

# Creating initial UNIX user passwords

Short guide by Henrik Lund Kramshøj  
March 2007

## Preface

Password are the keys to the kingdom and the attacker that can guess your password can access the same resources as you can.

People are notoriously bad at choosing passwords and should use password generators.

This policy and instruction is deliberately created to avoid

1. users sharing a common password such as passw0rd, abc123, start123, ...
2. users having an easy to guess initial password
3. administrator remembering the initial passwords of users

If the systems allow, the user should consider the use of pass phrases instead of passwords.

Further security measures would include using keys and certificates instead of passwords,

but for this document it is considered a fact that at least some servers use passwords.

This document describes implementing measures against easy to guess shared initial passwords.

## Prerequisites

To make use of these instructions the administrator should have:

- root access or similar security group access to create users and assign passwords - already in place
- have a tool to create users and assign passwords - already in place
- have a tool of their choice to generate passwords - administrator must select a tool

## Default Publication

It is expected that administrator has a tool for creating the user and assign password, such that the password is only entered once. Since I do not know the actual script used I will as an example assume that it is a simple script requiring only three parameters servername, username and password.

## Creating users

The procedure for creating UNIX user is thus changed in the first step where the administrator previously selected the password he is no longer allowed to choose a password, but **MUST** generate it securely.

Step 1a Add password generator to toolchain

It is recommended that the administrator add the password generator to the tool used for creating users such that the password is written to the screen while creating the users.

Step 1b alternative Run password generator and copy password

If the tool used by the administrator does not allow the password generator to be executed automatically it should be run in parallel and then the generated password pasted into the tool.

Step 2

Create users using the normal procedure

Step 3

The administrator would then copy that password into a mail for the user. When sending this email it should not be kept in the sent folder of the email program used, but deleted.

## How to use a password generator

Password generators can be found both as GUI programs and command line tools.

A password generator such as pwgen is run from the command line and produces a generated password.

Using the pwgen from Tytso/Sourceforge it would be:

```
hlk@bigfoot:pwgen-2.05$ ./pwgen -s 10 1
sZzs53E214
hlk@bigfoot:pwgen-2.05$ ./pwgen -s 10 1
50VqhsPOFs
hlk@bigfoot:pwgen-2.05$ ./pwgen -s 10 1
UhT0kc12ch
hlk@bigfoot:pwgen-2.05$ ./pwgen -s 10 1
Mnjug3zt5a
hlk@bigfoot:pwgen-2.05$ ./pwgen -sy 10 1
R9!S1\ot%C
hlk@bigfoot:pwgen-2.05$ ./pwgen -sy 10 1
```

## Default Publication

```
>-9&Tcj5Su  
hlk@bigfoot:pwgen-2.05$ ./pwgen -sy 10 1  
^V8&>-]^M^  
hlk@bigfoot:pwgen-2.05$ ./pwgen -sy 10 1  
E{3t|*_ "ER
```

Note the change in parameters requiring special characters in the last four passwords generated.

It is recommended to use this setting, but in some environments the normal generated password is enough.

## Recommended tools

Password Safe, can be run on both UNIX and Windows and includes password generator

<http://passwordsafe.sourceforge.net/>

Pwgen - multiple tools exist for UNIX with a name of password generator

As an example this one: <http://sourceforge.net/projects/pwgen>

Another one I have used from MacPorts is available from

<http://www.tricknology.org/ports/>

## Hints and tips

create an alias for your password generator such as:

```
pwgen -s 10 1
```

## FAQ

Q: What happens if the user does not change the initial password

A: The initial password is generated using a good password generator and should be at least as secure as passwords generated by the users.