



# Cizer.Net Reporting

Version 4.0

## Administrator's Guide



**PUBLISHED BY**

Cizer Software Corporation  
20098 Ashbrook Place, Suite 200  
Ashburn, VA 20147

Tech Support Line: 703-554-1450  
Hours of Operation: 8:30 am to 5:30 pm, ET, M-F

**Copyright** © 2006-2007 Cizer Software Corporation - Patent Pending

All rights reserved. No part of the contents of this manual may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

<b>Chapter 1: Installation and Configuration</b> -----	<b>1</b>
1.1 Prerequisites for Installation-----	1
1.1.1 Local Viewer-----	1
1.1.1.1 Web Farm Diagram-----	2
1.1.2 IFrame Viewer -----	3
1.1.2.1 Web Farm Diagram-----	4
1.1.3 Remote Viewer -----	5
1.1.3.1 Web Farm Diagram-----	6
1.2 Running the Installation -----	7
1.3 Advanced Configuration-----	11
1.4 Configuration with MS SharePoint Services -----	13
1.5 Web Farm Configuration-----	13
1.6 Applying Your Logo -----	15
1.6.1 Login Page Logo -----	15
1.6.2 Portal Page Logo-----	15
<b>Chapter 2: Cizer.Net Administration</b> -----	<b>16</b>
2.1 Accessing the Cizer .Net Administrator Interface-----	16
2.2 About the Cizer .Net Administrator Interface-----	17
2.3 Cizer .Net Management Interface: Security-----	17
2.3.1 Cizer .Net Security Model Overview-----	17
2.3.1.1 Authentication-----	18
2.3.1.2 Authorization -----	18
2.3.2 Password Expired-----	20
2.3.3 Invalid Password -----	20
2.3.4 Inactive Password-----	21
2.3.5 Locked Out Password-----	21
2.3.6 Reset Inactive Admin Password-----	22
2.3.7 Reset Admin Password-----	22
2.3.8 Reset User Password-----	22
2.3.9 Manage Application Users -----	23
2.3.9.1 General Tab -----	24
2.3.9.2 Roles Tab -----	24
2.3.9.3 Tasks Tab-----	25
2.3.9.4 Data Sources-----	25
2.3.9.5 Add a New User -----	26
2.3.9.6 Bulk Import Users -----	27
2.3.10 Manage Application Roles-----	28
2.3.10.1 General Tab -----	28
2.3.10.2. Tasks Tab -----	29
2.3.10.3 DataSources Tab-----	29
2.3.10.4 Items Tab-----	30
2.3.10.5 Add a New Role -----	30
2.4 Cizer.Net Management Interface: Application Settings -----	31
2.4.1 Activation -----	31
2.4.2 Server Settings -----	32
2.4.3 Application Values -----	33
2.4.3.1 Using Windows Authentication -----	34
2.4.4 Data Sources-----	35
2.4.4.1 Adding and Managing Data Sources-----	35
2.4.4.2 Connection String Examples -----	36
2.4.5 Quick Query Settings-----	37
<b>Appendix A: Report URL Call Extension</b> -----	<b>39</b>
<b>Appendix B: Configuration with Panorama NovaView</b> -----	<b>41</b>

## Chapter 1: Installation and Configuration

This user guide is intended primarily for administrators of Cizer.Net Reporting 4.0 Standard Edition, as well as the 4.0 Enterprise Edition's Company Administrators. It should also be used as a reference document for System Admins of Cizer.Net Reporting 4.0 Enterprise Edition.

### 1.1 Prerequisites for Installation

Before installing Cizer.Net Reporting on your reporting server, consider the type of viewer you wish to utilize. Each viewer has a slightly different set of requirements, listed on the following pages:

**Local Viewer** - default viewer

**IFrame Viewer**

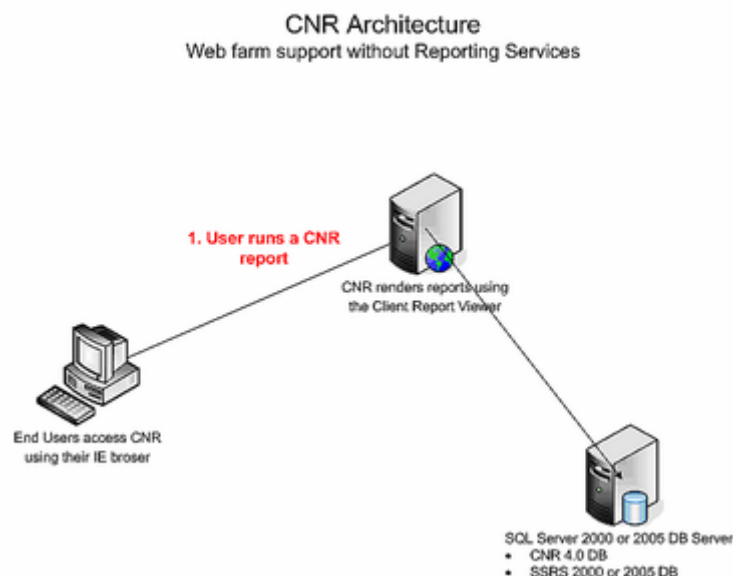
**Remote (Viewer Control)** - recommended when using SQL Server 2005

Security extensions have been created for both SSRS 2000 and 2005.

CNR 4.0 is now web farm capable with all three viewers listed above.

#### 1.1.1 Local Viewer

The Local Viewer is the default viewer for CNR 4.0 installations. This setting does not require SQL Server Reporting Services to be installed. When a user runs a report, CNR sends the RDL request to the viewer control for rendering. The user can then export the report out to Excel or PDF.



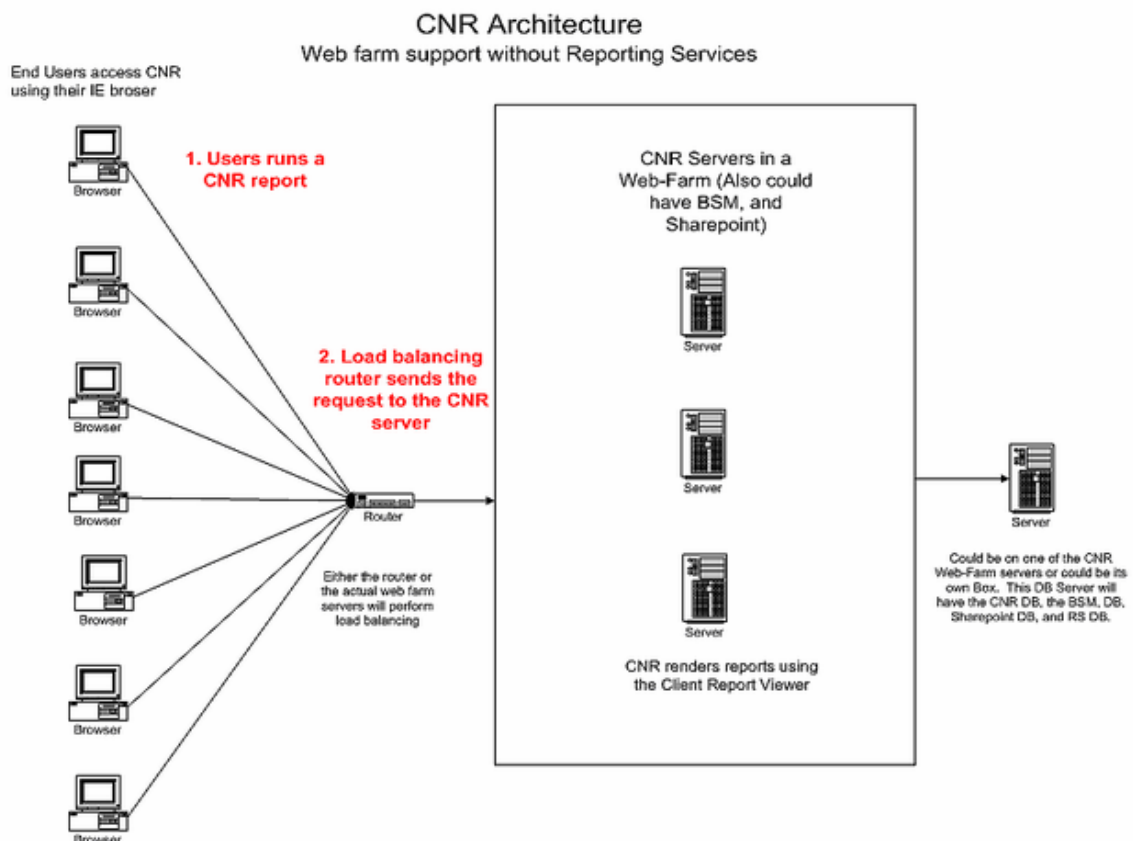
#### Local Viewer limitations:

