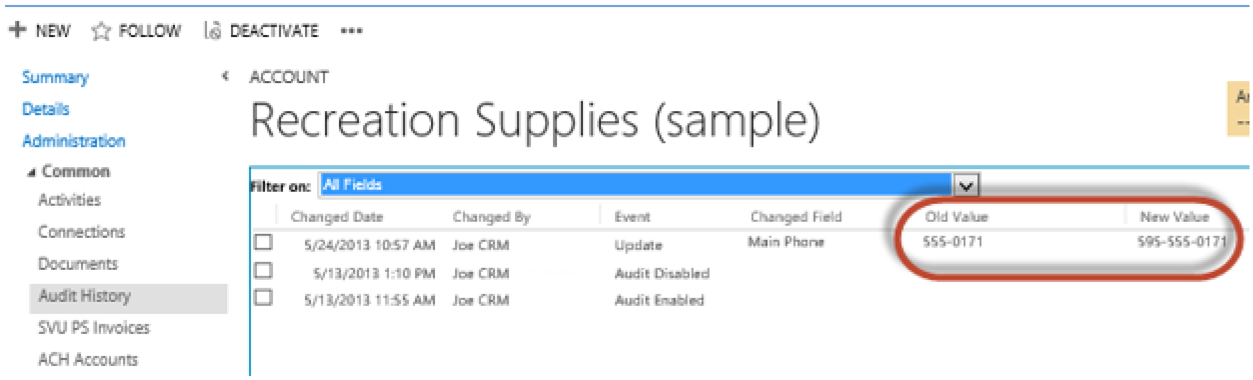
Auditing

Microsoft Dynamics CRM comes with several tools to help you manage data. One of these is the auditing feature, which allows you to track changes made to data in Dynamics CRM. It also tracks each time a user logs into your CRM system. If auditing is enabled, CRM automatically creates logs for the changes that are tracked. By default, auditing is not turned on.



Benefits

The Microsoft Dynamics CRM auditing feature has many benefits. It allows you to:

1. Analyze the history of a particular record
2. View a summary of everything that changed
3. Track when a user accessed CRM
4. Comply with regulation standards
5. Analyze user actions in order to improve business processes

Considerations when starting auditing

Start auditing at the organization level to allow auditing for entities and fields. When you start auditing for the first time, auditing is started by default on the following entities: Account, Contact, Goal, Goal Metric, Lead, Marketing List, Product, Quick Campaign, Rollup Query, and Sales Literature.

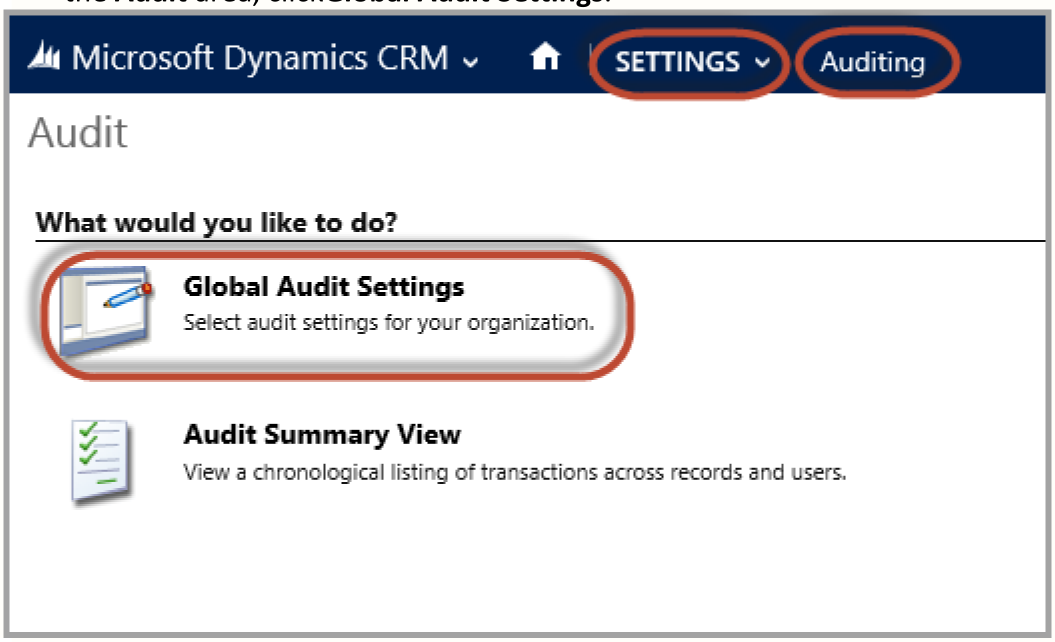
You may want to stop auditing for maintenance purposes or when the database space is limited. Stopping auditing at the organization level stops the tracking of changes for the entities or fields for the period for which auditing is stopped at the organization level. When you start organization-level auditing again, the same entities and fields are selected for auditing that were selected when you stopped auditing for the organization.

