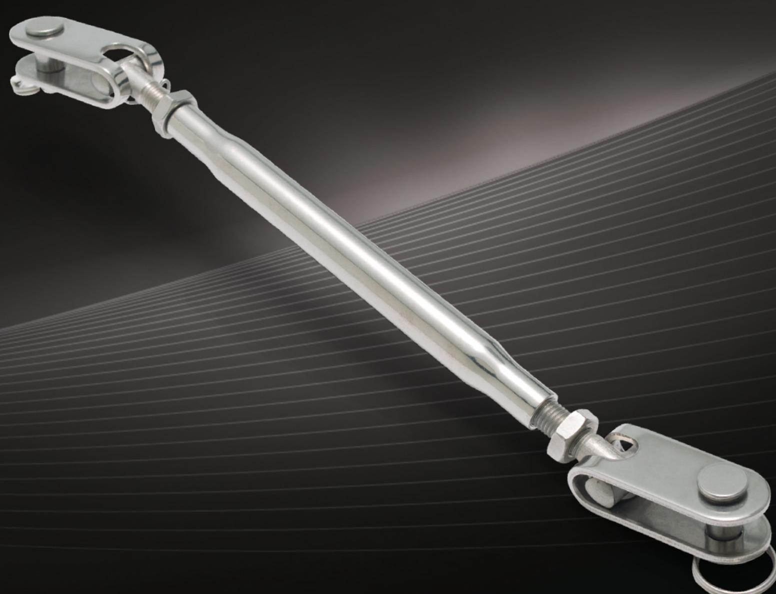
Microsoft

Foreword by Bill Patterson
Director, Product Management, Microsoft Dynamics CRM

Working with Microsoft Dynamics® CRM 2011



Mike Snyder, Jim Steger, and Kristie Reid

sonoma PARTNERS

Microsoft®

Working with

Microsoft Dynamics® CRM 2011

Mike Snyder

Jim Steger

Kristie Reid

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

Library of Congress Control Number: 2011923689

ISBN: 978-0-7356-4812-8

Printed and bound in the United States of America.

Third Printing: July 2014

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: Todd Merrill
Developmental Editor: Devon Musgrave
Project Editor: Valerie Woolley
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Matt Cooper
Copyeditor: Becka McKay
Indexer: Jean Skipp
Cover: Twist Creative • Seattle

Contents at a Glance

List of Figures

List of Tables

List of Sidebars

Table of Contents

Foreword

CRM continues to see accelerated growth and adoption around the world. As we move into a new phase of business computing, we have seen the retirement of complex, rigid, and inflexible CRM systems in favor of solutions that are simple, agile, and valuable to today's information worker. It is in this area that Microsoft Dynamics CRM continues to shine and leads organizations into a new world of empowerment and enhanced business productivity.

And we're only getting started.

Enter Microsoft Dynamics CRM 2011—a solution designed to amplify user adoption, help organizations discover new business insights, and fuel business productivity across your entire business network. Designed to meet the most comprehensive set of CRM needs across the cloud or in your own IT environment, Microsoft Dynamics CRM 2011 delivers the unparalleled flexibility, security, and scalability needed to manage crucial relationships, guide everyday interactions, optimize business processes, and deliver real-time business intelligence for every system user.

Mike Snyder, Jim Steger, and Kristie Reid yet again deliver the most comprehensive resource for Administrators and Developers of Microsoft Dynamics CRM 2011 to understand new concepts and master enhanced system capabilities. It seems that with every customer that I visit around the world, a copy of this resource has been used to enhance deployment success.

Working with Microsoft Dynamics CRM 2011 continues this tradition of excellence.

No matter where you find yourself in the system development life cycle—from solution envisioning, planning, developing, and stabilizing, this book provides a comprehensive reference for each project team member:

For users of Microsoft Dynamics CRM 2011, this guide provides comprehensive examples of mastering native functionality and enhanced capabilities.

For system implementers and customizers, this resource serves as a definitive guide to unleashing the full power of the solution framework to deliver tailored business applications.

For information technology administrators, this text provides an outstanding reference guide for planning, implementing, managing, and maintaining Microsoft Dynamics CRM 2011 across your organization.

Mike, Jim, and Kristie shine at explaining the essential topics, but also help readers see beyond the basics when it comes to customizing and extending Microsoft Dynamics CRM 2011 for unique system needs. The concepts and examples covered in this text are certain to accelerate your mastery of this innovative new release. Again, every deployment of Microsoft Dynamics CRM 2011—in the cloud or in your own IT environment—will greatly benefit from this resource guide. It has been a pleasure to work with both Mike and Jim in the development of this text, and I, like the readers who will follow me, keep this resource nearby when approaching each new business challenged to be solved with Microsoft Dynamics CRM 2011.

I look forward to hearing of your success in working with this new release.

Sincerely,

Bill Patterson
Director, Product Management
Microsoft Dynamics CRM
Microsoft Corporation

Introduction

We love Microsoft Dynamics CRM 2011, and we hope that by the time you finish reading this book, you will love Microsoft Dynamics CRM, too. We understand that you might be skeptical about the possibility of falling for a piece of software, but we want you to know right up front that our goal is to show you all of the wonderful and amazing benefits the Microsoft Dynamics CRM application can provide for your business.

Who Should Read This Book

We wrote this book for the people responsible for implementing Microsoft Dynamics CRM at their organization. If you're the person responsible for setting up or configuring Microsoft Dynamics CRM software on behalf of other users at your company, this book is for you. You might be an information technology professional or simply a Power User from the sales or marketing departments. You should be comfortable with technical concepts and understand the role of various Microsoft technologies such as Microsoft Exchange Server, Microsoft Active Directory, and Microsoft SQL Server. You don't need to be a coding expert to benefit from this book, but we hope that you can edit an XML file and that you understand how relational databases work.

This book can also help prospective customers with their software selection process as they evaluate the customization options that Microsoft Dynamics CRM offers. If you want to learn more about the software's capabilities before you make a purchase decision, we hope that this book provides some of the technical details you're looking for.

Who is this book not for? It's *not* for end users interested in learning how they will use Microsoft Dynamics CRM on a day-to-day basis because their company just went live with the software. If you don't have System Administrator rights, you won't be able to perform most of the steps in this book, so it probably won't provide much benefit for you. If you're not sure whether you have System Administrator rights, then this book probably isn't for you either. If you're interested in end-user topics, consider purchasing *Microsoft Dynamics CRM 2011 Step By Step* from Microsoft Press.

This book also *does not* tell you how to install the Microsoft Dynamics CRM software and troubleshoot any installation-related issues. We don't cover upgrading an existing Microsoft Dynamics CRM installation to Microsoft Dynamics CRM 2011. The Microsoft Dynamics CRM Implementation Guide gives excellent and detailed advice on the installation and upgrade processes, so we don't need to repeat that information here.

Organization of This Book

We divided *Working with Microsoft Dynamics CRM 2011* into 2 parts and 15 chapters. The two parts break down as follows:

- **Part 1, Overview and Setup** Provides a quick overview of the various components of Microsoft Dynamics CRM and explains how to configure some of the more frequently used areas of the software.
- **Part 2, Solutions** Goes deeply into how you can modify Microsoft Dynamics CRM to match the way your business works. Topics include adding new data fields, revising the user interface, creating reports and dashboards, and automating business processes by using workflow.

In resources such as the Implementation Guide, the software development kit (SDK), the User Interface Style Guide, and the online Help, Microsoft Dynamics CRM 2011 includes more than 1,500 pages of product documentation on how to use the software. This book is *only* 624 pages, so obviously it can't possibly cover every nook and cranny of how Microsoft Dynamics CRM works. Rather, our goal is to focus on the key areas most companies will need to set up, customize, and extend the software while providing plenty of examples and real-world advice. This book assumes that you can install the software and that you have a decent understanding of how to navigate the user interface. Consequently, if you want to learn more about using the software (as opposed to customizing the software), we recommend that you take advantage of the many Microsoft training options available for Microsoft Dynamics CRM, such as eCourses, classroom training, and the Foundation Library. Because of this book's space constraints, we decided not to repeat any information or samples already covered in the product documentation. Therefore, we frequently refer you to the SDK and the Implementation Guide.

One last thought regarding the organization of this book: We tried to eliminate any "marketing fluff" so that we could cram as much information as possible in this book. To that end, you will not read the reasons why customer relationship management (CRM) projects fail or read a discussion about the future of CRM software. We're straightforward and direct people, so we appreciate it when books present information in the same manner. We hope that you like this style, too.

Prerelease Software

We wrote most of this book using preproduction versions of Microsoft Dynamics CRM 2011. Microsoft released the final version of Microsoft Dynamics CRM 2011 just a week or two before we submitted the final copy to our editor, but we did review and test our examples using the final release. However, you might still find minor differences between the production release and the examples and screenshots included in this book.

Microsoft Dynamics CRM Online

As you learn in this book, Microsoft Dynamics CRM offers several different deployment options, including a Microsoft-hosted version of the software named Microsoft Dynamics CRM Online. Both versions of the software work identically in almost all areas, so our content and samples work for all versions of Microsoft Dynamics CRM, unless explicitly noted. If you're interested in Microsoft Dynamics CRM Online, we suggest that you check *http://crm.dynamics.com* for the latest information about that product.

System Requirements

We recommend that you refer to the Microsoft Dynamics CRM Implementation Guide for detailed system requirements. From a high level, you'll need the following hardware and software to run the code samples in this book:

Client

- Microsoft Windows 7 (both 64-bit and 32-bit versions), Windows Vista (both 64-bit and 32-bit versions), or Windows XP Professional SP3 operating system
- Microsoft Internet Explorer 7 or a later version
- Microsoft Office 2010, Microsoft Office 2007 with SP2, or Microsoft Office 2003 with SP3 (if you want to use Microsoft Dynamics CRM for Microsoft Office Outlook)

Server

- Microsoft Windows Server 2008 x64-based computers Microsoft SQL Server 2008
- Computer/processor: Quad-core x64 architecture 2 GHz CPU or higher such as AMD Opteron or Intel Xeon systems
- Memory: 8 gigabytes (GB) or more of RAM recommended
- Hard disk: 40 megabytes (MB) free space
- Network card: 10/100 megabits per second (Mbps) minimum, dual 10/100/1000 Mbps recommended

Code Samples

This book features a companion website that makes available to you all the code used in the book. The code samples are organized by chapter, and you can download code files from the companion site at this address:

http://aka.ms/648128/files/

Acknowledgments

We want to thank all of the people who assisted us in writing this book. If we accidentally omit anyone, we apologize in advance. We would like to extend a special thanks to the following people:

- **Bill Patterson** Bill sponsored the book project and helped make sure that all the pieces fell into place correctly. He also agreed to help us by writing the book's foreword.
- **Kara O'Brien** Kara did an amazing job (on a ridiculously tight timeline) of copyediting the initial drafts of each chapter and blending them together in a single cohesive product. We would never have completed this book on time without Kara's help!
- **Neil Erickson** We asked Neil, our Sonoma Partners network architect, to build and update more Microsoft Dynamics CRM environments than we care to admit. We want to thank Neil for all of his assistance.