1. Could have trouble rendering reports with large data sets or queries with long run times
2. Export options are limited to Excel and PDF
3. When exporting to Excel the user will have to save the report before viewing it
4. Cannot deploy reports to Reporting Services
5. No print option

### Local Viewer Requirements

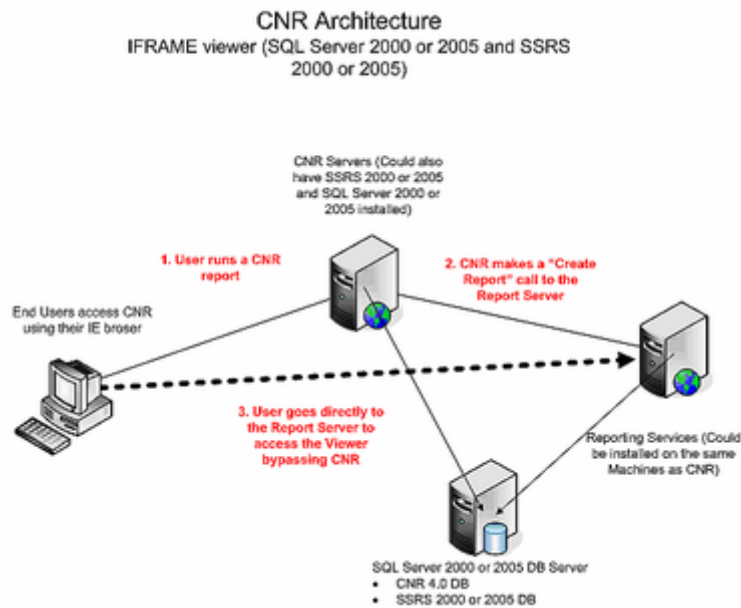
1. **Windows Server 2000 or 2003**
  
2. **Internet Information Services (IIS) 5.0 and Up:** IIS must be installed as a Windows Component *prior to* installing Cizer.Net Reporting. To install IIS go to Add/Remove Programs within the Control Panel. From the Add/Remove Programs window, select the Add/Remove Windows Components icon. This will bring up a list of Windows components installed on your server, make sure the IIS icon is selected. If IIS is not installed be prepared to have a Windows CD ready to load the necessary components.
  
3. **.Net Framework 2.0:** After the installation go to IIS Manager and Right Click the Cizer.Net Reporting Virtual Directory (Default installation path is *Web Sites | Default Web Site | CNR*) and select Properties. Under the ASP .NET tab make sure the ASP .NET version is 2.0.5027. Windows Server 2003 users need to look under the Virtual Directory Tab and make sure that CNR has its own Application Pool (Default Application Pool is *CNRAppPool*).
  
4. **SQL Server:** SQL Server 2000 with Service Pack 4 -OR- SQL Server 2005

#### 1.1.1.1 Web Farm Diagram



### 1.1.2 IFrame Viewer

When selecting the IFrame viewer, CNR will need to be able to access either SSRS 2000 or SSRS 2005. Connection information to SSRS 2000 or 2005 will need to be supplied in the CNR "Admin" section under "Server Settings". When a user runs a report, CNR generates an RDL file, sends it to SSRS 2000/2005 for rendering, and then the user goes directly to the report server to access the viewer, bypassing CNR. The user can then export the report to formats supported by SSRS 2000/2005 and print from the browser.



### IFrame Requirements

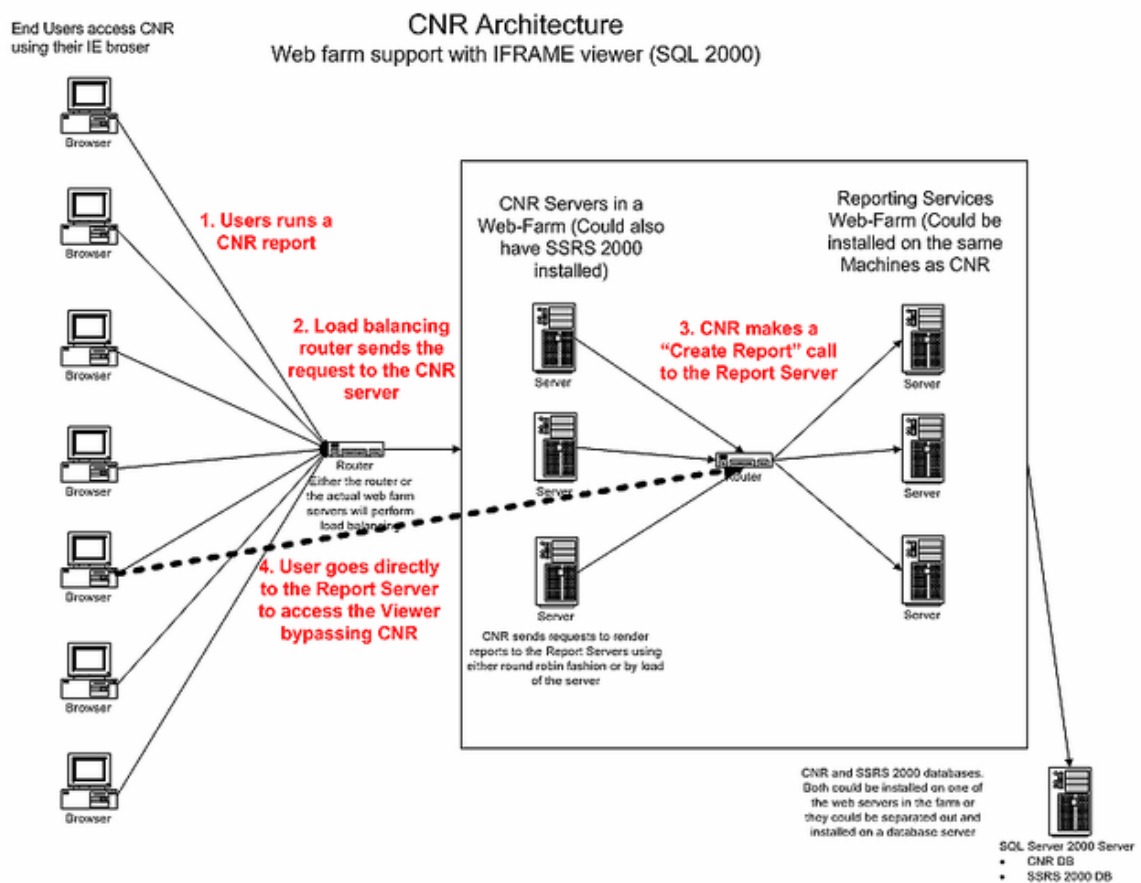
- 1. Windows Server 2000 or 2003**
- 2. Internet Information Services (IIS) 5.0 and Up:** IIS must be installed as a Windows Component *prior to* installing Cizer.Net Reporting. To install IIS go to Add/Remove Programs within the Control Panel. From the Add/Remove Programs window, select the Add/Remove Windows Components icon. This will bring up a list of Windows components installed on your server, make sure the IIS icon is selected. If IIS is not installed be prepared to have a Windows CD ready to load the necessary components.
- 3. .Net Framework 2.0:** After the installation go to IIS Manager and Right Click the Cizer.Net Reporting Virtual Directory (Default installation path is *Web Sites | Default Web Site | CNR*) and select Properties. Under the ASP .NET tab make sure the ASP .NET version is *2.0.5027*. Windows Server 2003 users need to look under the Virtual Directory Tab and make sure that CNR has its own Application Pool (Default Application Pool is *CNRAppPool*).
- 4. SQL Server:** SQL Server 2000 with SP 4 -OR- SQL Server 2005
- 5. SSRS 2000 SP2 or 2005:** SQL Server Reporting Services must be installed on the Cizer.Net server *prior to* the Cizer.Net installation. Visual Studio is listed as a prerequisite for Reporting Services but, Visual Studio does *not* need to be installed for Cizer.Net Reporting to function properly. During the installation for Reporting Services, you can skip the prompt to install Visual Studio.

