



1251 Waterfront Place, Suite 525
Pittsburgh, PA 15222
330 S Poplar Ave, Suite 103-E
Pierre, SD 57501
1-800-693-7800
www.macg.com

TNS Password Requirements

TNS Password Requirements

Summary

One of the potentially weakest links in computer security is the individual password. Despite Mid Atlantic's efforts to keep hackers out of system, easily-guessed passwords are still a big problem.

Mid Atlantic implements a strict password checking system for TNS User IDs to combat this problem. Each time change or reset your password, the system will prevent you from setting a password that is easily cracked.

In addition, Mid Atlantic now allows you to use "pass phrases" instead of passwords. Pass phrases are longer, but easier to remember than complex passwords, and if well-chosen can provide better protection against hackers. We are allowing this based on guidelines published by NIST.

Passwords are required to be changed after 60 days.

Password Rules

Mid Atlantic's TNS Password rules, based on password length are:

- 8-20, secure password: mixed case letters, numbers & symbols
- 20-100, pass phrase: no restrictions
- It *must not* be equal to your current password or previous passwords used over the last 12 months
- It *must not* contain your User ID
- It *must not* be a commonly used password that is blacklisted by Mid Atlantic. We maintain a list of passwords that are known to be hacked and insecure even though they fit into our criteria for passwords of 8-20 characters in length. *This list is not available for distribution.
- It *must* be composed only of characters in the Roman alphabet, numbers, or symbols on the US keyboard. Examples include characters such as # \$ % ! @.

Passwords must be changed every 60 day, which the user will be automatically prompted to change when logging in. After 60 days, a user is unable to log in until the password is changed. If the password is not changed after 120 days, the User ID is suspended and can only be reset by an authorized user administrator.

Creating a pass phrase

A pass phrase is basically just a series of words, which can include spaces that you employ instead of a single pass "word." Pass phrases should be at least 20 to 30 characters in length (spaces count as characters), but can be no less than 20 or it is considered a password and is required to follow the secure password rules above. Longer is better because, though pass phrases look simple, the increased length provides so many possible permutations that a standard password-cracking program will not be effective. It is always a good thing to disguise that simplicity by throwing in elements of weirdness, nonsense, or randomness. Here, for example, are a couple pass phrase candidates:

- pizza with crispy spaniels
- mangled persimmon therapy

Punctuate and capitalize your phrase:

- Pizza with crispy Spaniels!
- mangled Persimmon Therapy?

Add a few numbers or symbols, plus some deliberately misspelled words, and you'll create an almost unguessable key to your account:

- Pizza w/ 6 krispy Spaniels!
- mangl3d Persimmon Th3rapy?