Notes.net
Iris Today

by Christie Williams
(with Katherine Spanbauer)

Level: Intermediate
Works with: Domino 5.0
Updated: 09/04/2001

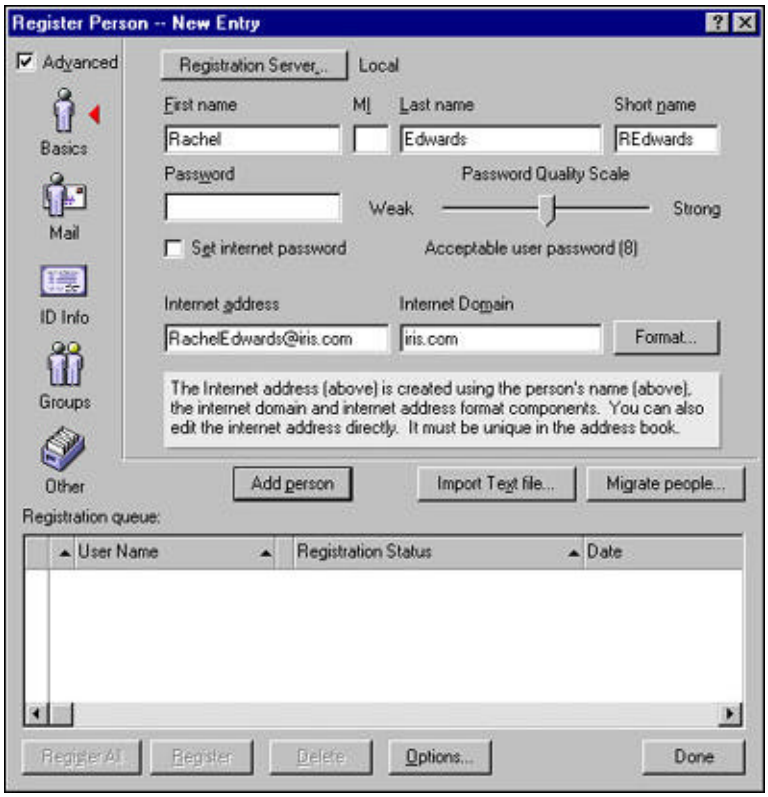
Users are notorious for choosing obvious passwords; after all, they want something that's easy to remember. But easy-to-remember does not always translate into something that keeps the user's ID file—and by extension, your company's information—secure.

Prior to R5, password strength was based on the length of the password. Beginning with R5, this feature was enhanced to use a password quality algorithm instead of relying solely on password length. The algorithm was designed to encourage users to choose better passwords to protect their ID files.

This article describes how password quality is used and provides details about the password quality algorithm. It assumes a basic understanding of Notes/Domino administrative tasks and the Notes log-in process.

Password quality basics

When registering new users, administrators assign a password strength, or quality, to the user's Notes ID file. The Password Quality Scale is an Advanced option on the Basics panel of the Register Person dialog box.



The following table describes the values on the password quality scale, from weak (0) to strong (16):

Password quality scale	Description	Examples
0	Password is optional	n/a
1	Allow any password	
2-6	Allow a weak password, even though it might be guessed by trial and error.	fish password (password quality scale 3) lightferret b 4D (password quality scale 6)
7-12	Require a password that is difficult to guess but might be vulnerable to an automated attack	pqlrtmxr wefourkings (password quality scale 8)
13-16	Require a strong password, even though the user may have difficulty remembering it	4891spyONu (password quality scale 13) lakestreampondriverocean stRem2pO() (password quality scale 15) stream8pond1river7lake2ocean (password quality scale 16)

Passwords can be of the same length and have different password quality ratings because of the difference in character complexity. For example, *password* is rated a 3, *pAssw0rd* is rated 10, *pwd46dwp* is rated 10, and *PwD46dWp* is rated 12.

By default, Domino defines a password quality of 8 for users, but administrators can raise or lower that in the Registration dialog box. (You can also control the default value; see the **Default password quality settings** section for more information.) The assigned password quality value is stored in the user's ID file during registration and is enforced by Notes when the user changes passwords.

Users can change their passwords whenever they want—when they feel their password has been compromised, for example—or if password checking is enabled, they will be prompted to do change passwords to comply with the password change interval. If password checking is enabled, Notes will prevent users from reusing passwords; it stores a history of passwords used in the user's ID file. (See the *Iris Today* article, "**Notes from Support: Password checking,**" for more information about password checking.)

