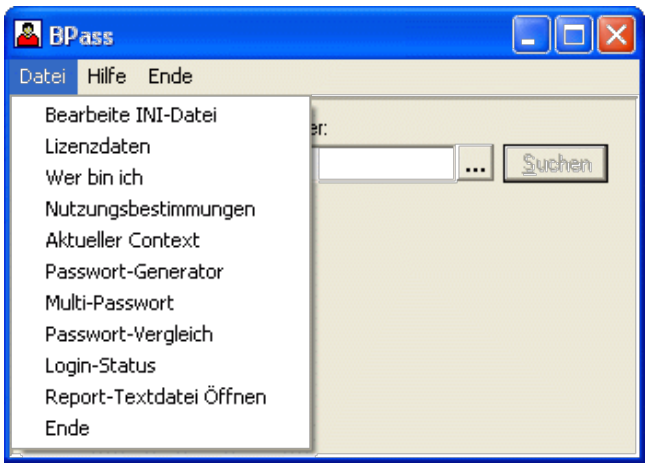
Eine weitere Möglichkeit, einen Benutzer zu suchen, ist ein Klick auf den Button ..., der den **Mini-NDS-Browser** öffnet.



Hier klickt man sich von Container zu Container durch, bis man beim gewünschten Benutzer angelangt ist.

Ein abschließender Klick auf den OK-Button überträgt den gewünschten User in das Such-Feld von BPass und man kann mit der Passworteingabe weiter bearbeiten, wie oben beschrieben.

3.1 Das Menü "Datei"



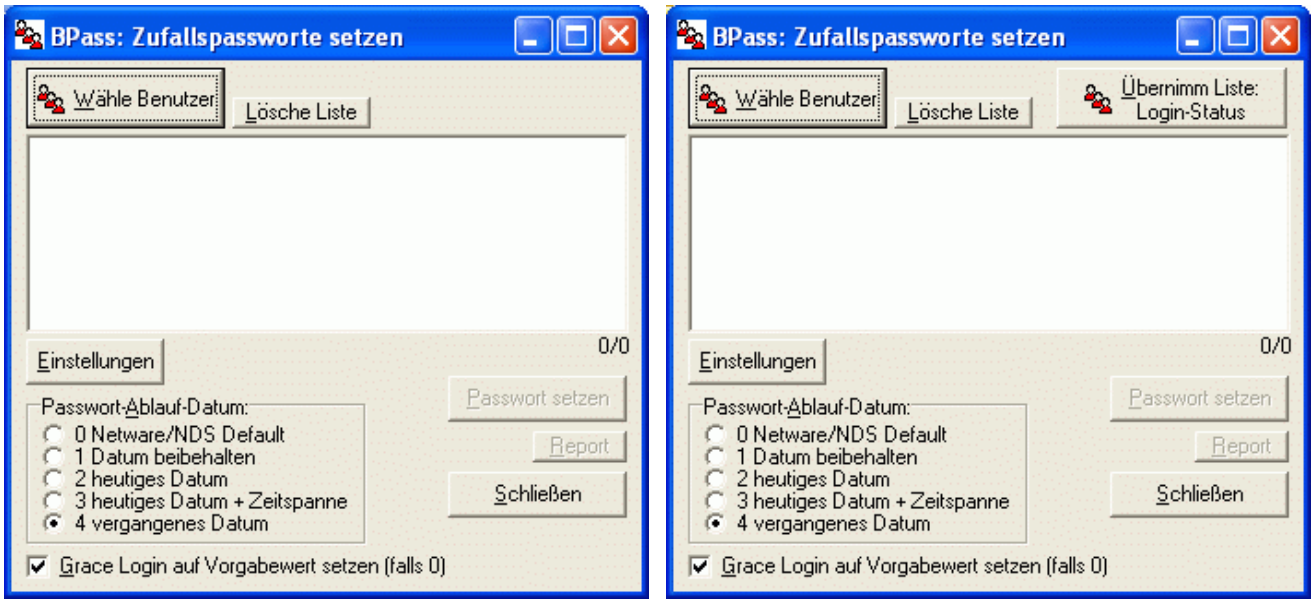
Neben dem schon oben besprochenen Menüpunkt "Bearbeite INI-Datei" gibt es noch die Eingabe der Lizenzdaten, den Text der Nutzungsbestimmungen, die Anzeige des eingeloggten Benutzers "Wer bin ich" und die Anzeige des aktuellen Kontextes. Diese Menüpunkte werden weiter unten besprochen.

Für diejenigen besonderen Benutzer, die in der INI-Datei unter "User mit Rechten für..." aufgeführt sind, stehen weitere mächtige Funktionen zur Verfügung, nämlich der Passwortgenerator, die Multipassworte, der Passwortvergleich und der Login-Status. Diese Menüpunkte werden jetzt im Folgenden beschrieben.

3.2 Passwort-Generator

Mit dem Passwort-Generator ist es möglich, z.B. nach dem Anlegen von vielen Benutzern z.B. mit BImport, mit BPass ein Passwort zuzuweisen.

Über den Datei-Menüpunkt "Passwort-Generator" startet folgendes Fenster:



Das linke Bild stellt den Normalfall dar. Falls jedoch aus dem Programmteil Passort-Vergleich, Multipassworte oder Login-Status schon eine Liste von Benutzern gewählt wurde, steht zur Übernahme der Button "Übernimm Liste..." zur Verfügung.
Damit lässt sich die gleiche Liste, die schon z.B. beim Passwortvergleich benutzt wurde, auch hier laden. So lassen sich z.B. diejenigen Benutzer mit Zufallspassworten versorgen, die beim Passwortvergleich durch ein leeres Passwort auffielen.

Über den Button "Wähle Benutzer" können Sie jetzt mit dem oben beschriebenen Mini-NDS-Browser verschiedene User oder auch ganze Container auswählen:

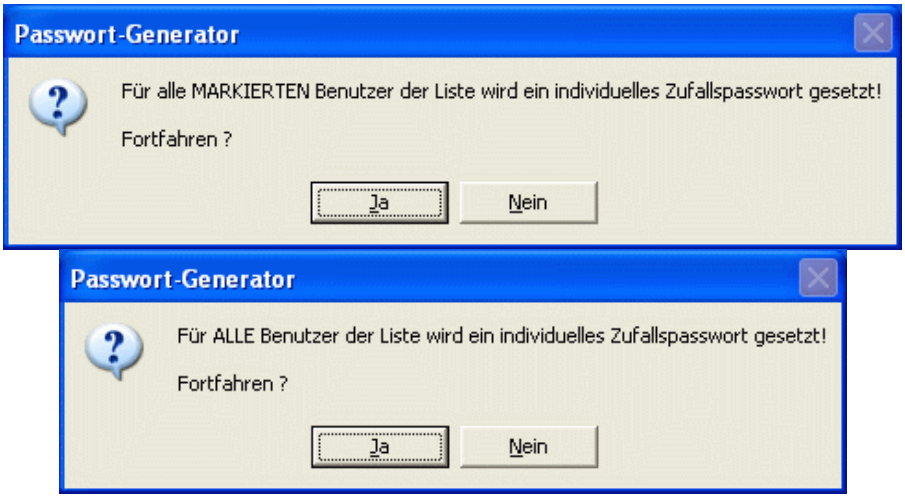
Anders als oben, können Sie jetzt im Mini-NDS-Browser auch mehrere Objekte markieren. Ein Klick auf den OK-Button fügt alle markierten Benutzer, bzw. alle Benutzer aus markierten Containern inclusive der Sub-Container in die Liste ein. Sie können natürlich den Button "Wähle Benutzer" mehrmals benutzen, um Benutzer aus Containern in die Liste hinzuzufügen, die Sie nicht "in einem Rutsch" markieren können. Außerdem können Sie sich unabhängig von den INI-Datei-Vorgaben frei in der NDS bewegen, denn die Passwort-Generator-Funktion ist ja für Personen mit administrativen Aufgaben gedacht und nicht z.B. für Lehrer.

Sie erhalten also schließlich eine Liste von Benutzern:

In dieser Liste können Sie wiederum -wenn Sie wollen- einzelne Benutzer markieren:

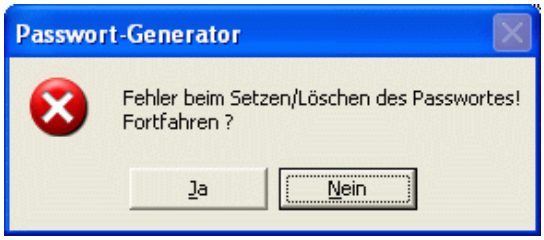
Unabhängig von den oben besprochenen Konfigurationseinstellungen lassen sich hier ebenfalls das Verhalten bzgl. Passwortablaufdatum und Kulanzanmeldungen einstellen.

Je nachdem, ob Benutzer markiert sind oder nicht, führt ein Klick auf den Button "Passwort setzen" auf eines der folgenden Kontrollfenster, z.B.:

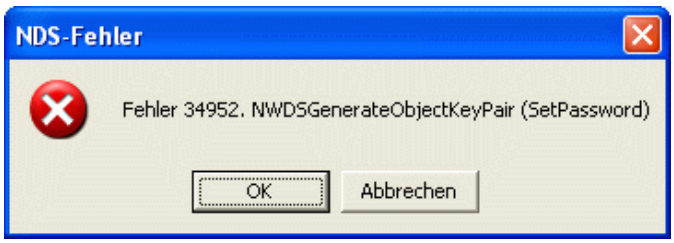


Der Ja-Button führt nun schließlich das Passwort-Setzen durch. Das Ergebnis sieht so aus:

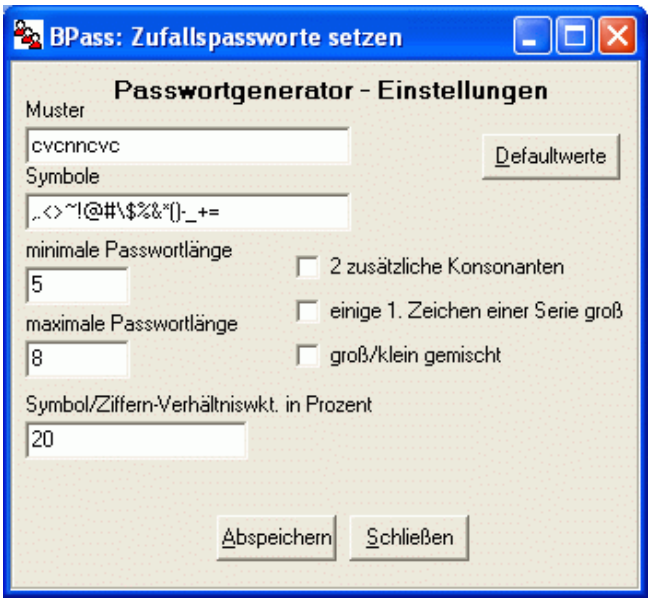
Sollten Fehler aufgetreten sein, erscheint ein Fehlerfenster:



Zuvor könnten aber auch schon explizitere Fehlermeldungen aufgetaucht sein. Treten viele Fehler auf, so sind in der Regel falsche Rechte gesetzt. Überprüfen Sie also zunächst die Voraussetzungen für die Anwendung von BPass. Ein Beispiel für ein weiteres Fehlerfenster ist:



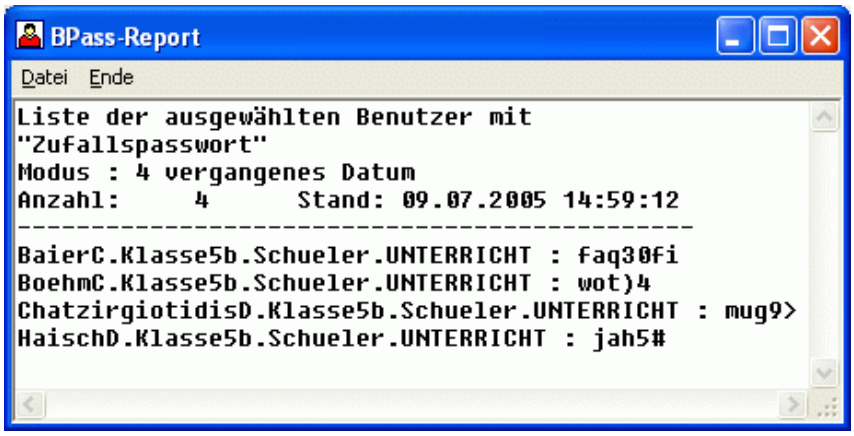
Bevor nun die Report-Funktion beschrieben wird, noch ein Wort zur Passwortgenerierung. Über den Button "Einstellungen" erhält man das Konfigurationsfenster des Passwortgenerators:



Über den Button „Abspeichern“ werden diese Einstellungen und die Einstellungen zum Passwortablaufdatum und den Kulanzanmeldungen in die BPass-INI-Datei übernommen.

Der Passwortgenerator generiert Zufallspassworte, die auch hohen Sicherheitsanforderungen genügen, auch mit den oben zu sehenden Standardeinstellungen. Der Passwortgenerator liefert sichere Zufallspassworte, die aber trotzdem erstaunlich gut zu merken sind.
Wer will, kann hier aber auch Veränderungen vornehmen. Siehe dazu das Kapitel Passwort-Generator-Einstellungen.

