



# **COOKBOOK** Role-based Security

## **Role-based Security**

*Web Site Factory* applications rely on *Microsoft ASP.NET* for security infrastructure. In *ASP.NET* applications, each user is assigned one or several roles. The roles that a user has determine what a user is able to do. For example, only users with the *Administrator* role can access the *Membership Manager*. You can secure your pages, fields, and the various actions through roles.

#### **Pages**

The current page being displayed does not have a user logged in. The only page available is *Home*, both on the *Site Map* and on the menu bar. The membership bar allows us to sign in. By default, there are two accounts available for use, administrator and standard user. Let's log in as administrator.

		Login to this website	Help
瓣 MyCompany		User Name: admin	
Home		Password:	ns •
Home > Home		Remember me next time	
Start		Forgot your password?	
Please select a page link in the table of contents below.	Sign in to access the protected site content.		
Site Map	Instructions		
Home	Two standard user accounts are automatically creater membership option has been selected for this applicat	d when application is initialized if ion.	
	The administrative account <b>admin</b> is authorized to ac membership manager. The standard <b>user</b> account is a with the exception of membership manager.	cess all areas of the web site and allowed to access all areas of the web s	ite
	Move the mouse pointer over the link <i>Login to this we</i> the page and sign in with one of the accounts listed b	<i>b site</i> on the right-hand side at the top elow.	of
	Administrative account: admin / admin123%		
	Standard user account: user / user123%		

You can see that after logging in, the sitemap and menu bar has been expanded. More options are available, including the *Membership* page.



Navigate to the *Membership* page. On this page, we can create, modify, and delete *Users* and *Roles*. This enables a high degree of control over who can access the application. However, this page is only

accessible to those users with administrative privileges. When we sign out, you can see that we have been given a redirect URL, and taken back to the home page and prompted to log in.

🖉 Start - Windows Internet Explorer		
€ http://localhost:30134/Northwind/Pages/Home.aspx?ReturnUrl=%2fNorth	hwind%2fPages%2fM 🔻 🖄 🐓 🗙 🚼 Goog	gle 🔎
🖕 Favorites 🖉 Start	🏠 🔻 🗟 👻 🖃	🖶 ▼ <u>P</u> age▼ <u>S</u> afety▼ T <u>o</u> ols▼ @▼
		Login to this website Help
🗱 MyCompany		User Name:
Home		Password:
Home > Home		Remember me next time
Start		Forgot your password?
Please select a page link in the table of contents below.	Sign in to access the protected site content.	Login
Site Map	Instructions	
Home	Two standard user accounts are automatically create membership option has been selected for this applicat	d when application is initialized if tion.

If we log in as a standard user, then we will be redirected again. The navigation enables access to all of the pages in the application except the *Membership* page, which is absent.



Let's change things up a bit. We will change the security so that only those users with administrative privileges will be able to access the *Order Details* page. Run *Code On Time Generator*, click on the project

name, and then press the *Design* button. Click on the *All Pages* tab at the top, and select *Order Details* page.

Project Designer				exit
() Home				
All Controllers All Commands	All Fields All Views All Data Fields	All Pages All User Controls		
This is a list of application pages.				
Quick Find 👂 New 🔻				View: Pages 🔻
Name	Index Title	Path	Style	Roles
Home	1000 Start	Home	Home	n/a
Customers	1010 Customers	Customers	Generic	n/a
Orders	1020 Orders	Customers   Orders	Generic	n/a
CustomerCustomerDemo	1030 Customer Demo	Customers   Customer Demo	Generic	n/a
OrderDetails	1040 Order Details	Customers   Order Details	Generic	Administrators
Employees	1050 Employees	Employees	Generic	n/a
EmployeeTerritories	1060 Employee Territories	Employees   Employee Territories	Generic	n/a
Categories	1070 Categories	Categories	Generic	n/a
Products	1080 Products	Categories   Products	Generic	n/a
CustomerDemographics	1090 Customer Demographics	Customer Demographics	Generic	n/a
«Previous   Page: 1 2 3 4   Nex	t»	Items per page: 10, 25, 50, 100   Sho	wing <b>1-10</b> (	of <b>32</b> items   Refresh

Press the *Edit* button, and change the *Roles* field to "Administrators". This will insure that only users with the administrator's role can see the page. Press *Ok*, then *Close*, and generate the application.