Learn more about working with Auditing in Microsoft Dynamics CRM:

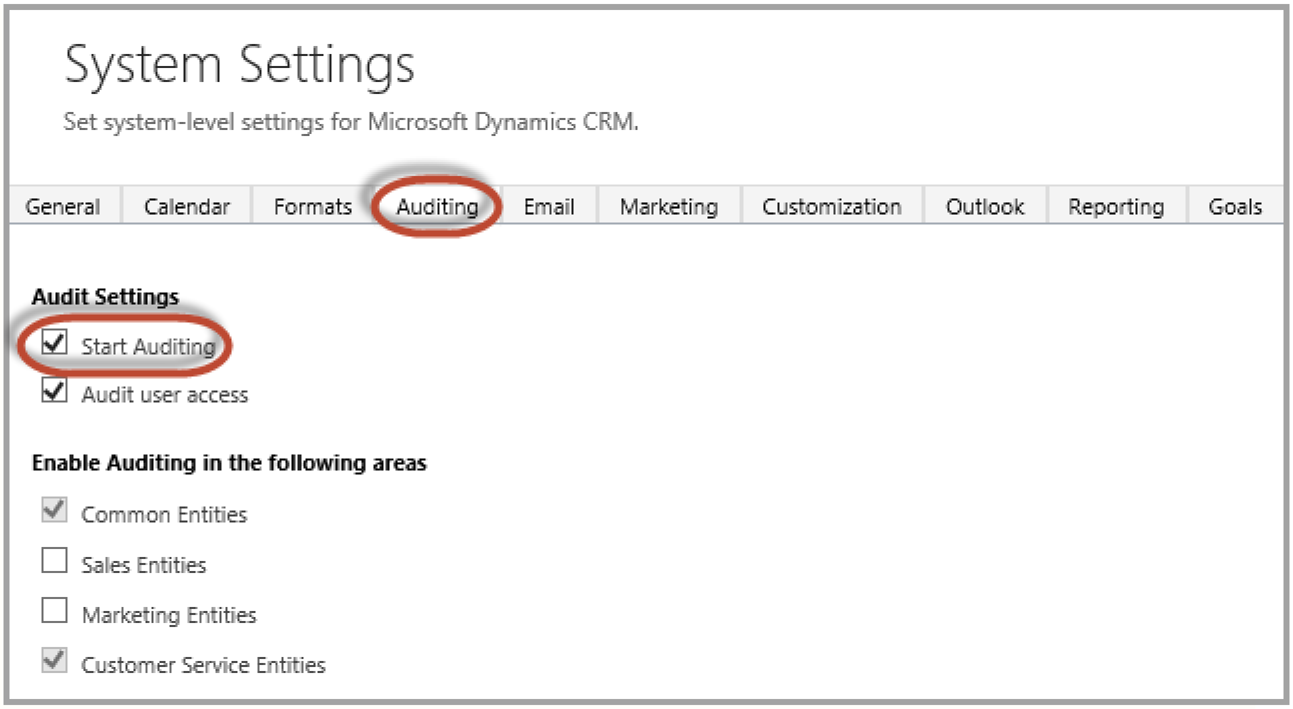
- How to Enable or Disable Auditing
- Enabling or Disabling Auditing on Specific Business Areas
- Auditing User Login Details
- Enabling or Disabling Auditing for Entities
- Enabling or Disabling Auditing for Fields
- Auditing Security Roles

How to Enable or Disable Auditing in Microsoft Dynamics CRM

1. In the **Navigation Pane**, click **Settings**. Then under **System**, click **Auditing**. In the **Audit** area, click**Global Audit Settings**.



1. To start audit tracking, in the **System Settings** dialog box, click the **Auditing** tab. Then select the**Start Auditing** check box.