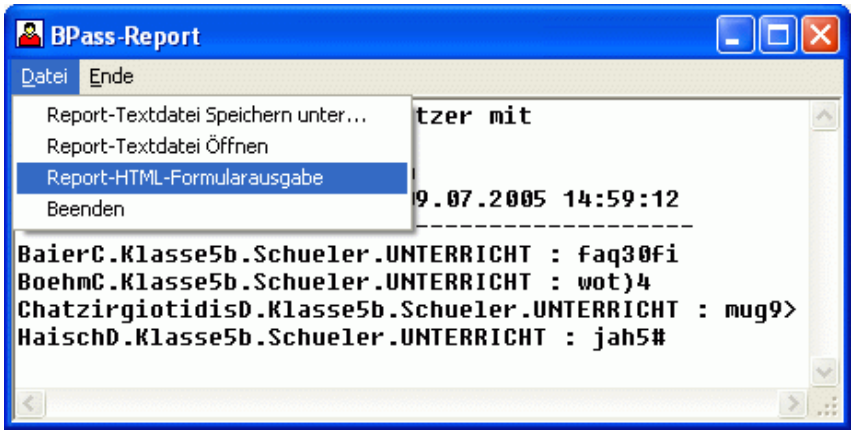
Report
Über den Button „Report“ öffnet sich ein Fenster, dass die soeben durchgeführte Zufallspasswortzuteilung in einfachem Text dokumentiert:

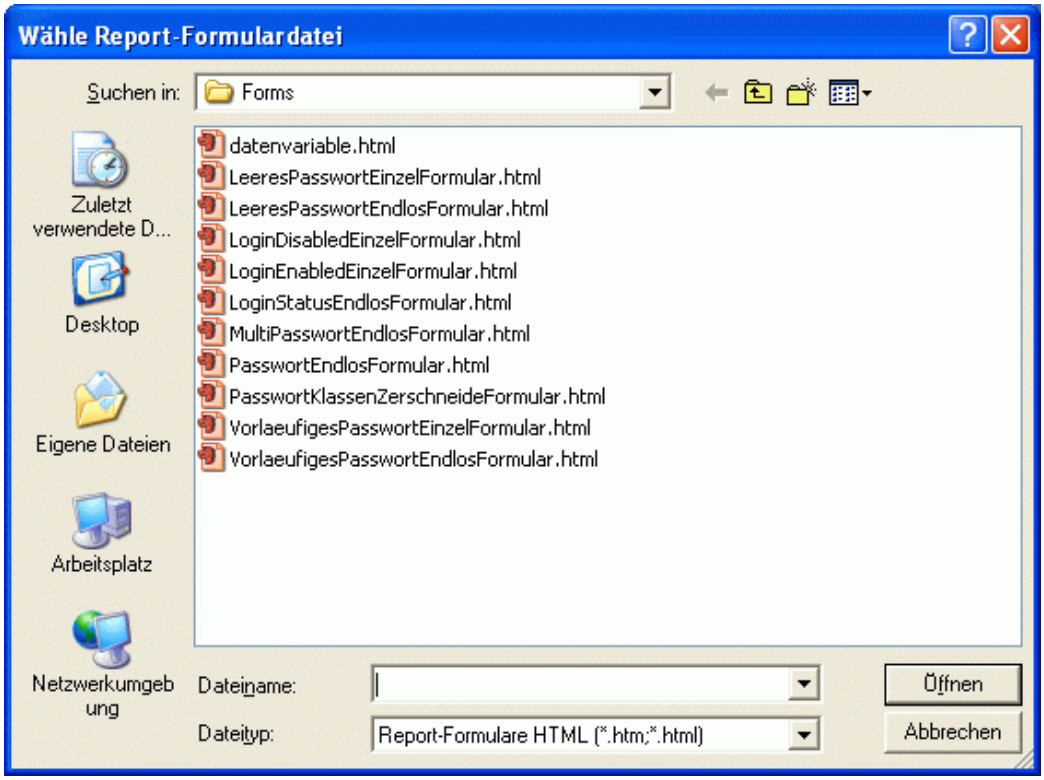


Im Kopf der Liste steht, was gezeigt wird, in welchem Modus bzgl. Ablaufdatum und Kulanzanmeldungen gearbeitet wurde, wie viele bearbeitete Benutzer die Liste enthält und das Datum und die Uhrzeit der Bearbeitung. Danach folgt die Liste der bearbeiteten Benutzer mit qualifiziertem Benutzernamen einem Doppelpunkt und dahinter das zugewiesene Zufallspasswort.

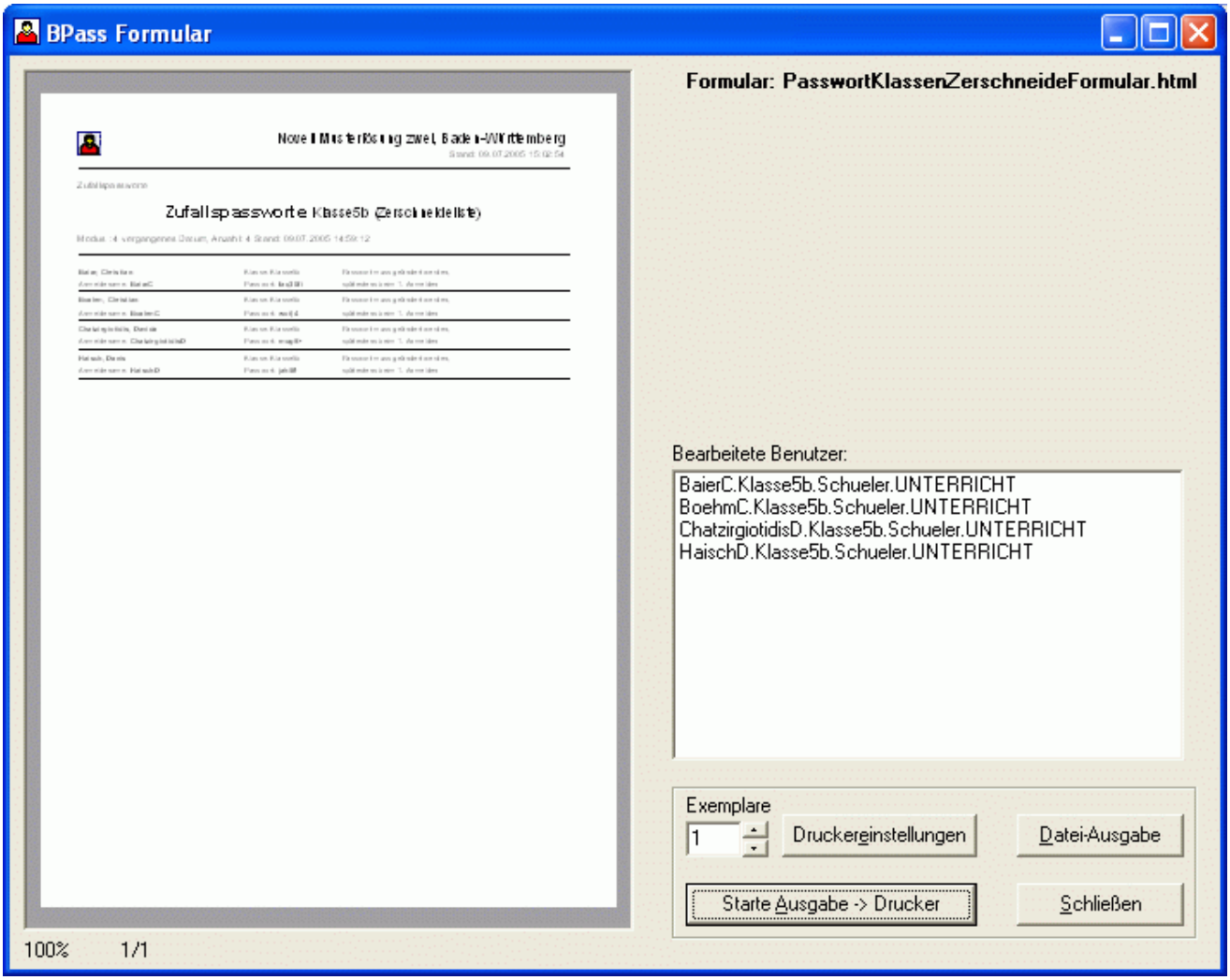
Mit dieser Liste lassen sich nun verschiedene Aktionen durchführen:

- Per Drag&Drop können Textteile aus der Liste in andere Anwendungen übernommen werden.
- Die Liste kann über das Datei-Menü als reine Textdatei abgespeichert werden.
- Die Liste kann als HTML-Formular ausgegeben werden.





Für eine Liste der Zufallspassworte ist das vorgefertigte Formular **`PasswortEndlosFormular.html`** oder **`PasswortKlassenZerschneideFormular.html`** geeignet. Wählen wir z.B. Letzteres.
(Hinweis: Die Datei datenvariable.html ist keine Formularschablone, sondern enthält Hinweise für eigene Formularerstellung.)



Links im HTML-Browser erscheint die (erste) Seite, die sich mittels linker/rechter Maustaste über der Seite vergrößern/verkleinern lässt. Rechts wird das gewählte Formular genannt und in einer Liste die bearbeiteten Benutzer. Über die Buttons unten rechts lässt sich die Liste zum Druck oder als Datei ausgeben und das Fenster schließen.
Erstreckt sich die Liste über mehrere Seiten, so erscheinen noch Buttons zum Blättern.
Das linke Browserfenster dient vor allem der Kontrolle, ob das richtige Formular gewählt wurde und auch zur Kontrolle bei der Entwicklung eigener Formulare. (Siehe dazu Kapitel HTML-Report-Formular-Erstellung).

Hinweis: Bei der Formularausgabe handelt es sich um eine echte HTML-Ausgabe.

Speziell das Formular **`PasswortKlassenZerschneideFormular.html`** ist so eingerichtet, dass es die Benutzer „containerweise“, also in der Musterlösung „klassenweise“ ausgibt. Zwischen jedem Container/jeder Klasse wird ein Seitenumbruch eingefügt. Der Ausdruck dieser Liste ist also besonders für den Klassenlehrer gedacht, der die Liste in Streifen zerschneidet, damit er jedem Schüler seine Daten übergeben kann.
Das Formular **`PasswortEndlosFormular.html`** ist mehr als Übersicht für den Administrator/Netzberater/BenutzerAdmin gedacht.

Hinweis: Im BPass-Report-Fenster gibt es im Dateimenü noch den Punkt „Report-Textdatei öffnen“. Dieser Punkt ist dafür gedacht, eine bereits zuvor gespeicherte Report-Textdatei erneut zu laden, um sie der Report-HTML-Formularausgabe zuzuführen. Ebenso findet sich dieser Punkt im Hauptdateimenü von BPass.

3.3 Multi-Passworte

Nach dem Anlegen von vielen Benutzern z.B. mit BImport, kann mit mit BPass ein vorläufiges und für alle

gleiches Default-Passwort zugewiesen werden.

Ein Klick auf den Menüpunkt "Multi-Passworte" im Datei-Menü führt zu folgendem Fenster:

Die Benutzerwahl erfolgt genauso, wie im Kapitel "Passwort-Generator" beschrieben; ebenso das Markieren bestimmter Benutzer. Auch die (von der allgemeinen INI-Einstellung unabhängige) Bearbeitung des Passwort-Ablaufdatums und der Kulanzanmeldung funktioniert entsprechend. Der Button "Einstellung speichern" übernimmt diese Einstellungen in die INI-Datei.

Ggf. erscheint oben im Fenster der Button "Übernimm Liste...", falls eine Benutzerliste aus einem anderen Programmteil vorliegt.

Das für alle gewählten Benutzer gleiche Passwort wird -wie üblich- zweimal eingegeben. Ggf. können die Felder zum Passwort-Löschen auch frei gelassen werden. Ein Klick auf den Button "Passwort-Setzen" setzt bzw. löscht die Passworte.

Die Report-Funktion verhält sich natürlich genauso wie die des Passwort-Generators. Eine passende HTML-Formularschablonen ist z.B. **`MultiPasswortEndlosFormular.html`**.

3.4 Passwort-Vergleich

Dieser Programmteil ist für das Aufspüren von Benutzern mit leerem Passwort oder einem Standardpasswort wie z.B. 12345 gedacht. Es dient nicht zum Ausspionieren von Passworten. Auch ein sogenannter „Brute Force“-Angriff ist damit nicht möglich, denn nur das Vergleichen mit einem leeren oder dem richtigen Passwort ist schnell, alle anderen Fälle langsam!!!
(Insofern ist selbst das 12345-Beispiel kritisch!)

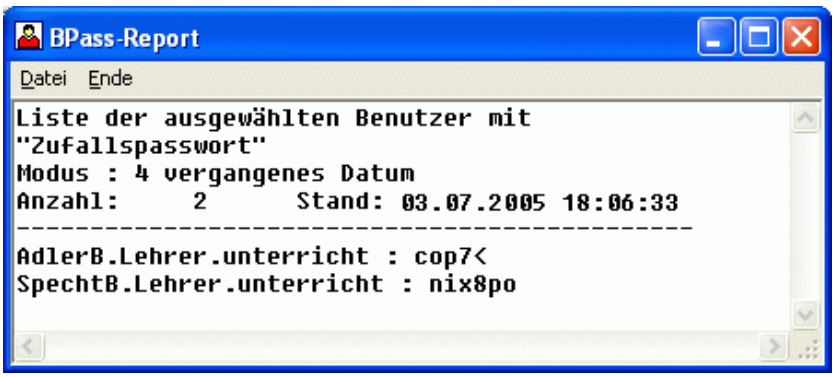
Die Benutzung dieses Programmteils gleicht grundsätzlich dem Passwortgenerator bzw. den anderen BPass-Programmteilen.

