Source:
https://support.industrysoftware.automation.siemens.com/docs/teamcenter/10.1/PDF/en_US/tdocExt/pdf/utilities_reference.pdf → Chapter1 Getting started with Teamcenter utilities

Manage password files

To provide the best password security, you can store an encrypted password in a designated file and directory location on a local disk. You create the file containing the encrypted password using Teamcenter Environment Manager (TEM) or the install utility. An environment variable contains the password string to be encrypted. The variable is designated in TEM or by an install utility argument. The environment variable is not maintained, it is used only during the encryption process to ensure the clear text password is not persisted.

For more information about password encryption, see the install utility.

Note You can update the encrypted Teamcenter user password using TEM or the install utility. However, this does not change the password in the Teamcenter database. This must be done manually.

The encryption process uses an AES 256-bit encryption key.

For information about managing the encryption key, see the System Administration Guide.

The -pf argument provides enhanced password security by allowing you to place an unencrypted password in a text file and secure the file using operating system-level security. This is stronger security than is provided by the -p argument, in which passwords are placed on the utility program command line, allowing a user to run ps -ef to display all running utilities and gain access to the utilities' passwords. The file must contain only the password.

Do not include user names or other text. The password must be one line; new lines and carriage returns are considered a terminator. The password must also be in character encoding consistent with the processes reading it.

You must place the file on a local disk to ensure that access control is managed securely by the operating system representing the file.

• To prepare the password file on UNIX, run chmod 400 file-name.

• To prepare the password file on Windows, right-click the file and choose Properties, and then click the Security tab and ensure that Administrators is the only group with read access on the local machine.

Note File access control becomes complicated when mapping between UNIX and Windows platforms.

• On UNIX, do not place the password file on disks mounted from other machines. You can run df to obtain a list of such disks.

• On Windows, do not place the password file on drives shared with other machines. Using a removal disk (usb) ensures that even local administrators only have access when the disk is physically present.