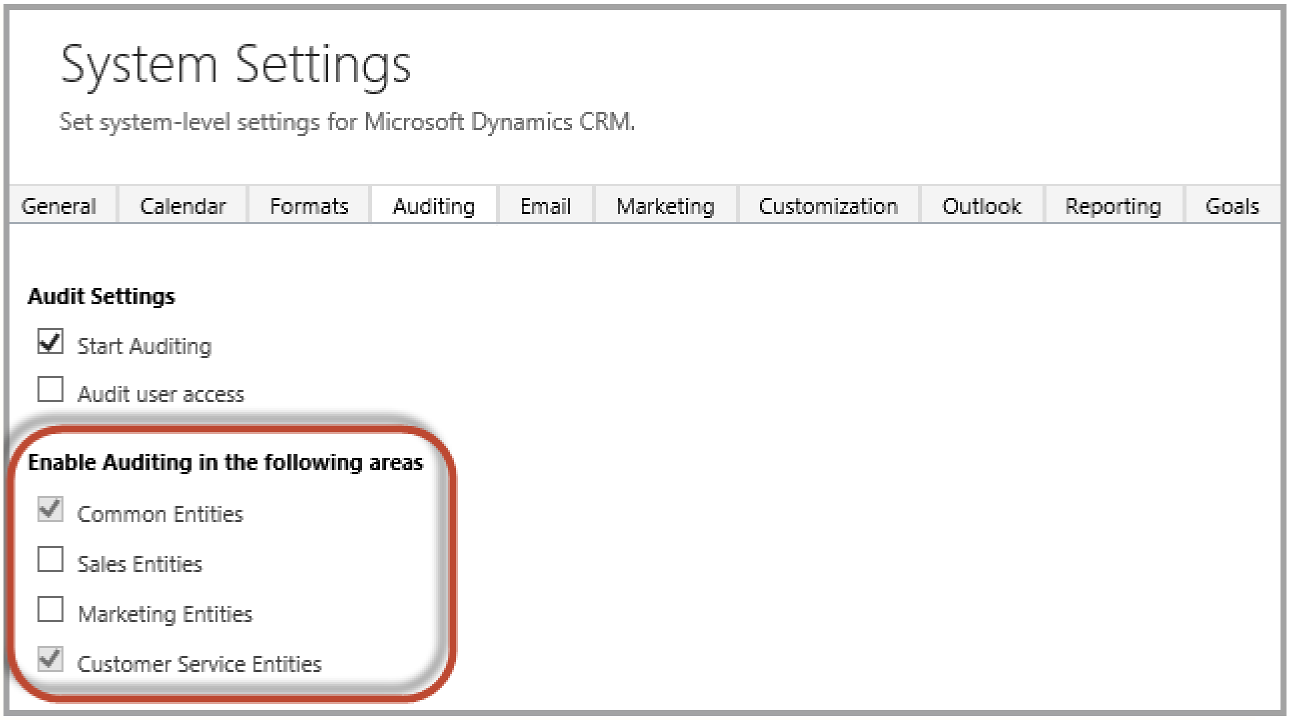


To simply stop auditing tracking altogether, navigate to the same area in the **How to Start Auditing** section above, except this time clear the **Start Auditing** check box.

Enabling or Disabling Auditing on Specific Business Areas

To start or stop auditing on specific business areas, navigate to the same place as you would if you were turning on auditing, and select or clear the following check boxes:

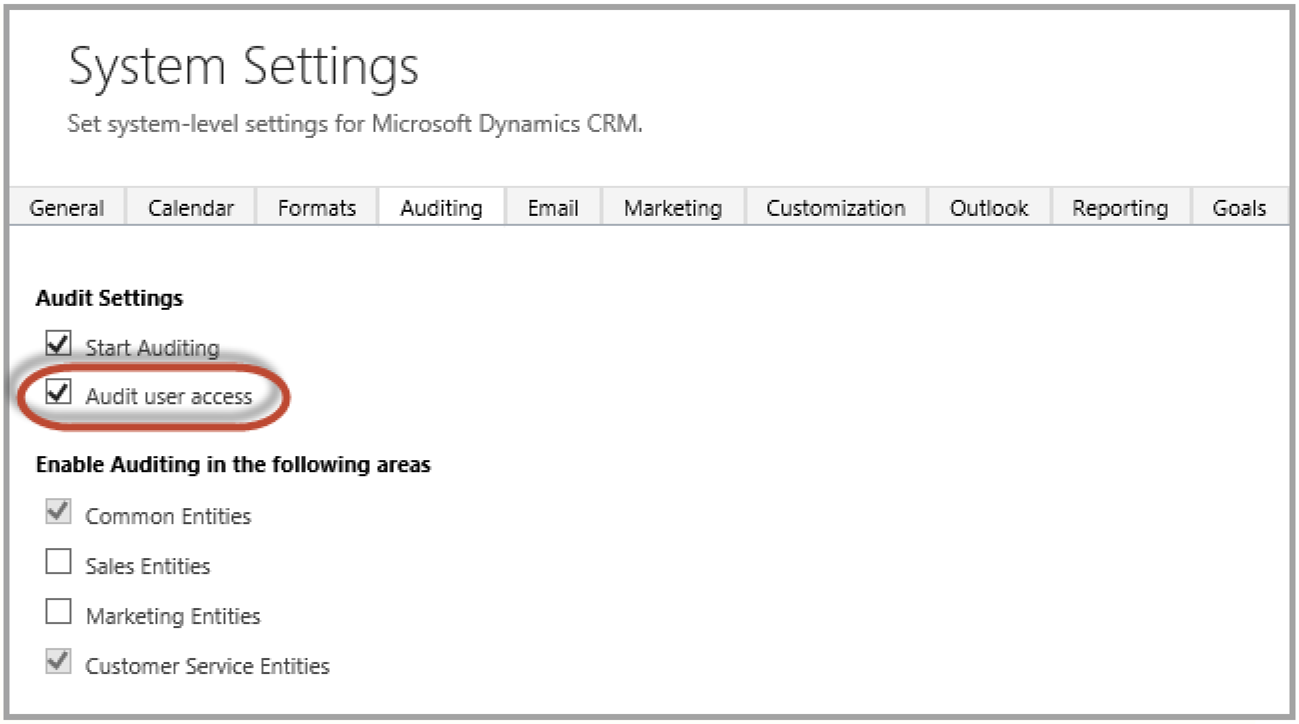
- **Common Entities.** This check box is selected by default when you start auditing for the first time.
- **Sales Entities.** When you select or clear this check box, auditing is started or stopped for the following entities: Competitor, Opportunity, Invoice, Order, and Quote.
- **Marketing Entities.** When you select or clear this check box, auditing is started or stopped for the Campaign entity.
- **Customer Service Entities.** When you select or clear this check box, auditing is started or stopped for the following entities: Case, Contract, and Service.



Auditing User Login Details

This task can only be performed by those with System Administrator or System Customizer security roles, and is used to track when a user logs on to Microsoft Dynamics CRM Online. The audit log of user access is available in the **Audit Summary View** page. To start auditing for login details:

1. In the **Navigation Pane**, click **Settings**. Then under **System**, click **Auditing**.
2. In the **Audit** area, click **Global Audit Settings**.
3. To start tracking user access details, in the **System Settings** dialog box, click the **Auditing** tab. Then select the **Audit User Access** check box. (This check box will be greyed out if you do not have the security role to edit it.)