In den Bildern ist die Suche nach einem leeren und dem 12345-Passwort gezeigt, wobei mit Erfolg gefunden wurde (Häkchen!):

Die Reportfunktionen entsprechen denen im Passwortgenerator incl. HTML-Ausgabe. Für die Formularausgabe sind die folgenden Formulare geeignet:

`LeeresPasswortEinzelFormular.html`: Für jeden solchen Benutzer wird eine eigene Seite ausgegeben mit einem Hinweis, sich ein Passwort zu geben, da andernfalls sein Account gesperrt werden muss. Auch Tipps zur eigenen Passwortvergabe dazu stehen auf dem Blatt.
`LeeresPasswortEndlosFormular.html`: Eine Liste für den Administrator/Netzwerkberater/BenutzerAdmin.

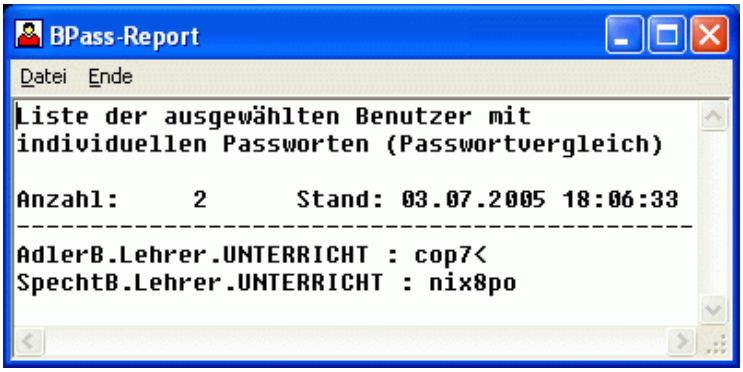
Individueller Passwortvergleich
Eine besondere Funktion ist durch den Button „Lade Liste“ gegeben. Wurde beim Setzen von Zufallspassworten im dortigen BPass-Report-Fenster die zugehörige Liste als Textdatei abgespeichert,



so können die Benutzer in dieser Liste jetzt übernommen werden. Das sieht dann etwa so aus:

Was jetzt im Feld „Passwort, nach dem gesucht werden soll“ steht, spielt hier keine Rolle. Nach dem Klick auf dem Button „Passwort suchen“, werden jetzt die Passworte individuell verglichen, also im Beispiel oben für AdlerB das Passwort *cop7<*, für SpechtB das Passwort *nix8po* usw.
Achtung: Ist die Benutzerliste lang, kann die Suche ziemlich lange dauern, wenn die Passworte nicht übereinstimmen!

Nach der Suche könnte das Ergebnis etwa so aussehen:



Auf Grund dieser Daten weiß der Administrator/Netzwerkberater/BenutzerAdmin, wen er ggf. darauf aufmerksam machen muss, sich ein neues Passwort zu geben oder wem ggf. der Account zu sperren ist. Für die Formularausgabe sind die folgenden Formulare geeignet:

`VorlaeufigesPasswortEinzelFormular.html`: Für jeden solchen Benutzer wird eine eigene Seite ausgegeben mit einem Hinweis, sich ein neues Passwort zu geben, da andernfalls sein Account gesperrt werden muss. Auch Tipps zur eigenen Passwortvergabe dazu stehen auf dem Blatt.
`VorlaeufigesPasswortEndlosFormular.html`: Eine Liste für den Administrator/Netzwerkberater/BenutzerAdmin.

Die Möglichkeit, für die bearbeiteten Benutzer den Login-Status zu verändern, wird im Kapitel „Login-Status“ ausführlich beschrieben.

3.5 Login-Status

Ähnlich, wie der Programmteil „Passwort-Vergleich“ ist dieser Programmteil für das Aufspüren von Benutzern mit einem bestimmten Login-Status gedacht.

Die Login-Status Suche kann für folgende Fälle vorgewählt werden:

- Login verboten
  Sinnvoll z.B. auf der Suche nach Benutzern, deren Account gesperrt wurde und jetzt wieder frei geschaltet werden soll.
- Login erlaubt
  Sinnvoll z.B. bei der Suche, ob bestimmte Accounts frei geschaltet sind.
- Login verboten oder erlaubt
  Sinnvoll z.B. zur Erstellung einer Liste, die den jeweiligen Login-Status für die Liste der Benutzer enthält.

Wie schon weiter oben beschrieben, lässt sich über den Button „Report“ ein Report erstellen. Für die Formularausgabe sind die folgenden Formulare geeignet:

`LoginDisabledEinzelFormular.html`: Für jeden solchen Benutzer wird eine eigene Seite ausgegeben mit einem Hinweis, dass sein Account gesperrt ist und warum.
`LoginEnabledEinzelFormular.html`: Für jeden solchen Benutzer wird eine eigene Seite ausgegeben mit einem Hinweis, dass sein Account wieder frei geschaltet ist. Außerdem wird er aufgefordert, sich ein Passowort zu geben.
`LoginStatusEndlosFormular.html`: Eine Liste für den Administrator/Netzwerkberater/BenutzerAdmin.

Im unteren Teil des oben gezeigten Fensters kann nun für die zuvor bearbeiteten Benutzer der Login-Status geändert werden. Vor dem Klick auf den Button „Login-Status setzen“, muss dazu der gewünschte Login-Status ausgewählt werden. Folgende Einstellungen sind möglich:

Die ausgewählten Benutzer erhalten den Login-Status: **enabled**.

Die ausgewählten Benutzer erhalten den Login-Status: **disabled**.

