Microsoft

Working With

MICROSOFT DYNAMICS™ CRM 3.0

Mike Snyder
Jim Steger

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number 2005939238

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWT 1 0 9 8 7 6

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to *mspinput@microsoft.com*.

Acquisitions Editor: Ben Ryan
Project Editor: Valerie Woolley
Technical Editor: Joe LeBaron
Copy Editor: Crystal Thomas
Production: Elizabeth Hansford
Indexer: Ginny Munroe

Body Part No. X11-89442

Table of Contents

Chapter 3

Managing Security and Information Access

In this chapter:

If you've deployed software systems in the past, you already know that you must design your CRM solution to appropriately restrict information based on individual user permissions. Controlling how your users access customer data is a mission-critical component of any business application. Microsoft designed the Microsoft CRM security model to support the following goals:

- Provide users with only the information they need to perform their jobs; do not show them data unrelated to their positions.
- Simplify security administration by creating security roles that define security privileges, and then assign users to one or more security roles.
- Support team-based and collaborative projects by enabling users to share records as necessary.

Microsoft CRM provides an extremely granular level of security throughout the application. By customizing the security settings, you can construct a security and information access solution that will most likely meet the needs of your organization. The process to customize the Microsoft CRM security settings requires you to configure your organization structure, decide which security roles your system users (employees) will have, and then define the security privileges associated with each security role.

Although you might not expect to, you will find yourself constantly tweaking and revising the security settings as your business evolves. Fortunately, the Microsoft CRM security model makes it easy for you to update and change your security settings on the fly.

More Info Although the security settings user interface appears similar to Microsoft CRM 1.2, Microsoft completely revamped the technical security structure in the Microsoft CRM 3.0 database to eliminate the use of security descriptors. Because of this, you can change and modify your security settings without the performance issues that some Microsoft CRM 1.2 users experienced if their system contained a large number of records.

In this chapter, we'll review the following security topics:

- Mapping your needs
- Security concepts
- Users and licenses
- Security roles and business units
- Sharing records

Mapping Your Needs

For the first step in planning security settings for your deployment, we recommend that you create a rough model of your company's current operational structure (by using a tool such as Microsoft Office Visio). For each section of your organization layout, you should identify the approximate number of users and the types of business functions those users perform. You will need this rough organization map to plan how you want to set up and configure security in your Microsoft CRM deployment.

To put this type of organization mapping into a real-world context, let's consider an example organization. Figure 3-1 shows the business structure for the Microsoft CRM sample company, Adventure Works Cycle.

Each box in the figure represents a business unit in Microsoft CRM, and you can structure parent and child relationships between business units. *Business units* represent a logical grouping of business activities, and you have great latitude in determining how to create and structure them for your implementation.

Tip Sometimes people refer to business units with the abbreviation BU.

One constraint of configuring business units is that you can specify only one parent for each business unit. However, each business unit can have multiple child business units. Also, you must assign every Microsoft CRM user to one (and only one) business unit.

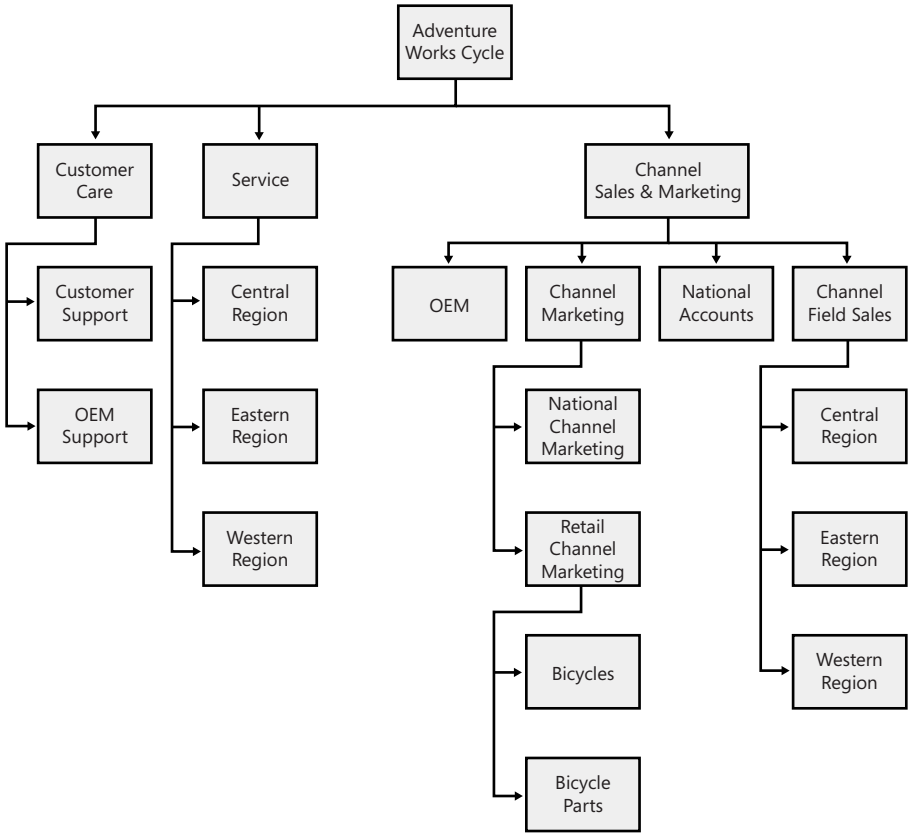


Figure 3-1 Organization structure for the sample company, Adventure Works Cycle

For each user in your organization structure, you should try to determine answers for questions such as the following:

- To which areas of Microsoft CRM will the users need access (such as Sales, Marketing, and Customer Service)?
- Do users need the ability to create and update records, or will read-only access suffice?
- Will you need to structure project teams or functional groups of users that work together on related records?
- Can you group users together by job function or some other classification (such as finance, operations, and executive managers)?

After you develop a feel for how your organization and users will use Microsoft CRM, you can start to configure the Microsoft CRM application to meet those needs.

Real World For smaller organizations, mapping out your Microsoft CRM organization model might take only 15 minutes. However, you might want to budget several days to map out the security model for enterprise organizations with hundreds of users spread geographically throughout the country. You should also not expect to get the security model *done*, because it will constantly change over time.

Don't spend too much time trying to perfect your organizational model right now. The goal of the exercise is to research and develop more details about how your organization intends to use Microsoft CRM so you can configure the security settings correctly. This organizational model won't be your final version, but it can help you think through and consider the ramifications of the security settings you choose.

Security Concepts

After you've developed a rough organization model with information about the different types of users in your system, you must translate that information into Microsoft CRM security settings. Before we explain how to configure the security settings in the software, let's explain two of the key topics related to Microsoft CRM security:

- Security model concepts
- Integrated Windows authentication

Once you understand these concepts, we'll get into the details of configuring the software to meet your specific needs. Because of the many security customization options offered in Microsoft CRM, very rarely do we see an organization structure that Microsoft CRM's security settings can't accommodate.