When using the Change Password dialog box, the user types in a new password. If using a client prior to R4, password length is checked and enforced. If using the R5 client, the password quality algorithm is used to evaluate the password and assign it a value on the password quality scale.

If the password's value falls below the required password quality value, the password is unacceptable and the user is prompted with the message "Your password is insufficiently complex. Add more characters or varied characters."

If you want to offer users more specific guidance about which passwords

will be acceptable, you need to understand how the password quality algorithm works.

Understanding the algorithm

In previous releases of Notes, passwords were required only to meet a minimum assigned length. In R5, length is just one component of judging the password's quality. For example, if a user's ID requires a password strength of 8, *password* would be an acceptable password in R4, but it would not be acceptable in R5 because it is a word that can be found in the dictionary. Notes uses the spell check dictionary, as configured in User Preferences. [The dictionary used to create the examples in this article was English (United States).]

A password's strength is based on several factors. A password starts out with a rating equal to the length of the password. It receives a 25 percent bonus if it contains one of the following, and a 50 percent bonus if it contains two or more:

- Mixed case
- Numbers
- Punctuation

Digits in the last position and uppercase letters in the first position do not qualify as bonus characters because these are commonly used modifications to passwords to evade password-checking mechanisms.

In addition, the rating decreases if the password contains anything that can be programmatically determined to be predictable, for example, words in a dictionary or repeating characters.

Developing rules for users

Users appreciate guidance in what will constitute an acceptable password, but the algorithm was not designed to adhere to a precise set of rules. However, if administrators understand the algorithm formula as described above, they should be able to define rules that fit their policies and the password quality algorithm, if they choose to do so.

For example, here are some sample password rules about what is considered acceptable for several password quality ratings. Note that these rules may actually exceed the minimum quality required, in order to be conservative. Remember that in addition to the following, single words from the dictionary should always be avoided and special characters located in the first and last position may not be sufficient to pass the algorithm's test.

Rules for a quality rating of 6:

- Choose a password that contains at least six characters and includes at least one of the following: number, mixed case, punctuation.
- Choose a password that contains at least six characters and that does not include a single word from the dictionary.

Rules for a quality rating of 8:

- Choose a password that contains at least six characters and that includes at least two of the following: number, mixed case, punctuation.
- Choose a password that contains at least seven characters and that includes one number and one uppercase letter.
- Choose a password that contains at least eight characters and that includes at least one of the following: number, mixed case, punctuation.
- Choose a password that contains at least eight characters and that does not include words from the dictionary.

Rules for a quality rating of 10:

- Choose a password that contains at least eight characters and that includes at least two of the following: number, mixed case, punctuation.

- Choose a password that contains at least ten characters and that includes at least one of the following: number, mixed case, punctuation.
- Choose a password that contains at least 12 characters and that does not include words in the dictionary.

Remember that, as helpful as such rules are to users, passwords that don't match the specific rules might still meet the required password quality rating.

Here is a table of passwords that meet the each password quality rating in the password quality scale. We strongly recommend that users do not choose any of these examples as their actual passwords.

Password Quality	Examples
3	dog password pwd 2d4
4	5786 atof r2d2
5	d0gs doGs scAle
6	sCa1e dogcat pw46wp
7	cat7dog catSrOK
8	tyughvbn one21two rt 7uj
9	one2 1two onetwothree
10	pAssw0rd pwd46dwp
11	winD39_BP the way we were
12	PwD46dWp rtyughjkbnml GoneWithTheWind
13	Gone With The Wind 4891spyONu
14	tree forest grass rock thedogisontheporch
15	thecathidesunderthebed tdiotp&tchutb
16	thecowjumpedoverthemoon thedishranawaywiththespoon stream8pond1river7lake2oceanz

General guidance for users
In addition to rules, there are several tips you can give users that will help them in choosing passwords:

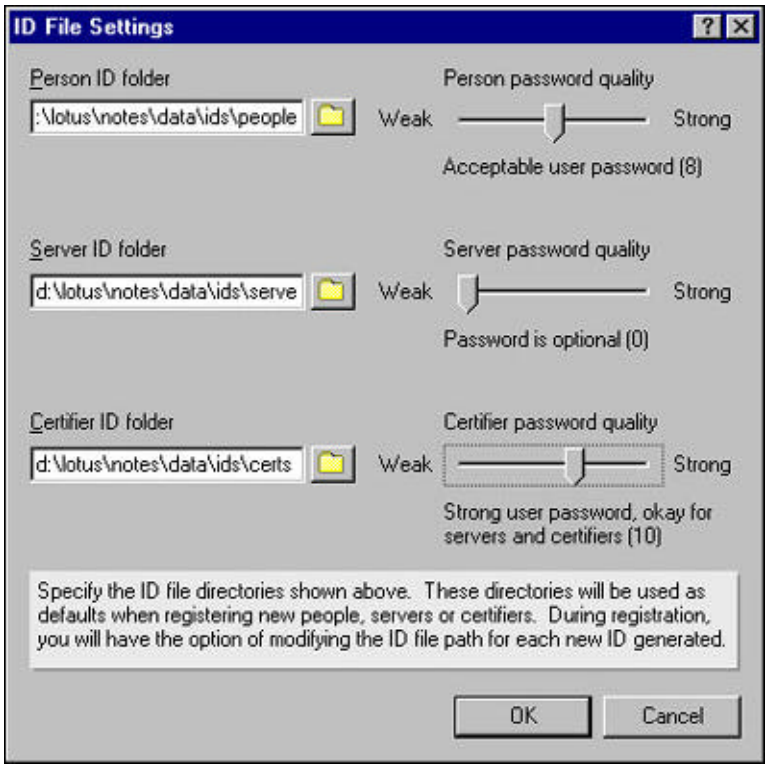
- Avoid words that are in the dictionary as these create weaker passwords.
- Include mixed case, numbers, and punctuation in the password. These increase the password's strength.
- You can make a password stronger without making it longer by avoiding words and/or breaking up alphabetic characters with numbers and punctuation. Using mixed case within strings of alphabetic characters is also helpful.
- Use a passphrase rather than a password. A passphrase, such as a complete sentence, is difficult for an attacker to guess. Including misspelled words in the phrase makes it an even stronger password.

Additional considerations

There are several other points to keep in mind when administering password quality.

Default password quality settings

As previously mentioned, the default password quality for users is 8. The default for certifier IDs is 10 and for servers, it is 0. You can change any of these defaults in the ID File Settings dialog box, which you access from the Administration Preferences dialog box.



For example, if your organization determines that users' passwords should have a password quality of 13—to prevent vulnerability to automated attacks—you can change the user (Person) default to 13 rather than modify the Registration setting each time you register users.

Changing a previously registered user's password quality setting

You can change a user's password quality setting only when manually recertifying users. During manual recertification, a safe copy of the ID file is sent to the administrator to be recertified. This method allows settings within the ID file itself to be modified. The user then merges this safe copy into their ID files, accepting the ID file changes and the new certificate.

When recertifying users from the Person view of the Domino Directory (names.nsf), only the certificate is updated. When the user authenticates with their home server after recertification, their ID file is automatically updated with the new certificate.

Note that in the next release of Notes/Domino, Rnext, the use of policy documents will make changes to password quality settings more automated.

Upgrading from R4 to R5
When upgrading from R4 to R5, the switch to evaluation of passwords using the algorithm takes effect only when users change their passwords. It does not check for password quality when the client is upgraded. So, for organizations that enforce password change intervals, users will need to be aware that they may need to choose better passwords than they had in the past. If password expiration is not used, users will not be forced to change their passwords to comply with the new password quality scale. However, it will be enforced whenever the user either chooses to change their password or is prompted to change their password.

Be aware that administrators cannot choose to use password length rather than the password quality algorithm with R5. In Rnext, administrators will have that choice.

Conclusion

Although the password quality algorithm itself is intricate, working with it need not be difficult. It's easy to assign an appropriate quality, and providing guidance to users helps them select new passwords without frustration. The bottom line is that password quality is a flexible and important method for keeping users' passwords secure.

About Katherine Spanbauer
Katherine is the Product Manager for Security, primarily focusing on Notes and Domino. Her current responsibilities include representing customer requirements to development, triaging critical issues, and communicating product features both within Lotus and to customers. Since joining Lotus in 1992, she has held various roles in the Technical Support, Professional Services and Product Management organizations. Katherine is a graduate of the University of Wisconsin, where she earned her Bachelor of Business Administration degree.