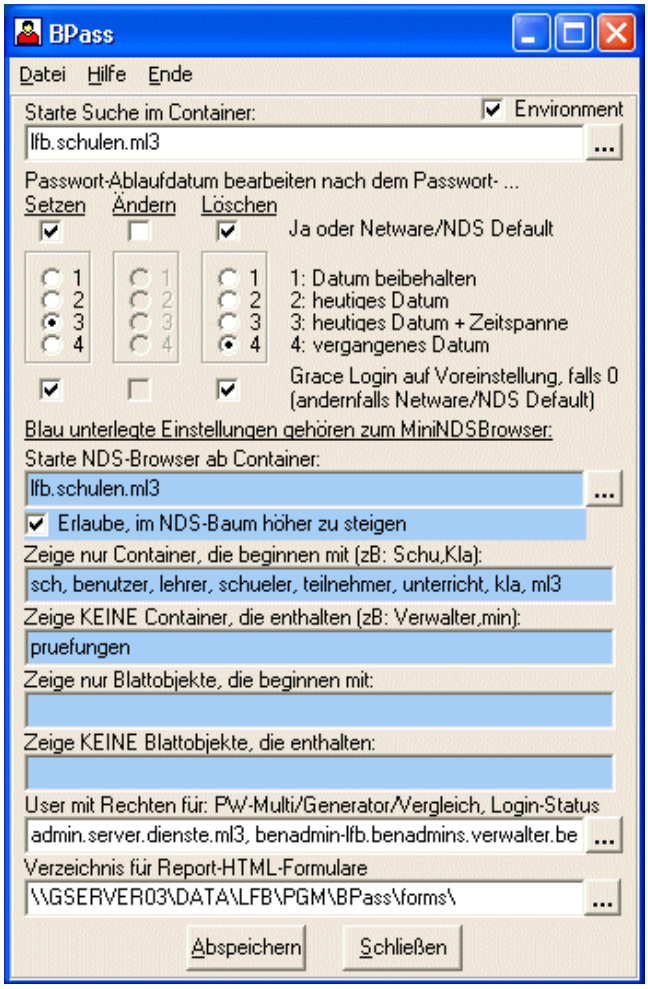
Keine Änderung. Diese Einstellung ist die Defaulteinstellung, damit nicht versehentlich so leicht enabled oder disabled gesetzt wird.

Nach dem Setzen des Login-Status kann über den Button „Report“ eine geeignete Ausgabe erfolgen.

4 Weitere Eigenschaften von BPASS

Vorgaben speichern

BPass kann die von Ihnen gemachten Vorgaben, nämlich den Kontext, ab dem gesucht werden soll, und diverse Anzeigeoptionen für den Mini-NDS-Browser in einer INI-Datei (bpass.ini) speichern. Über das Menü "Datei" und dann "Bearbeite INI-Datei" erhält man:



Einzelheiten siehe weiter oben.

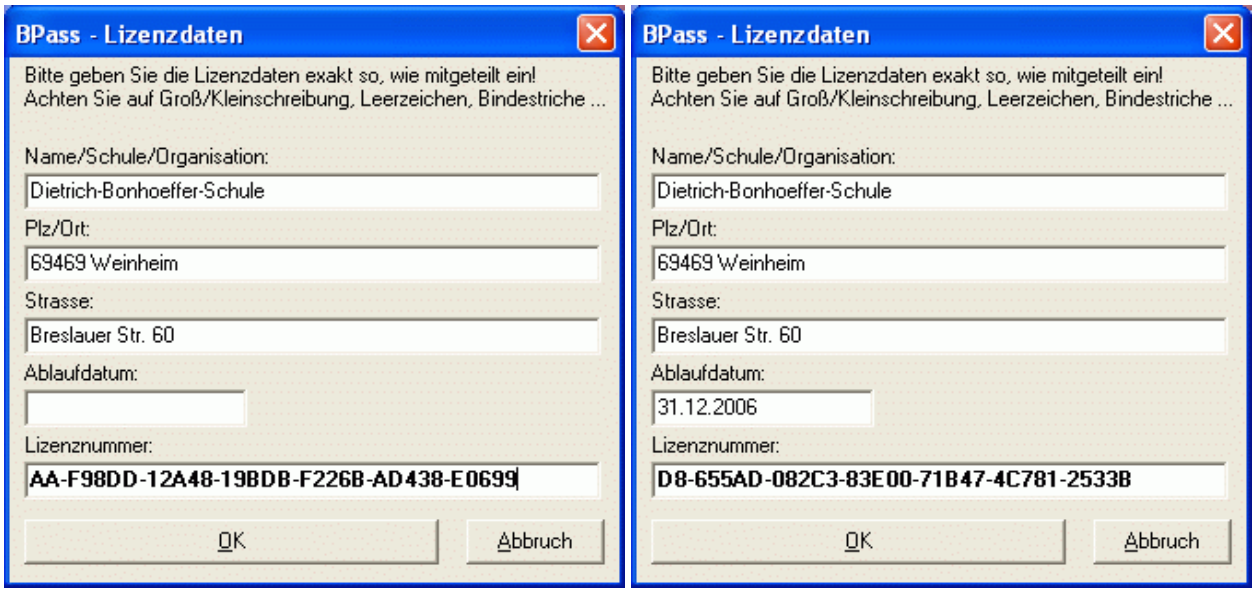
Existiert bpass.ini nicht, während Sie BPass.exe starten, erscheint eine Fehlermeldung. BPass nimmt dann einfach die im Programm voreingestellten Standardwerte. Um aber entweder diese Fehlermeldung zu unterdrücken oder BPass mit selbstgemachten Voreinstellungen zu starten, sollten Sie die Voreinstellungen abspeichern. (bpass.ini liegt immer in dem Verzeichnis, aus dem heraus BPass.exe gestartet wurde). Da ein normaler Nutzer von BPass hier keine Schreibrechte haben sollte, kann ein solcher Nutzer die Voreinstellungen (,die der Admin gemacht hat,) nicht ändern!

Nutzungsbestimmungen

Ebenfalls im Dateimenü (und im Hilfemenü) finden Sie die Nutzungsbestimmungen.

Lizenzdaten

Sie müssen die Ihnen bei der Registrierung mitgeteilten Lizenzdaten eingeben. Über den Menüpunkt "Datei/Lizenzdaten" erhalten Sie das Eingabefenster. Dort müssen Sie die Lizenzdaten exakt, wie sie Ihnen mitgeteilt wurden, unter Beachtung von Groß/Kleinschreibung, Leerzeichen, Bindestriche usw. eingeben (bei zeitlich unbegrenzter Nutzung bleibt das Ablaufdatum-Feld leer):



Ein Klick auf den OK-Button speichert die Lizenzdaten ab.

Auch Musterlösungsnutzer benötigen Lizenzdaten! Gelegentlich kann es zeitlich eingeschränkte Testversionen, die als solche erkennbar sind, geben, für die keine Lizensierung nötig ist. Auch gibt es zeitlich begrenzte Vollversionen. Ansonsten ist BPass für nicht lizensierte Nutzer eine zeitlich begrenzte Demoversion, die alle Funktionen hat, aber die Demo-Eigenschaft öfters meldet und nur zwei Benutzer in vielen Programmteilen bearbeiten kann.
(Die Lizenzdaten oben im Bild sind nur ungültige Beispieldaten!)