Security Model Concepts

The Microsoft CRM security model uses two main concepts:

- Role and object-based security
- Organization structure

Role-Based and Object-Based Security

Microsoft CRM uses security roles and role-based security as its core security management techniques. A *security role* describes a set of access levels and privileges for each of the entities (such as Leads, Accounts, or Cases) in Microsoft CRM. All Microsoft CRM users must have one or more security roles assigned to them. Therefore, when a user logs on to the system, Microsoft CRM looks at the user's assigned security roles and uses that information to determine what the software will allow that user to do and see throughout the system. This is known as *role-based security*.

The security model also allows you to define different security parameters for the various records (such as Lead, Account, Contact, and so on) because each record has an owner. By comparing the business unit of the record owner with the security role and business unit of a user, Microsoft CRM determines that user's security privileges for a single record. You can think of configuring access rights on the individual record level (not the entity level) as *object-based security*. Figure 3-2 illustrates this concept.

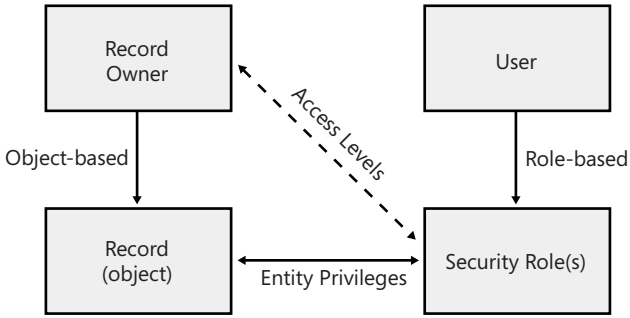


Figure 3-2 Role-based security and object-based security combine to determine user privileges

In summary, Microsoft CRM uses a combination of role-based and object-based security to manage access rights and privileges throughout the system.

Organization Structure

In addition to security roles, Microsoft CRM uses an organization's structure as a key concept in its security model. Microsoft CRM uses the following definitions to describe an organization's structure:

- **Deployment** A single installation of Microsoft CRM.
- **Organization** The company that owns the deployment. The organization is the top level of the Microsoft CRM business management hierarchy. Microsoft CRM automatically creates the organization based on the name that you enter during the software installation. You cannot change or delete this information. You can also refer to the organization as the *root business unit*.
- **Business unit** A logical grouping of your business operations. Each business unit can act as parent for one or more child business units. In the sample organization in Figure 3-1, you would describe the Customer Care business unit as the parent business unit of the Customer Support and OEM Support business units. Likewise, you would refer to the Customer Support and OEM Support business units as child business units.
- **User** Someone who typically works for the organization and has access to Microsoft CRM. Each user belongs to one (and only one) business unit, and each user is assigned one or more security roles.

Later in this chapter, we'll explain how these terms relate to setting up and configuring security roles.

Integrated Windows Authentication

Microsoft CRM uses Integrated Windows authentication (formerly called NTLM, and also referred to as Microsoft Windows NT Challenge/Response authentication) for user security authentication in the Web browser and Microsoft Office Outlook interfaces. By using Integrated Windows authentication, users can simply browse to the Microsoft CRM Web site and Internet Explorer automatically passes their encrypted user credentials to Microsoft CRM and logs them on. This means that users log on to Microsoft CRM (authenticate) by using their existing Microsoft Active Directory directory domain accounts, without having to explicitly sign in to the Microsoft CRM application. This integrated security provides great convenience for users, because there's no need for them to remember an additional password just for the CRM system. Using Integrated Windows authentication also helps system administrators, because they can continue to manage user accounts from Active Directory services. For example, disabling a user in Active Directory prevents him or her from logging on to Microsoft CRM, because the user's logon and password will not work anymore.

More Info Disabling or deleting users in Active Directory prevents them from logging on to Microsoft CRM, but it does not automatically disable their user records in Microsoft CRM. Because all active users count against your licenses, make sure that you remember to disable their user records in Microsoft CRM to free up their licenses. Also, if you change a user's name in Active Directory, you must manually update it in Microsoft CRM.

Most companies install Microsoft CRM on their local intranet in the same Active Directory domain to which users log on. By default, the User Authentication security settings in Microsoft Internet Explorer 6.0 automatically log users on to any intranet site to which they browse, including Microsoft CRM. This default setting will work fine for almost all of your users.

However, you might find that you want to alter the default security settings to change how the Internet Explorer browser handles user authentication. Typical reasons to modify the Internet Explorer security settings include:

- You want to log on to Microsoft CRM impersonating one of your users during setup and development.
- Your Microsoft CRM deployment resides in a different Active Directory domain (or on the Internet) and you want to change the log on settings.
- You want to explicitly trust the Microsoft CRM Web site to allow for pop-up windows.

To view your Internet Explorer 6 security settings, click Internet Options on the Tools menu in Internet Explorer. The Security tab in the Internet Options dialog box displays Web content zones, including Internet, Local Intranet, Trusted Sites, and Restricted Sites, as shown in Figure 3-3.

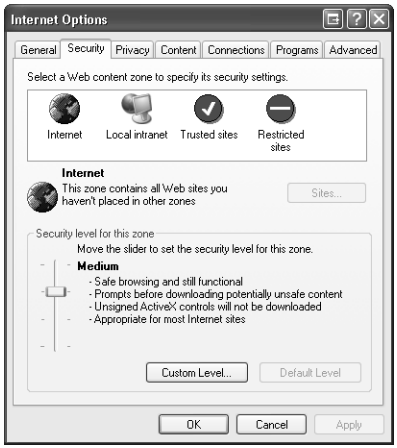


Figure 3-3 Web content zones in Internet Explorer

By altering the security settings, you can change how Internet Explorer passes your logon information to various Web sites, such as your Microsoft CRM Web site.

Turning off automatic logon in the Local intranet zone

1. On the **Security** tab, click **Local intranet**, and then click **Custom Level**.
2. In the **Security Settings** dialog box, scroll down until you see the **User Authentication** section, and then select **Prompt for user name and password**.

When you disable automatic logon, Internet Explorer does not automatically pass your user credentials to Microsoft CRM (or any other Web site on your local intranet). Instead, it prompts you to enter your user name and password when you browse to the Microsoft CRM server. This prompt gives you the opportunity to enter any user credentials that you want, including user credentials from a different domain. As an administrator, you might want to log on as a different user during your setup and configuration phase to confirm that your security settings are correct.

Warning The Microsoft CRM client for Outlook requires automatic logon, so you should not set this value to **Prompt for user name and password** if you need to use the Microsoft CRM client for Outlook.

In addition to disabling automatic logon, you might want to add Microsoft CRM as a trusted site in Internet Explorer or list it as part of your Intranet zone. The steps and benefits of either are almost identical, but we'll review adding Microsoft CRM as a trusted site.

Adding a trusted site to Internet Explorer

1. On the **Security** tab, click **Trusted sites**, and then click **Sites**.
2. In the **Trusted sites** dialog box, enter the address of your Microsoft CRM server (include the http:// portion of the address), and then click **Add**. You might need to clear the **Require server verification** check box if your Microsoft CRM deployment does not use https://.
3. Click **OK**.

Adding a trusted site to Internet Explorer will accomplish two things in regard to Microsoft CRM:

- Internet Explorer will automatically pass your user credentials to the Web site and attempt to log you on. You might want to set this up for your Microsoft CRM users who are not located on your local intranet (such as offsite or remote users) so that they do not have to enter a user name and password each time they browse to Microsoft CRM.
- The Internet Explorer Pop-up Blocker allows pop-up windows for any Web site listed in your Trusted Sites zone.