In addition, we want to thank these members of the Microsoft Dynamics CRM product team who helped us at one point or another during the book project:

Abhishek Agarwal	Shamiq Islam	Nirav Shah
Inna Agranov	Raju Kulkarni	Manoj Shende
Andrew Bybee	Rubaiyat Khan	Derik Stenerson
Maureen Carmichael	Amy Langlois	Craig Ungar
Jim Daly	Nick Patrick	Praveen Upadhyay
Rich Dickinson	Manisha Powar	Sandhya Vankamamidi
Ajith Gande	Girish Raja	Mahesh Vijayaraghavan
Abhijit Gore	Venkata Ramana	Brad Wilson
Humberto Lezama Guadarrama	Michael Scott	Zhen Zhang
Peter Hecke	Vishal Sahay	

Thank you to the following Sonoma Partners colleagues who assisted with reviewing the content and providing feedback:

Brian Baseggio	Chris Labadie	Jeff Meister
Brad Bosak	Brendan Landers	Corey O'Brien
Jacob Cynamon-Murphy	Bob Lauer	Steven Oxley
Matt Dearing	Peter Majer	Jason Tyner
Mike Dearing	Sean Massa	Matt Weiler

Of course, we also want to thank the folks at Microsoft Press who helped support us throughout the book-writing and publishing process:

- **Ben Ryan** Ben championed the book project and he helped us through the process.
- **Valerie Woolley** Once again, working with Valerie has been a delight. She did a great job of helping us through the book production process, and she also helped fight for additional page count when it looked like we had written too much!
- **Christian Holdener** As our project editor, Christian did a great job of staying on top of the timeline and helping to get this book in print in time for the Microsoft Convergence conference.

Last but not least, we want to thank Matt Cooper. As the technical editor for the book, Matt worked around the clock to confirm the technical accuracy of the text. This included reviewing and testing all of our code samples and double-checking our facts.

Mike Snyder's Acknowledgments

I want to thank my wife, Gretchen, who tolerated the long nights and weekends that this book consumed over the past few months. Despite the fact that I kept disappearing into my office to sneak out some work, she supported me 100 percent from start to finish. Even though they won't be able to read this note for years, I want to thank my children, who provided me with the motivation to undertake this project. I also want to recognize my parents and my wife's parents who assisted my family with various babysitting stints. I would like to thank all of my coworkers at Sonoma Partners who helped pick up the slack created by my time commitment to this book.

Jim Steger's Acknowledgments

I would like to thank my wife, Heidi, and my children for their continued support in this undertaking. In addition to the Microsoft Dynamics CRM product team members we thanked above, I want to give an additional thank you to the following people who graciously spent time reviewing content and helping explain functionality: Matt Cooper, Ajith Gande, Nick Patrick, Jim Daly, Rubaiyat Khan, Richard Dickinson, Andrew Bybee, and Amy Langlois. Finally, I wish to express my gratitude to my associates at Sonoma Partners for their assistance during this process.

Kristie Reid's Acknowledgments

I first want to thank Mike and Jim for giving me the opportunity to help them with this project. They have both been an integral part of the successes that I have had implementing Microsoft Dynamics CRM solutions. Of course, I would not be able to do the work that I enjoy without my husband, Jon, who patiently took care of our remarkable kids, Maggie and Dylan, during the long hours I spent on my computer writing chapters. I also want to acknowledge my husband's parents, who entertained my family during our trips to see them while I hid out in their house working. Finally, I want to thank everyone at Sonoma Partners who helped me in so many ways during this process.

Errata & Book Support

We've made every effort to ensure the accuracy of this book and its companion content. If you do find an error, please report it on our Microsoft Press site:

1. Go to *www.microsoftpressstore.com*.
2. In the Search box, enter the book's ISBN or title.
3. Select your book from the search results.
4. On the book's catalog page, find the Errata & Updates tab.
5. Click View/Submit Errata.

You'll find additional information and services for your book on its catalog page. If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority and your feedback our most valuable asset. Please tell us what you think of this book at

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*

Chapter 3

Managing Security and Information Access

In this chapter:

If you've deployed multiple systems in the past, you already know that you must design your customer relationship management (CRM) solution to restrict information appropriately 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 Dynamics 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 user rights, 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 Dynamics 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 Dynamics CRM security settings requires that you 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 continually tweaking and revising the security settings as your business evolves. Fortunately, the Microsoft Dynamics CRM security model makes it easy for you to update and change your security settings on the fly.

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 organizational layout, you should identify the approximate number of users and the types of business functions those users perform. You will need this rough organizational map to start planning how you want to set up and configure security in your Microsoft Dynamics CRM deployment.

Important Your Microsoft Dynamics CRM business unit structure should not necessarily match your operational structure. You should configure the Microsoft Dynamics CRM business unit hierarchy to match your security needs, not to create an exact model of your organizational structure. Whereas the operational and Microsoft Dynamics CRM security business unit structures typically remain consistent for smaller organizations, midsize and enterprise organizations usually need to design a Microsoft Dynamics CRM business unit structure that does not match their organizational chart.

To put this type of organizational mapping into a real-world context, consider an example organization. Figure 3-1 shows the business structure for a fictional company named Adventure Works Cycle.

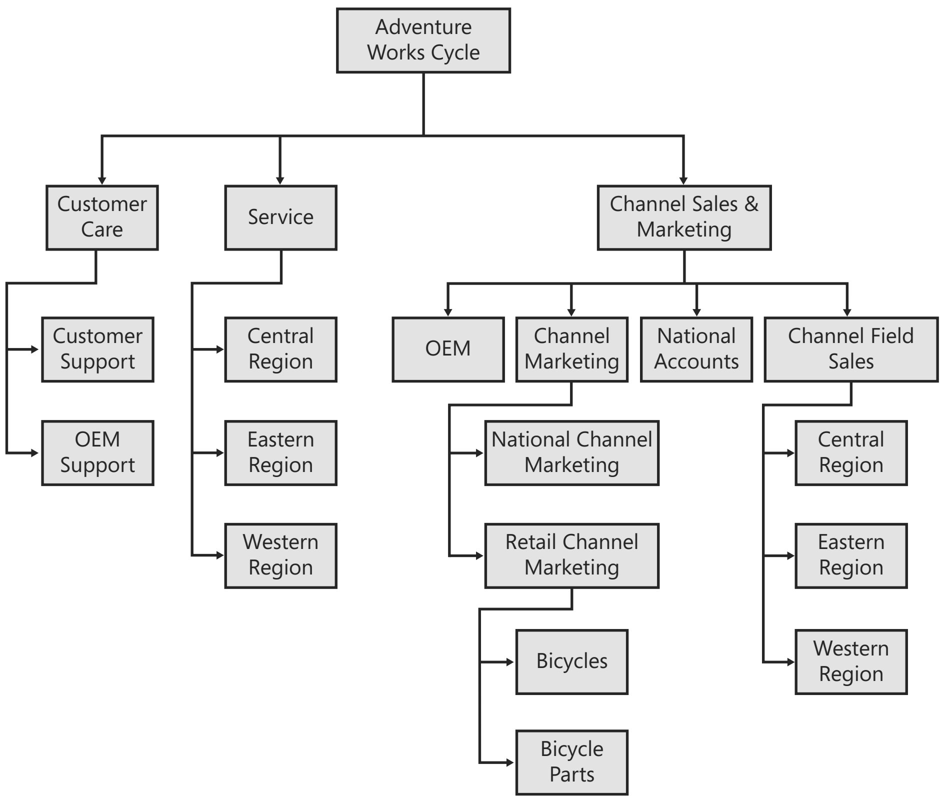


FIGURE 3-1 Organization structure for a sample company called Adventure Works Cycle

Each box in the figure represents a business unit in Microsoft Dynamics 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 by using the acronym 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 Dynamics CRM user to one (and only one) business unit.

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

- Which areas of Microsoft Dynamics CRM will the users need access to (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)?

As you map out your business units and users, you will probably find situations where users from different business units need to work together on a set of shared set of records. However the Microsoft Dynamics CRM security only allows you to specify one business unit per user. In these types of situations, you should consider the use of *teams* in Microsoft Dynamics CRM. Teams are a group of users that share and collaborate on records. Even though you specify a single business unit for a team, each team can consist of users from one or many business units.

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

> **Real World** For smaller organizations, mapping out your Microsoft Dynamics CRM organization model might take only 15 minutes. However, you may want to budget a few hours 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 Dynamics CRM so that 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 organizational model with information about the different types of users in your system, you must translate that information into Microsoft Dynamics CRM security settings. Before we explain how to configure the security settings in the software, we explain two of the key topics related to Microsoft Dynamics CRM security:

- Security model concepts
- User authentication

After you understand these concepts, we can get into the details of configuring the software to meet your specific needs. Because of the many security customization options offered in Microsoft Dynamics CRM, very rarely do we see an organizational structure that Microsoft Dynamics CRM security settings cannot accommodate.

Security Model Concepts

The Microsoft Dynamics CRM security model uses two main concepts:

- Role- and object-based security
- Organizational structure

Role-Based and Object-Based Security

Microsoft Dynamics 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 Dynamics CRM. All Microsoft Dynamics CRM users must have one or more security roles assigned to them. Therefore, when a user logs on to the system, Microsoft Dynamics 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*.

With this security model, you also can 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 Dynamics 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.

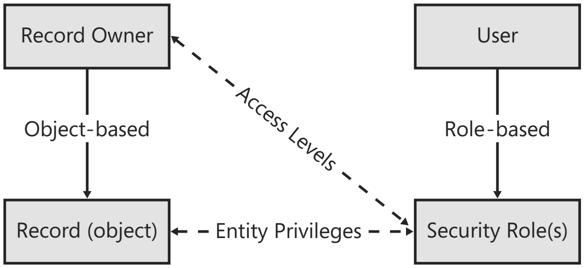


FIGURE 3-2 Role-based security and object-based security combine to determine user rights.

> **Important** Both users and teams can own records in Microsoft Dynamics CRM 2011.

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

Organizational Structure

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

- **Organization** The company that owns the deployment. The organization is the top level of the Microsoft Dynamics CRM business management hierarchy. Microsoft Dynamics 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 a 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.
- **Team** A group of users that work together. Team members can belong to different business units.
- **User** Someone who typically works for the organization and has access to Microsoft Dynamics 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 explain how these terms relate to setting up and configuring security roles.

User Authentication

Microsoft Dynamics CRM supports three different types of security methods to authenticate users when they try to log on to the system:

- Integrated Windows authentication
- Claims-based authentication
- Microsoft Windows Live ID

Customers that purchase Microsoft Dynamics CRM and deploy the software on premises will use Integrated Windows authentication, and they have the option to deploy a claims-based authentication for Internet-facing deployments of Microsoft Dynamics CRM as well. For on-premises deployments of Microsoft Dynamics CRM, each user who logs on to the system needs to use a Microsoft Active Directory account.

Only customers who use Microsoft Dynamics CRM Online will use Microsoft Windows Live ID to authenticate and log on to the system.

Integrated Windows Authentication

Microsoft Dynamics 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 in the Microsoft Dynamics CRM for Outlook interfaces. By using Integrated Windows authentication, users can simply browse to the Microsoft Dynamics CRM website and Microsoft Internet Explorer automatically passes their encrypted user credentials to Microsoft Dynamics CRM and logs them on. This means that users log on to Microsoft Dynamics CRM (authenticate) by using their existing Microsoft Active Directory directory domain accounts, without having to sign in to the Microsoft Dynamics CRM application explicitly. 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 the Active Directory directory service prevents him from logging on to Microsoft Dynamics 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 Dynamics CRM, but it does not automatically disable their user records in Microsoft Dynamics CRM. Because all active users count against your licenses, make sure that you remember to disable their user records in Microsoft Dynamics CRM to free their licenses. Also, if you change a user's name in Active Directory, you must manually update it in Microsoft Dynamics CRM. We strongly recommend that you deactivate the user in Microsoft Dynamics CRM before deactivating his or her Active Directory account.

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

However, you may 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 the following:

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

To view your Internet Explorer 8 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.

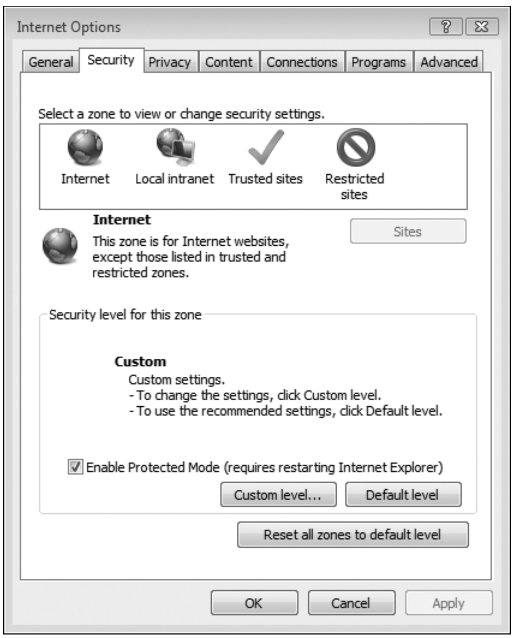


FIGURE 3-3 Web content zones in Internet Explorer

By altering the security settings, you can change how Internet Explorer passes your logon information to various websites, such as your Microsoft Dynamics CRM website.