Ablaufdatum

Demo- und Testversionen haben ein Ablaufdatum. In Ausnahmefällen kann auch eine Vollversion ein Ablaufdatum haben, in der Regel sind lizensierte Versionen jedoch zeitlich unbegrenzt nutzbar. In diesem Fall bleibt das Ablaufdatum-Feld leer.

Ist ein Ablaufdatum gesetzt, so funktioniert das Programm nach Überschreiten dieses Datums nicht mehr. Im Hilfe-Menü können Sie nachschauen, auf welches Datum das Ablaufdatum gesetzt ist.

WhoAmI

Einen Überblick, als wer Sie angemeldet sind, finden Sie mit dem Menüpunkt "Datei" und dann "WhoAmI". Der dabei angezeigte Context ist der, der zuletzt versucht wurde, nicht der, der zu Ihrer NDS-Position gehört.

Aktueller Context

Denselben Context können Sie sich auch unter Menüpunkt "Datei" und dann "Aktueller Context" anzeigen lassen.

Kommandozeilen-Parameter

Starten Sie BPass aus einer DOS-Box oder dem "Start/Ausführen"-Feld oder aus einer Batch-Datei oder mit einer Windows-Verknüpfung, können Sie folgende Kommandozeilen-Parameter benutzen:

bpass /sc=<Such-Container>	Der hier vorgegebene Such-Container überschreibt den Eintrag aus der INI-Datei. Beispiel: bpass /sc=lehrer.unterricht
bpass /ini=<Dateiname>	Statt der Standard-INI-Datei bpass.ini kann eine andere INI-Datei gewählt werden. Beispiel: bpass /ini=n:\benutzer\neu.ini
bpass /noini	Damit wird die INI-Datei ignoriert. Die Suche beginnt bei [root].

Erweiterte Such-Eingabe

Sie können im Eingabefeld "Passwort ändern für Benutzer" auch einem Benutzernamen den Container hinzufügen. BPass "addiert" zu diese Eingabe automatisch den voreingestellten Such-Container. So wird nach der Eingabe

sperlingh.klasse8a

in unserem Musterumgebung direkt in **`klasse8a.schuler.unterricht`** gesucht.

(Achtung:Die Eingabe sperlingh.klasse8a.schueler ist falsch, da dies intern zu sperlingh.klasse8a.schueler.schueler.unterricht würde.)

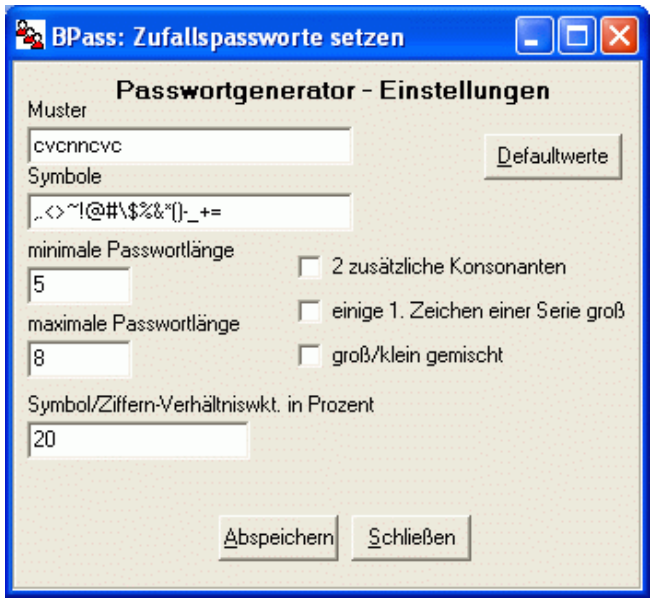
Mit Hilfe des Schrägstrichs "/" können Sie im Eingabefeld "Passwort ändern für Benutzer" aber auch Zusatzinformationen eingeben, mit denen Sie den Start der Suche beeinflussen können. Sie überschreiben damit die Vorgabe der INI-Datei.

Bespiel: Sie wollen Ihr eigenes Passwort ändern. Ihr NDS-Eintrag befindet sich aber nicht im Container, der momentan zur Schülersuche dient. Geben Sie also ein:

spechtb/	Durchsucht die gesamte NDS ab **`[root]`** nach allen Benutzern, deren Usernamen mit "spechtb" beginnt
sp/	Durchsucht die gesamte NDS ab **`[root]`** nach allen Benutzern, deren Usernamen mit "sp" beginnt
spechtb/unterricht	Duchsucht den gesamten Container **`unterricht`** nach allen Benutzern, deren Usernamen mit "spechtb" beginnt
s/lehrer.unterricht	Duchsucht den gesamten Container **`lehrer.unterricht`** nach allen Benutzern, deren Usernamen mit "s" beginnt

5 Passwort-Generator-Einstellungen

Über den Button „Einstellungen“ im Fenster des Passwort-Generators erscheint die Konfiguration des Passwortgenerators:



Über den Button „Abspeichern“ werden diese Einstellungen und die Einstellungen zum Passwortablaufdatum und den Kulanzanmeldungen in die BPass-INI-Datei übernommen.

Der Passwortgenerator generiert Zufallspassworte, die auch hohen Sicherheitsanforderungen genügen, auch mit den oben zu sehenden Standardeinstellungen. Der Passwortgenerator liefert sichere

Zufallspassworte, die aber trotzdem erstaunlich gut zu merken sind.
Wer will kann hier aber auch Veränderungen vornehmen. Im Einzelnen bedeuten die Einstellungen:

Muster
Nach dem Muster werden die Zufallspassworte gebildet. Dabei wird ein Zeichen im Passwort nach dem Zeichen im Muster gebildet, und zwar:

- **c:** Konsonant, klein (lower case consonant)
- **v:** Vokal, klein (lower case vowel)
- **l:** Buchstabe (lower case letter)
- **C:** Konsonant, groß oder klein (mixed case consonant)
- **V:** Vokal, groß oder klein (mixed case vowel)
- **L:** Buchstabe, groß oder klein (mixed case letter)
- **d:** Ziffer (digit)
- **s:** Symbol
- **n:** Nicht-Buchstabe, also Zahl oder Symbol

Jedes Musterzeichen wird für die betreffende Position genau einmal angewendet. Ist die maximale Passwortlänge größer als die Musterlänge, werden weitere zufällige Vokale und/oder Konsonanten angefügt, andernfalls wird ggf. das Passwort auf die vorgegebene Länge gekürzt.