SQL Server Reporting Services should be configured as follows:

- Open Internet Explorer.

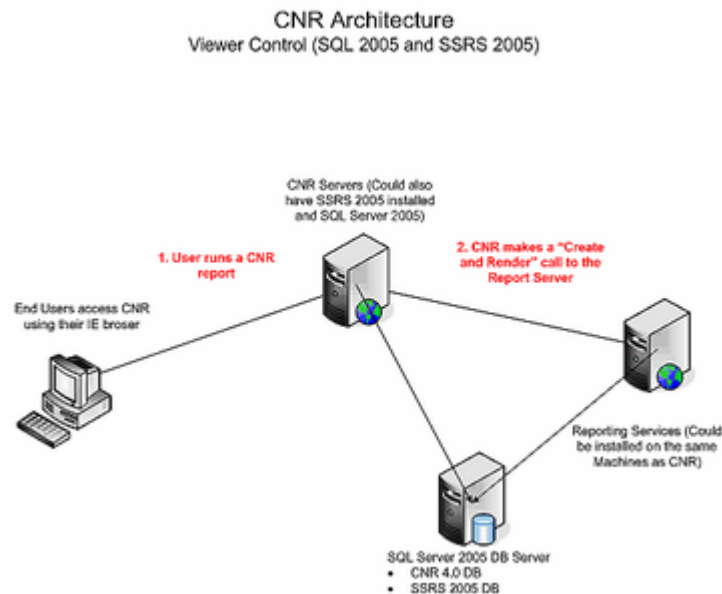
- b. In your browser, bring up SQL Server Reporting Services Report Manager by navigating to Report Manager (i.e. [http://Reporting\\_Services\\_server\\_name/Reports](http://Reporting_Services_server_name/Reports))
- c. Click on the Properties Tab.
- d. Click on the New Role Assignment button.
- f. Enter "EveryOne" in the Group or user name text box.
- g. Select Content Manager as a role.
- h. Click on the OK button.

### 1.1.2.1 Web Farm Diagram



### 1.1.3 Remote Viewer

This Remote Viewer, or Viewer Control, requires SQL Server 2005 and SSRS 2005 and is the ***recommended setting for CNR when using SQL Server 2005***. Connection information to SSRS 2005 will need to be supplied in the CNR "Admin" section under "Server Settings". When a user runs a report, CNR generates an RDL file and makes a "Create and Render" call to SSRS 2005. The user can then export the report to all formats supported by SSRS 2005 and print from the browser.



### Remote (View Control) Requirements

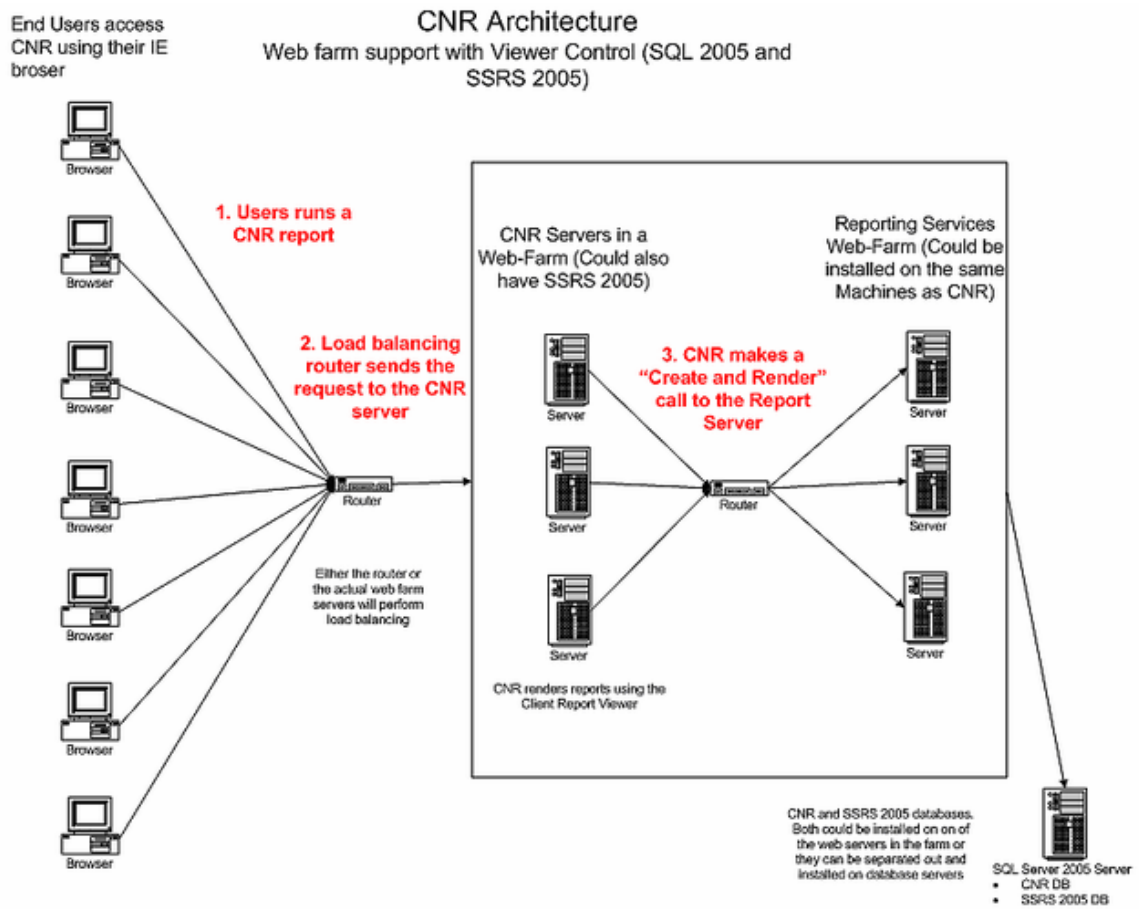
1. **Windows Server 2003**
2. **IIS 6.0:** IIS must be installed as a Windows Component *prior to* installing Cizer.Net Reporting. To install IIS go to Add/Remove Programs within the Control Panel. From the Add/Remove Programs window, select the Add/Remove Windows Components icon. This will bring up a list of Windows components installed on your server, make sure the IIS icon is selected. If IIS is not installed be prepared to have a Windows CD ready to load the necessary components.
3. **.Net Framework 2.0:** After the installation go to IIS Manager and Right Click the Cizer.Net Reporting Virtual Directory (Default installation path is *Web Sites | Default Web Site | CNR*) and select Properties. Under the ASP .NET tab make sure the ASP .NET version is 2.0.5027. Windows Server 2003 users need to look under the Virtual Directory Tab and make sure that CNR has its own Application Pool (Default Application Pool is *CNRAppPool*).
4. **SQL Server 2005**
5. **SSRS 2005:** SQL Server Reporting Services must be installed on the Cizer.Net server *prior to* the Cizer.Net installation. Visual Studio is listed as a prerequisite for Reporting Services but, Visual Studio does *not* need to be installed for Cizer.Net Reporting to function properly. During the installation for Reporting Services, you can skip the prompt to install Visual Studio.