Turning off automatic logon in the Local intranet zone

1. In 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 Dynamics CRM (or any other website on your local intranet). Instead, it prompts you to enter your user name and password when you browse to the Microsoft Dynamics 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 may want to log on as a different user during your setup and configuration phase to confirm that your security settings are correct.

In addition to disabling automatic logon, you may want to add Microsoft Dynamics 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; you use the following steps to add Microsoft Dynamics CRM as a trusted site.

Adding a trusted site to Internet Explorer

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

Adding a trusted site to Internet Explorer accomplishes two things in regard to Microsoft Dynamics CRM:

- Internet Explorer will automatically pass your user credentials to the website and attempt to log you on. You may want to set this up for your Microsoft Dynamics 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 Dynamics CRM.
- The Internet Explorer Pop-up Blocker allows pop-up windows for any website listed in your Trusted sites zone.

> **Caution** Intranet sites and trusted sites in Internet Explorer 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 automatically install signed Microsoft ActiveX controls on your computer.

Microsoft Dynamics CRM and Pop-up Blockers

Many users utilize 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 may also block some of the web browser windows that Microsoft Dynamics 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 Dynamics CRM application.

Internet Explorer 8 includes a pop-up blocker, but the default setting allows sites in the Local intranet and Trusted sites zones to open pop-up windows. If Internet Explorer does not recognize Microsoft Dynamics 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 from the Microsoft Dynamics CRM website. (On the Tools menu, point to Pop-Up Blocker, and then click Pop-up Blocker Settings to enter the Microsoft Dynamics CRM address.)

Some pop-up blockers do not allow you to enter a trusted address manually like the Internet Explorer pop-up blocker does. Therefore, you have to browse to the website you want to allow, and then click some sort of Allow Pop-ups button.

Here's another trick related to pop-up windows: You can reference the same Microsoft Dynamics CRM website by using several different techniques. For example, you could access Microsoft Dynamics CRM by using any of the following:

- Computer (NetBIOS) name (Example: *http://crm*)
- Internet Protocol (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 Dynamics CRM server, Internet Explorer 8 treats each of these as different websites. Therefore, you could configure different security settings in Internet Explorer for each of these URLs. For example, you can browse to the NetBIOS name by using Integrated Windows authentication to log on as yourself, but you could configure Internet Explorer to prompt for a logon when you browse to the IP address to impersonate a user.

Claims-Based Authentication

Although many users will access Microsoft Dynamics CRM over a local intranet connection using Integrated Windows authentication, Microsoft Dynamics CRM also offers customers the option of deploying Microsoft Dynamics CRM as an Internet-facing deployment (often abbreviated as *IFD*). In an IFD scenario, customers could browse over the Internet to a custom URL address such as *http://crm.yourdomainname.com* to access your Microsoft Dynamics CRM system. Using this access method, users do not need to create a virtual private network (VPN) connection to your network. They could use any type of standard Internet connection to access their data remotely. If you want to set up an IFD deployment, Microsoft Dynamics CRM 2011 requires federated services that support claims-based authentication. Most companies will use Active Directory Federation Services 2.0 (AD FS 2.0) for their federation services.

More Info Microsoft Windows Server introduced a claims-based access platform where it added support for the WS-Trust, WS-Federation, and SAML 2.0 protocols. Microsoft Dynamics CRM 2011 discontinues the Microsoft Dynamics CRM 4.0 forms-based authentication design for IFD and it uses the new claims-based option instead. After claims is properly enabled in your environment, you still need to go through the CRM IFD setup steps to make your CRM application accessible outside of your network. For more information on setting up claims-based authentication for Microsoft Dynamics CRM, please refer to the Microsoft Dynamics CRM Implementation Guide at *http://www.microsoft.com/downloads*.

When users browse to the external IFD URL that you configure, users see a logon screen like the one shown in Figure 3-4.

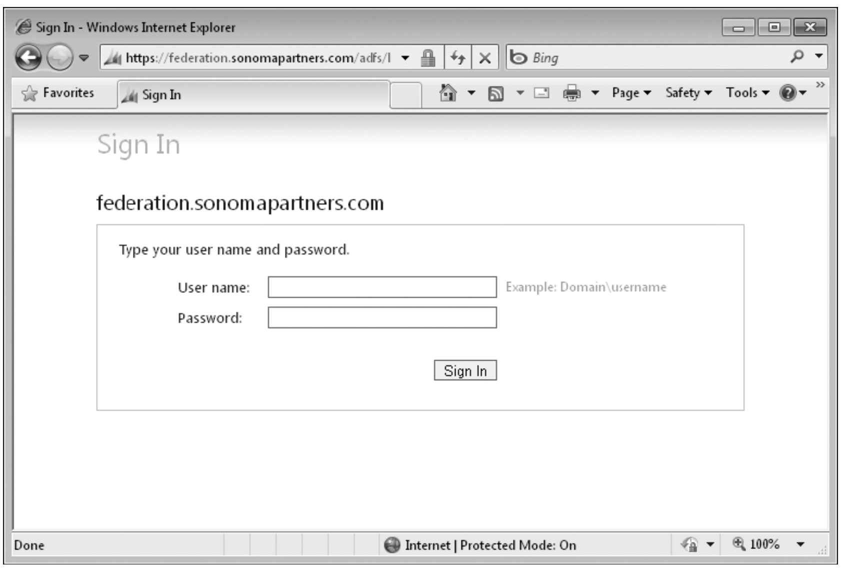


FIGURE 3-4 Internet-facing deployment logon screen

At the logon screen, the user can enter his or her Active Directory user name and password into the specified form fields. After users log on to Microsoft Dynamics CRM by using the web form, the system will behave in a nearly identical way as when users connect to the system over the local intranet using Integrated Windows authentication. However, some parts of the system, such as the dynamic worksheets in Microsoft Office Excel, will not work correctly unless the user also has Microsoft Dynamics CRM for Outlook installed on the computer.

Important When accessing Microsoft Dynamics CRM through forms-based authentication, some portions of the software such as dynamic worksheets will require that the user install the Microsoft Dynamics CRM for Outlook.

The Microsoft Dynamics CRM Implementation Guide explains how to set up and configure claims-based authentication and IFD, so we won't repeat that material here.

Windows Live ID

As we previously stated, only Microsoft Dynamics CRM Online customers will use Windows Live ID to authenticate when they log on to their system. Microsoft offers Windows Live ID as a single sign-on service that businesses and consumers can use throughout various Internet websites. By allowing people to use a single logon and password, Windows Live ID simplifies the end-user experience regarding authentication.

More Info Microsoft previously referred to Windows Live ID as the Microsoft Passport Network. Windows Live ID works with MSN Messenger, MSN Hotmail, MSN Music, and many other websites.

When users browse to *http://crm.dynamics.com* and log on, they are prompted to enter their Windows Live ID credentials, as shown in Figure 3-5.

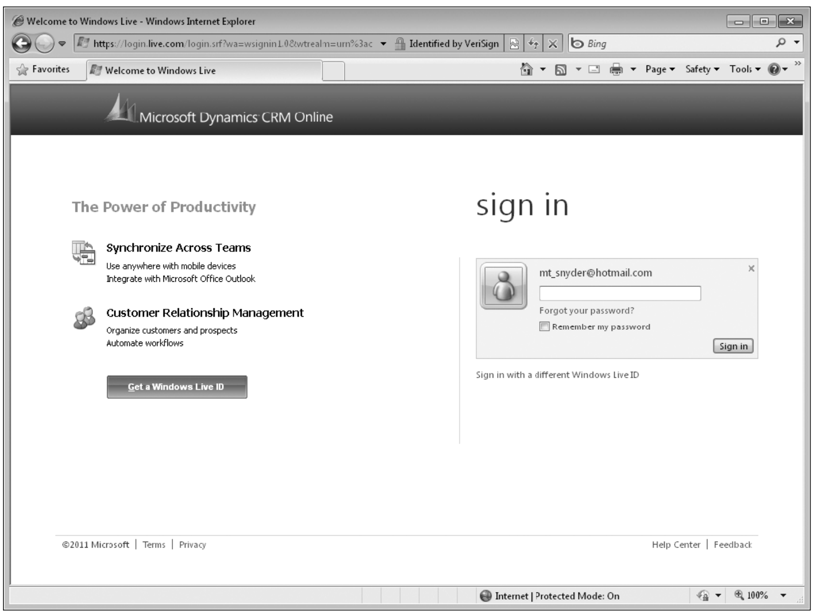


FIGURE 3-5 Entering Windows Live ID credentials on Microsoft Dynamics CRM Online

Please note that when you invite a user to your Microsoft Dynamics CRM Online organization, you must use the email address of that user's Windows Live ID account.

Managing Users

A user is someone with access to Microsoft Dynamics CRM who typically works for your organization. To manage users in Microsoft Dynamics CRM, browse to Administration 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.
- Assign a Client Access License type.

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

As an administrator, in addition to adding new users you will also need to do the following:

- Disable old users and reassign their records to different users.
- Monitor the number of Microsoft Dynamics CRM licenses you're using to make sure you are compliant.

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

Reassigning User Records

As part of the usual course of business, employees will leave your organization and you'll need to adjust their user record in the system accordingly. When a user stops working with your Microsoft Dynamics CRM deployment, you should disable the user's record by clicking the Disable button located in the ribbon. When you disable the user, she can no longer log on to your Microsoft Dynamics CRM system. However, disabling a user will not change her record ownership because disabled users can still own records.

> **Note** To maintain data integrity, Microsoft Dynamics CRM does not allow you to delete users.

After disabling the user, you will also probably want to reassign his or her records to a different user in the system. By doing so, you can make sure that a different user will address any open activities or follow-ups that the previous user didn't complete yet. We recommend that you reassign the records using one of two methods:

- Bulk reassign
- Manually reassigning active records

Bulk Reassign

If you open a user record in Microsoft Dynamics CRM, you will see the Reassign Records button in the ribbon. When you click the Reassign Records button, the dialog box shown in Figure 3-6 appears.

FIGURE 3-6 Reassign Bulk Records dialog box

When you select a different user and click OK, Microsoft Dynamics CRM reassigns all of the records from the old user to the new user you specified. Although this provides a quick and easy method to reassign records, it moves all of the old user's records regardless of their state. This typically does not accomplish what most customers want because it changes the owner of inactive records such as completed activities, qualified leads, won opportunities, and so on. This caused some confusion for one of our customers because it changed the data that appeared in the commission and sales activity reports! In addition, the bulk reassign can confuse users looking at the activity history for a particular account because the owner of the old inactive activities changes from the previous user to the new user.

Note Reassigning records only changes the owner of a record. It does not change the user who created or modified the record; that information stays intact.

In light of these constraints, we consider the Reassign Bulk Records option something of a brute force tool that you should use only in limited circumstances.

Manually Reassign Active Records

Although no one likes to see the word *manual* appear in any task description, we strongly encourage you to reassign the records manually from the old user to a new user instead of using the Reassign Bulk Records tool. By doing so, you maintain the history of the data linked to the previous user. At first this may appear easy to accomplish because you can simply select the active records for the various entities and assign them to a new owner. For example, you could select just the open leads, cases, and opportunities and assign them to a new owner. However, Microsoft Dynamics CRM maintains entity relationships between records so that actions taken against a parent record cascade down to its children records. For example, when you change the owner of an opportunity record, Microsoft Dynamics CRM automatically changes the owner of the activities related to that opportunity based on the relationship configuration.