Security	Roles
Security settings for this page.	Administrators
User ? to allow anonymous access to the page.	List all roles that are authorized to access the page. Separate mutliple roles with a comma.
* - indicates a required field	OK Delete Cancel

When the web application loads in your browser, you can see that you are still logged in as a standard user. The *Order Details* page is no longer available in the navigation. You can try entering the URL for *Order Details* page. This will only redirect you back to the home page.

🍘 Start - Windows Internet Explorer	
🚱 🔵 🔻 🙋 http://localhost:30134/Northwind/Pages/Home.aspx?ReturnUrl=%2fNortl	nwind%2fPages%2fO1 🔻 🙍 😽 🗙 😵 work timesheet 🖉 🔻
🖕 Favorites 🏾 🍘 Start	🟠 🔻 🖾 🔻 🖃 🖶 Y Page 🕶 Safety 🕶 Tools 🕶 🕢 👻
History Permalink	Welcome user, Today is Monday, October 25, 2010   My Account   Logout   Help 📩
瓣 MyCompany	
Home Customers   Employees  Categories  Customer Demographics Region	Reports  Site Actions
Home > Home	
Start	
Please select a page link in the table of contents below.	Sign in to access the protected site content.
Site Map	Instructions

🕞 🕞 💌 🔊 http://localhost:30134/Northwind/Pages/OrderDetails.aspx 🗸 🔯 🤣 🖌 🚼 work timesheet 👂										
Favorites									Safety 🔻 Tools 🔻 🔞	
History   Permaink Welcome admin. Today is Monday. October 25, 2010. LiNe Account   Linguit   Hein										
MyCompany										
Home Customers -	Employees 🝷	Categories - Custo	mer Demogra	ohics R	legion • Reports • N	Membership			Site Actions •	
	Home > Cust Order	tomers > Order Details Details								
bout	This is a list o	of order details.								
nis page allows order etails management.	Quick Fi	ind 🔎 🛋 N	ew Order Det	ails A	ctions - Report -			View	Order Details 🔹	
ee Also	Order Customer#	Product Name	Unit Price Qu	antity Di	scount Order Customer Company Name	Order Employee Last Name	Order Ship Via Company Name	Product Category Name	Product Supplier Company Name	
Orders Customer Demo	VINET	Queso Cabrales	\$14.00	12	0 Vins et alcools Chevalier	Buchanan	Federal Shipping	Dairy Products	Cooperativa de Quesos 'Las Cabras'	
	VINET	Singaporean Hokkien Fried Mee	\$9.80	10	0 Vins et alcools Chevalier	Buchanan	Federal Shipping	Grains/Cereals	Leka Trading	
	VINET	Mozzarella di Giovanni	\$34.80	5	0 Vins et alcools Chevalier	Buchanan	Federal Shipping	Dairy Products	Formaggi Fortini s.r.l.	
	TOMSP	Tofu	\$18.60	9	0 Toms Spezialitäten	Suyama	Speedy Express	Produce	Mayumi's	
	TOMSP	Manjimup Dried Apples	\$42.40	40	0 Toms Spezialitäten	Suyama	Speedy Express	Produce	G'day, Mate	
	HANAR	Jack's New England Clam Chowder	\$7.70	10	0 Hanari Carnes	Peacock	United Package	Seafood	New England Seafood Cannery	
	HANAR	Manjimup Dried Apples	\$42.40	35	0.15 Hanari Carnes	Peacock	United Package	Produce	G'day, Mate	
	HANAR	Louisiana Fiery Hot Pepper Sauce	\$16.80	15	0.15 Hanari Carnes	Peacock	United Package	Condiments	New Orleans Cajun Delights	
	VICTE	Gustaf's Knäckebröd	\$16.80	6	0.05 Victuailles en stock	Leverling	Speedy Express	Grains/Cereals	PB Knäckebröd AB	
	VICTE	Ravioli Angelo	\$15.60	15	0.05 Victuailles en stock	Leverling	Speedy Express	Grains/Cereals	Pasta Buttini s.r.l.	
	« Previous	Page: 1 2 3 4 5 6 7	8910	Next »		Items per pa	ge: <b>10</b> , 15, 20, 25	Showing <b>1-10</b> of	2153 items   Refresh	
	© 2010 MyCo	ompany. All rights res	erved.							

