Stand: 22.9.2008

BPass – Neuerungen in der Version 3.x

0. Inhaltsverzeichnis

1. Vorwort

Die neue Version von BPass beinhaltet neben den bekannten Eigenschaften ein umfassendes Passwortmanagement. Herzstück ist ein konfigurierbarer Passwortgenerator, der es gestattet, Benutzern sogenannte sichere Zufallspassworte zuzuweisen. Der bereits bekannte 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 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 bisherige Passwortvergabe von BPass ist eine genaue Konfiguration hinzugekommen. 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.

BPass ist damit zu einem Passwort-Management- Werkzeug geworden. BPass, der kleine Bruder von BImport, ist erwachsen geworden!

Viel Erfolg mit BPass wünscht Ihnen
Uwe Labs.

2. NDS-Defaults für das Passwort - Setzen,Ändern,Löschen -

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 neuen 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.

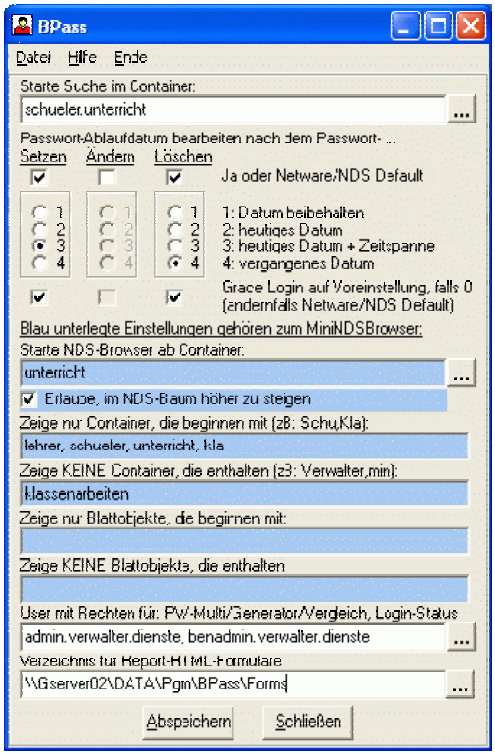
Eigenes Passwort löschen

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

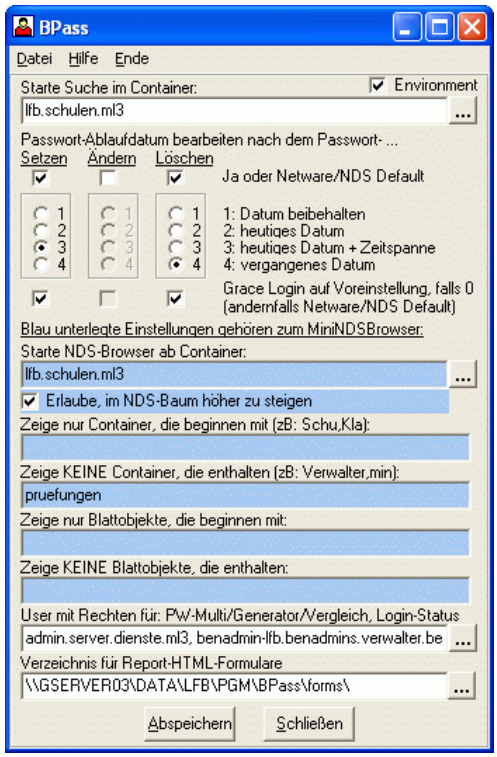
3. Konfigurationseinstellungen

Die 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.

Für ML2:



Für ML3:



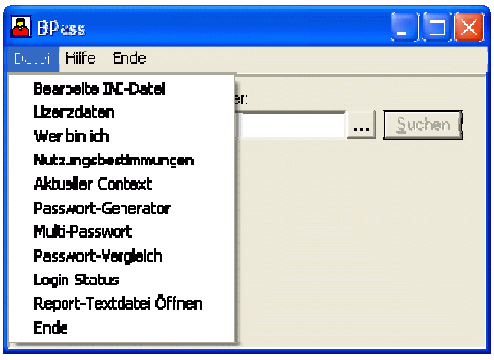
Die blau unterlegten Felder beziehen sich auf den Mini-NDS-Browser und sind jetzt dadurch besser erkennbar.