More Info We explain entity relationships and cascading actions in detail later in Chapter 9, "Entity Relationships."

By default, Microsoft Dynamics CRM cascades the reassign action to all of the children records in almost all of the entity relationships. In this scenario, if you change the owner of an Account, all of its related records such as Cases, Opportunities, Quotes, Orders, and so on will also receive the new owner even if those related records are inactive. Likewise, when Microsoft Dynamics CRM changes the owner of the related records, it will cascade that reassignment action to all of the children records of the Cases, Opportunities, Quotes, Orders, and so on. Again, that reassignment would also apply to both active and inactive records, which most customers would not want to happen.

To avoid this scenario, we recommend that you change the default entity relationship behaviors before you start reassigning records. You should configure the cascading behavior from Cascade All to Cascade Active so that it takes action only against active children records, as shown in Figure 3-7 for the Account to Task entity relationship.

Unfortunately, you can't change this entity relationship behavior for the entire system in one place. You need to configure the relationships manually for each of the various entity relationships.

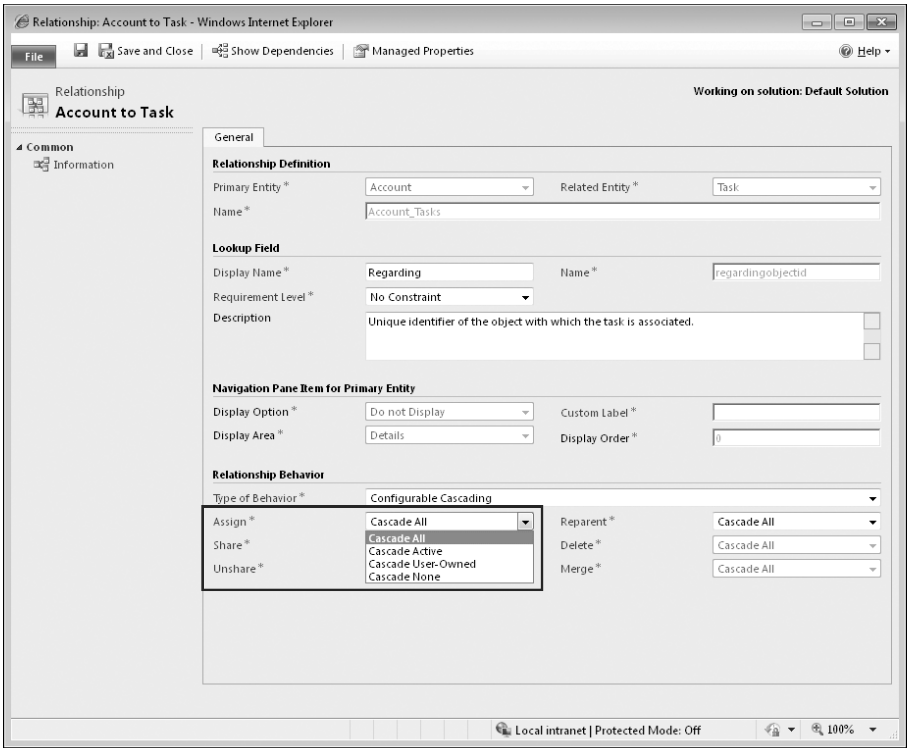


FIGURE 3-7 Changing the default relationship behavior between entities before reassigning records

Monitoring License Usage for Compliance

With the on-premise version of Microsoft Dynamics CRM, you need to keep track of the number of active Microsoft Dynamics CRM licenses your company uses to ensure that you do not use more licenses than you should. As we mentioned earlier, Microsoft Dynamics CRM licensing trusts customers to monitor their own usage because the software lets customers add as many servers and users as they want (regardless of how many they actually purchased). Therefore, the administrator needs to monitor license usage on a consistent basis to ensure compliance.

> **Note** Microsoft Dynamics CRM Online licensing differs from on-premise licensing because it uses a hard enforcement on the number of user licenses. If you try to add more users than you have licenses for, the system will send you an error message and reject the action.

If you want to view a summary of your current active licenses, start the Microsoft Dynamics CRM Deployment Manager on the Microsoft Dynamics CRM web server, right-click the Microsoft Dynamics CRM link in the left column, and select Properties. The Microsoft Dynamics CRM Properties dialog box opens. Click the License tab (shown in Figure 3-8).

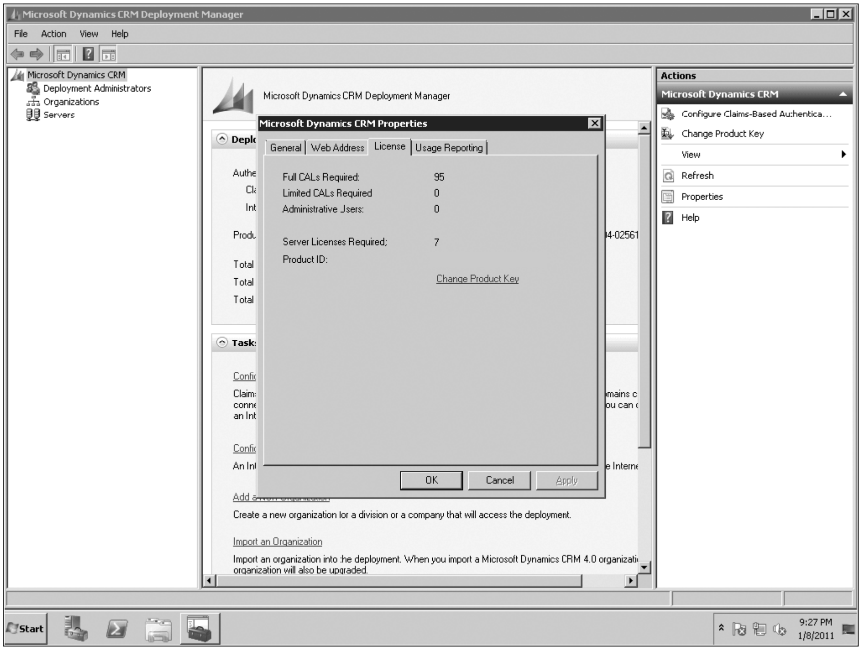


FIGURE 3-8 License summary in Microsoft Dynamics CRM Deployment Manager

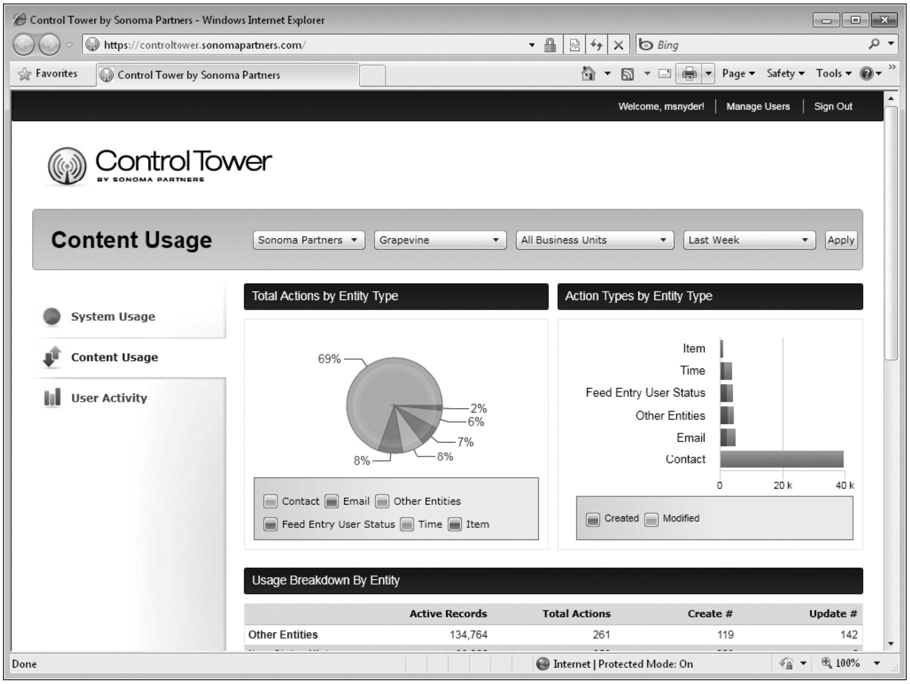
As you can see in Figure 3-8, Microsoft Dynamics CRM reports the number of different users for each of the different license types: Full, Limited, and Administrative. It also shows how many server licenses should be owned. You must purchase the corresponding number of licenses to match the number of Full and Limited users in your system, but you do not need to purchase user licenses for administrative users.

Microsoft Dynamics CRM allows you to set up multiple organizations in a single Microsoft Dynamics CRM deployment, and this license summary will display the total number of users across all of the organizations. Unfortunately, you cannot run this license summary tool for a single organization, so if you need this information detailed by organization, you must log on manually to each organization and perform a query to determine the number of active users in each category.

Measuring End User Usage

The license summary shows you how many enabled Microsoft Dynamics CRM users your system contains. However, just because you enable a user to access Microsoft Dynamics CRM, that doesn't mean that user is actively using the system! Because Microsoft Dynamics CRM licensing is based on a named user model (not a concurrent user model), you're paying a license fee for each user you enable. To maximize your software investment you should make sure that the enabled users actively use Microsoft Dynamics CRM.

Unfortunately, Microsoft Dynamics CRM doesn't include any pre-built tools or utilities to provide you with end-user usage reporting. You can create your own custom reports based on data fields such as created on, modified on, and possibly the audit data. Unfortunately, relying just on this data to provide you with usage data might not tell you the complete story because auditing might not be enabled for all entities and all data fields. In addition you should be careful about enabling audit for *everything* because that might negatively impact your system performance.



To help provide our Microsoft Dynamics CRM customers with detailed usage information, our firm Sonoma Partners created a proprietary cloud-based solution named Control Tower that helps customers answer these questions:

- Are people using your CRM system?
- How are people using your CRM system?
- How is a specific user interacting with your CRM system?

The Control Tower application takes nightly snapshots of the data and provides web-based reports from an Azure-hosted website. By offloading the reporting to a different server and not requiring auditing to be enabled for all entities, Control Tower provides a quick and efficient end-user reporting tool. For more information about Control Tower, visit *http://www.sonomapartners.com*.

Security Roles and Business Units

As we explained earlier, Microsoft Dynamics CRM uses a combination of role-based security and object-based security to determine what users can see and do in the deployment. Instead of configuring security for each user one record at a time, you assign security settings and permissions to a security role, and then you assign one or more security roles to a user. Microsoft Dynamics CRM includes the following 14 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
- **Delegate** A user that can perform actions on behalf of another user
- **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
- **Schedule Manager** A user who manages services, required resources, and working hours
- **Scheduler** A user who schedules appointments for services
- **System Administrator** A user who defines and implements the process at any level
- **System Customizer** A user who customizes Microsoft Dynamics 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 predefined rights and permissions typically associated with these roles so that you can 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.

When you assign multiple security roles to a user, Microsoft Dynamics CRM combines the user rights so that the user can perform the highest-level activity associated with any of her roles. In other words, if you assign two security roles that have conflicting security rights, Microsoft Dynamics CRM grants the user the least-restrictive permission of the two. Security roles combine together to grant users all of the permissions for all of their assigned security roles. If one of a user's security roles grants a permission, that user *always* possesses that permission, even if you assign him another security role that conflicts with the original permission. For example, consider a fictional Vice President of Sales named Connie Watson. Figure 3-9 shows that Connie has two security roles assigned to her: Salesperson and Vice President of Marketing.

FIGURE 3-9 Multiple security roles assigned to a user

In the Microsoft Dynamics CRM default security roles, a user with only the Salesperson security role cannot create new announcements, but the Vice President of Marketing security role can. Because Microsoft Dynamics CRM grants the least-restrictive permission across all of a user's roles, Connie is able to create announcements in this example because she is also assigned the Vice President of Marketing security role.