If you logout, and log in as admin, the page will be available.

### **Fields**

Fields can also be secured through roles. You can specify some roles to only view the field as read-only, and specify other roles to not view the field at all.

Suppose that you need to protect certain fields from modification and/or viewing by unwanted users. *Northwind* allows editing of the *CustomerID* field, which could be disastrous if changed. Let's make this a read only field for standard users.

History Permalink					Welcome <b>admin</b> , Too	day is Monday	, October 25, 20	010   My Account   Logout   Help
🎁 MyCompany								
Home Customers -	Employees 🔹	Categories  Customer	Demographics	Region - Repo	orts • Membership			Site Actions •
	Home > Custo	ners						
About	This is a list	of customers.						
This page allows customers management.	Quick F	ind 🔎 🛋 New	Customers Ac	tions - Repor	t <del>-</del>			View: Customers •
See Also	Customer a	Company Name	Contact Name	Contact Title	Address	City	Region Posta Code	Country Phone
<ul> <li>Orders</li> <li>Customer Demo</li> </ul>	ALFKI	Alfreds Futterkiste	Maria Anders	Sales Representative	Obere Str. 57	Berlin	n/a 12209	9 Germany 030-0074321
Order Details	ANATR	Ana Trujillo Emparedados y	Ana Trujillo	Owner	Avda. de la Constitución	n México	n/a 05021	1 Mexico (5) 555-4729

Run *Code On Time Generator*, click on the name of the project, and press the *Design* button. Click on the *Customers* controller in the *All Controllers* list. Navigate to the *Fields* tab, and select the *CustomerID* field.

Project Designer exit											
O Home > Controller: Customers											
Controller	Commands	Fields	Views	Categories	Data Fields	Action Groups	Actions				
This is a list of	fields.										
Quick Find	Q	New 🝷	Preview	V							View: Fields •
Name		Ind	ex Type	Allow Nu	lls Is Prima	ry Key Rea	d Only	QBE	Sort	LEV	Label
CustomerID	•	·	1 String	No	Yes	No		Yes	Yes	No	Customer #
CompanyName	e		2 String	No	No	No		Yes	Yes	No	Company Name

Edit *CustomerID*. Change the *Write Roles* field to "Administrators". If you wanted the field completely hidden to standard users, you can write "Administrators" in the *Read Field*. Save the field, press *Close*, and generate the application.

Security Specify read/write access to the field. List the roles authorized to read and/or write field values. Use comma to separate multiple roles. Read more about field-level security here.	"Read" Roles "Write" Roles Administrators
* - indicates a required field	OK Delete Cancel

When the web application loads in the browser, log in as standard user. When you edit a customer record, the *CustomerID* field will be read only.

