Pathscrambler Security Enhancements

Pathscrambler Security Enhancements

Blog by Andy Holzman

"From simple encoding to strong encryption, read on to learn about the latest security our third iteration of the path scrambler brings"

With this blog we announce a change to the Pathscrambler encryption of the Uniface assignment files that will become available in one of the upcoming patches.

We have enhanced the security provided by the Pathscrambler, the Uniface utility used to encrypt sensitive information and values in assignment files and login strings. The Pathscrambler will now append a digest to any assignment file line or string in which it has encrypted some text. This ensures that the encrypted line cannot be tampered with in any way.

The difference in behavior is significant enough that we can speak of an old and a new Pathscrambler, although there are no changes in the way the Pathscrambler is used to encrypt files and strings.

The previous Pathscrambler functionality is still supported, so older assignment files will continue to work as they did before. However, it is no longer possible to regenerate those encrypted assignment files or strings using the new Pathscrambler. It will always generate new files and strings with the enhanced security.

There are some consequences to this extra security:

- Any assignment file line or string with a digest cannot be altered in any way.

For example, previously any text not encrypted could be changed. With the new Pathscrambler, not even a space can be changed, as this would invalidate the digest.

- The encrypted line or string must be used in its entirety. A single line or string cannot contain a mixture of old and new encryption. This has an impact in the way that an encrypted string can be used in the open Proc statement and with the{{ /log}} command line qualifier.

For example, in the past, the string used in the open statement for a database path could be dynamically constructed in Proc, possibly using an encrypted password string that had been supplied by the Pathscrambler. This is no longer possible. The complete open string must be provided by the Pathscrambler, otherwise the digest validation will fail.

You can still dynamically construct an open string for a database path using the $password function, but no other parts of the string can be provided by the Pathscrambler. $user can be used as that does not encrypt the data.

- All the lines in an assignment file must be of the same encryption. You cannot mix lines from an old assignment file and a new one.

It is possible to still include an old assignment file in a newly encoded one, using #FILE, but you cannot mix actual lines in the same assignment file. You cannot cut and paste some lines from an older assignment file into a new one. This means that it is no longer possible to start with a previously-encoded file that contains some of the older Pathscrambler's encoding, and then add new encoding to it. The result would be a mixture of encodings, which is not allowed.

- The output from the Pathscrambler cannot be re-submitted to the Pathscrambler. If previously encrypted items are submitted to the Pathscrambler, the resulting strings will not be usable by Uniface. If changes are required, they must be done in the original un-encrypted file, and that file should be re-submitted to the Pathscrambler.

We strongly recommend that anyone that has security concerns about the contents of their assignment files, should use the new Pathscrambler to encrypt their assignment files.