Security Role Definitions

Before we explain how to modify security roles, we quickly cover the terminology related to security roles. To view and manage the settings for a security role, browse to Administration in the Settings area and click Security Roles. Double-click one of the roles listed in the grid. Figure 3-10 shows the Salesperson default security role settings.

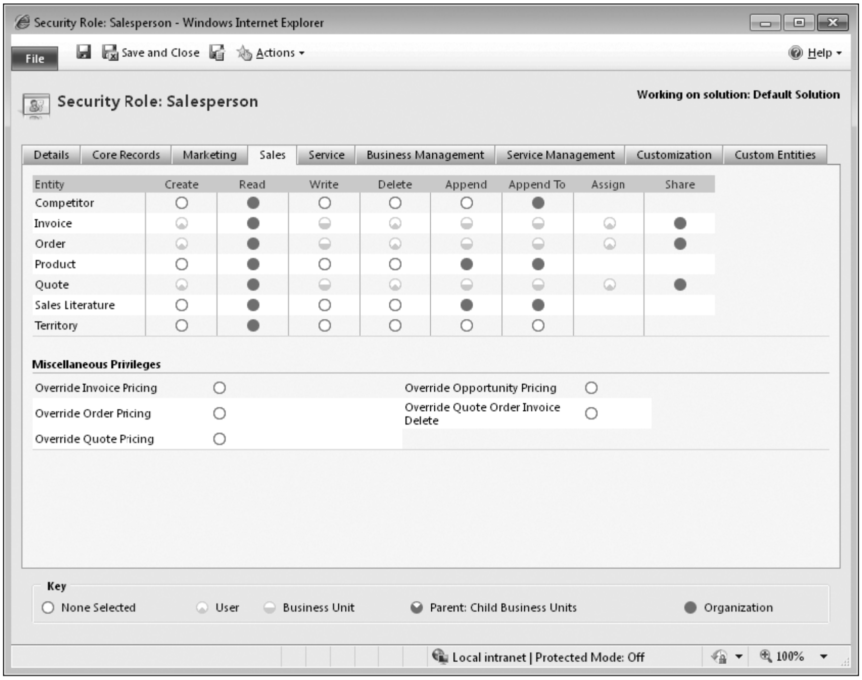


FIGURE 3-10 Salesperson security role settings

The columns in the top table represent entity privileges in Microsoft Dynamics CRM. *Privileges* give a user permission to perform an action in Microsoft Dynamics CRM such as Create, Read, or Write. The bottom section lists additional miscellaneous privileges including Override Quote Pricing and Override Invoice Pricing. Microsoft Dynamics 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 Dynamics 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 organizational 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 her business unit but only read records owned by users in different business units.

> **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 for the Organization access level. However, the different access levels determine on which records in Microsoft Dynamics CRM the user can execute the privilege.

In the following subsections, we 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 3-10), Microsoft Dynamics 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 or team 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 Units 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.

Consider an example scenario to understand access levels in a real-world context. Figure 3-11 shows five business units, six users, and six Contact records.

We 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 to which it is linked. 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 Units	No	No	Yes	Yes	Yes	Yes
Organization	Yes	Yes	Yes	Yes	Yes	Yes

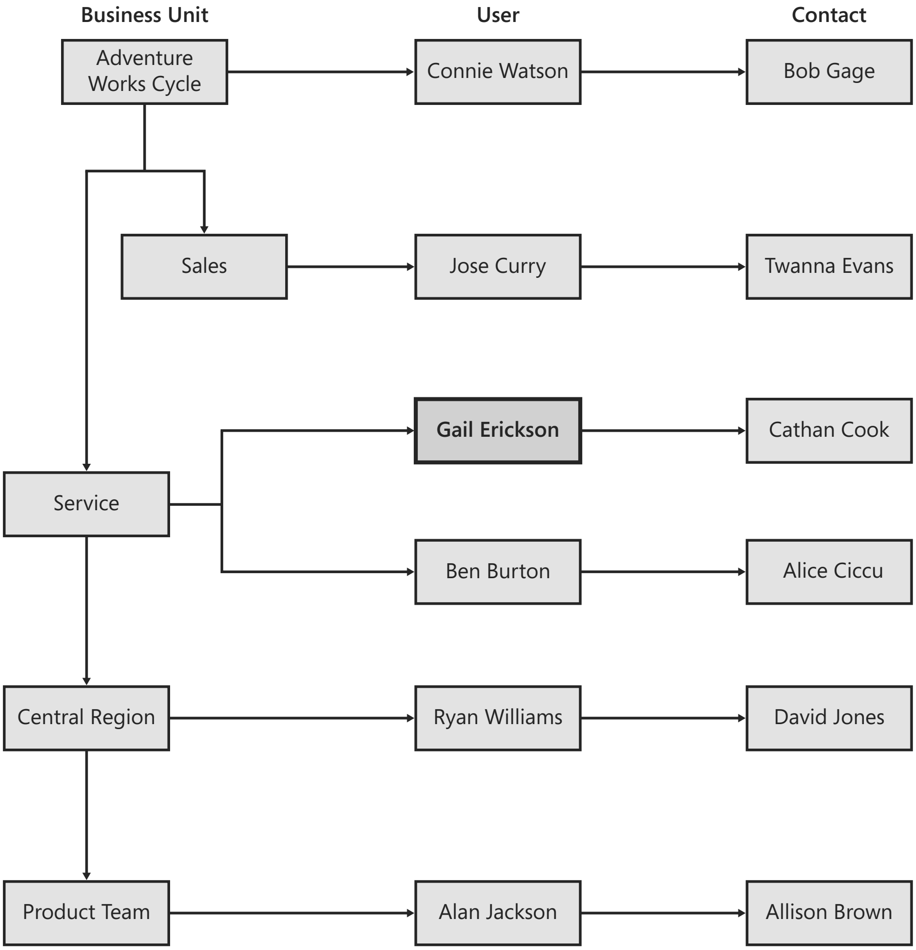


FIGURE 3-11 Access levels example

For the Business Unit access level, Microsoft Dynamics CRM grants 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 Units access level, Microsoft Dynamics CRM grants 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 that the record owner belongs to
- The business unit of the logged-in user

> **Important** Microsoft Dynamics CRM treats records owned by teams the same as if a user in the team's business unit owned it. For example, if team ABC from the Sales business unit owned the Twanna Evans record, the security system would function the same as the user Jose Curry owning the Twanna Evans record.

Table 3-2 summarizes how Microsoft Dynamics 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 nonchild business unit
None	Deny	Deny	Deny	Deny
User	Grant	Deny	Deny	Deny
Business Unit	Grant	Grant	Deny	Deny
Parent: Child Business Units	Grant	Grant	Grant	Deny
Organization	Grant	Grant	Grant	Grant

By now you should have a good understanding of how Microsoft Dynamics CRM determines whether to grant security privileges to users based on access levels. Now we 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 in Microsoft Dynamics CRM, and you bundle privileges together in 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 Dynamics CRM such as Mail Merge and Export to Excel. In this section, we explore the following topics:

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

Entity Privileges

As Figure 3-10 showed earlier, privileges such as Create, Read, and Write apply to the entities in Microsoft Dynamics 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

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

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

In Microsoft Dynamics CRM, you can also 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.

More Info If you're wondering what the Web Wizard entities are, they refer to web pages Microsoft Dynamics CRM Online users see during sign up. They are only for Microsoft Dynamics CRM internal use—any changes you make will not have any impact.

Troubleshooting Entity Privilege Errors

Sometimes when you're adjusting Microsoft Dynamics CRM security roles, you may later get an error message telling you that the user does not have permission to complete an action. You may think to yourself, "What in the world is this talking about?" After you review the security roles, you wonder which privilege could *possibly* be missing that would result in this error.

Many times you will need to grant a user a security privilege that would not be obvious to you by simply looking at the security role configuration screens. For example, would you guess that you need the Append To Order privilege before you can create an Appointment record?

If you find yourself getting stuck trying to track down the appropriate privileges that a user needs to perform an action, we recommend that you refer to the Microsoft Dynamics CRM software development kit (SDK) because it contains documentation regarding the various privileges users need to complete certain actions. You can find this information in the "Privileges by Message" section of the SDK. For example, you'll see something like this for the privileges needed to create an appointment:

- prvAppendActivity
- prvAppendToAccount
- prvAppendToActivity
- prvAppendToContact
- prvAppendToContract
- prvAppendToIncident
- prvAppendToInvoice
- prvAppendToLead
- prvAppendToOpportunity
- prvAppendToOrder
- prvAppendToQuote
- prvAppendToService
- prvCreateActivity
- prvReadActivity
- prvShareActivity

Although at first this list appears a little cryptic, you can use this information as a starting point to determine which privileges the user will need in a security role to perform the desired action. Unfortunately, in Microsoft Dynamics CRM 4.0 we did find a few instances for which the SDK documentation did not list *all* of the necessary privileges. In those instances, we recommend you enable system tracing for the server. The trace should capture the exact privilege identifier, which you can use to look up the missing privilege. Because this approach requires server and database administration rights it won't work with Microsoft Dynamics CRM Online. Therefore, you would need to rely on a more tedious trial-and-error method to toggle off and on the other privileges in the security role to figure out what the user needs.

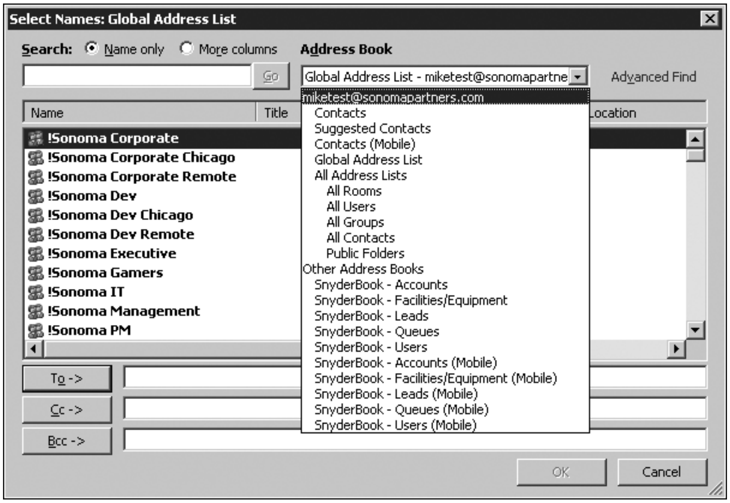
Miscellaneous Privileges

In addition to entity privileges, Microsoft Dynamics CRM includes additional miscellaneous privileges in each tab of the security role editor. The privilege name often provides enough information about what the privilege covers, but sometimes the description can leave you guessing. This is especially true for miscellaneous privileges that relate to areas of the application that you may not use often. In the following list, we provide a little more description about each of the miscellaneous privileges and, in some cases, where to find the related feature.