Neu hinzu gekommen ist das Feld „Verzeichnis für Report-HTML-Formulare“. Hier liegen die HTML-Schablonen für die HTML-Reportausgabe. (Leeres Feld bedeutet: BPass-Programmverzeichnis).

Bemerkung: Damit BPass überhaupt seine Aufgaben erfüllen kann, müssen für diejenigen Benutzer, die die Passworte anderer bearbeiten sollen (z.B. Lehrer, BenutzerAdmin) , gewisse Trustee-Rechte gesetzt sein, nämlich: „Password Expiration Time“, Password Management“ und „Password Required“ jeweils auf Supervisor und Vererbbar *(Supervisor und Inhertiable)*.

4. Menüpunkt „Datei“

Neue Menüpunkte:



- Passwort-Generator
- Passwort-Vergleich
- Login-Status
- Report-Textdatei öffnen

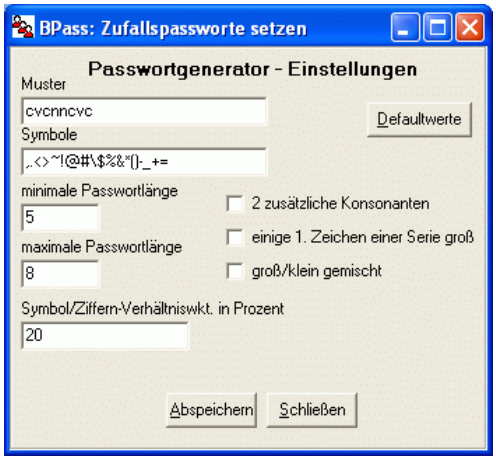
Die genannten Menüpunkte können nur von Personen aufgerufen werden, die bei den Kofigurationsdaten im Feld „User mit Rechten für PW-Multi/Generator/Vergleich,Login-Status“ aufgeführt sind.

5. Passwort-Generator

Genau wie vom Programmteil „Multi-Passwort“ gewohnt, erfolgt die Benutzerwahl. Ein Klick auf den Button „Passwort setzen“ lässt die Bearbeitung ablaufen, wonach die bearbeiteten Benutzer ein Häkchen in der Liste bekommen.

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

Über den Button „Einstellungen“ 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. Siehe dazu das Kapitel „Passwort-Generator-Einstellungen.

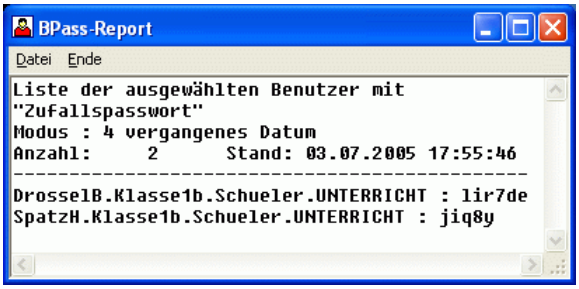
Listenübernahme

Ist zuvor der Programmteil „Passwort-Vergleich“ gelaufen, so erscheint im Fenster der Button „Übernimm Liste...“:

Damit lässt sich die gleiche Liste, die schon 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.

Report

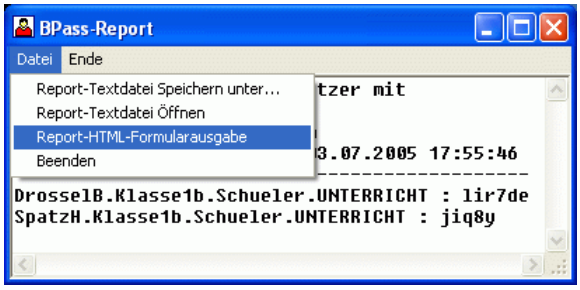
Über den Button „Report“ öffnet sich ein Fenster, dass die soeben durchgeführte Zufallspasswortzuteilung in einfachem Text dokumentiert:

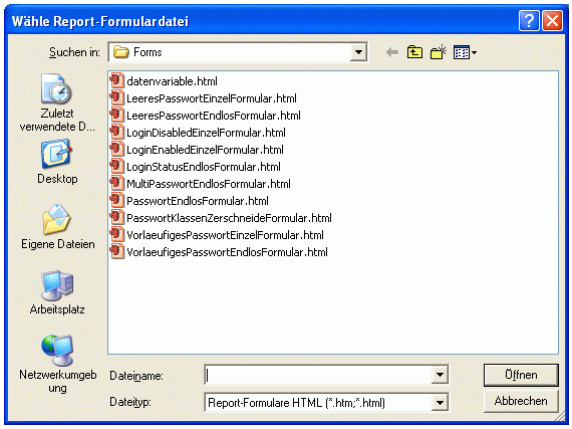


Im Kopf der Liste steht, was gezeigt wird, in welchem Modus bzgl. Ablaufdatum und Kulanzanmeldungen gearbeitet wurde, wie viele bearbeitete Benutzer die Liste enthält und das Datum und die Uhrzeit der Bearbeitung. Danach folgt die Liste der bearbeiteten Benutzer mit qualifiziertem Benutzernamen einem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

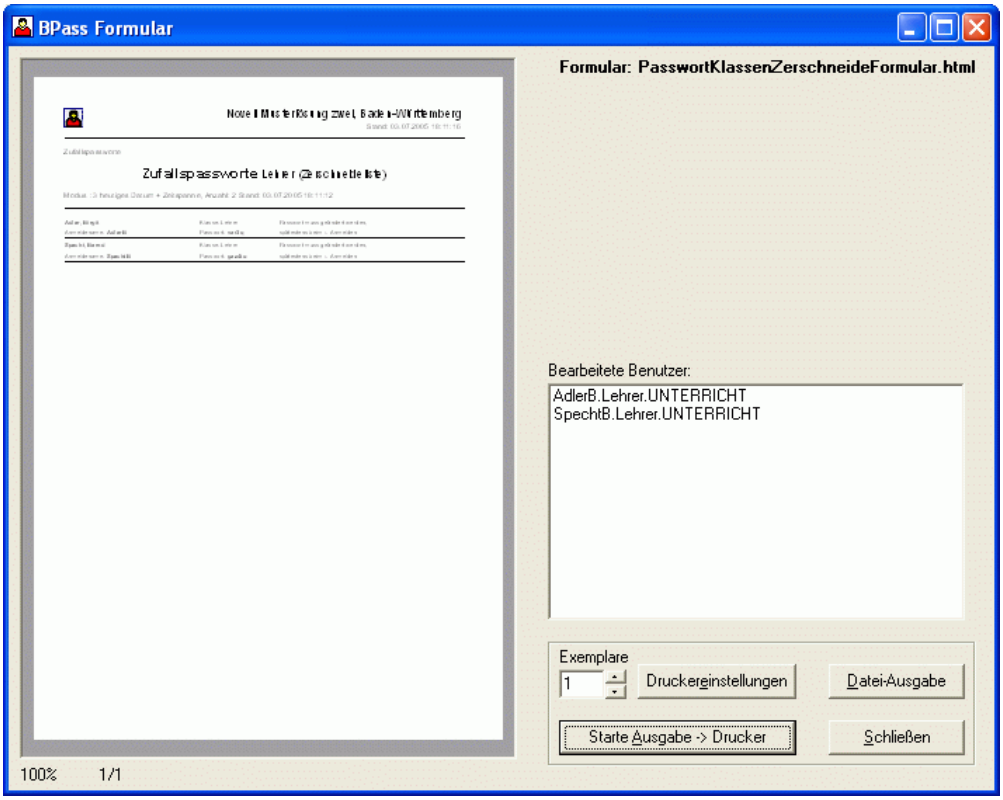
Mit dieser Liste lassen sich nun verschiedene Aktionen durchführen:

- 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.

