c360 Field Level Security User Guide

Microsoft Dynamics CRM 3.0 compatible

c360 Solutions, Inc.
www.c360.com

Table of Contents

Table of Contents 2
c360 Field Level Security 3
Overview 3
Accessing Field Level Security 4

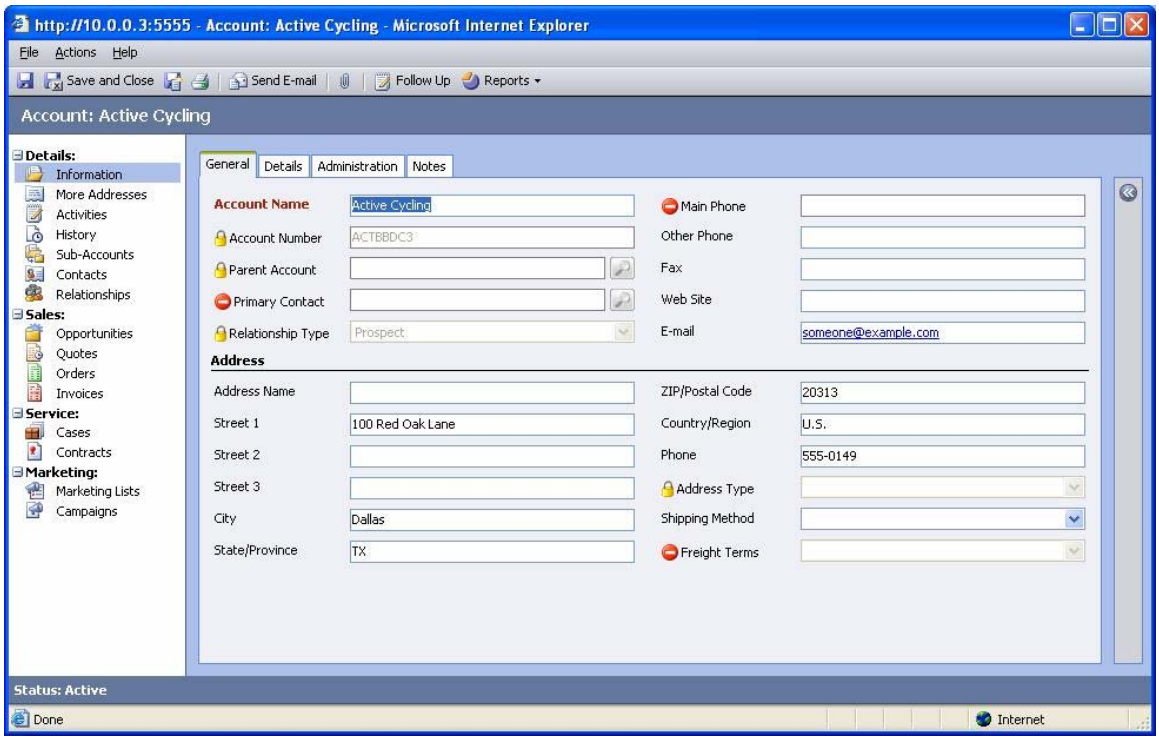
c360 Field Level Security _____

Overview

c360 Field Level Security enhances the security capability of Microsoft CRM 3.0 by restricting access to CRM data on a field level basis. By using Field-Level Security, administrators will be able to restrict access to specific fields in CRM entities. The fields can be **disabled** (read-only), **forbidden** (deny access) or **hidden** (remove field from view) for any CRM **security role** in a **business unit** (or team), thus allowing dynamic field privilege access while maintaining the CRM security model.

Field-Level Security supports **all CRM field types** such as lookup, string, float, nvarchar, currency, datetime, memo fields while ensuring that fields are secured from all a**reas**
of CRM including entity forms, CRM Views, Advanced Find views, lookup views, Bulk Edit, Excel Export, Print pages, Form Assistant, Merge Forms.

By using c360 Field Level Security, you can define security privileges for any field in a CRM entity (including **custom entities**) and be sure that access is only available to the users who are allowed to see it.



Accessing Field Level Security

Field Level Security supports the configuration of individual fields for each of the Microsoft CRM entities. To create field privileges you must have access to the customization area. Follow the next guidelines to configure field's privileges:

1. Go to the "Settings" section of the MS-CRM application.
2. Select Customization and choose to Customize Entities.
3. Select one of the entities for customization (for the evaluation version, choose "Contacts").
4. Click to customize form and views and open the Form.
5. Double click on one of the fields to configure field's properties.
6. Click on the Privileges Tab. (See Figure 2)