SQL Server Reporting Services should be configured as follows:

- a. Open Internet Explorer.
- b. In your browser, bring up SQL Server Reporting Services Report Manager by navigating to Report Manager (i.e. [http://Reporting\\_Services\\_server\\_name/Reports](http://Reporting_Services_server_name/Reports))
- c. Click on the Properties Tab.

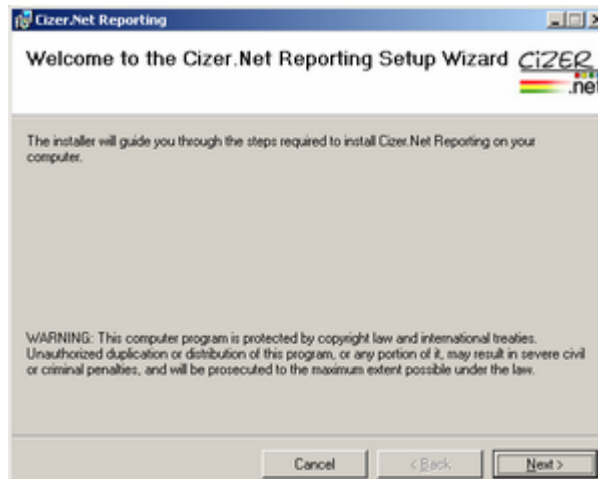
- d. Click on the New Role Assignment button.
- f. Enter "EveryOne" in the Group or user name text box.
- g. Select Content Manager as a role.
- h. Click on the OK button.

### 1.1.3.1 Web Farm Diagram

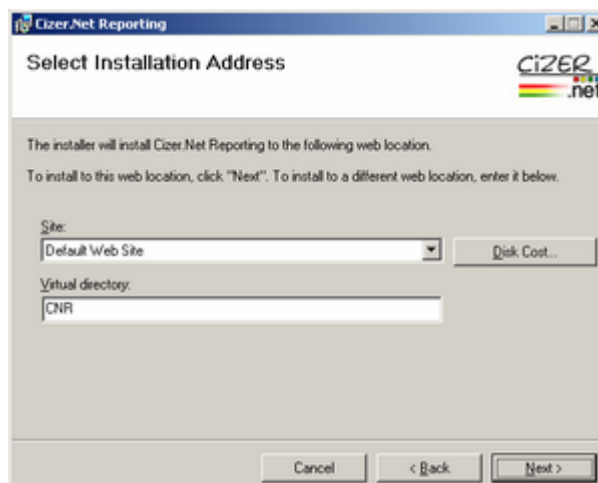


### 1.2 Running the Installation

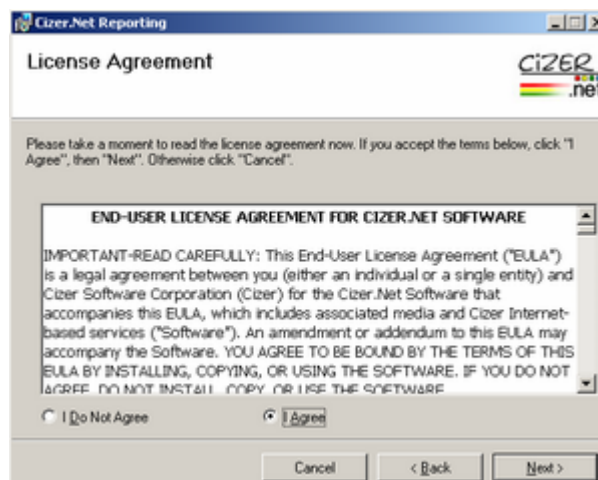
1. Start the Setup Wizard by clicking on the .msi file.



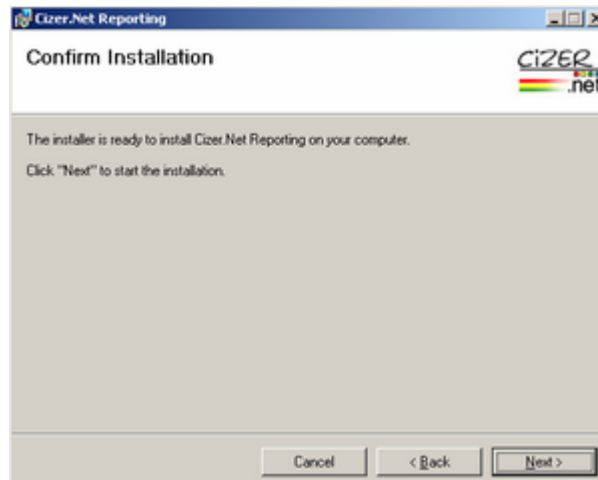
2. Enter the name of the Virtual Directory to which the files will be installed. Verify the Port and edit if required. *NOTE: Disk Cost refers to the amount of hard drive space that will be used to install the files.*



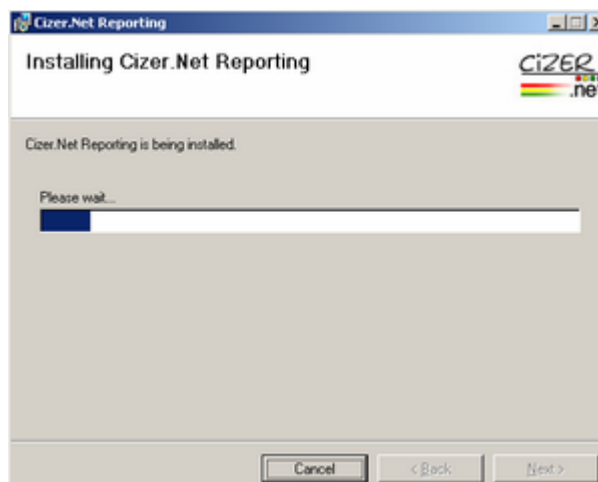
3. Review the Cizer.Net Reporting License Agreement; click "I Agree" and click Next.



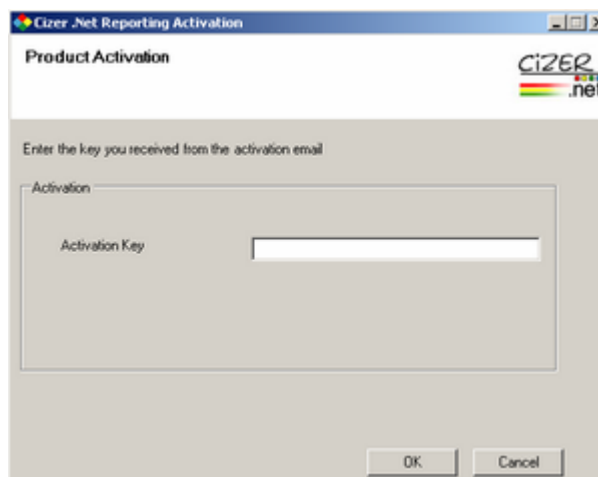
4. Click Next to continue when you are ready to begin the installation.



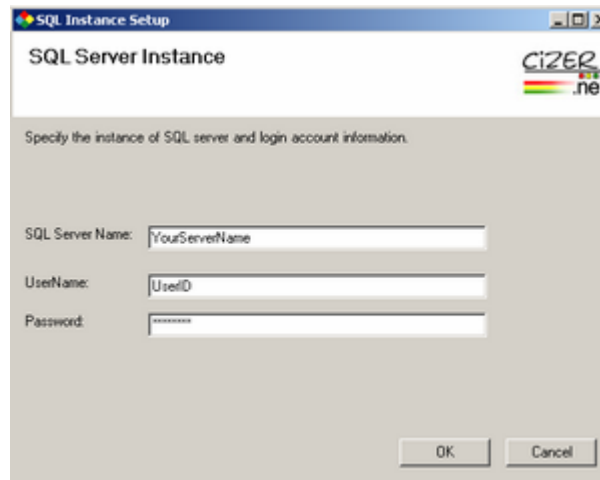
5. The progress bar indicates the files are being installed.



