DCI Security Settings

DCI contains security settings that are unique to each customer's instance of DCI. It is important that customers understand these settings and choose the right configuration for their organization. For more information, or for assistance in changing these settings, reach out to your DCI Contact.

Setting Name	Setting Description	Configuration Options
Unauthorized Access Tolerance	DCI prevents users from accessing pages they do not have rights to access. This setting (in combination with Message Templates) allows you to be notified after a user attempts to access an unauthorized page a specified number of times. To use this setting, a number must be specified for your instance, and you must activate your message template called "Unauthorized Access Tolerance Exceeded."	A number must be specified for your instance. If you do not want to use this setting, do not activate the associated message template.
Automatic Password Expiration	When enabled, this setting requires users to reset their password immediately upon enabling the setting, and then every "X" days as specified in the "Password Expiration Days" setting. This applies to all system users.	This setting is either ON or OFF. When ON, the Password Expiration Days setting must also be used.
Password Expiration Days	When "Automatic Password Expiration" is ON, use this setting to specify how often users must reset their passwords.	Enter as a number of days.
Password History Count	When users are required to reset their passwords, DCI can restrict them to not reuse a previous password up to "X" number of passwords. Use this setting to determine how far back users are restricted from reusing a previous password.	Enter a number that represents the number of previous passwords that cannot be reused.