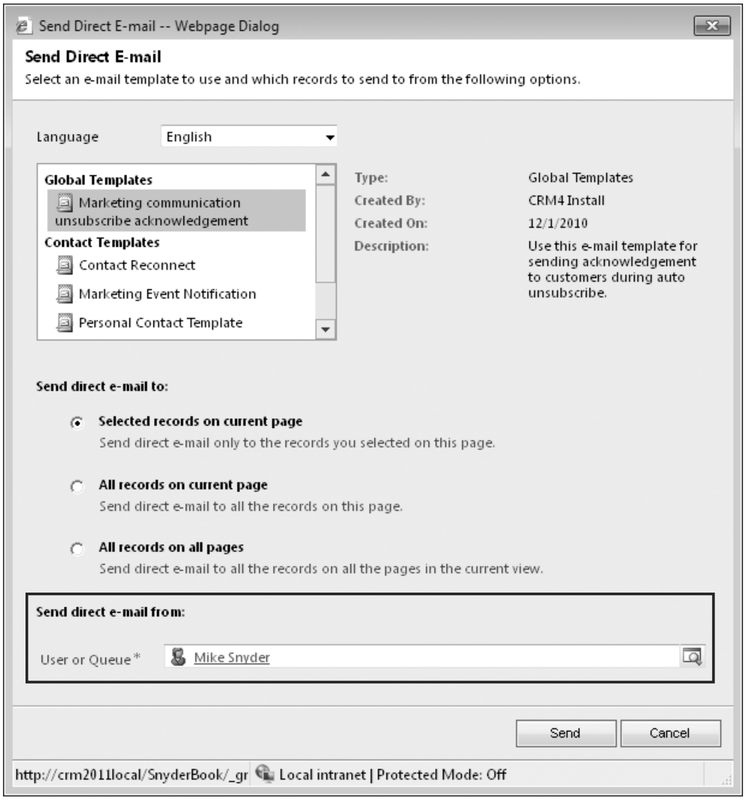
- **Add Reporting Services Reports** Permits the user to upload an existing Reporting Services report file to Microsoft Dynamics CRM. Reporting Services files are in the RDL format. This privilege differs from the Create privilege of the Report entity, which refers to creating a new report by using the Report Wizard or by adding another file type (such as an Excel file or PDF report).
- **Delete Audit Partitions** Permits the user to delete an audit partition. Microsoft Dynamics CRM creates audit partitions for each three-month period.
- **Publish Duplicate Detection Rules** Permits the user to publish duplicate detection rules configured in the data management section.
- **Publish Mail Merge Templates to Organization** Permits the user to make mail merge templates available to the entire organization. Individually owned mail merge templates follow the standard Microsoft Dynamics CRM security model.
- **View Audit History** Permits the user to access the Audit History located on an individual record.
- **View Audit Summary** Permits the user to access the Audit Summary View located in the Auditing area of Settings.
- **Bulk Delete** Permits the user to use the Bulk Deletion Wizard.
- **Manage User Synchronization Filters** Provides the ability for a user to modify a different user's synchronization and offline filters in Microsoft Dynamics CRM for Outlook. Please note there is no user interface to do this—it must be accomplished through custom programming.
- **Publish E-mail Templates** Permits the user to make a personal email 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 the user can click Make Template Available to Organization in the ribbon.
- **Publish Reports** Allows a user to make a report available (or viewable) to the entire organization. For Reporting Services reports, this privilege will also allow the user to publish the report to the Reporting Services web server for external use.

- **View Audit Partitions** Allows a user to view the audit log partitions.
- **Configure Internet Marketing module** Permits a user to configure the Internet marketing module that can be set up as an external web page that captures inbound leads.
- **Use Internet Marketing module** Permits a user to access the Internet marketing module data, but not set it up or configure it.
- **Create Quick Campaign** Permits the user to create a single activity and distribute it to multiple records by using a marketing quick campaign. The user also needs to have the correct security configuration to create the quick campaign activities.
- **Override Quote Pricing** Permits the user to override the calculated price of a quote (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 the system-generated price of an invoice and manually enter new invoice pricing. Users can access the Override Price button when they're editing an Invoice Product attached to an Invoice.
- **Override Order Pricing** Permits the user to override the system-generated price of an order and manually enter new order pricing. Users can access the Override Price button when they're editing an Order Product attached to an Order.
- **Override Opportunity Pricing** Permits the user to override the system-generated price of an opportunity and manually enter new opportunity pricing. Users can access the Override Price button when they're editing an Opportunity Product attached to an Opportunity.
- **Override Quote Order Invoice Delete** Permits the user to delete inactive Quotes, Orders, and Invoices.
- **Publish Articles** Permits the user to publish unapproved Knowledge Base articles. Users access the Approve (publish) button on the grid toolbar of the Unapproved Article Queue located in the Knowledge Base area.
- **Act on Behalf of Another User** Provides delegation capabilities to a user.
- **Assign Manager for a User** Allows a user to change the manager of an existing user.
- **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. This feature does not apply to all entities.
- **Enable or Disable Business Unit** Permits the user to enable or disable business units.

- **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 toolbar.
- **Go Offline** Permits a user with Microsoft Dynamics CRM for Outlook with Offline Access 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 work premises, the offline option raises a potential security question that you must consider.
- **Mail Merge** Permits the user to create mail merge items such as letters, email messages, envelopes, and labels. This privilege refers to creating mail merge items using Microsoft Dynamics CRM for Outlook.
- **Override Created on or Created by for Records during Data Import** Permits the user to include new values for the Created on and Created by fields while using the Data Import Wizard. This would be helpful when you're migrating data from an old system into Microsoft Dynamics CRM and you want to preserve the original values. Without this privilege, all imported records imported by a user will be stamped with that user's information for Created by and Created on.
- **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 toolbar. You cannot vary this privilege by entity type.
- **Reparent Business unit** Just as it sounds, permits the user to reparent a business unit.
- **Reparent User** Again just as it sounds, permits the user to reparent a different user.
- **Send Invitation** Permits a user to send an email invitation to an employee to join the organization. This privilege applies only to Microsoft Dynamics CRM Online deployments.
- **Update Business Closures** Permits the user to modify business working hours and closure information. Users access the Business Closures information in the Settings area.
- **Approve E-mail Addresses for Users or Queues** Permits the user to approve valid email addresses for users and queues. This additional security step prevents a user from fraudulently gaining access to a mailbox he or she should not be able to access.
- **Assign Territory to User** Permits the user to add or remove users from a sales territory. Users access the Sales Territories information in the Business Administration section of the Settings area.
- **CRM Address Book** Permits a user of the Microsoft Dynamics CRM clients for Outlook to select CRM records from his or her address book in Outlook.



- **Enable or Disable User** Permits the user to enable or disable users.
- **Go Mobile** Permits the user to access the Microsoft Dynamics CRM Mobile Express user interface.
- **Language Settings** Permits the user to access the language settings for the organization, including installing new language packs.
- **Merge** Permits the user to merge two records into a single record. Users with this privilege can access the Merge feature from the grid toolbar.
- **Perform In-sync Rollups on Goals** Permits the user to roll up goal data on demand, instead of waiting for the next scheduled update period.
- **Read License Info** Permits the user to access information about the Microsoft Dynamics CRM license information via the Application Programming Interface. No user interface is associated with this privilege.
- **Reparent Team** Permits the user to reparent a team.
- **Send E-mail as Another User** Permits the user to select a different user or queue for the From address of an email message sent with the Microsoft Dynamics 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 email (such as Contact or Account)
  - Read privileges on the E-mail Template entity



- **Sync to Outlook** Permits a user of Microsoft Dynamics CRM for Outlook to synchronize Microsoft Dynamics CRM data such as Contacts, Tasks, and Appointments to his or her Outlook file.
- **Web Mail Merge** Same as the Mail Merge privilege, but permits the user to access the mail merge functionality in the web interface without using Microsoft Dynamics CRM for Outlook.
- **Browse Availability** Permits the user to view the Service Calendar located in the Service area.
- **Delete Own Calendar** Permits users to delete the service calendar related to their work hours.
- **Search Availability** Permits the user to search for available times when scheduling a Service activity.
- **Create Own Calendar** Permits users to create new work hours for themselves.
- **Read Own Calendar** Allows users to see their own work hours and calendar.
- **Write Own Calendar** Allows users to modify their work hours and the associated calendar.

- **Execute Workflow Job** In addition to proper permissions to the System Job entity, users need this privilege to execute manual workflow rules or automatic workflow rules.
- **Import Customizations** Permits the user to import a configuration file into Microsoft Dynamics CRM.
- **Modify Customization Constraints** This privilege does not impact the system; Microsoft refactored this feature but did not remove the privilege.
- **Export Customizations** Permits the user to export system customizations from Microsoft Dynamics CRM to a configuration file.
- **Publish Customizations** Permits the user to publish customizations applied to an entity.
- **ISV Extensions** This privilege exists for backward compatibility with Microsoft Dynamics CRM 4.0. During the upgrade process, Microsoft Dynamics CRM converts custom 4.0 controls to ribbon buttons in Microsoft Dynamics CRM 2011 and then uses this privilege to determine which ribbon buttons users should see in the upgraded environment.

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 simply selecting the access level for a security role, saving the role, and then logging on to Microsoft Dynamics 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 may want to impersonate a different user when you log on to Microsoft Dynamics CRM. We explained earlier in the chapter how you can modify your Internet Explorer security settings so that Microsoft Dynamics 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.

Privilege Impact on Application Navigation

Microsoft Dynamics CRM includes more than 100 entities and thousands of features in the Sales, Marketing, and Customer Service areas. However, very few organizations will use *all* of the entities that Microsoft Dynamics 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 is to modify user security roles and privileges, which also changes the user interface.

Important You should modify security roles—instead of modifying the site map—to hide areas of Microsoft Dynamics CRM that your organization does not use. By modifying security roles, you also can 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 12, "Solution: Client Extensions (Ribbon and SiteMap)," 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 Dynamics 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 14 default security roles include an Organization access level for the Read privilege on all of the entities, so 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 create a streamlined user interface that can help new users learn the system more quickly and that lets existing users navigate more efficiently.

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

Figure 3-12 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.

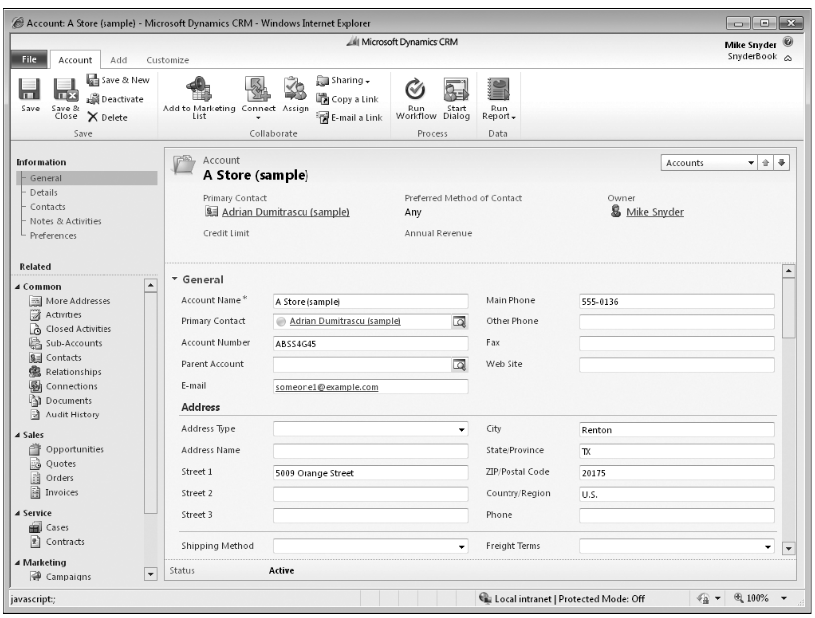


FIGURE 3-12 Account record as seen by a user with the default Customer Service Representative security role

In reality, most customer service representatives don't need to see all of this information on an Account record. Instead, 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 can appear like the one shown in Figure 3-13.