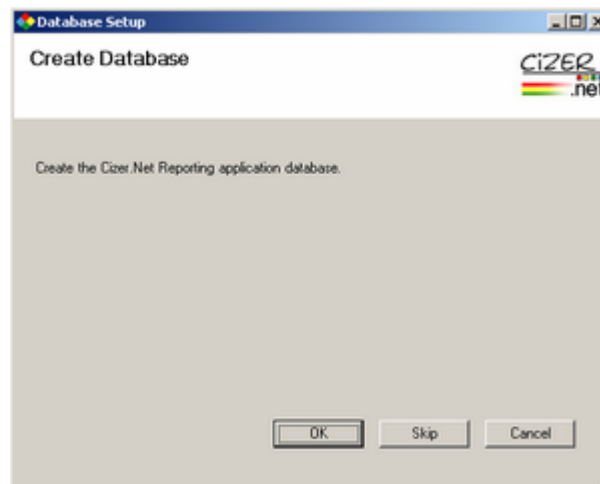
6. Enter the Activation key you receive from the Cizer Help Desk. This may be either an Evaluation (Eval) Key with a limited time restriction or it may be your Permanent Key. If you have received an Eval Key, you may continue with the installation and replace it with a Permanent Key before the Eval Key expires (See section 2.4.1; "Activation"). No reinstallation will be required to convert an Eval Key to a Permanent Key.



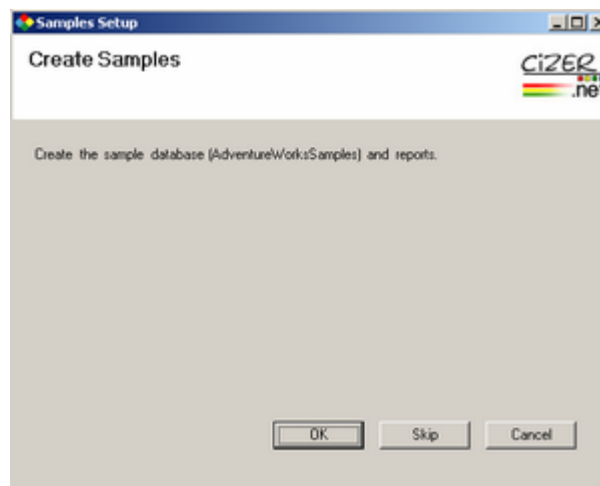
7. Enter the information for the SQL Server database instance you wish to use for the Cizer.Net database installation. *Enter the actual Server Name; do not use [local].*



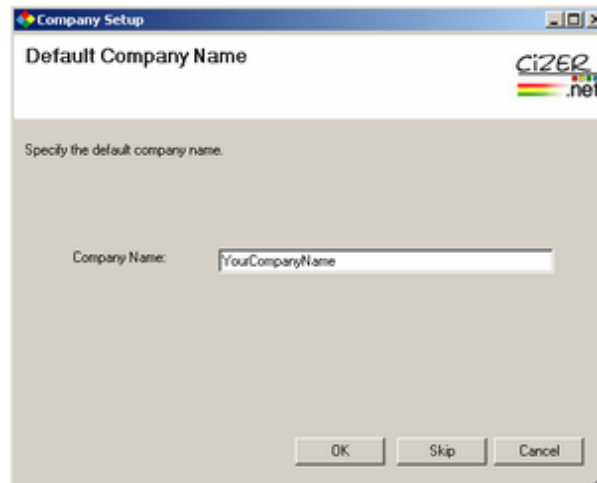
8. The installation will automatically create the Cizer.Net Reporting application database for you. Click OK to create a new database. **IMPORTANT:** *If you've already set up a Cizer.Net database with Users and Roles and do not wish to overwrite the current database, click Skip.*



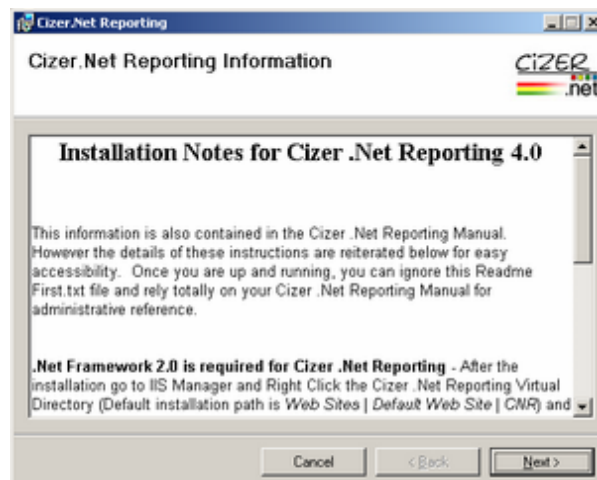
9. Sample reports are available for installation. If you do not wish to have the sample reports installed on your Cizer.Net application, click Skip.



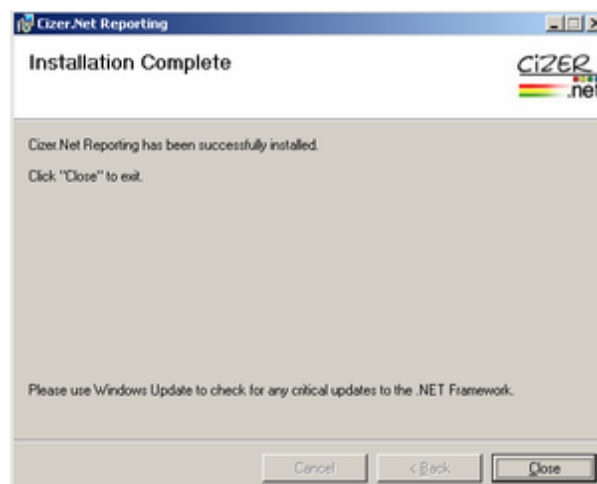
10. A company is automatically created during the Cizer.Net installation. Enter the name you wish to use. If you skip this screen, the company will be named "Default". You can change the company folder name through "Folder Management" at a later date.



11. The following text provides important information which should be reviewed before using Cizer. The same information is provided in printed form in the Cizer.Net Reporting Admin Guide as well as the Readme First.txt file that is included in the downloadable zip file. The installation and configuration text is provided in the actual installation screen for your convenience.



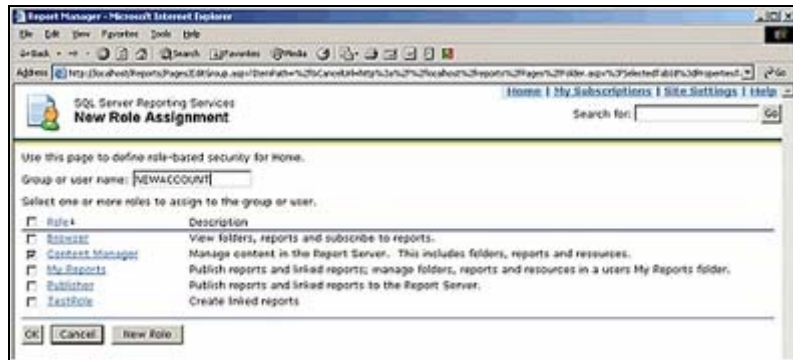
12. Click Close to complete the installation and close the installation wizard.



### 1.3 Advanced Configuration

The following configuration is necessary when installing Cizer.Net on one machine while utilizing Microsoft Reporting Services on a separate machine. Note that we use NEWACCOUNT as an example.

1. Create a user account on your domain that the Cizer.Net web application will use for impersonation.
2. Add the new user account to Reporting Services with a role of Content Manager.



3. Add the new user account to the Administrators Group on the machine running Cizer.Net.



4. Edit the Identity element of the Cizer.Net web.config, located by default in C:\inetpub\wwwroot\CNR. (Add and remove comment code from the following lines.)

