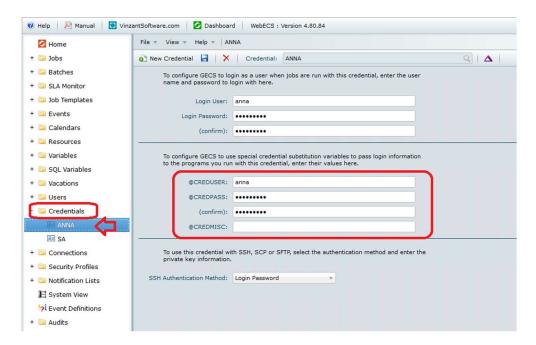# Using Predefined Encrypted Passwords with GECS

GECS can automate your jobs securely by allowing you to define credentials with encrypted passwords. These credentials can be used when GECS launches a job. It is beneficial to have the ability to update credential information in one place without having to change information within your jobs.
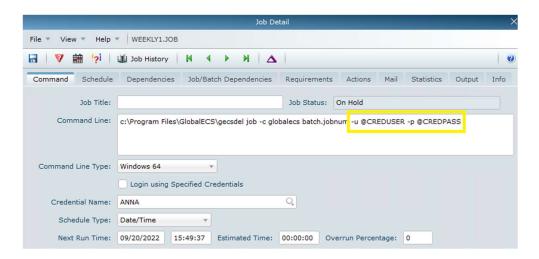
The credential records also include three special substitution variables that can be substituted at the agent just before your job's command line is run. The substituted value isn't shown on the statistics page after the job is run. These variables can all be defined in a credential along with the login username and password. These variables can be used like any substitution variable. With the added bonus that the passwords in the credential are transmitted to the agent encrypted to help keep them secure.

From your GECS Administrator program please configure a GECS Credential using the @CREDUSER, @CREDPASS fields as shown below:

 If you are running this utility from a job your command line should look something like this:

NOTE: The Credential Name must be populated in order to use the @CREDUSER/@CREDPASS.

If you are running a script that is running the utility, you would put @CREDUSER and @CREDPASS on the command line of your job. Then in your script when you use -u and -p you would use %1 and %2 instead of the variables.

If you have any further questions, please contact your Vinzant Software support team.