Caution Intranet sites and trusted sites in Internet Explorer 6 become quite powerful, so you must use caution when deciding which sites you will trust. For example, the default security settings for trusted sites in Internet Explorer 6 automatically install signed Microsoft ActiveX controls on your machine.

Microsoft CRM and Pop-up Blockers

Many users install a pop-up blocker add-in for Internet Explorer in an attempt to limit the number of pop-up advertisements they see when browsing the Internet. Unfortunately, some of these pop-up blockers might also block some of the Web browser windows that Microsoft CRM uses. Consequently, you'll probably need to let your users know how to configure their pop-up blockers to allow pop-up windows from the Microsoft CRM application.

The most common problem caused by pop-up blockers manifests itself when users initially log on to Microsoft CRM. If your users say something like, "the window just disappeared," you can pretty safely assume that pop-up blocker software caused the problem. When users log on to Microsoft CRM, a new browser window pops up, and the original browser window closes. However, if the user's pop-up blocker stops the new window from appearing, it appears to the user that the original window simply disappeared, because Microsoft CRM closed their original browser window.

Internet Explorer 6.0 on Microsoft Windows XP SP2 includes a pop-up blocker, but the default setting allows sites in the Intranet and Trusted Sites zones to launch pop-up windows. If Internet Explorer doesn't recognize Microsoft CRM as an intranet site, or if you

don't want to add it as a trusted site, you can configure the pop-up blocker to allow pop-up windows form the Microsoft CRM Web site (on the Tools menu, point to Pop-Up Blocker, and then click Pop-up Blocker Settings to enter the Microsoft CRM address).

Some pop-up blockers do not allow you to manually enter a trusted address like the Internet Explorer pop-up blocker. Therefore, you have to browse to the Web site you want to allow and then click some sort of "Allow Pop-ups" button. However, because the Microsoft CRM window disappears on initial log on, you might wonder how you could ever open the Web site to allow pop-ups. A simple trick is to browse to *http://*<crmserver>*/loader.aspx,* and then Microsoft CRM will launch in the same Internet Explorer window instead of popping up a new one. From this page, you can click the Allow Pop-ups button to always allow pop-ups for your Microsoft CRM Web site. Here's another trick related to pop-up windows: you can reference the same Microsoft CRM Web site by using several different URLs. For example, you could access Microsoft CRM by using any of the following:

- NetBIOS name (Example - http://crm)
- IP address (Example - http://127.0.0.1)
- Fully qualified domain name (Example - http://crm.domain.local)
- A new entry in your Hosts file (add by editing C:\WINDOWS\system32\drivers\etc\hosts)

Although all of these URLs take you to the same Microsoft CRM server, Internet Explorer 6 treats each of these as different Web sites. Therefore, you could configure different security settings in Internet Explorer for each of these URLs. For example, you might browse to the NetBIOS name by using Integrated Windows authentication to log on as yourself, but configure Internet Explorer to prompt for a log on when you browse to the IP address to impersonate a user.

Users and Licenses

A user is someone with access to Microsoft CRM and typically works for your organization. Before you can add and configure users, you must add user accounts to Active Directory. To manage users in Microsoft CRM, browse to Business Unit Settings in the Settings area, and click Users. For each user, you must complete the following security-related tasks:

- Assign one or more security roles to the user.
- Assign the user to one business unit.
- Assign the user to one or more teams.

The combination of these three settings determines a user's access to information in Microsoft CRM.

Note Although most of your users will be employees of your organization, you can create user accounts for trusted third-party vendors or suppliers if you want to grant them access to your system. Obviously, you should carefully structure the business units and security roles to make sure that third-party users don't see information that you don't want them to view.

Every user that you add to Microsoft CRM automatically counts against the number of Microsoft CRM licenses that you purchased, with one exception. If you select the Restricted Access Mode check box on a user record, that user can perform administrative functions within Microsoft CRM such as changing settings and customizations, but the user will not count as an active licensee because he or she cannot access any of the sales, service, or marketing functions.

When a user stops working with your Microsoft CRM deployment, you should disable the user's record by clicking Actions, and then clicking Disable on the user record menu bar. To maintain data integrity, Microsoft CRM does not allow you to delete users. Disabling a user will not change his or her record ownership because disabled users can still own records.

Tip If you change a user's business unit, Microsoft CRM removes all of that user's security roles because roles vary by business unit. In such a situation, remember to grant the user security roles again; otherwise, he or she won't be able to log on to Microsoft CRM.

If you want to view a summary of your current active licenses, launch the Microsoft CRM Deployment Manager on the Microsoft CRM Web server, and then click License Manager. Right-click a license and select License Summary (shown in Figure 3-4).

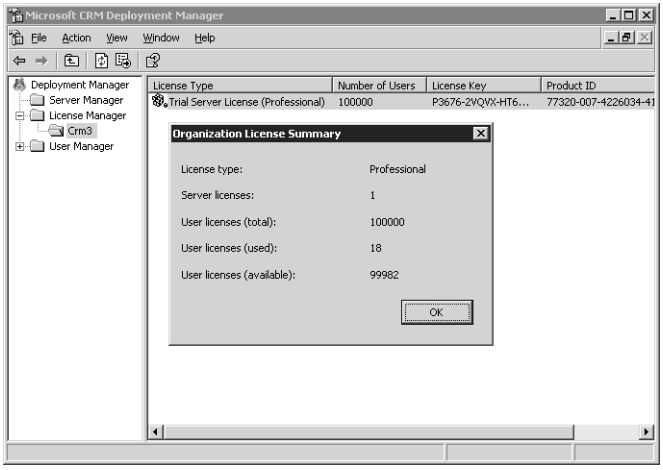


Figure 3-4 License summary in Microsoft CRM Deployment Manager

Security Roles and Business Units

As we explained earlier, Microsoft CRM uses a combination of role-based security and object-based security to determine what users can see and do within the deployment. Instead of configuring security for each user one record at a time, you assign security settings and privileges to a security role, and then you assign one or more security roles to a user. Microsoft CRM includes the following 13 predefined security roles:

- **CEO-Business Manager** A user who manages the organization at the corporate business level
- **CSR Manager** A user who manages customer service activities at the local or team level
- **Customer Service Representative** A customer service representative (CSR) at any level
- **Marketing Manager** A user who manages marketing activities at the local or team level
- **Marketing Professional** A user engaged in marketing activities at any level
- **Sales Manager** A user who manages sales activities at the local or team level
- **Salesperson** A salesperson at any level
- **Scheduler** A user who schedules appointments for services
- **Schedule Manager** A user who manages services, required resources, and working hours
- **System Administrator** A user who defines and implements the process at any level
- **System Customizer** A user who customizes Microsoft CRM records, attributes, relationships, and forms
- **Vice President of Marketing** A user who manages marketing activities at the business unit level
- **Vice President of Sales** A user who manages the organization at the business unit level

These default security roles include pre-defined rights and privileges typically associated with these roles, allowing you to save time by using them as the starting point for your deployment. You can edit any of the default security roles, except for System Administrator, to fit the needs of your business.