History Permalink		Welcome user, Today is Monday, October 25, 2010   My Account   Logout   Help
瓣 MyCompany		
Home Customers •	Employees Categories Customer Demographics Region Reports	Site Actions *
	Home > Customers Customers	
Summary	This is a list of customers.	
Customer#	Ouidk Find     P Record	View: Customers -
ALFKI	Customer#1 Company Name Contact Name Contact Title Address	City Region Postal Code Country Phone
Company Name		
Alfreds Futterkiste	ALFKI Alfreds Futterkiste Maria Anders Sales Representa Obere Str. 5	7 Berlin 12209 Germany 030-0074321
Contact Name	Sava Canaal	
Maria Anders	Cancel	

If we log in as administrator, the *CustomerID* field will be editable again.

History	Permalink					١	Welcome <b>admir</b>	, Today is Monda	y, October 25	5, 2010   My Acc	count   Logout   Help
🎁 М	yCompany										
Home	Customers -	Employees 🔻	Categories 🔹	Customer Demographic	s Region •	Reports -	Membership				Site Actions -
		Home > Custor	mers Ners								
Summa	ary	This is a list o	f customers.								
Custome	er#	Quick Fi	ind 🔎	Record -						View:	Customers •
ALFKI Compan	iy Name	Customer#↑	Company Nam	ne Contact Name	Contact Title	Address	City	Region	Postal Code	Country	Phone
Alfreds F Contact	Futterkiste Name	ALFKI	Alfreds Futte	rkist Maria Anders	Sales Represent	Obere Str.	57 Berlin		12209	Germany	030-0074321
Maria Ar	nders Title	Save	Cance	el							

## Actions

Suppose that you have a need to prevent some users from executing certain actions. By default, the standard user account can create, edit, and delete products. Let's change this so that the standard user can only view the products. Administrator will be the only role that can create, edit, and delete. There are several locations we will have to modify, such as the dropdown, the buttons on the action bar, and the buttons in detail view.

This will be done by switching to *Code On Time Generator*, clicking on the project name, and pressing on the *Designer* button. Select the *Products* controller. Switch to the *Action Groups* tab.

Project De	signer				exit						
G Home > Controller: Products											
Controller	Commands Fields Vi	ews Categories Data Fields	Action Groups Act	tions							
This is a list o	of data controller action grou	ups.									
Quick Find	P New -	Insert • Preview			View: Action Groups •						
Id	Scope	Header Text		Flat Rendering							
<u>aq1</u>	▼ Grid	n/a		No							
ag2	Form	n/a		No							
ag3	Action Bar	New		Yes							
ag4	Action Bar	Edit/Delete		Yes							
ag5	Action Bar	Actions		No							
ag6	Action Bar	Record		No							
ag7	Action Bar	Report		No							
ag8	Row	n/a		No							
					Showing 1-8 of 8 items   Refresh						

Click on *ag1*, or *Action Group 1*. Click on the actions tab. You can see that there is *Select*, *Edit*, a blank action, *Duplicate*, and *New*. These actions correspond to the dropdown next to the product name in the application.

Edit the *Edit* action. In the *Roles* field, type in "Administrators". This will insure that only users with the *Administrators* role can edit. Perform the same with *Delete*, *Duplicate*, and *New*.

Project Designer											
G Home > Controller: Products > Action Group: ag1											
Action Group Actions											
This is a list of data controller actions. Actions are available in the specified UI scope of the group if all "when" conditions are met.											
Quick Find P Record  View: Actions											
Command Name	Command Argument	Header Text	When Last Command Name	When Last Command Argument	When Key Selected	When HRef (Regex)	When View (Regex)	When Tag (Regex)	Roles	Scope	
Select	editForm1	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Grid	
Edit	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Administrators	Grid	
Delete	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Administrators	Grid	
n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Grid	
Duplicate	createForm1	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Administrators	Grid	
New	▼ grid1		N/A 🔹		N/A 🔻				Administrators	Grid	
Save	Cancel	]									
								Showing	1-6 of 6 items   F	Refresh	

Go back to the *Action Group* list. Navigate to *ag2*. Here is a long list of actions. Most of these are activated when a previous action has been selected, such as *Edit, New,* or *Duplicate*. In this case, the only actions that need modification would be the first two, without a *When Last Command Name* argument. Insert "Administrators" in their *Role* fields.