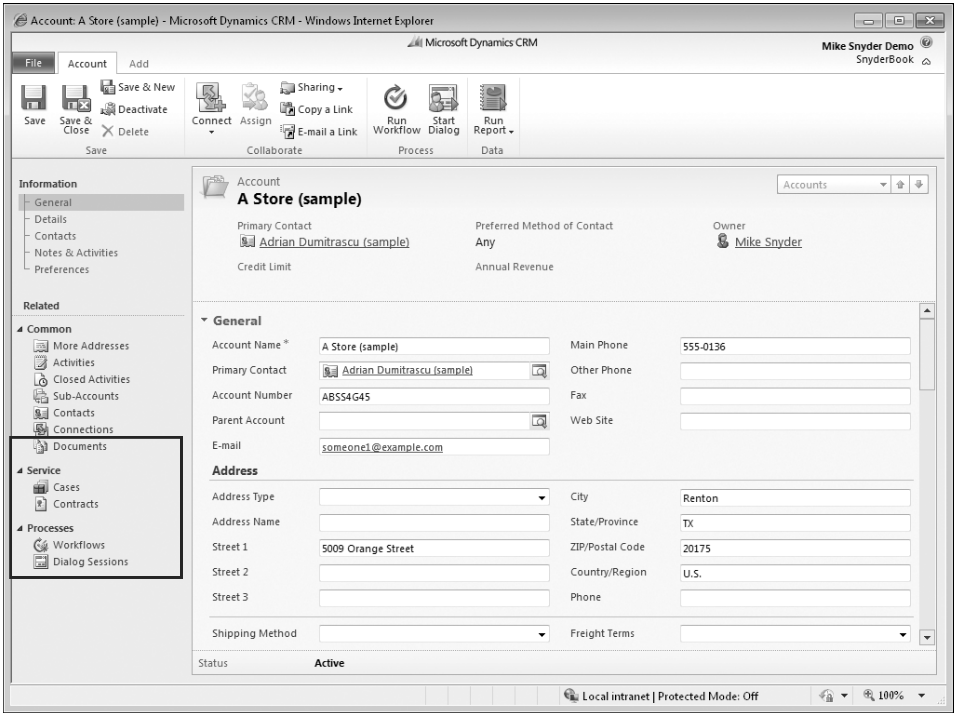


FIGURE 3-13 Account record as seen by a user with a revised Customer Service Representative security role

You can see that we removed the Sales and Marketing links from the navigation pane by modifying the security role. This provides a much cleaner user interface, which your users will appreciate. Likewise, you could also revise the Salesperson security role so that salespeople see only entities that they need to perform their jobs.

Security Role Inheritance

If your deployment includes multiple business units, you must understand how Microsoft Dynamics CRM inherits security roles in the business unit hierarchy. When you create a new security role in a business unit, Microsoft Dynamics 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 Dynamics 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 3-14.

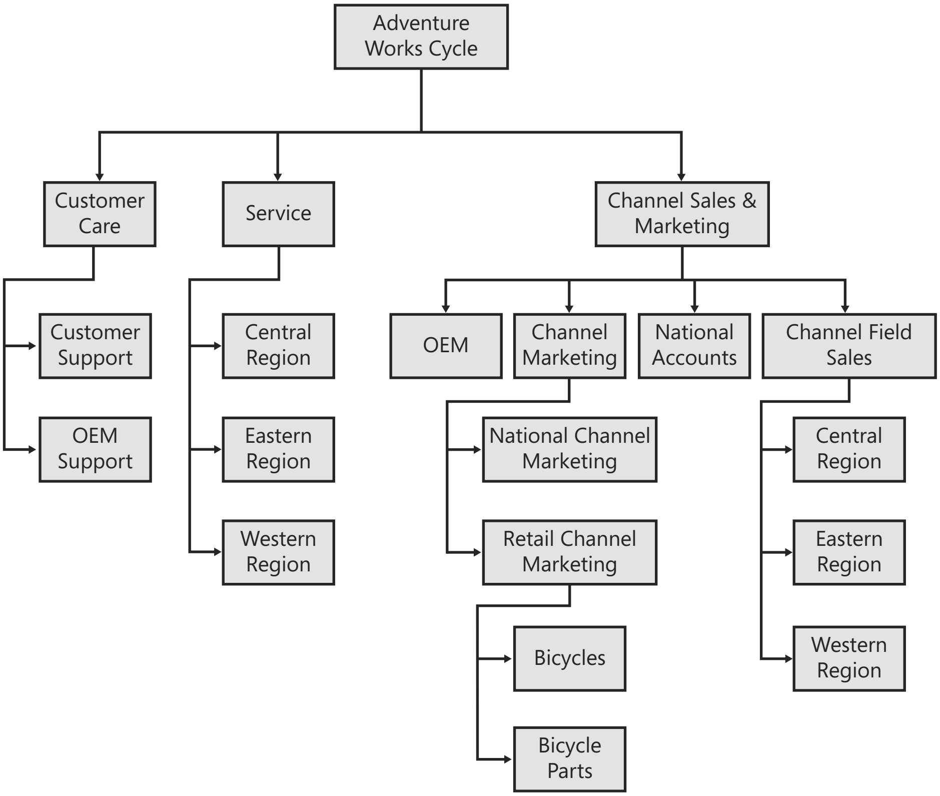


FIGURE 3-14 Organizational structure for the sample company Adventure Works Cycle

If you create a new security role called Director assigned to the Customer Care business unit, Microsoft Dynamics CRM automatically creates noneditable copies of the Director security role in the Customer Support and OEM Support business units because they are children of the Customer Care business unit. Any changes you make to the Director security role are automatically propagated to all of the Director security roles in the child business units. When you view the security roles for one of the other business units, such as Service or OEM, you do 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 create a new security role, Microsoft Dynamics 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 lookup if you want to create a role in a nonroot business unit.

Every user belongs to only one business unit, and you can assign users security roles only 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 Dynamics CRM inherits security roles to children business units, you cannot make the privileges of a security role be different for each business unit. However, you can create a varying number of security roles for each business unit in 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.

Field Level Security

So far we reviewed security role and configuration settings from an entity perspective, but what if there are sensitive data fields on the entity record that you want to secure? We refer to managing the securing of a single field as *field level security*. Some examples of data fields that you want to secure might include:

- A contact's social security or credit card numbers
- An account's sales numbers
- A lead's ranking or priority

In the contact example, it might be OK if a user had the ability to edit or view all of the contact's information *except* for the social security number. However by giving a user a security role with the edit privilege to the contact entity, that user could edit *all* of the contact fields. Fortunately, Microsoft Dynamics CRM 2011 includes a new field level security feature that allows you to configure security permissions down to an individual field level. Figure 3-15 shows how Microsoft Dynamics CRM could lock down the social security field so that certain users could not view or edit the data in the field. You can also see that Microsoft Dynamics CRM includes a key icon to indicate to users that the field is secured.

> **Tip** Microsoft Dynamics CRM always displays the masked out characters on the form in a secured field if a user does not have access. This is true even if that data field does not contain any data.

Field level security extends beyond the record form to cover *all* aspects of the Microsoft Dynamics CRM, including the advanced find feature, the audit history, Microsoft Dynamics CRM for Outlook with Offline Access and the programming API. Therefore, if a user does not have access to a specific field, Microsoft Dynamics CRM will honor that restriction everywhere in the system. The field security model even allows users to *share* secured fields on a record with other users that might not have access to the secured field (assuming the sharer has the appropriate sharing security settings to do so).

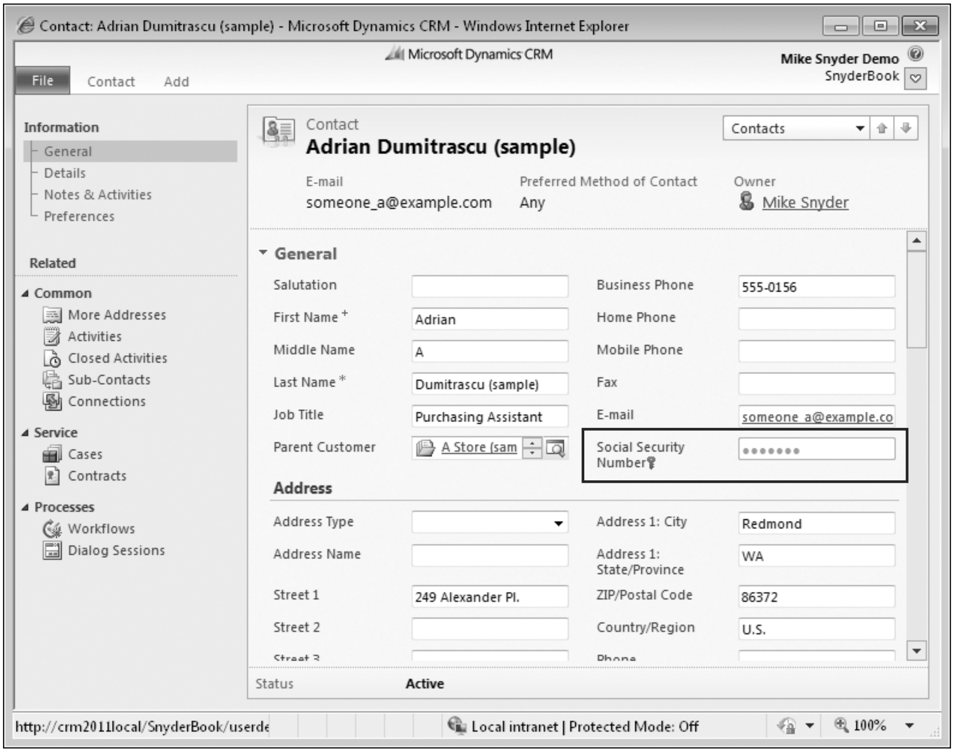


FIGURE 3-15 Field level security activated on the social security number field

Setting up field level security takes a few simple steps:

- Enable field security for the data field you want to secure.
- Create a field security profile and assign to users/teams.
- Edit field level permissions with the field security profile.

Enabling Field Security

By default none of the Microsoft Dynamics CRM data fields have field level security enabled. To enable field level security for a specific field, you must select the Enable button for Field Security on the field editor (Figure 3-16). Chapter 6, "Entity: Fields and Option Sets," covers how to use the entity and field editor in detail.

Unfortunately, you can only enable field security for custom fields that you add to the system. You cannot turn on field security for the default system fields created in the initial Microsoft Dynamics CRM installation. Some of the default fields that you might want to enable field security for (but cannot) include contact birth date, contact home phone, contact mobile phone, and so on. Of course you could create new custom fields to track this data and then secure it. However, if you used custom data fields, the information would not synchronize to a user's Outlook file, so you must consider the trade-off benefits between securing those fields versus having the ability to synchronize phone numbers into Outlook.

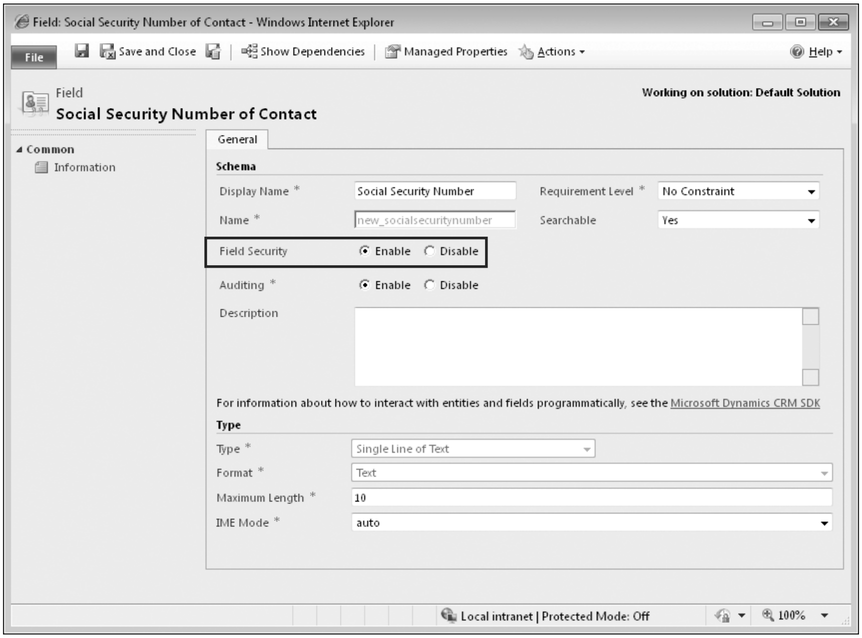


FIGURE 3-16 Enabling field level security for a field

When you enable field security, no user can access that field until you explicitly give him or her permission. However, users with the System Administrator security role will always have full access to all secured fields in Microsoft Dynamics CRM.