Tip You can also copy the default security roles by clicking Copy Role on the More Actions menu on the grid toolbar. Copying roles and then modifying the copies greatly reduces the setup time required to create new roles.

When you assign multiple security roles to a user, the privileges are combined so that the user can perform the highest-level privilege associated with any of his or her roles. In other words, if you assign two security roles with conflicting security rights, Microsoft CRM grants the user the least-restrictive permission of the two. For example, consider a fictional Vice President of Sales named Connie Watson. Figure 3-5 shows that Connie has two security roles assigned to her: Salesperson and Vice President of Marketing.

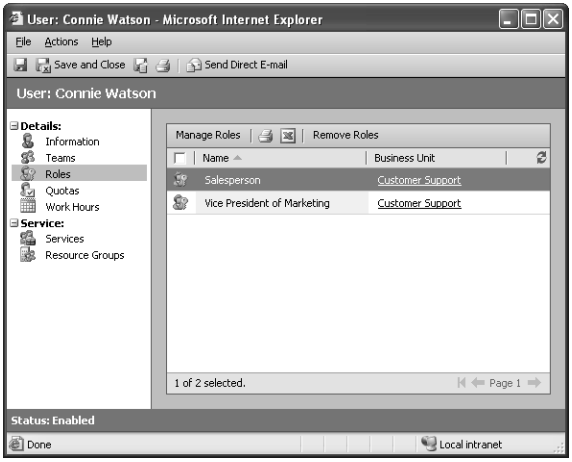


Figure 3-5 Multiple security roles assigned to a user

Using the Microsoft CRM default security roles, a user with the Salesperson security role cannot create new announcements, but the Vice President of Marketing security role can. Because Microsoft CRM grants the least-restrictive privilege across all of a user's roles, in this example, Connie would be able to create announcements because of her Vice President of Marketing security role.

Important Security roles combine together to grant users all of the privileges for all of their assigned security roles. If one of a user's security roles grants a privilege, that user *always* possesses that privilege, even if you assign him or her another security role that conflicts with the original privilege.

Security Role Definitions

Before we explain how to modify security roles, let's quickly cover the terminology related to security roles. To view and manage the settings for a security role, browse to Business Unit Settings in the Settings area, and click Security Roles. Then double-click one of the roles listed in the grid. Figure 3-6 shows the Salesperson default security role settings.

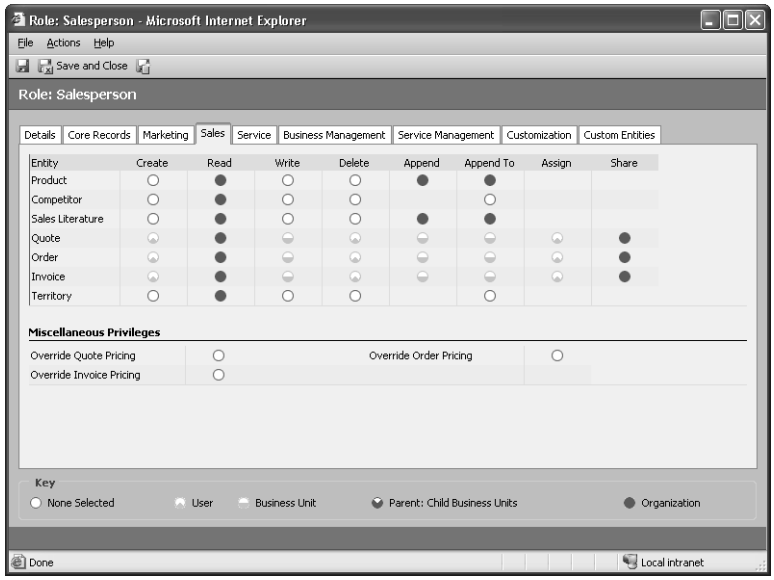


Figure 3-6 Salesperson security role settings

The columns in the top table represent entity privileges within Microsoft CRM. *Privileges* give a user permission to perform an action within Microsoft CRM such as Create, Read, or Write. The bottom table lists additional miscellaneous privileges such as Override Quote Pricing and Override Invoice Pricing. Microsoft CRM divides the privileges of a security role into subsets by creating tabs for the functional areas, such as Marketing, Sales, Service, and so on. Each tab in the security role editor lists different entity privileges and miscellaneous privileges for entities in Microsoft CRM.

The colored circles in the security role settings define the access level for that privilege. *Access levels* determine how deep or high in the organization business unit hierarchy the user can perform the specified privilege. For example, you could configure access levels for a security role so that a user could delete any record owned by someone in his or her business unit, but only read records owned by a user in a different business unit.

Important The actions that privileges grant to users (such as Create and Delete) do not vary by access level. For example, the Read privilege for the User access level offers the same action (functionality) as the Read privilege with Organization access level. However, the different access levels determine on which records in Microsoft CRM the user can execute the privilege.

Let's explore configuring access levels for a security role in more detail.

Access Levels

As you can see in the key (located at the bottom of Figure 3-6), Microsoft CRM offers five access levels:

- **None Selected** Always denies the privilege to the users assigned to the role.
- **User** Grants the privilege for records that the user owns, in addition to records explicitly shared with the user and records shared with a team to which the user belongs. We explain sharing records later in this chapter.
- **Business Unit** Grants the privilege for records with ownership in the user's business unit.
- **Parent: Child Business Units** Grants the privilege for records with ownership in the user's business unit, in addition to records with ownership in a child business unit of the user's business unit.
- **Organization** Grants the privilege for all records in the organization, regardless of the business unit hierarchical level to which the object or user belongs.

Note The User, Business Unit, and Parent: Child Business Unit access levels do not apply to some privileges, such as Bulk Edit and Print (found in the Business Management tab under Miscellaneous Privileges), because the concept of user ownership or business units doesn't apply to those privileges. No user or business unit owns Bulk Edit or Print because they're just actions. Therefore, these types of privileges offer only two access levels: None Selected and Organization. In these scenarios, you can think of None Selected as "No" and Organization as "Yes" in regard to whether the user possesses that privilege.

Let's consider an example scenario to illustrate access levels in a real-world context. Figure 3-7 shows five business units, six users, and six Contact records.

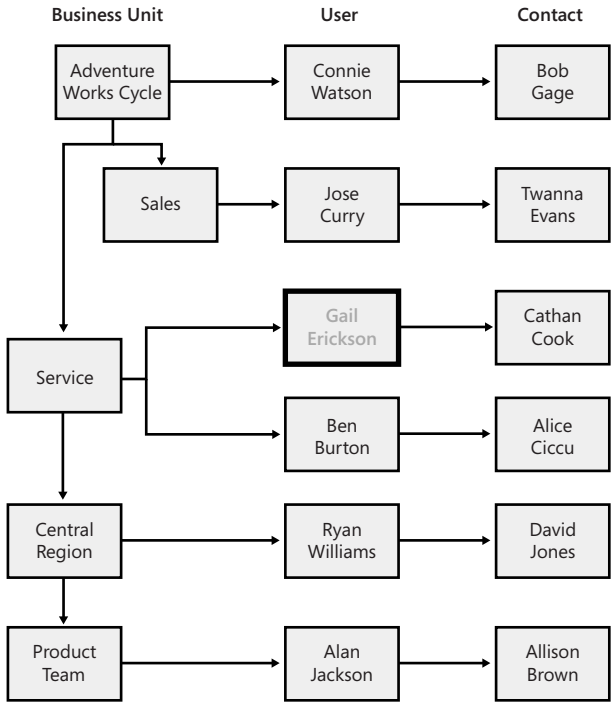


Figure 3-7 Access levels example

We will examine the impact of configuring different access levels for a single privilege (Contact Read) in the context of a fictional user named Gail Erickson. Gail belongs to the Service business unit, which is a child of the Adventure Works Cycle business unit and is also a parent of the Central Region business unit. Each of the Contacts shown is owned by the user record that it is linked to. Table 3-1 shows which Contact records Gail could read for each of the five possible access level configurations.