Symbole
Diese Liste darf nicht zu kurz sein, da sonst beim Musterzeichen n die Wahrscheinlichkeit zugunsten der Ziffern und zu ungunsten der Sonderzeichen ausfällt. Ist die Liste leer, werden für das Musterzeichen n nur Ziffern erzeugt. (siehe auch die Symbol/Ziffern-Verhältniswahrscheinlichkeit)

Minimale/Maximale Passwortlänge

Symbol-Ziffernverhältnis in Prozent
Wahrscheinlichkeit (in Prozent (in 10er Schritten)) mit der beim Musterzeichen n ein Symbol/Ziffer gesetzt wird.
Beispiele:

0	erzwingt Ziffer
100	erzwingt Symbol oder Ziffer
70	mit 70% Wahrscheinlichkeit erscheint ein Symbol oder eine Ziffer, mit 30% Wahrscheinlichkeit wird ein Musterzeichen n ignoriert.

Zwei zusätzliche Konsonanten
Mit einer gewissen Wahrscheinlichkeit werden bis zu zwei zusätzliche Konsonanten in das Passwort eingefügt. Die Passwortlänge kann dadurch bis zu 2 Zeichen größer werden, als die maximale Passwortlänge angibt.

Einige 1.Zeichen einer Serie groß
Mit einer gewissen Wahrscheinlichkeit wird der 1.Buchstabe einer Buchstabenserie ein Großbuchstabe.

Groß/Klein gemischt
Groß/Kleinbuchstaben zufällig gemischt (bei Musterzeichen c).

Der Button "Defaultwerte" setzt die oben im Bild zu sehenden Standardwerte.
Der Button "Abspeichern" speichert die Einstellungen in die INI-Datei.

6 Eigene Report-HTML-Formulare erstellen

Für BPass gibt es eine Reihe von vorgefertigten Report-HTML-Formularen, hier kurz Schablonen genannt. Für spezielle Zwecke oder bei Nichtgefallen können aber auch eigene Schablonen erstellt werden.

Bei einer solchen Schablone handelt es sich zunächst einmal um eine ganz gewöhnliche HTML-Datei. HTML-Dateien können mit „gewöhnlichen“ oder speziellen Editoren ganz normal erstellt werden. Dabei können alle gestalterischen „Register“ gezogen werden, auch CSS.

Datenvariable

Damit der Formulargenerator von BPass jedoch seine speziellen Daten platzieren kann, die ja während der Schablonenerstellung noch nicht bekannt sind, muss die Schablone sogenannte Datenvariable enthalten, die als Platzhalter für die eigentlichen BPass-Daten stehen.

So könnte z.B. innerhalb der Schablone, der Satz stehen:
Der Benutzer @SurName|, @GivenName| mit dem Anmeldenamen **@CN|** hat den Accountstatus **@LoginState|**.

Im Ausführungsfall könnte sich vielleicht daraus ergeben:
Der Benutzer **Specht, Bernd** mit dem Anmeldenamen **SpechtB** hat den Accountstatus **disabled**.

Die Datenvariable @SurName, @GivenName, usw. werden also während der Formulargenerierung von BPass mit den aktuellen Daten gefüllt. Sie sind jeweils mit dem Zeichen | zu begrenzen.

Vielleicht möchte man bei der Ausgabe nicht so viel Platz verschenken und beim Vornamen nur die ersten 5 Zeichen ausgeben. Voilà: @GivenName=1/5| tut das Gewünschte. Vom 1. Zeichen an werden 5 Zeichen ausgegeben. (1/0 bedeutet: volle Länge ohne angehängte Leerzeichen).

Datenvariable gibt es ca. 30 Stück. Sie sind in der Datei **`datenvariable.html`** aufgelistet und erklärt.
(Mit einem HTML-Browser betrachtet sieht diese Datei etwas eigenartig aus, da viele doppelte @-Zeichen zu sehen sind. Mit dem BPass-Formulargenerator aufgerufen, liefert sie jedoch für einen Benutzer gleich dessen Daten. Dabei sollte die Liste z.B. im Passwortgeneratorfenster am besten jedoch nur einen einzigen Benutzer enthalten, damit man nur eine einzige Ausgabeseite erhält.
Trotzdem ist die Datei `datenvariable.html` auch mit einem normalen Browser oder HTML-Editor gut lesbar. Datenvariablen können dabei gut per Drag&Drop in die eigene Schablone übernommen werden.)

Steuerbefehle

Damit jedoch auch zwischen Einzelseiten- und Endlos- Ausgaben unterschieden werden kann, gibt es noch eine Reihe von Steuerbefehlen, die als HTML-Kommentare in die Schablone einzufügen sind.
Z.B. könnte für eine Ausgabe verlangt werden, dass ein Kopfbereich auf der ersten Seite erscheint, dann aber fortlaufend eine Zeile für jeden Benutzer der Liste wiederholt wird; auf der ersten Seite 40 mal (da ist ja auch der Kopf drauf), auf den folgenden Seiten 50 mal.
Die folgenden Steuerbefehle tun dies:

```
<!--OSListform=HeadOnlyFirstPage-->
...
<html>
…
<!--OSHeadBegin-->
Text für den Kopf...
...
<!--OSHeadEnd-->
<!--OSTextblockBegin-->
<!--OSTextblockRepeatPerPage=50-->
<!--OSTextblockRepeatFirstPage=40-->
@SurName|, @GivenName| @CN| @LoginState|
<!--OSTextblockEnd-->
...
```

Alle Steuerbefehle werden ebenfalls in **`datenvariable.html`** erklärt.

Für das Erstellen von eigenen Schablonen lohnt sich das Studium der mitgelieferten Schablonen.

7 Tipps

Die Programmteile „Passwort-Vergleich“ und „Login-Status“ dienen dem Administrator/Netzwerkberater/BenutzerAdmin als Pflegewerkzeuge, um eventuelle Sicherheitslücken aufzudecken, übersichtlich über Reports zu dokumentieren und ggf. Benutzer adäquat zu benachrichtigen.

Nachdem mit BImport Benutzeraccounts angelegt wurden, dienen die BPass-Programmteile „Passwort-Generator“ oder Multipassworte“ zur Festlegung von Passworten und zur Ausgabe dazugehöriger Reports und Listen.

Für die Musterlösung ist dabei zu beachten, dass die Standardeinstellung für einen Benutzeraccount u.a. ein Passwortablaufdatum und eine Kulanzanmeldung=1 beinhaltet. Für das Setzen oder Löschen eines fremden Passwortes z:B. des Schülers durch den Lehrer oder das Setzen von Zufalls- oder Multpassworten ist in BPass die Standardeinstellung

- Passwortablaufdatum auf ein vergangenes Datum setzen
- Kulanzanmeldungen (*Remaining Grace Login*) auf den Vorgabewert setzen, falls 0.

vorgesehen.

Damit wirkt ein neues Passwort wie ein Einmal-Passwort. D.h., der Benutzer wird danach beim ersten Anmeldevorgang aufgefordert, sich ein neues Passwort zu geben.

- Ende -

Viel Erfolg mit BPass.

Zurück zur OSSOS - Homepage