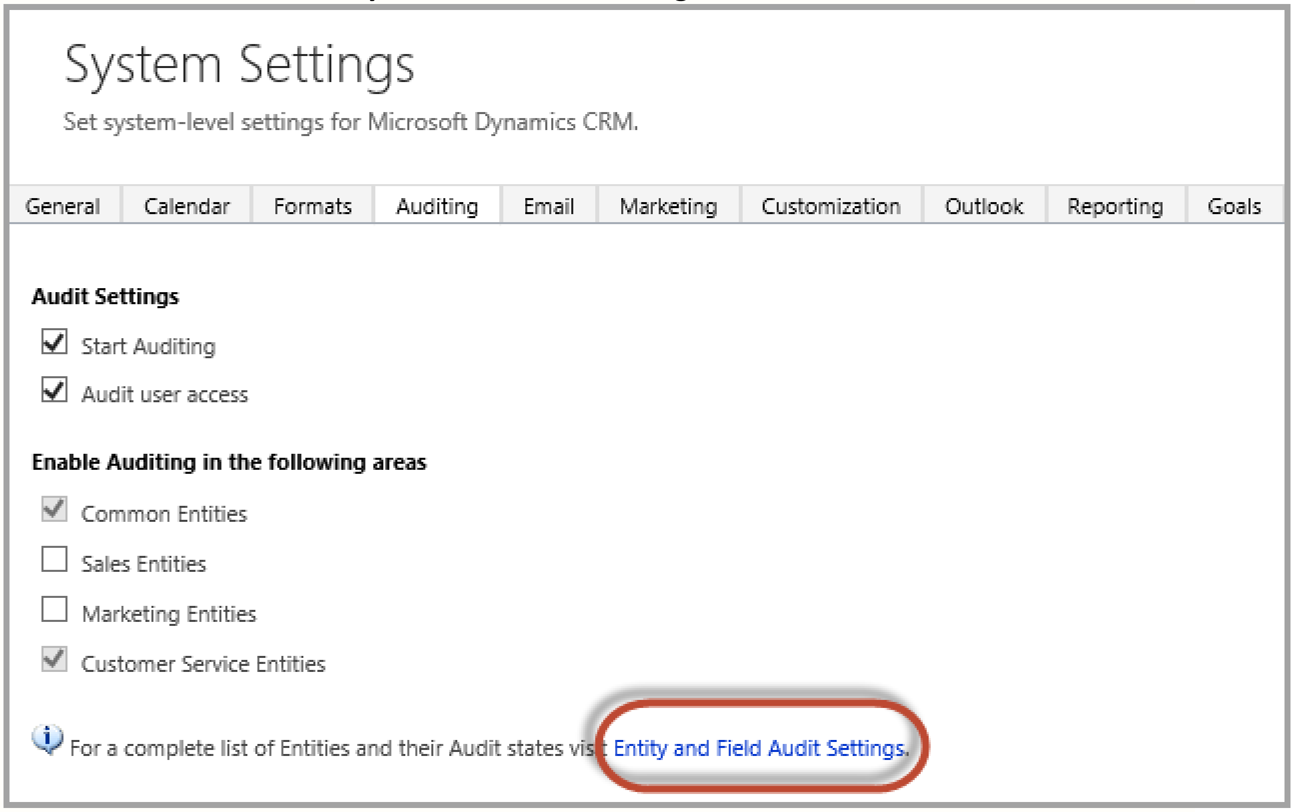
To stop tracking user login details, clear the **Audit User Access** check box.

Enabling or Disabling Auditing for Entities

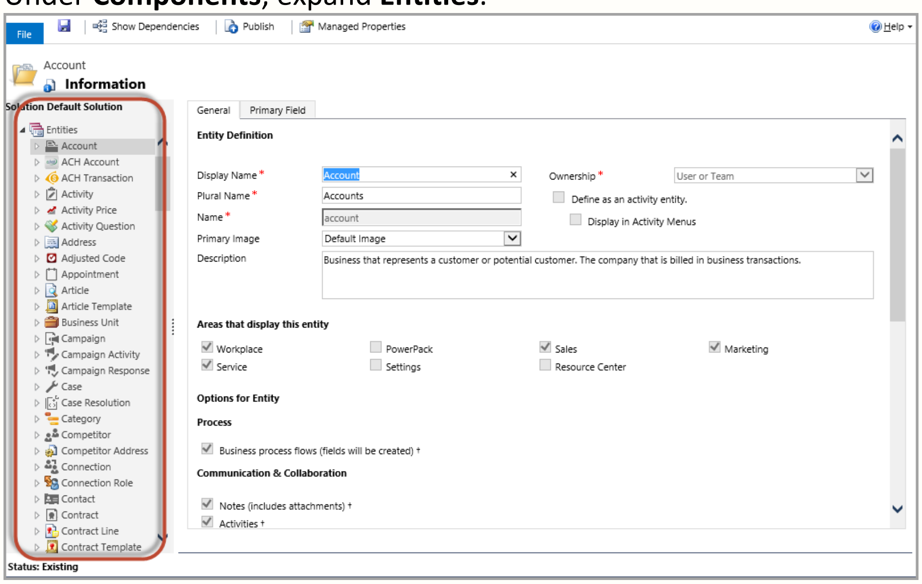
This task also requires the System Administrator or System Customizer security role. Auditing for entities won't work if you don't have organization-level auditing turn on, so make sure that's turned on first.