Table 3-1 Read Privileges for Gail Erickson by Access Level

Read privilege access level for the Contact entity	Bob Gage	Twanna Evans	Cathan Cook	Alice Ciccu	David Jones	Allison Brown
None	No	No	No	No	No	No
User	No	No	Yes	No	No	No
Business Unit	No	No	Yes	Yes	No	No
Parent: Child Business Unit	No	No	Yes	Yes	Yes	Yes
Organization	Yes	Yes	Yes	Yes	Yes	Yes

For the Business Unit access level, Microsoft CRM would grant Gail the Read privilege for the Alice Ciccu contact because Ben Burton owns that record and he belongs to the same business unit as Gail. For the Parent: Child Business Unit access level, Microsoft CRM would grant Gail the read privilege for the David Jones and Allison Brown records because the Central Region and Product Team business units are children of the Service business unit that Gail belongs to, and both the David Jones and Allison Brown records are owned by users that belong to these child business units.

As this example illustrates, configuring access levels for a security role requires that you understand and consider the following parameters:

- The organization and business unit hierarchy
- Record ownership and the business unit to which the record owner belongs
- The business unit of the logged-in user

Table 3-2 summarizes how Microsoft CRM grants and denies privileges based on these parameters.

Table 3-2 Privileges Granted Based on Access Level and Record Ownerships

Privilege access level	Record owned by user	Record owned by different user in same business unit	Record owned by user in any child business unit	Record owned by user in any non-child business unit
None	Deny	Deny	Deny	Deny
User	Grant	Deny	Deny	Deny
Business Unit	Grant	Grant	Deny	Deny
Parent: Child Business Unit	Grant	Grant	Grant	Deny
Organization	Grant	Grant	Grant	Grant

By now you should have a good understanding of how Microsoft CRM determines whether to grant security privileges to users based on access levels. Now we'll discuss what each of the privileges means and the actions that they allow users to perform in the system.

Privileges

Privileges define what users can view and do within Microsoft CRM, and you bundle privileges together within a security role definition. Some of the privileges describe actions that users can take against entity records such as delete or create, and other privileges define features in Microsoft CRM such as Mail Merge and Export to Excel. In this section, we will explore:

- Entity privileges
- Miscellaneous privileges
- Privilege impact on application navigation

Entity Privileges

As Figure 3-6 showed, some privileges such as Create, Read, and Write apply to the entities within Microsoft CRM. For each entity type and privilege, you can configure a different access level. The following list describes the actions that each privilege allows:

- **Create** Permits the user to add a new record
- **Read** Permits the user to view a record
- **Write** Permits the user to edit an existing record
- **Delete** Permits the user to delete a record
- **Append** Permits the user to attach another entity to, or associate another entity with, a parent record
- **Append To** Permits the user to attach other entities to, or associate other entities with, the record
- **Assign** Permits the user to change a record's owner to a different user
- **Share** Permits the user to share a record with another user or team
- **Enable/Disable** Permits the user to activate or deactivate records

More Info Not all of the entity privileges apply to all of the entities in Microsoft CRM. For example, the Share privilege does not apply to any of the entities on the Service Management tab. The Enable/Disable privilege only applies to the Business Unit and User entities.

The Append and Append To actions behave a little differently than the other privileges because you must configure them on two different entities to work correctly. To understand the Append and Append To actions better, consider the analogy of attaching a sticky note to a wall. To configure the sticky note concept using Microsoft CRM security privileges, you would need to assign Append privileges to the sticky note and then configure Append To privileges to the wall. Translating that concept to Microsoft CRM entities, if you want to attach (or append) a Contact to an Account, the user would need Append privileges for the Contact and Append To privileges for the Account record.

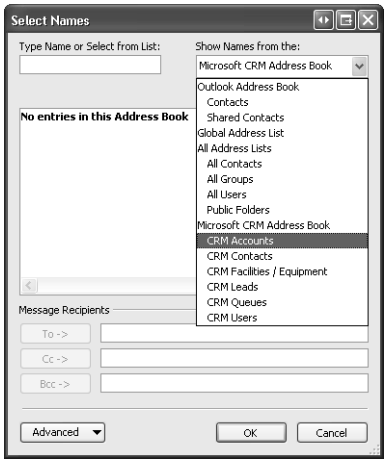
Microsoft CRM also allows you to configure entity privileges for any custom entities that you create in your deployment. You can configure all five access levels for each custom entity for all of the entity privileges, except the Enable/Disable action.

Miscellaneous Privileges

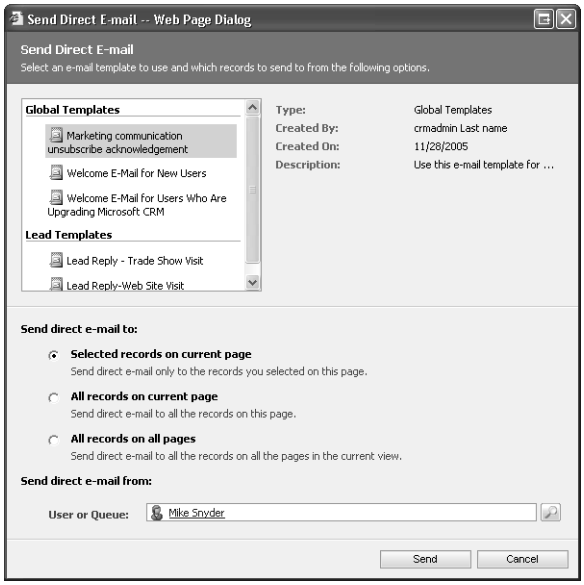
In addition to entity privileges, Microsoft CRM includes additional miscellaneous privileges on each tab of the security role editor. The privilege name often provides enough information about what it does, but sometimes the description might leave you guessing. This is especially true for miscellaneous privileges that relate to areas of the application that you might not use

often. In the following list, we provide a little more description about what each of the miscellaneous privileges means and, in some cases, where to find the related feature.