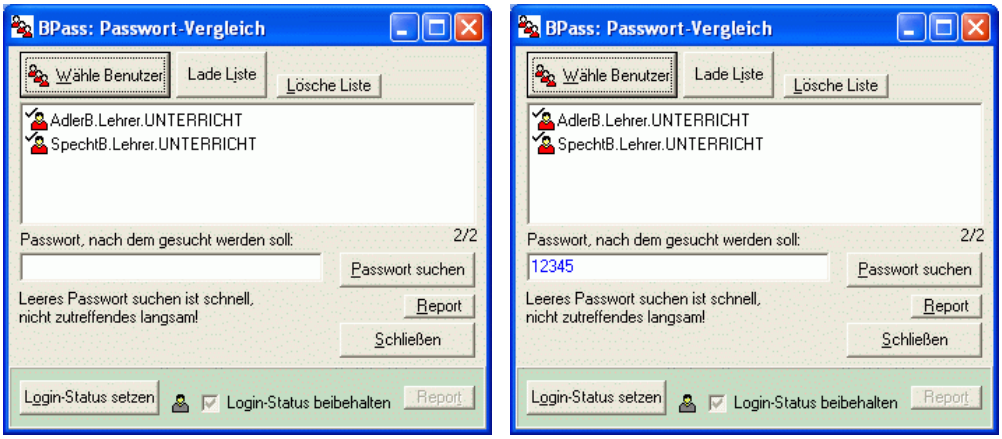
Hinweis: Im BPass-Report-Fenster gibt es im Dateimenü noch den Punkt „Report-Textdatei öffnen“. Dieser Punkt ist dafür gedacht, eine bereits zuvor gespeicherte Report-Textdatei erneut zu laden, um sie der Report-HTML-Formularausgabe zuzuführen. Ebenso findet sich dieser Punkt im Hauptdateimenü von BPass.

6. 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:

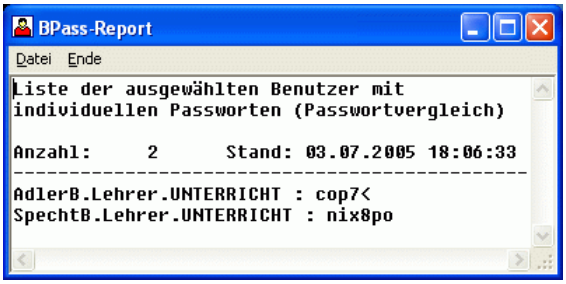
`LeeresPasswortEinzelFormular.html`: Für jeden solchen Benutzer wird eine eigene Seite ausgegeben mit einem Hinweis, sich ein Passwort zu geben, da andernfalls sein Account gesperrt werden muss. Auch Tipps zur eigenen Passwortvergabe dazu stehen auf dem Blatt.
`LeeresPasswortEndlosFormular.html`: Eine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

7. Login-Status

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

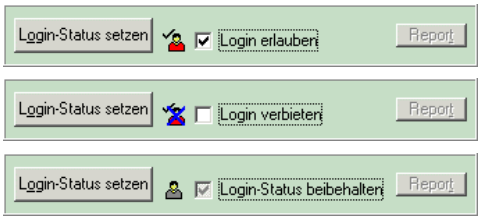
Die Login-Status Suche kann für folgende Fälle vorgewählt werden:

- 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:

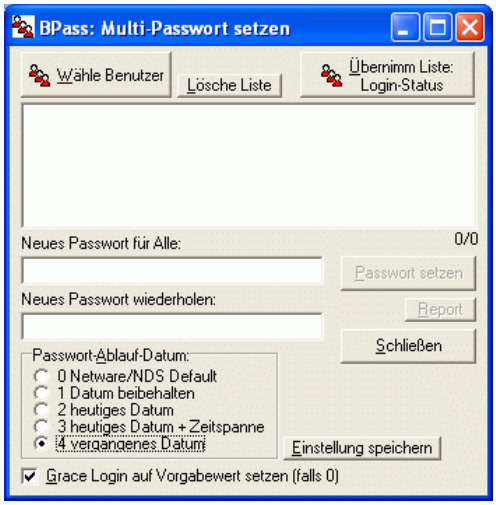


Die ausgewählten Benutzer erhalten den Login-Status: **enabled**.
Die ausgewählten Benutzer erhalten den Login-Status: **disabled**.
Keine Änderung. Diese Einstellung ist die Defaulteinstellung, damit nicht versehentlich so leicht enabled oder disabled gesetzt wird.