Change the line:

```
<identity impersonate="false" />
```

to:

```
<!--<identity impersonate="false" />-->
```

And change the line:

```
<!--<identity impersonate="true" userName="DOMAIN\NEWACCOUNT" password="NEWACCOUNT" />-->
```

to:

```
<identity impersonate="true" userName="DOMAIN\NEWACCOUNT" password="NEWACCOUNT" />
```

Remember to change the username and password to that of the new user account.



```
Web.config - Notepad
File Edit Format Help

on the local web server. This setting is recommended for security purposes, so
that you do not display application detail information to remote clients.
-->
<customErrors mode="RemoteOnly" />
<!-- AUTHENTICATION
This section sets the authentication policies of the application. Possible modes are "Windows",
"Forms", "Passport" and "None".
"None" No authentication is performed.
"Windows" IIS performs authentication (Basic, Digest, or Integrated Windows) according to
its settings for the application. Anonymous access must be disabled in IIS.
"Forms" you provide a custom form (web page) for users to enter their credentials, and then
you authenticate them in your application. A user credential token is stored in a cookie.
"Passport" authentication is performed via a centralized authentication service provided
by Microsoft that offers a single logon and core profile services for member sites.
-->
<authentication mode="None" />
-->
<authentication mode="Windows" />
<authentication impersonate="false" />
<!--identity impersonate="true" userName="domain/newaccount" password="newaccount" />
-->
<!-- AUTHORIZATION
This section sets the authorization policies of the application. you can allow or deny access
to application resources by user or role. wildcards: "*" mean everyone, "?" means anonymous
(unauthenticated) users.
-->
```

### 1.4 Configuration with MS SharePoint Services

1. Enable Microsoft Reporting Services to coexist with Microsoft SharePoint Services by following the instructions from the RS Setup documentation (rssetup.chm). This information is found under the help topic "Troubleshooting a Side-by-Side installation of Reporting Services and Windows SharePoint Services".
2. Add Cizer.Net Reporting to the Windows SharePoint Services list of exclusions.

```
STSADM.EXE -o addpath -url http://localhost/CNR -type exclusion
```

3. Set the trust level of the "system.web" configuration element in the Cizer.Net Reporting web.config file by adding a line directly under <system.web> and inserting the code below. By default, the web.config file is located at C:\inetpub\wwwroot\CNR.

```
<trust level="Full" originUrl="" />
```

4. Use the IIS Manager to ensure that Cizer.Net Reporting is in an application pool that is separate from the SharePoint server.

For instructions on configuring MS Reporting Services with MS SharePoint Services, visit Microsoft's web site at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/RSinstall/htm/gs\\_installingrs\\_v1\\_9fdy.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/RSinstall/htm/gs_installingrs_v1_9fdy.asp).

### 1.5 Web Farm Configuration

1. Choose one of the servers in the web farm to act as the Session Server / Image Server. Go to that server's Services panel. Set the "ASP.NET State Service" to Automatic and start the service.
2. The CNR Web.config file needs to be modified on ALL of the web farm servers. Web.config is located on c:\inetpub\wwwroot\CNR\web.config.

i) Use the ConnectionString.exe utility to create a new connection string with the database server name, SQL server user id and password. See "Updating the Encrypted Connection String to the Cizer Database.doc" for directions on using ConnectionString.exe.

ii) After the <appSettings> tag, uncomment the following code and replace SERVERNAME with the name of your Session Server / Image Server.

```
<!--<add key="WebFarmImageServerHTTP"
value="http://SERVERNAME/cnr/temp/image/" />
<add key="WebFarmImageServerShare"
value="\\SERVERNAME\CNRTemp\Image\" />-->
```

iii) Uncomment the following code found immediately after the </httpHandlers> tag:

```
<!--<machineKey
validationKey="02A48D6985B61473A440F2C6D94E7E8B1E3B26572D040BC250EE808C84FAE144F
B105ABE42FF5ADD95624B020A44357ED4CABB7BAB82C7416010CD28216F51A3 "
```

```
decryptionKey="EB4AB0EA2028BE6F549765756D7A548D4EF312FDF8BEF9B6035141D7D9A935D4"  
    validation="SHA1"  
/>-->
```

iv) Comment out the following code:

```
<sessionState mode="InProc" stateConnectionString="tcpip=127.0.0.1:42424"  
sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes"  
cookieless="false" timeout="20" />
```

and remove the comments from this code:

```
<!--<sessionState mode="StateServer"  
stateConnectionString="tcpip=ServerName:42424" cookieless="false" timeout="20"  
/>-->
```

Note: Be sure to change **ServerName** to the name of your session / image server.

3. On the Session / Image server open Windows Explorer and navigate to `c:\inetpub\wwwroot\CNR\temp\images`. Share this folder and grant Change permissions on the share to "Everyone".

4. On the Session / Image server open the registry editor and change the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet\_state\Parameters\AllowRemoteConnection key value to 1.

**Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft and Cizer cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

### 1.6 Applying Your Logo

You can replace the Cizer.Net logo on the login page with your company logo, and you may also add a logo to the Cizer.Net Portal page. Both logos must be saved in the Image folder of the Cizer.Net application.

#### 1.6.1 Login Page Logo

The Login page logo must be a jpeg and should be approximately 145 pixels in width by 95 pixels in height. It must be named CORPLOGO\_LOGIN.jpg. Save this jpeg on the Cizer server in `Inetpub\wwwroot\CNR\Image`. The existing Cizer.Net logo is also named CORPLOGO\_LOGIN.jpg; if you wish to save the Cizer.Net logo you will need to rename it. If not, simply replace CORPLOGO\_LOGIN.jpg with your company logo of the same name. The Login page will now display your company logo.

*Note: The Image folder file path name will be different if the default Virtual Directory name (CNR) was changed during installation. In this case the file path name will reflect whatever name was entered during installation (Inetpub\wwwroot\NAME\Image).*

#### 1.6.2 Portal Page Logo

The Portal page logo must be a jpg and should be approximately 140 pixels in width and 90 pixels in height. It must be named CORPLOGO\_PORTAL.jpg. Save this jpeg on the Cizer Server in `Inetpub\wwwroot\CNR\Image`. A placeholder image by the same name already exists in this folder. Simply replace the existing jpg with your company logo of the same name. The Portal page will now display your company logo.

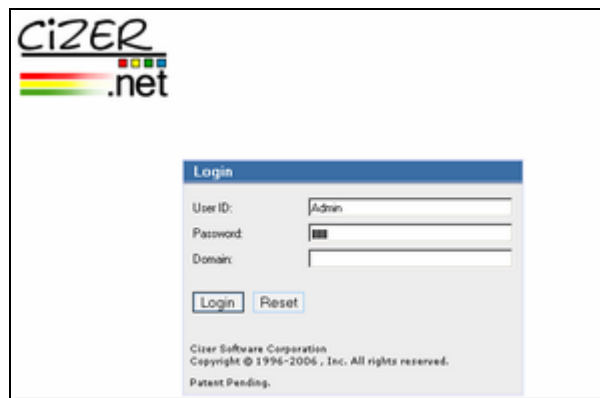
*Note: The Image folder file path name will be different if the default Virtual Directory name (CNR) was changed during installation. In this case the file path name will reflect whatever name was entered during installation (Inetpub\wwwroot\NAME\Image).*

## Chapter 2: Cizer.Net Administration

### 2.1 Accessing the Cizer .Net Administrator Interface

To Open the Cizer.Net Reporting application, follow these steps:

1. Open Internet Explorer.
2. Enter the URL as the machine name/CNR or the Virtual Directory Name you specified during install (ex. `http://machine_name/CNR`) and press Enter.
3. Enter "Admin" for both User ID and Password (password is case sensitive). If you are part of a hosted application, your User ID will be assigned to you by the host administrator. The Password and User ID are always the same the first time you log on. You will be asked to change the password after you log in for the first time.



4. Once you login, you will see the "Home" page, Cizer.Net's Portal interface. Access the Administrative interface by selecting "Admin" under "Settings" in the control panel on the left. From the Admin interface, you can return to the Portal page by selecting "Home" from the bottom menu bar, as well as the Global Libraries.