- **Publish E-mail Templates** Permits the user to make a personal E-mail Template available to the organization. Users can access this feature by browsing to Templates in the Settings section, and opening a personal E-mail Template by double-clicking it. Then they can click Make Template Available to Organization located under the Actions menu.
- **Override Quote Pricing** Permits the user to override a quote's calculated price (based on products added to the quote) and manually enter new quote pricing. Users can access the Override Price button when they're editing a Quote Product attached to a Quote.
- **Override Invoice Pricing** Permits the user to override an invoice's system-generated price and manually enter new invoice pricing. Users can access the Override Price button when they're editing a Invoice Product attached to an Invoice.
- **Override Order Pricing** Permits the user to override an order's system-generated price and manually enter new order pricing. Users can access the Override Price button when they're editing an Order Product attached to an Order.
- **Publish Articles** Permits the user to publish unapproved Knowledge Base articles. Users access the Approve (publish) button in the grid toolbar of the Unapproved Article Queue located within the Knowledge Base area.
- **Assign Role** Permits the user to add or remove security roles from user records in the Settings section.
- **Bulk Edit** Permits the user to edit multiple records at the same time. Users with this privilege can access the feature from an entity's grid toolbar. The bulk edit action does not apply to all entities.
- **Print** Permits the user to create a printer-friendly display of a grid. Users with this privilege can access this feature by clicking the Print button on the grid tool bar. You cannot vary this privilege by entity type.
- **Merge** Permits the user to merge two records together into a single record. Users with this privilege can access the Merge feature from the grid toolbar.
- **Go Offline** Permits a user with the Microsoft CRM laptop client for Outlook installed to work in an offline mode. Working offline creates a local copy of the database on the laptop. Because the user can remove the laptop (with the offline data) from your work premises, the offline option raises a potential security question that you must consider.
- **CRM Address Book** Permits a user of the Microsoft CRM clients for Outlook (laptop and desktop) to select CRM records from his or her address book in Outlook.



- **Update Business Closures** Permits the user to modify business working hours and closure information. Users access the Business Closures information within the Settings area.
- **Assign Territory to User** Permits the user to add or remove users from a sales territory. Users access the Sales Territories information within the Settings area.
- **Go Mobile** Permits the user to synchronize Microsoft CRM data with Microsoft Windows Mobile-based devices such as Pocket PCs.
- **Export to Excel** Permits the user to export the grid data to Microsoft Office Excel. Users with this privilege access the Export to Excel feature from the grid tool bar.
- **Mail Merge** Permits the user to create mailing items such as letters, envelopes, and labels. Users with this privilege can use the Mail Merge feature in the Microsoft CRM client for Outlook (either version) located under the More Actions menu on the grid toolbar for the Lead, Account, and Contact entities.
- **Sync to Outlook** Permits a user of either Microsoft CRM client for Outlook to synchronize Microsoft CRM data such as Contacts, Tasks, and Appointments to his or her Outlook file.
- **Send E-mail as Another User** Permits the user to select a different user or queue for the From address of an e-mail sent with the Microsoft CRM Send Direct E-mail feature. The Send Direct E-mail button appears on grids only if the user has the following security privileges:
  - Read and Append privileges on the Activity entity.
  - Append To privileges for the entity to which the user is sending direct e-mail (such as Contact or Account).
  - Read privileges on the E-mail Template entity.



- **Manage Reports** Permits the user to add, modify, or delete reports. Chapter 7 explains managing reports in detail.
- **Search Availability** Permits the user to search for available times when scheduling a Service activity.
- **Browse Availability** Permits the user to view the Service Calendar located in the Service area.
- **ISV Extensions** Determines whether Microsoft CRM displays customizations, such as custom menu items and toolbar buttons, from the ISV.config file to the user. Note that this setting applies to all or none of the ISV extensions—you cannot turn on specific ISV extensions by using this setting.

More Info At the time this book went to press, Microsoft had not yet released the mobile version of Microsoft CRM 3.0 for Pocket PCs and Windows Mobile-based devices. Therefore, we cannot definitively describe how the Go Mobile privilege will behave.

If you're still not sure what a specific privilege does or whether it will do what you want, you can easily test a privilege by enabling it for a security role, saving the role, and then logging on to Microsoft CRM as a user with only that security role. Remember that if your personal account has a System Administrator role, you have organization access level rights for all privileges, so don't log on as a System Administrator to test security privileges. Testing security privileges is a good example of when you might want to impersonate a different user when you log on to Microsoft CRM. We explained earlier in the chapter how you can modify your Internet Explorer security settings so that Microsoft CRM prompts you to enter a user name and password instead of using Integrated Windows authentication.

Note Miscellaneous privileges don't apply to custom entities that you create.

Field-Level Security

You configure privileges and access levels based on entire entity records in Microsoft CRM, not on the individual attributes for each entity. For example, you cannot use security role configurations to specify that users can view a contact's name and phone number but not the social security number or home address. If a user possesses the Read privilege for a Contact record, they can view *all* of the Contact's attributes displayed on the form.

However, you can take advantage of Microsoft CRM's robust programming model to dynamically hide attributes on a form or disable certain attributes based on the user's security role. You would use the form *onLoad* event to execute this type of custom script. Chapter 10, "Client-Side SDK," explains how to use the form *onLoad* event, and it includes sample code.

There's one caveat that you should know about when using the form *onLoad* event to hide attributes on a form: A user could still view the "hidden" data by performing an Advanced Find and adding the hidden column to his or her output result set. Users couldn't edit data with this technique, but they could view all attributes of any entity that they have privileges to read. Users could also potentially view this hidden information by exporting to Excel or running reports that contain this information.

Therefore, using the form *onLoad* event doesn't really provide true field-level security if you need to hide data from users, but you could restrict users from editing specific attributes on the entity form by using this technique.

Privilege Impact on Application Navigation

Microsoft CRM includes over 100 entities and thousands of features within the Sales, Marketing, and Customer Service areas. However, very few organizations will use *all* of the entities that Microsoft CRM offers to track and manage their customer data. Consequently, users commonly request to see only the areas of the application that their organization actually uses. For example, if your organization doesn't use the Sales Literature or Invoices entities, your users won't want to see these entities as they navigate through the user interface.

Although it would be technically possible to use the site map to remove some areas of the navigation (Sales Literature and Invoices, in this example), the better solution would be to modify your users' security roles and privileges, which would also change the user interface.

Important You should modify security roles, instead of modifying the site map, to hide areas of Microsoft CRM that your organization does not use. Modifying security roles also allows you to change the display of the entity navigation pane, which is an area of the user interface that you cannot edit by using the site map. Chapter 6, "Relationships and Custom Entities," explains the site map in more detail and discusses when you should modify it.

If you modify a security role and set the access level of the Read privilege for an entity to None Selected, Microsoft CRM automatically removes that entity from the user interface for users with that security role, including the menu bar, the application navigation pane, and the entity record. Most of the thirteen default security roles include an Organization access level for the Read privilege on all of the entities, so the users will see all of the entities in the application navigation. Therefore, we recommend that you change the Read privilege access level to None Selected for any entity that you're not using in your deployment. By doing so, you'll create a streamlined user interface that will help new users learn the system more quickly and let existing users navigate more efficiently.

Tip To see the updated application navigation after you modify a security role, you might have to refresh your Web browser window or restart Outlook.

Figure 3-8 shows the Account record for a user with the default Customer Service Representative security role assigned. Because that role includes the Read privilege for most of the entities, the user can see all of the links in the entity navigation pane, such as Quotes, Orders, Invoices, Marketing Lists, and Campaigns.

