Procedure for a Stolen Computer

706 TDO KB February 25, 2026 IT resources, Reporting Tools, Site Configuration 7.72K

Overview

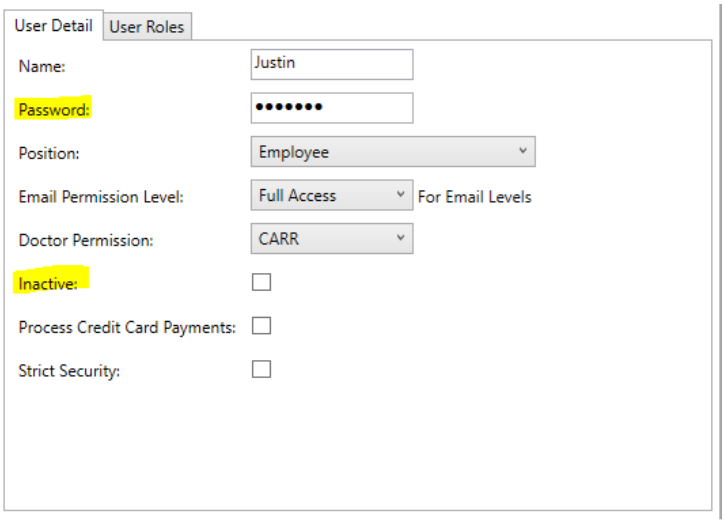
This article will give you steps to ensure that your TDO software does not get compromised in the event that a computer or tablet is stolen.

Detailed Instructions

NOTE: These are steps are primarily related to TDO software. There may be additional steps to take with law enforcement or your IT outside of these steps.

In the event that a computer or tablet is stolen from your office, it is recommended to immediately change all active users' TDO passwords.

- To do this in version 12, go to the **Setup** tab, select **Site Configuration >Add/Edit User Names and Passwords**.
- To do this in version 11, go to **Administrative >Add/Edit User Names and Passwords**.



From this menu, you can select a user and change their password by deleting the password in the **Password** field and typing a new one.

NOTE: This is only necessary for users not marked "Inactive".

While it is unlikely that your TDO database has been accessed, if you would like to find out for sure, you can check the EHR Audit Log by going to **Reporting Tools > Administrative > EHR Audit Log** in version 12, or **Reports > Administrative > EHR Audit Log** in version 11. This report will show you the last time that TDO was accessed. It is also recommended to immediately have your IT change your Windows passwords and Wi-Fi password.