DCI Security Settings

Description: In this topic, the user will learn about the different 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 assistance with changing organizational security settings, please submit a support ticket.

Setting Name	Setting Description	Configuration Options
Unauthorized Access Tolerance	• Prevents users from accessing pages they do not have rights to access • This setting combined with Message Templates allows system administrators to be notified after a user attempts to access an unauthorized page a configured number of times	To receive notifications, activate the message template called "Unauthorized Access Tolerance Exceeded." Specify the number of attempts for the instance.
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
PIN Expiration Days	When "Automatic Password Expiration" is ON, use this setting to specify how often users must reset their PIN.	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 restrict users from reusing a previous password.	Enter a number that represents the number of previous passwords that cannot be reused

Related articles

- March 2021 Release Notes
- DCI Security Settings
- Employee Profile Overview - Video