Field Security Profiles

Like security roles, field security profiles offer a way for administrators to group together a set of security settings. Obviously the field security profiles apply to field security settings. To manage the field security profiles, click the Settings button, click Administration, and then click Field Security Profiles. By default Microsoft Dynamics CRM includes a system administrator field security profile.

When you create new profiles, try to create them in functional groups to help reduce the amount of maintenance work required. To create a new profile, click the New button in the grid and a new form will open. After you name it, click Save. Now you can add the users and teams that this field security profile should apply to.

Now click the Field Permissions link in the left-hand navigation to start editing the field level permissions. You will see a list of all the data fields in the system with field security enabled (Figure 3-17).

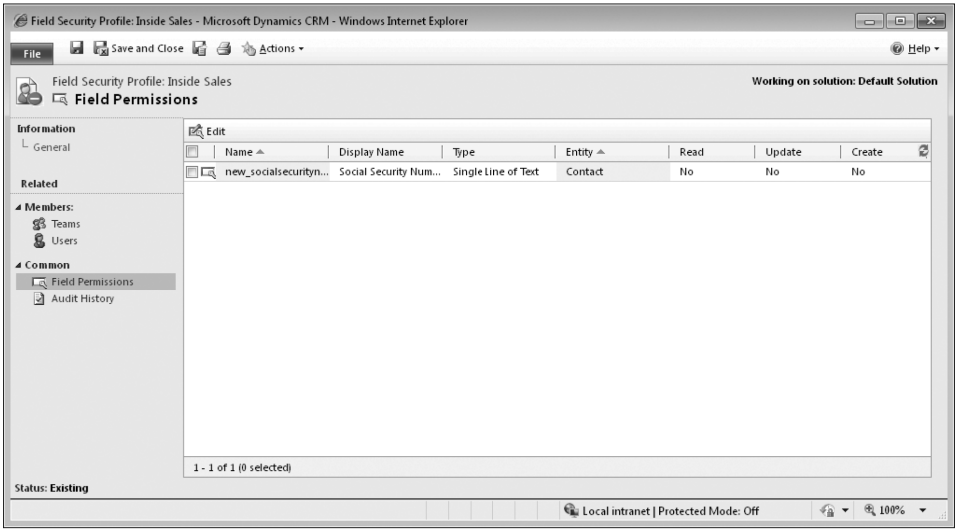


FIGURE 3-17 List of fields with field security enabled

Select which secured fields you want to work with and then click the Edit button to launch the Edit Field Security dialog box, as shown in Figure 3-18.

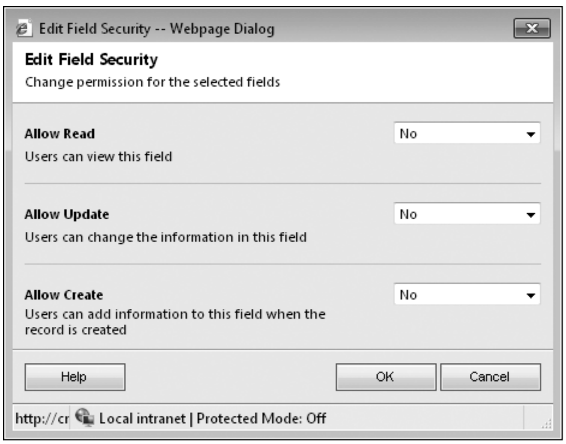


FIGURE 3-18 Edit read, update, and create permissions for a secured field

By changing these values to Yes, users or teams with this field security profile assigned to them will now be able to perform reads, updates, or creates on the secured fields. The Allow Create option is interesting because this allows the user to enter data in this field while creating a record, but when the record is created the field is secured and the user can no longer access it.

In summary, field level security is a powerful new feature in Microsoft Dynamics CRM 2011 that allows administrators to set up a very detailed and flexible security model to meet most organization's needs.

Sharing Records

Despite the numerous security options and configuration choices 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) that has 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 is not possible using the security configurations covered so far. If Laura gives 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 Dynamics 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 usually have the necessary privileges to do so.

To share records, users must have a security role assigned the appropriate Share privilege. To set up a share such as the one described in the Woodgrove Bank example, open the entity record and click Sharing on the Actions menu of the entity menu bar. In the Share dialog box, select the users with whom you want to share this record by clicking Add User/Team. Use the Lookup tool to find the records that you want, and then click OK. Microsoft Dynamics CRM adds the users to the page, as shown in Figure 3-19.

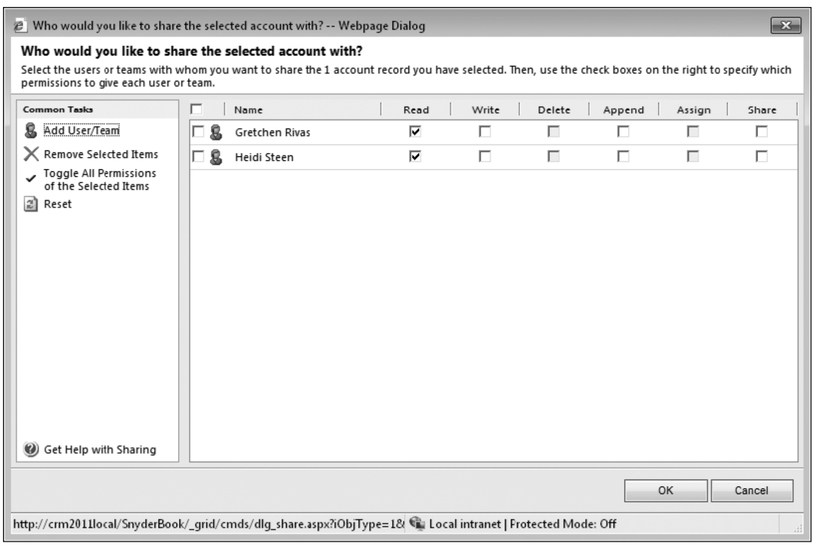


FIGURE 3-19 Sharing records with users

Next, specify which privileges you want to share with these users. In the Woodgrove Bank example, Laura Owen can select the Read and Write privileges so that Gretchen and Heidi can edit this record. Note that the Delete and Assign privilege check boxes are unavailable 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 possess the privilege themselves. For example, a user cannot share Delete privileges for a record if she does 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 of the privileges that you want to revoke.

Tip In addition to sharing records through the user interface, you can also programmatically share records using the application programming interface. Therefore you could set up automation to share records with specific users or teams when certain conditions are met. However, take care not to create too many automated shares because the user interface doesn't contain a tool to help you quickly identify a group of records with sharing permissions (though you can examine one record at a time). For example, it would be difficult to answer the question "Which of the existing accounts in the system have shares set up on them?" Therefore, creating too many shares might become a maintenance headache down the road.

Sharing with Teams

In the Coho Vineyard & Winery example, it is easy to set up the share because you need to select only two users. But what if Laura wants to share the Woodgrove Bank record with 100 users? What if she wants to share five different records with those same 100 users? It would be a pretty miserable and time-consuming process to share records manually one user at a time in these examples. Fortunately, with Microsoft Dynamics CRM you can set up and configure teams of users to expedite the sharing process. By sharing a record with a team instead of with individual users, you do not have to select user records manually 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 participate in the share.

You can create and modify teams by browsing to Administration in the Settings area, and then clicking Teams. When you create a team, you specify the business unit that the team belongs to, and then you simply add members to the team.

If you use a large number of teams, you can configure the security settings so that users see only a subset of all of the teams. To do this, configure the Team entity privilege in 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 grant a security role only 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. By using this type of configuration, you can 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).

Sharing Secured Fields

In addition to sharing entire records between users, you can also shared secured fields, assuming the sharing user has access to the secured fields. To share secured fields, click the Sharing button in the ribbon and then select Share Secured Fields (Figure 3-20).

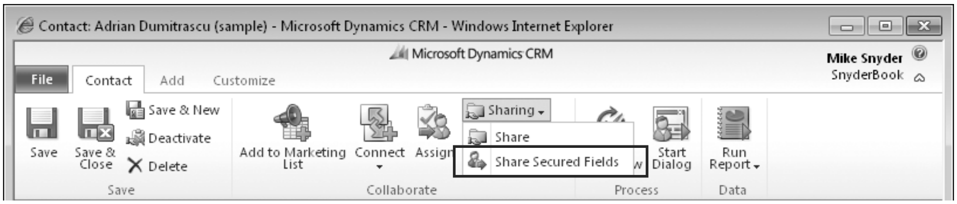


FIGURE 3-20 Sharing secured fields

After you click this button, Microsoft Dynamics CRM will launch a sharing dialog box (as seen in Figure 3-21) where the sharer can select which secured fields and permissions he or she wants to share. Just like record level sharing, you can shared secured fields with specific users or teams.

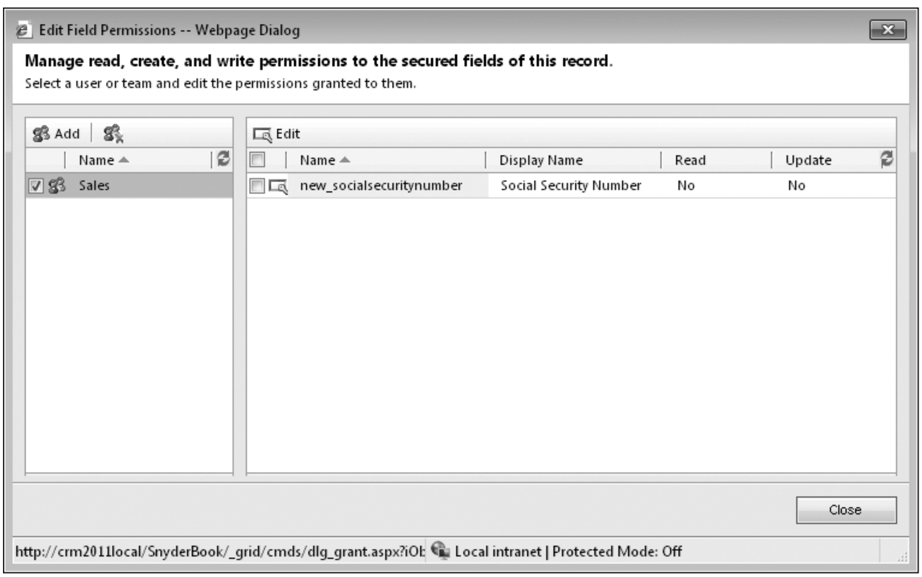


FIGURE 3-21 Sharing secured fields

Sharing and Inheritance

When you share a record with a team or user, child entities of the shared record inherit the same sharing settings as the parent record. In the Woodgrove Bank example, Gretchen and Heidi can 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. A record with inherited sharing privileges can also have its own sets of sharing privileges. and Microsoft Dynamics CRM maintains two different sets of sharing privileges for the 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 has an access level of None Selected for the Activity entity, she is not able to view activities related to Woodgrove Bank even if someone shares Read privileges with her for that Account record. Likewise, she needs to have at least a User access level for the Account entity to view the Woodgrove Bank account record after Laura shares it with her.

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

Summary

Microsoft Dynamics CRM includes a powerful and highly configurable security model that you can use to configure and restrict information access according to your business needs. The on-premise version of Microsoft Dynamics CRM uses Active Directory to manage user accounts and passwords. On-premise users accessing Microsoft Dynamics CRM by the local intranet authenticate with Integrated Windows authentication, whereas users accessing Microsoft Dynamics CRM by an Internet-facing deployment use claims-based authentication. All users of Microsoft Dynamics CRM Online use Windows Live ID as their user authentication method.

By combining role-based and object-based security settings with your organization's business unit structure, in Microsoft Dynamics CRM you can accommodate very complex security and information access needs. Field level security allows administrators to secure specific data fields, providing even more control over access to sensitive information. Microsoft Dynamics CRM also supports project-based and collaborative work by enabling users to share records with teams and individual users.

Index

Symbols and Numbers

A

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

W

X