Weak Password Detection

Overview

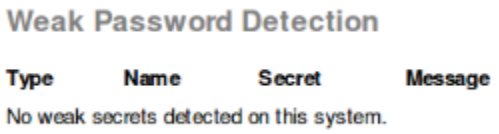
The Weak Password Detection module shows an administrator any user accounts, extensions or trunks that have weak registration passwords. Weak passwords represent a huge security risk and should be updated as soon as possible.

> No single security practice will keep you secure. This module should be used as part of an overall security strategy

Logging In

- From the top menu click **Reports**
- In the drop down click **Weak Password Detection**

Generating a Weak Passwords Report



If the module detects weak passwords it will flag the extensions in the report so you can update them. A system with no detected weak passwords will show the above screen upon logging in.

If weak passwords are detected they will appear in the report with a reason for the detection.

Creating New Extensions with Strong Passwords

In newer versions of FreePBX the secret field will automatically populate with a secure password. If you override the generated password, the Extensions module, by default, will prompt you to enter passwords that are at least six characters and contain both numbers and two alpha characters.

When Creating an Extension- The PBX will prompt you to enter a valid password if it does not pass validation, however, weak extensions can be registered to the system by:

- Bulk Extension Import - There is no data validation when using the Bulk Extension module to create a new extension.
- Backup/Restore Module - There is no data validation when restoring a back-up. If the original system had weak extensions, they will be restored to the server.

Removing Strong Password Requirement

In the event you have hardware that is incompatible with the strong password validation, you can remove the requirement by adjusting the device settings in the Advanced Settings Menu of your PBX.

Require Strong Secrets - Toggle this option to **False** and then save to remove the “Strong Secrets” data validation when creating extensions.

Tips

It is recommended to always use complex extension passwords. The latest version of the PBX software will auto generate a strong alpha-numeric password with 32 digits. Although the system will only report on weak passwords when less than 6 digits, it is a best practice to use stronger passwords. When combined with an endpoint manager, there is no additional hardship by using the longer passwords and it adds an additional barrier to enhance the security of your PBX.

See: http://en.wikipedia.org/wiki/Password_strength for more on password strength.