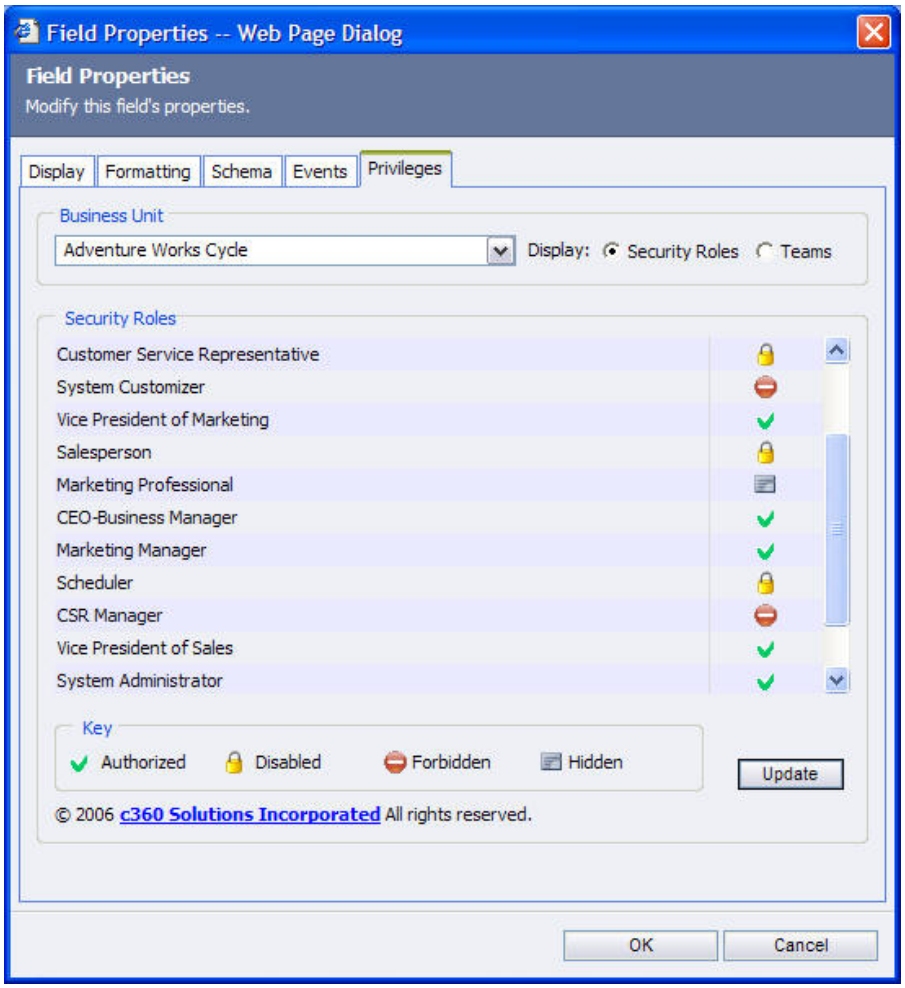
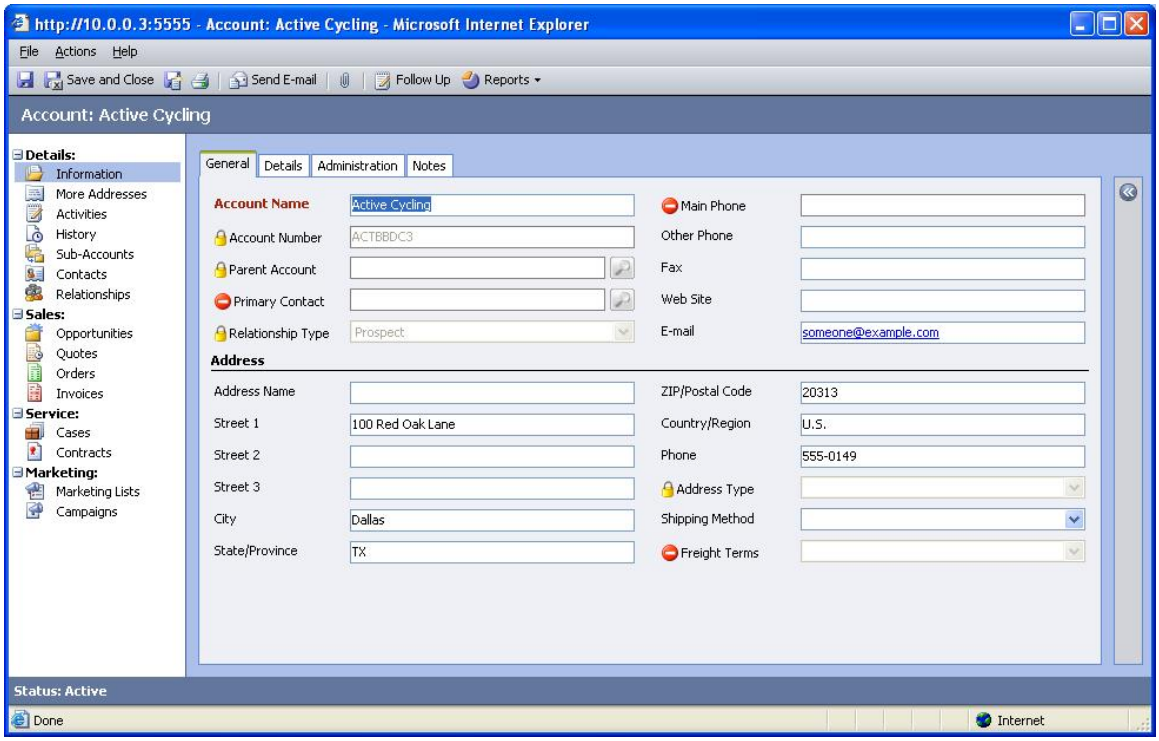


Figure 2: Field Level Security Configuration screen

7. Choose a Business Unit. A list with all the security roles for the specified Business Unit will appear. (In case you selected to display Teams a list of teams for the specified Business Unit will appear)
8. Click on the "Privilege" icon to change the access privileges.
9. Click on the Update button to save your work.
10. Close the Properties window.



The field-level security/privilege is defined for Security Role/Team for the specified Business Unit. The security model stays intact while allowing highly dynamic and customizable capabilities in the field's level of configuration.

Fields defined as "Forbidden/Hidden" and appear in one of the views will be blocked if the user has no access to it (This rule applies also for the Advanced Find Views).

Note:
There is no need to "Publish" or perform any other action. The changes are reflected immediately!

No JavaScript is used! The form will not contain Forbidden data at client side!