## 2.2 About the Cizer .Net Administrator Interface



Cizer.Net Administration takes place from the Admin portal. The control panel for all administrative tasks is located on the left. When selecting one of those tasks, the corresponding management screen displays in the working area on the right. You may access the portal page ("Home"), reports, queries, parameters and templates at any time by selecting the desired area from the menu bar located at the bottom of the screen.

**Security** – Security in this application is very granular. You can control who sees what features and data by user or role, and security can be applied all the way down to the field-level values. Users and Roles are managed under Security.

**Application Settings** – This is the sector that allows you to manage and maintain connections between the Cizer.Net application, Microsoft Reporting Services and various Data Source connections. This is also where your activation key is stored, and where you configure Quick Query to display your customized format.



## 2.3 Cizer .Net Management Interface: Security

### 2.3.1 Cizer .Net Security Model Overview

The Cizer.Net Security Model is based upon the core security concepts of authentication and authorization. Authentication can be defined as the process used for obtaining a user's credentials and validating the user to the application. Authorization is the process by which users are permitted access to resources within the application. Developed on these core concepts, the security module used by Cizer.Net Reporting provides an administrator with a variety of methods for validating users to an application and for restricting the application resources granted to its users.

### 2.3.1.1 Authentication

The Cizer.Net security model allows an administrator to choose from three providers for collecting user credentials to identify them in the application. These options are available for selection from the web management interface and can be set at the individual user level.

#### 1. Windows

The Windows security provider works with the existing Windows domain account and password to identify a user in the application. This model requires that the user's Windows account be added to the Cizer.Net security database through the Cizer.Net Admin interface or batch process and be granted application permissions. The Windows account is stored solely for the authorization of user rights with all authentications provided through the Windows domain.

#### 2. Forms

The Forms security provider relies on the Cizer.Net security database for all account management and authentication. User accounts, passwords, and activation information are stored in the security database and administered through the Cizer.Net Admin interface. Account passwords are automatically expired on creation, forcing the user to change their password with first login and automatically setting the next account expiration date. Invalid authentication attempts are logged by the system and the account is expired after reaching an invalid attempt threshold.

#### 3. Custom

The custom security provider removes the authentication process from the Cizer.Net application and requires the client to assume this responsibility. The custom provider model requires that the client application authenticate the user and then request a security token from the Cizer.Net security module. The security module returns an encrypted token comprised of the userid and current timestamp. The client then passes the encrypted security token as a URL call to the Cizer.Net security module, at which point the token is decrypted and the expiration timestamp is validated. This model requires that the custom account be added to the Cizer.Net security database through the Cizer.Net Admin interface or batch process and be granted application permissions.

### 2.3.1.2 Authorization

#### Users & Roles

A highly flexible and secure role-based model is used for authorizing user access to Cizer.Net application resources. The **role** is the highest level of authorization detail in the security model and is comprised of a collection of data sources, tasks and items. **Tasks** define a specific action within the application and represent permissions such as publish, save, run, or admin. The **item** defines specific objects in the application such as tables, views, SQL text, and stored procedures. User permissions are granted at both the role and user level by allowing the administrator to assign users to application roles and override role-defined tasks permissions at the user level. The authorization of application tasks and items plays an integral part in the security process and is the primary reason that clients choosing the Windows or custom security model must add their users to the Cizer.Net security database even while authenticating through a different model.

### Row Level Data Security

The role-based authorization model also includes the ability to restrict data at the row level, providing an additional layer of information security. The data restriction is achieved by exposing the current user id (%UserID%) as a silent parameter that can be included as a SQL Where clause constraint in a Cizer .Net "User Query" which functions like a view on the Cizer.Net Reporting Services server.

The silent user id (%UserID%) data restriction can also be used to filter the parameter values available to the user, but including it in the parameter SQL Where clause.

This architecture enables an administrator to create cross-reference table that can provide filters to any enterprise data store. For example a cross-reference table for Finance Funds might simply have a column of UserID's and a column of FinanceFunds. Thus the user would only see those Finance Funds corresponding to their user id, and the Finance Funds would be included as a SQL constraint for all database queries.

For the following examples, assume the user has logged into Cizer.Net as fsmith or sjones, which is available within Cizer.Net as %UserID%:

**fsmith:**

**Table: User\_Fund**

<u>User</u>	<u>FinanceFund</u>
fsmith	311
fsmith	210

**Table: Fund\_Balance**

<u>FinanceFund</u>	<u>FundBalance</u>
311	1982.35
210	1000.21

**sjones:**

**Table: User\_Fund**

<u>User</u>	<u>FinanceFund</u>
sjones	311
sjones	245
sjones	248

**Table: Fund\_Balance**

<u>FinanceFund</u>	<u>FundBalance</u>
311	1982.35
245	3245.76
248	21.55

Example Parameter SQL to return Funds available to the user:

```
Select FinanceFund from User_Fund where User = %UserID%
```

Example Query SQL to return Balances available to the user:

```
Select * from Fund_Balance join User_Fund on (Fund_Balance.FinanceFund = User_Fund.FinanceFund) where User_Fund.User = %UserID%
```

### 2.3.2 Password Expired

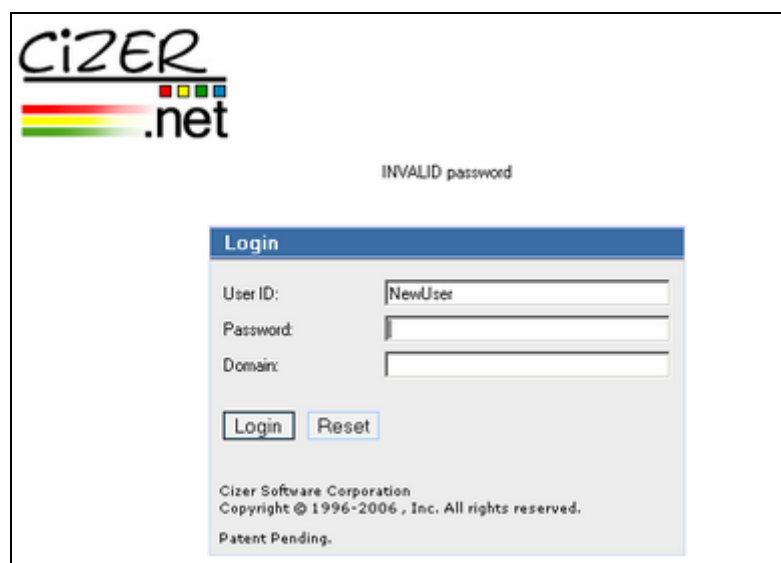
The first time a user logs in, or when a user password is reset, the user must login using their user ID as **both** the ID and Password values. The Password Expired screen displays whenever a user logs in for the first time, or after they're password has been reset.

On initial setup the defaulted system account will be "Admin" with "Admin" as the password. Immediately after pressing the login button you will be prompted to change the password. User passwords can be reset by an Administrator only, for users that are not using Windows authentication.



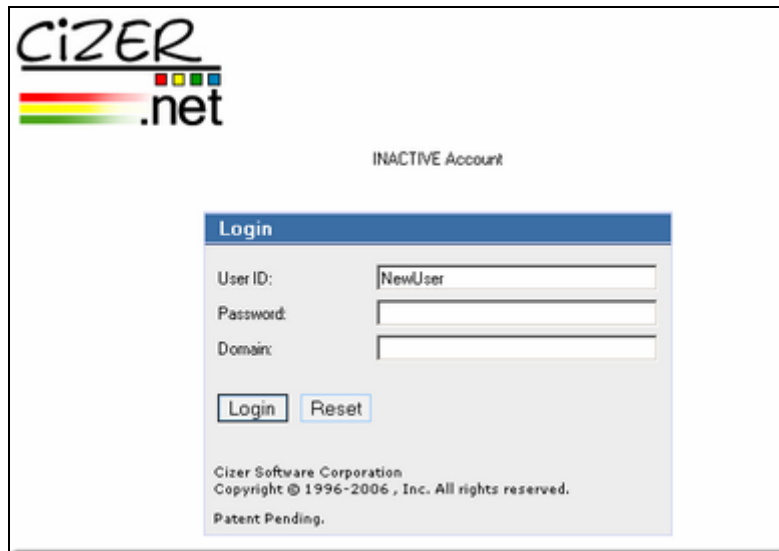
### 2.3.3 Invalid Password

The Invalid Password message on the login screen indicates that the password was entered incorrectly. After the third incorrect attempt your password will become inactive. See Section 3.6.3 "Configure Application Values" to allow an unlimited number of **Admin** logon attempts.