1. In the **Navigation Pane**, click **Settings**. Then under **System**, click **Auditing**.

2. In the **Audit** area, click **Entity** and **Field Audit Settings**.



3. Under **Components**, expand **Entities**.



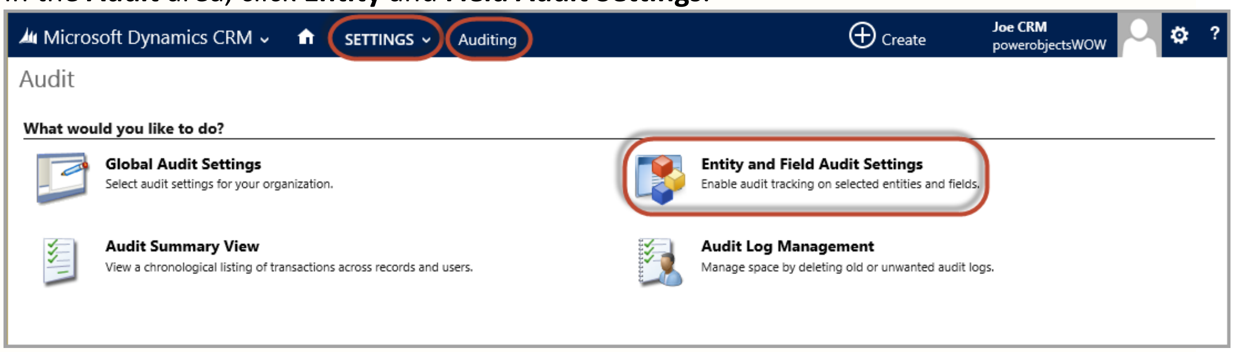
4. Click the entity for which you want to start or stop auditing. To start auditing, on the **General** tab, in the **Options for Entity** section, select the **Auditing** check box. To stop auditing, clear the check box.

By default, when you start or stop auditing for an entity, you also start or stop auditing for all the fields of this entity.

Enabling or Disabling Auditing for Fields

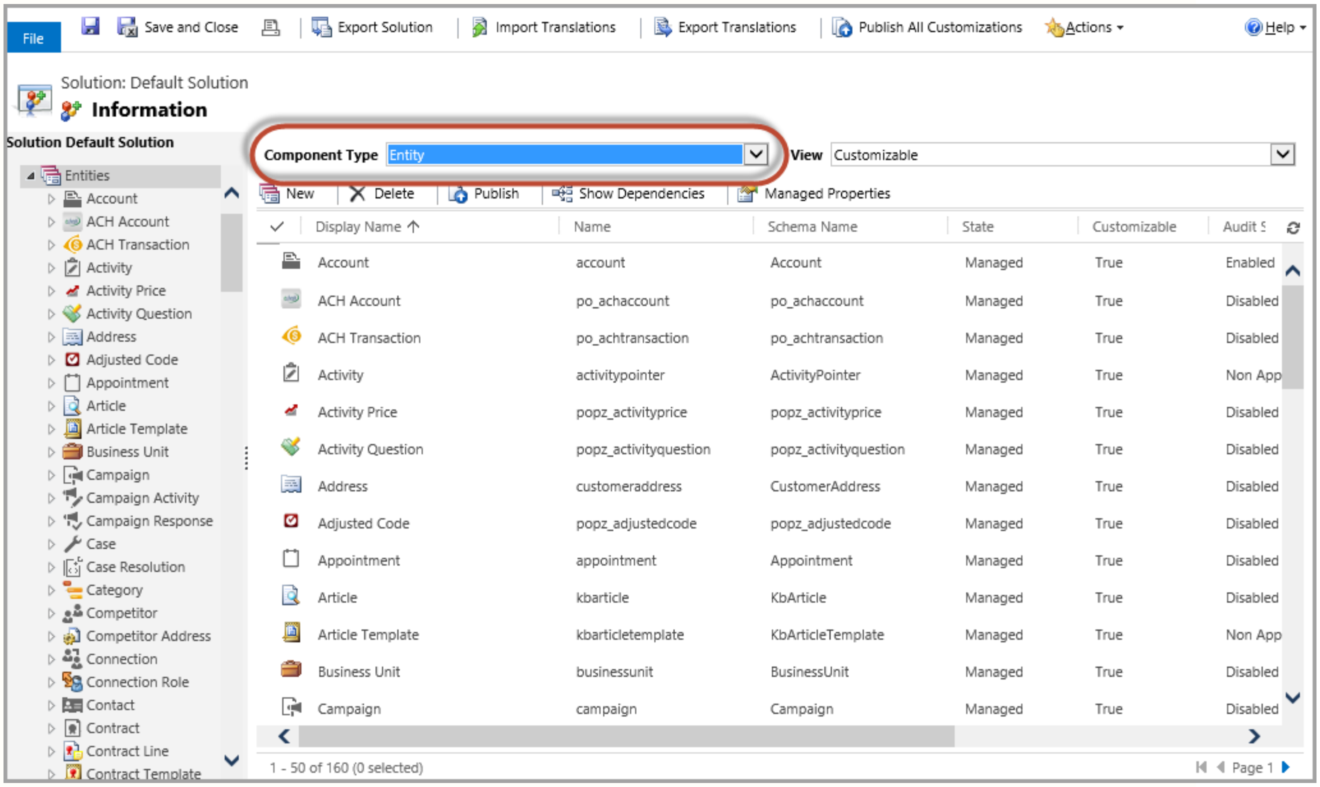
Again, you must have System Administrator or System Customizer rights to complete this task. By default, when you enable auditing for an entity, auditing is also enabled on all of an entity's fields. You can select or clear fields for which you want to enable auditing. To do so:

1. In the **Navigation Pane**, click **Settings**.
2. Under **System**, click Auditing.
3. In the **Audit** area, click **Entity** and **Field Audit Settings**.

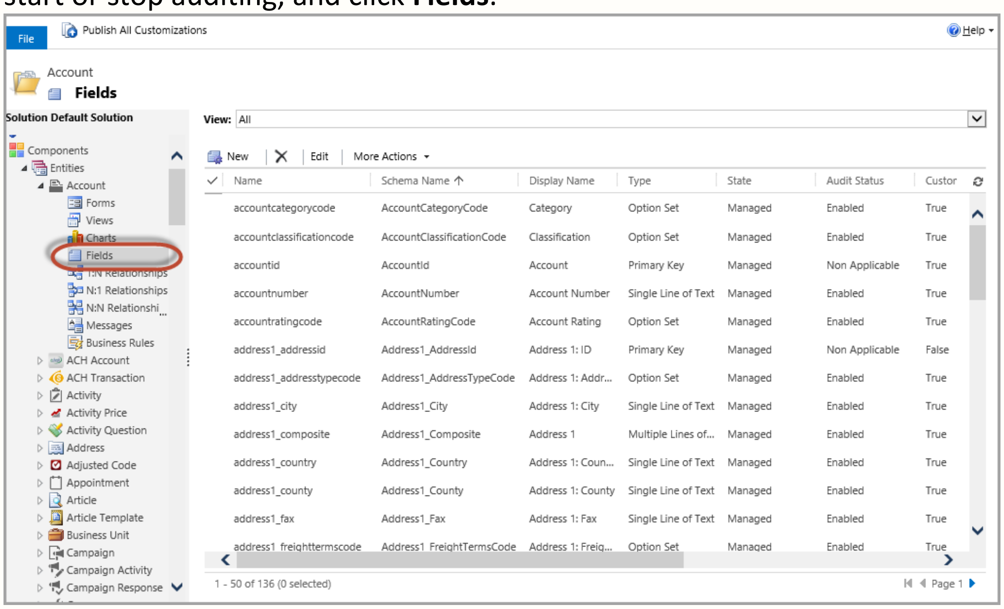


4. Under the **Components** drop-down menu, select **Entities**

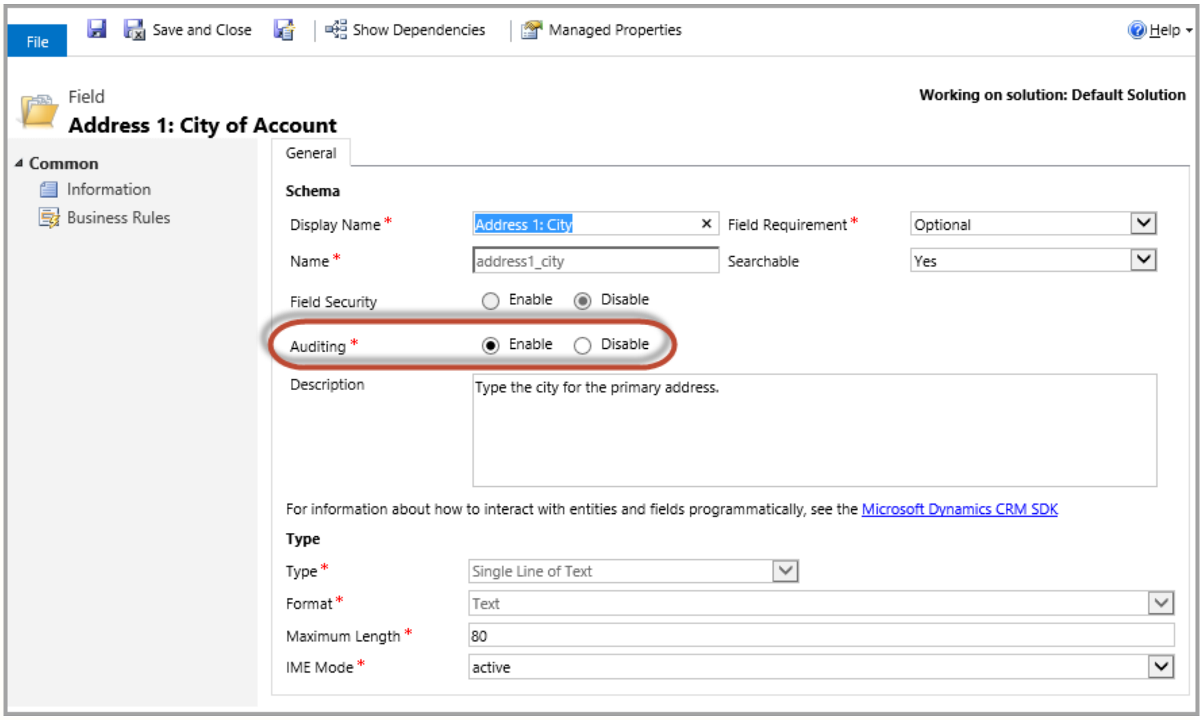
.