Project Designer											
G Home > Controller: Products > Action Group: ag2											
Action Group Actions											
This is a list of data controller actions. Actions are available in the specified UI scope of the group if all "when" conditions are met.											
Quick Find	P Recor	d 🕶							View: Actio	ns 🔹	
Command Name	Command Argument	Header Text	When Last Command Name	When Last Command Argument	When Key Selected	When HRef (Regex)	When View (Regex)	When Tag (Regex)	Roles	Scope	
Edit	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Administrators	Form	
Delete	•		N/A 👻		N/A 🔻				Administrators	Form	
Save	Cancel										
Cancel	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Form	

Go back to the *Action Group* list, and click on *ag3*. This action is the *New Product* button on the action bar. Change the *Role* field to "Administrators".

Project Designer											
G Home > Controller: Products > Action Group: ag3											
Action Group	Actions										
This is a list of da	ta controller actions.	Actions are av	vailable in the speci	fied UI scope	of the group	if all "whe	n" condit	ions are me	et.		
Quick Find	P Record	•							View:	Actions •	
Command Name	Command Argument	Header Whe Text Nan	en Last Command me	When Last Command Argument	When Key Selected	When HRef (Regex)	When View (Regex)	When Tag (Regex)	Roles	Scope	
New	▼ createForm1	N/	′A <b>▼</b>		N/A 🔻				Administ	rators Action Bar	
Save	Cancel										

On the *Action Group* list, navigate to *ag4*. These are the buttons that appear on the action bar when you select a record, *Edit* and *Delete*. Add "Administrators" to the *Role* fields of these actions. Now, generate the application.

Project Designer											
S Home > Controller: Products > Action Group: ag4											
Action Group	ctions										
This is a list of data controller actions. Actions are available in the specified UI scope of the group if all "when" conditions are met.											
Quick Find	P Recor	d 🔻							View: Acti	ions 🔹	
Command Name	Command Argument	Header Text	When Last Command Name	When Last Command Argument	When Key Selected	When HRef (Regex)	When View (Regex)	When Tag (Regex)	Roles	Scope	
Edit	editForm1	n/a	n/a	n/a	Yes	n/a	grid 1	n/a	Administrators	Action Bar	
Delete	•		N/A 👻		Yes 🔻		grid 1		Administrators	Action Bar	
Save	Cancel										

Login as user, and navigate to *Products*. First thing you will notice is that there is no *New Products* button. When you activate the dropdown menu, the only option available is *Select*. When you go into detail view, the only button available is *Close*.

