Important Notes About Deleting or Deactivating User Accounts

Last Modified on 12/05/2019 6:04 pm EST

If a user should no longer have access to Incident Management, you have the option of disabling that user's account or deleting it. However, it's recommended that user accounts are disabled rather than deleted. If a user needs access to other Resolver apps, you can remove them from their Incident Management user group to remove their access to Incident Management only.

> ⚠️ Deleting or disabling a user will also remove their access to any additional Resolver apps.

Deleting a user account prevents the user from logging into your organization and accessing any data and apps, but it also removes that user from any objects they were assigned to via a user group, which may affect your reporting. Disabling an account also prevents the user from logging in and accessing data and apps, but the user is not removed from any assigned objects, thus maintaining your records.

Also note that deleting an account does **not** remove the user from your Core database. If you require that one or more users are removed from the database, contact Resolver Support for assistance.