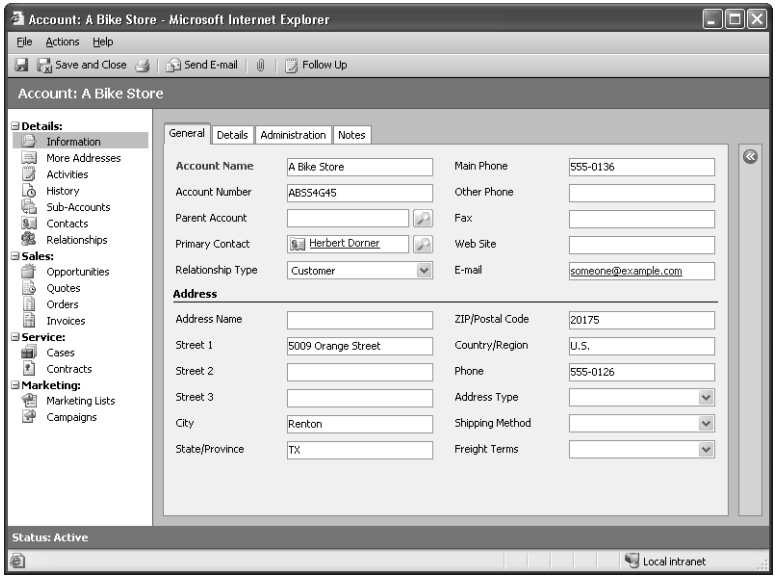


Figure 3-8 Account record as seen by a user with the default Customer Service Representative security role

In reality, most customer service representatives don't need to see all of this information on an Account record. Instead, let's assume that you want your customer service representatives to see only the information shown in the Details and Service groups. By modifying their security roles and setting the Read privilege to None Selected for the entities that you want to hide, the revised Account form might appear like the one shown in Figure 3-9.

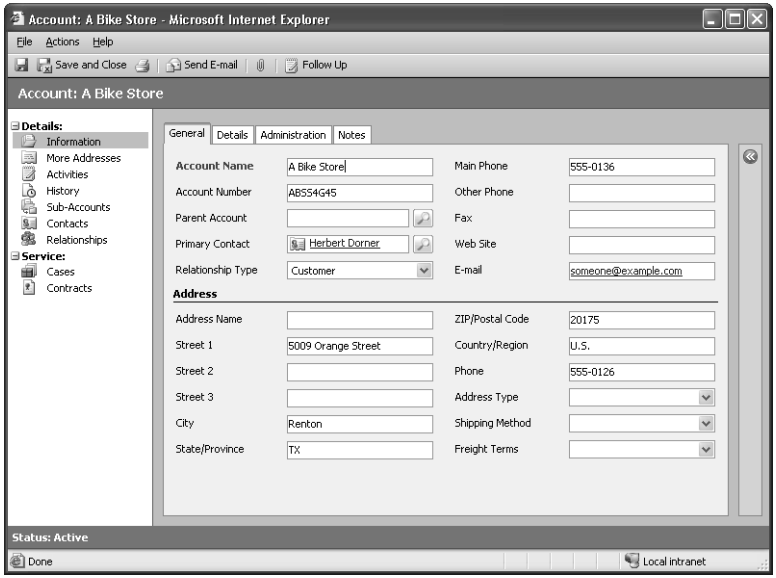


Figure 3-9 Account record as seen by a user with a revised Customer Service Representative security role

This provides a much cleaner user interface that your users will appreciate. Likewise, you could also revise the Salesperson security roles so that salespeople see only entities that they need to perform their jobs.

Security Role Inheritance

If your deployment includes multiple business units, you should understand how Microsoft CRM inherits security roles within the business unit hierarchy. When you create a new security role in a business unit, Microsoft CRM creates an instance (copy) of that security role for every business unit that is a child of the business unit for which you created the new security role. If you try to edit the security role in one of the child business units, you will see a warning message stating, "Inherited roles cannot be modified or updated." You can edit only the parent security role, and then Microsoft CRM automatically copies your changes to all of the security roles in the child business units. Consider the organization hierarchy of the sample organization Adventure Works Cycle, as shown in Figure 3-10.

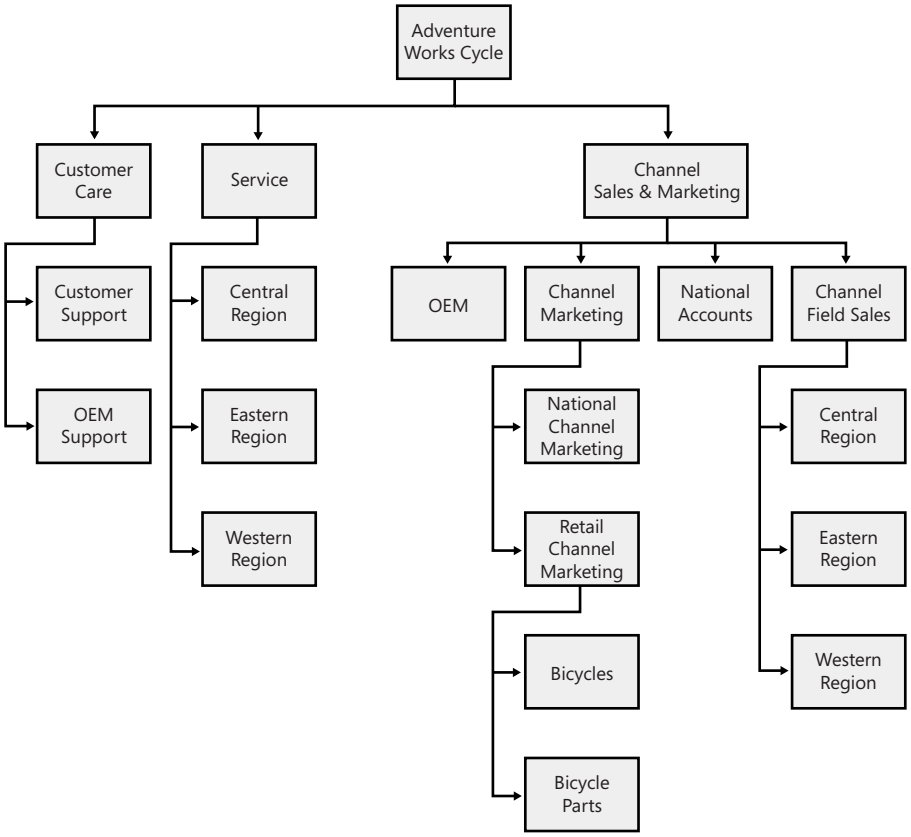


Figure 3-10 Organization structure for the sample company, Adventure Works Cycle

If you create a new security role called Director assigned to the Customer Care business unit, Microsoft CRM automatically creates non-editable copies of the Director security role in the Customer Support and OEM Support business units because they're children of the Customer Care business unit. Any changes you make to the Directory security role are automatically propagated to all of the Director security roles in the child business units. If you viewed the security roles for one of the other business units, such as Service or OEM, you would not see the Director security role listed, because the Service and OEM business units are not children of the Customer Care business unit.

Tip When you a create a new security role, Microsoft CRM assigns the security role to the root business unit by default, so make sure that you remember to change the role's business unit by using the business unit look up if you want to create a role in a non-root business unit.