History   Permalink Welcome user, Today is Monday, October 25, 2010   My Account   Logout   Helc											
瓣 MyCompany											
Home Customers - Er	mployees 🔹	Categories -	Customer Den	nographics	Region 💌	Reports	5 🕶				Site Actions •
	Home > Ca Produ	ategories > Produc ICTS	:ts								
Summary	This is a lis	t of products.									
Product Name	Quick	Find 🔎	Actions -	Report -							View: Products -
Chang Supplier Company Name	Product Na	me	Supplier Com	pany Name	Categor	y Name (	Quantity Per Unit	Unit Price	Units In Stock	Units On Order	Reorder Level Discontinued
Exotic Liquids Category Name	Chai		Exotic Liquids		Beverag	es b	l0 boxes x 20 bags	\$18.00	39	0	10 No
Beverages	Chang	•	Exotic Liquids		Beverag	es 🖸 2	24 - 12 oz bottles	\$19.00	17	40	25 No
Quantity Per Unit 24 - 12 oz bottles	Aniseed S	/ru Select	Exotic Liquids	,	Condime	nts 1	12 - 550 ml bottles	\$10.00	13	70	25 No
Unit Price \$19.00	Chef Anto Seasoning	n's Cajun	New Orleans Delights	Cajun	Condime	nts 4	<del>1</del> 8 - 6 oz jars	\$22.08	53	0	0 No
About	Chef Anto	n's Gumbo Mix	New Orleans Delights	Cajun	Condime	nts 3	36 boxes	\$21.36	0	0	0 Yes
This page allows products management.	Grandma's Spread	Boysenberry	Grandma Kell Homestead	y's	Condime	nts 1	12 - 8 oz jars	\$25.00	120	0	25 No
Home	Uncle Bob' Pears	s Organic Dried	Grandma Kell Homestead	y's	Produce	1	.2 - 1 lb pkgs.	\$30.05	15	0	10 No
Employees	Northwood	ls Cranberry Sauce	Grandma Kell Homestead	y's	Condime	nts 1	12 - 12 oz jars	\$40.00	6	0	0 No
<ul> <li>Customer Demographics</li> <li>Region</li> </ul>	Mishi Kobe	Niku	Tokyo Trader	s	Meat/Po	ultry 1	18 - 500 g pkgs.	\$97.00	29	0	0 Yes
= Reports	Ikura		Tokyo Trader	s	Seafood	1	12 - 200 ml jars	\$31.00	31	0	0 No
	« Previous	Page: 1 2 3 4	5678   Ne	xt »			Ite	ms per page	: <b>10</b> , 15, 20, 25	Showing 1-1	LO of 77 items   Refresh

Logout, and login as administrator. You can see that the New, Edit, and Delete buttons have returned.

History Permalink							Welco	ome <b>admi</b> i	n, Today is	Monday, Octob	oer 25, 2010	My Account   Logout   Help
🎁 MyCompany												
Home Customers - E	mployees 🝷	Cal	tegories 🔻	Customer Demographics	Region	Repor	rts 🔹 Me	mbership				Site Actions -
	Home > Ca Produ	atego JCt	ries > Product S	s								
About	This is a lis	t of p	roducts.									
This page allows products management.	Quick	Find	Q	New Products	Actions 🔹	Report	,					View: Products
See Also	Product Na	me		Supplier Company Nam	e Categ	ory Name	Quantity P	er Unit	Unit Price	Units In Stock	Units On Order	Reorder Level Discontinued
Home     Qustomers	me Chai Chai ployees Chang 🗸		Exotic Liquids	Bever	Beverages		20	\$18.00	39	0	10 No	
= Employees			•	Exotic Liquids	Bever	Beverages 24		bottles	\$19.00	17	40	25 No
Customer Demographics	Aniseed S		Select	Exotic Liquids	Condi	ments	12 - 550 m	bottles	\$10.00	13	70	25 No
Reports     Membership	Chef Anto Seasoning Chef Anto	×	Edit Delete Duplicate	New Orleans Cajun Delights	Condi	ments	48 - 6 oz ja	ars	\$22.08	53	0	0 No
				New Orleans Cajun Delights	Condi	ments	36 boxes		\$21.36	0	0	0 Yes
	Grandma's Spread	Grandma's Boysenberry Spread		Grandma Kelly's Homestead	Condi	Condiments		ars	\$25.00	120	0	25 No
	Unde Bob's Organic Dried Pears Northwoods Cranberry Sauce		Grandma Kelly's Homestead	Produ	ce	12 - 1 lb pk	ıgs.	\$30.05	15	0	10 No	
			Grandma Kelly's Homestead	Condi	Condiments		jars	\$40.00	6	0	0 No	
	Mishi Kobe	Niku		Tokyo Traders	Meat/	Poultry	18 - 500 g	pkgs.	\$97.00	29	0	0 Yes
	Ikura			Tokyo Traders	Seafo	od	12 - 200 m	l jars	\$31.00	31	0	0 No
	« Previous	Pa	ge: 1 2 3 4	5 6 7 8   Next »				Item	s per page	: 10, 15, 20, 2	5   Showing 1-	10 of 77 items   Refresh