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

8. Multipassworte

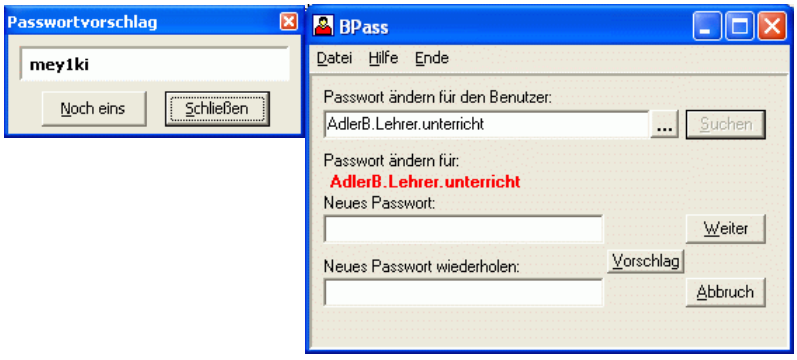
Beim Programmteil „Multipassworte“, der dazu dient, einer Menge von Benutzern dasselbe Passwort zu geben oder das Passwort zu löschen, ist ebenfalls unabhängig von den oben besprochenen Konfigurationseinstellungen das Verhalten bzgl. Passwortablaufdatum und Kulanzanmeldungen einstellbar. Über den Button „Einstellung speichern“ können diese Einstellungen in die INI-Datei übernommen werden.



Eine schon im Programmteil „Login-Status“ bearbeitete Benutzerliste kann hier übernommen werden.

9. Passwort-Vorschlag

Im BPass-Hauptprogramm, bei dem sich Benutzer einzeln ein Passwort setzen können oder bei dem ein Berechtigter einem anderen Benutzer ein Passwort gibt (z.B. Lehrer/Schüler) gibt es jetzt einen Button „Vorschlag“. Mittels des weiter oben und weiter unten beschriebenen Passwort-Generators wird dabei dem Benutzer ein Zufallspasswort vorgeschlagen.



Bei Nichtgefallen kann sich der Benutzer mit dem Button „Noch eins“ beliebig viele Passworte vorschlagen lassen. Ein vorgeschlagenes Passwort kann er aber nicht per Drag&Drop in die Felder „Neues Passwort“ und „Neues Passwort wiederholen“ übernehmen. Dadurch ist der Benutzer gezwungen, sich durch eigenhändige Eingabe an sein neues Passwort zu gewöhnen.

10. 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

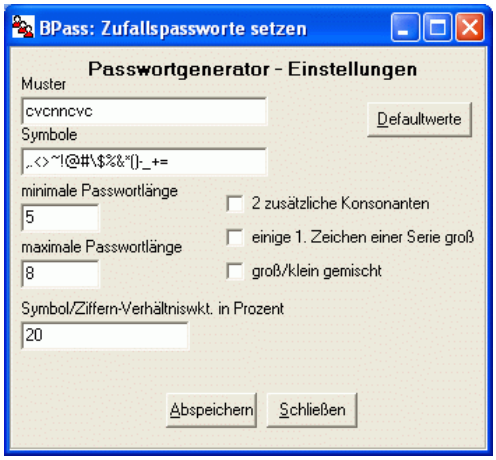
- Passwortablaufdatum auf ein vergangenes Datum setzen
- Kulanzanmeldungen *(Remaining Grace Login)* auf den Vorgabewert setzen, falls 0.

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.

11. 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.

12. 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.