5. In the left-hand navigation, expand the entity that has the fields for which you want to start or stop auditing, and click **Fields**.



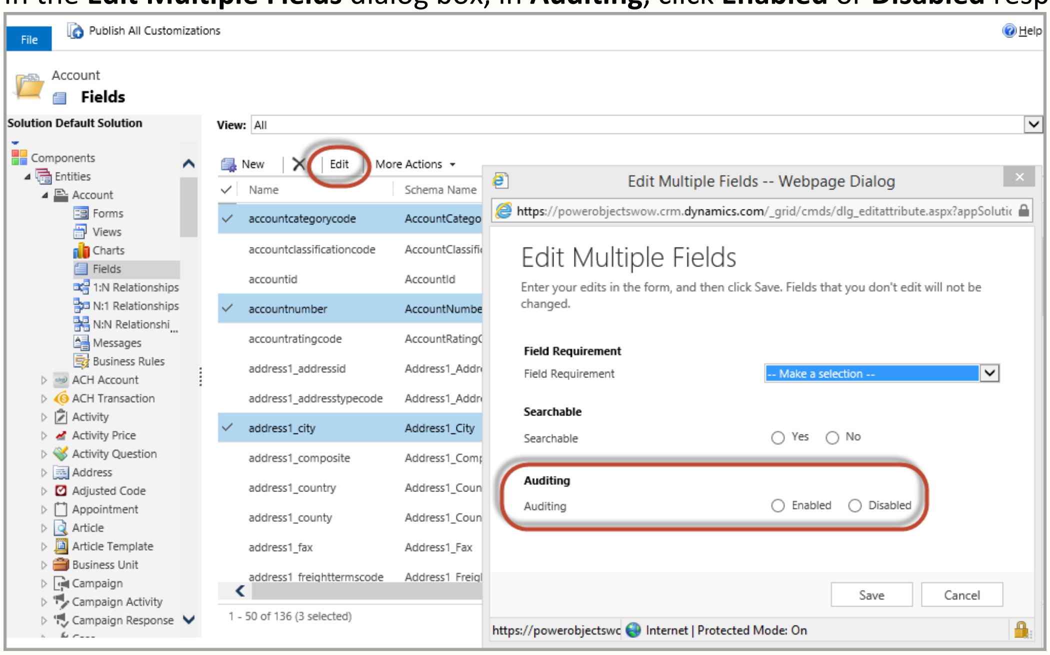
6. In the field list, to start or stop auditing for a single field, open that field and in the **Auditing** field click **Enabled** or **Disabled**.



7. Click **Save** and **Publish All Customizations**.

You can also start or stop auditing for more than one field at a time.

1. On the **Actions** toolbar, click **Edit**.
2. In the **Edit Multiple Fields** dialog box, in **Auditing**, click **Enabled** or **Disabled** respectively.



3. Click **Save** and **Publish All Customizations**.

Auditing security roles

Whether or not a user can access an audit history is based on security roles. These security roles include:

- View Audit History
- View Audit Summary
- View Audit Partitions
- Delete Audit Partitions