Every user belongs to only one business unit, and you can only assign users security roles from the business unit to which they belong. Therefore, in this example, you could not assign the Director security role to users who belong to any business unit other than Customer Care, Customer Support, and OEM Support. You can view all of the security roles for a single business unit by using the business unit view filter drop-down list to select a specific business unit.

Because Microsoft CRM inherits security roles to children business units, you cannot vary the privileges of a security role to be different for each business unit. However, you can create a varying number of security roles for each business unit within your deployment. The ability to create unique security roles for each business unit gives you great flexibility to create and configure security roles to meet your organization's needs.

Sharing Records

Despite the numerous security options and configuration choices we've already discussed, you will probably encounter scenarios in which users need to share and collaborate on records that the business unit hierarchy does not support. Consider a fictional company called Coho Vineyard & Winery (the root business unit) with two children business units named Vineyard and Winery. Coho Vineyard & Winery CEO Laura Owen (user assigned to root business unit) owns the Woodgrove Bank account. However, the security roles for Gretchen Rivas (assigned to Vineyard business unit) and Heidi Steen (assigned to Winery business unit) do not have the Write privilege for the Account entity. The CEO decides that she wants Gretchen and Heidi to work on a special project related to Woodgrove Bank for which they will need to edit the record. However, Laura doesn't want them to edit any other Account records that she owns other than Woodgrove Bank. This type of security configuration would not be possible with the security configurations we've covered so far. If Laura gave Gretchen and Heidi privileges to edit Account records for the Organization, they would be able to edit *any* Account, not just the Woodgrove Bank record. Fortunately, Microsoft CRM allows users to share records to accommodate exactly this type of collaboration scenario. *Sharing* records allows a user to grant privileges for a specific record so that other users can work with the shared record, even though they would not normally have the necessary privileges to do so.

To share records, users must have a security role with the appropriate Share privilege. To set up a share like the Woodgrove Bank example, open the entity record and click Sharing... on the Actions menu of the entity menu bar. On the Share dialog page, select the users that you want to share this record with by clicking Add User/Team. Use the Lookup tool to find the records that you want, and then click OK. Microsoft CRM adds the users to the page, as shown in Figure 3-11.

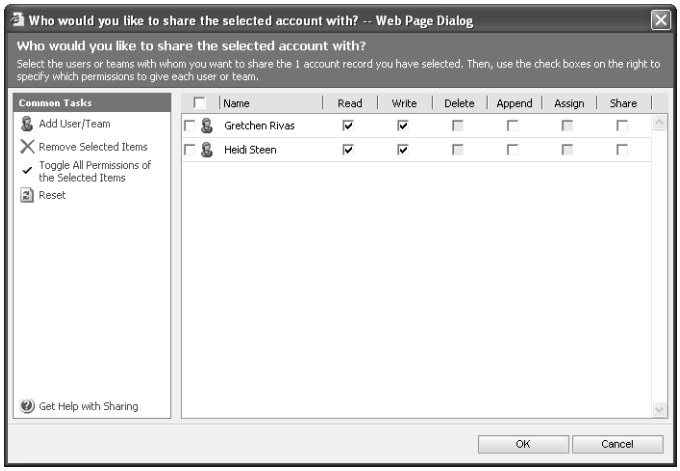


Figure 3-11 Sharing records with users

Next, specify which privileges you want to share with these users. In the Woodgrove Bank example, Laura Owen would select the Read and Write privileges so that Gretchen and Heidi could edit this record. Note that the Delete and Assign privilege check boxes are disabled because Laura doesn't have those privileges for this record, and therefore cannot share them with any other user.

More Info Users can't share a privilege if they do not posses the privilege themselves. For example, a user could not share Delete privileges for a record if he or she did not have the Delete privilege for that record.

With this share in place, Gretchen and Heidi can now read and write just the Woodgrove Bank Account record. Of course, you can revoke a share at any time by simply opening the record and clearing the check boxes for the privileges that you want to revoke.

Teams

In our Coho Vineyard & Winery example, it was easy to set up the share because we needed to select only two users. But what if Laura wanted to share the Woodgrove Bank record with 100 users? What if she wanted to share five different records with those same 100 users? It would be a pretty miserable and time-consuming process to manually share records one user at a time in these examples. Fortunately, Microsoft CRM allows you to set up and configure *teams* of users to expedite the sharing process. By sharing a record with a team instead of individual users, you do not have to manually select user records for each share that you create. Rather, you simply select the team that you want to share with, and all of the users in that team will participate in the share.

You can create and modify teams by browsing to Business Unit Settings in the Settings area and clicking Teams. When you create a team, you specify the Business Unit to which the team belongs, and then you simply add members to the team.

Important Although you assign a team to a business unit, you can add any user in the organization to a team, regardless of his or her business unit. You cannot change a team's business unit once it is created.

If you use a large number of teams, you can configure the security settings so that users only see a subset of all of the teams. To do this, configure the Team entity privilege within a user's security role with an access level appropriate for each team's business unit. For example, if you create a team that belongs to the root business unit but you only grant a security role with a User access level for the team privilege, users with that security role won't see that root business unit team in the user interface unless they personally created that team. This type of configuration allows you to restrict the teams that each user is allowed to view (and share records with) in case you want to hide specific teams (such as executive or financial teams).

Caution Once you create a team, you cannot delete it or disable it. If you no longer want to use a team, all you can do is remove all of its members. Therefore, you should use some discretion when creating teams, or you might end up with a bunch of abandoned teams with no members.

You might wonder if it's possible to have a team own a record, instead of just sharing a record with a team. Unfortunately, you cannot set a team as the owner of a record such as a Lead, Account, or Contact.

Sharing and Inheritance

When you share a record with a team or user, child entities of the shared record can inherit the same sharing settings as the parent record. In the Woodgrove Bank example, Gretchen and Heidi could edit the Account record and its related entities, such as Tasks, Phone Calls, and Notes, because they inherit the same share as their parent record.

More Info For shared records (directly shared or inherited), users receive only the shared privileges for the entity if they have at least a User access level for that entity. For example, if Heidi had an Access Level of None Selected for the Activity entity, she would not be able to view activities related to Woodgrove Bank even if someone shared Read privileges with her for that Account record. Likewise, she would need to have at least a User access level for the Account entity to view the Woodgrove Bank account record after Laura shared it with her.

You can configure how Microsoft CRM shares related records by editing the relationship behavior between two entities. For example, you might want Microsoft CRM to inherit sharing with related entities such as Tasks, but not with a different related entity such as Activities. Chapter 6 explains in detail how to configure relationship behaviors between entities.

Note Microsoft CRM knowledge base article ID #908504 explains that sharing inheritance two levels or deeper might lose its sharing inheritance.

Summary

Microsoft CRM includes a powerful and highly configurable security model that allows you to configure and restrict information access according to your business needs. Microsoft CRM uses Integrated Windows authentication and Active Directory to manage user accounts and authentication. By combining role-based and object-based security settings with your organization's business unit structure, Microsoft CRM allows you to accommodate very complex security and information access needs. Microsoft CRM also supports project-based and collaborative work by enabling users to share records with teams and individual users.