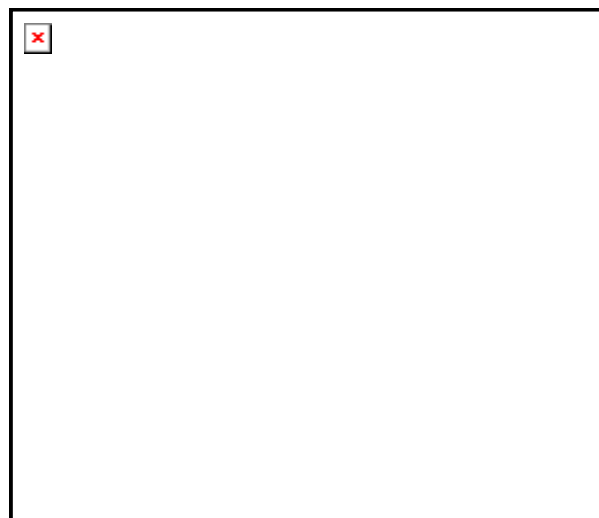
### 2.3.4 Inactive Password

The Inactive Password message on the login screen denotes that, because of failed attempts at logging in using an incorrect password, the system has locked the user from the database. In order to regain access to Cizer.Net, the administrator must reset the password in "User Management". If the **administrator** account becomes inactive, you must use the *Reset Inactive Password* query in Query Analyzer. This query automatically resets the admin password to "Admin".



### 2.3.5 Locked Out Password

When the user is validating through Windows authentication, the system will lock the User ID from the network after three incorrect login attempts.



**In order to regain access**, the domain administrator must go to the domain controller, and uncheck the Locked Out Password attribute for the user's domain account.


### 2.3.6 Reset Inactive Admin Password

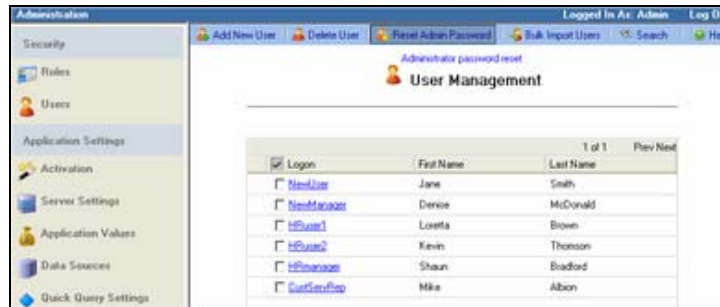
The Reset Inactive Password stored procedure resets the administrator password only. This stored procedure can be run in Query Analyzer against the CizerNet database. The Administrator is reset to password "Admin" by running the stored procedure in Query Analyzer against the Cizer Security Database. Upon logging in as "Admin", with "Admin" also as the password, you will see the password Expired screen, where you follow standard protocol to enter a new password.

```
secResetPassword 1, 'D07938B7C94BD412'
```



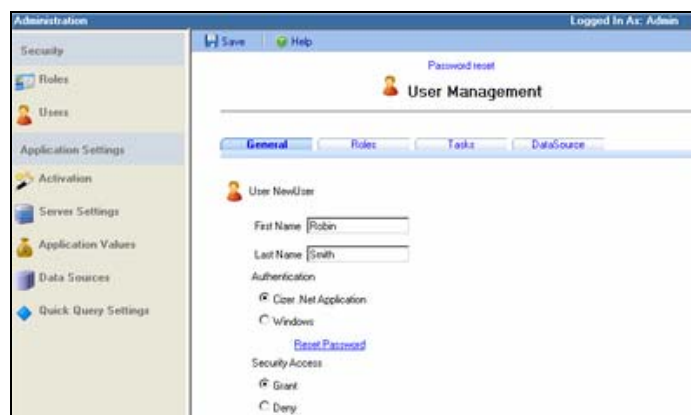
### 2.3.7 Reset Admin Password

 Located on the top menu bar of the User Management screen, "Reset Admin Password" also resets the Admin password to "Admin". You will be prompted to change the reset password upon logging in.




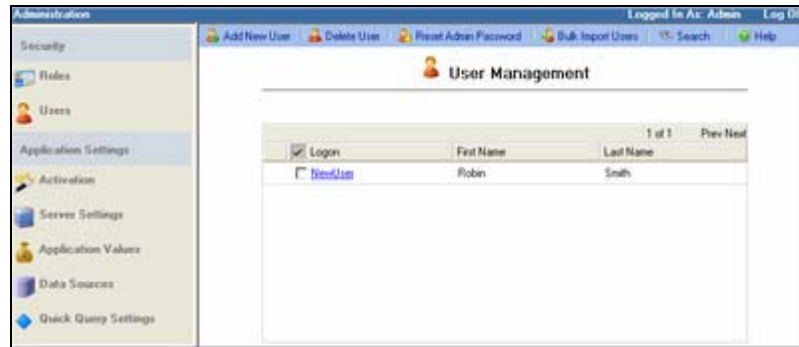
### 2.3.8 Reset User Password







The User Reset Password link allows the administrator to reset the User's password that has been deactivated for failed login attempts **when using Cizer.Net Authentication**. Resetting the password automatically defaults the password to be the same as the user id.



### 2.3.9 Manage Application Users

 The Users screen allows you to add or remove users in Cizer.Net Reporting. The default Administrator user ID account is "Admin" with "Admin" as the password. The top toolbar menu includes "Reset Admin Password". If you reset the Admin password it will always default to "Admin".

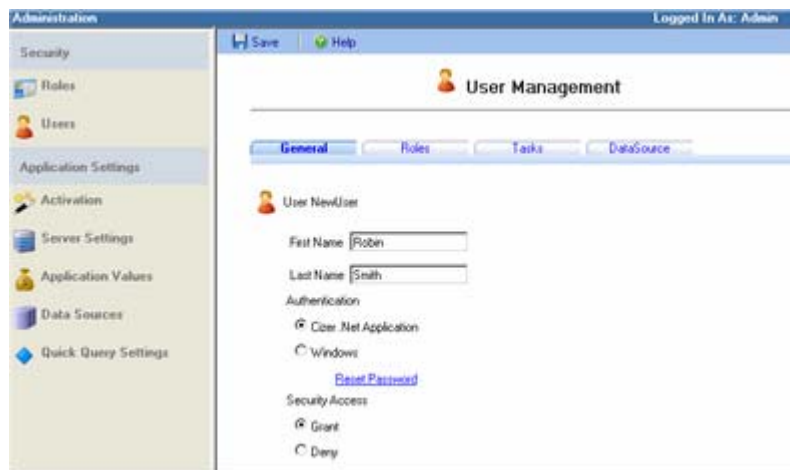


Toolset Items:	
	<b>Add New User:</b> See Section 2.3.9.5; " <i>Add a New User</i> ".
	<b>Delete User:</b> Deletes User when associated checkbox is marked. <b>Note: No warning message is displayed; user is immediately deleted.</b>
	<b>Reset Admin Password:</b> See Section 2.3.7; " <i>Reset Admin Password</i> ".
	<b>Bulk Import User:</b> See Section 2.3.9.6; " <i>Bulk Import Users</i> ".
	<b>Search:</b> When clicked, search criteria text boxes display above the User list. Enter a "Logon ID", "First Name" and/or "Last Name". For each entry, select the "Starts With", "Contains" or "Exact Match" radio button to narrow your search.
	<b>Help:</b> Access on-line help.

### 2.3.9.1 General Tab

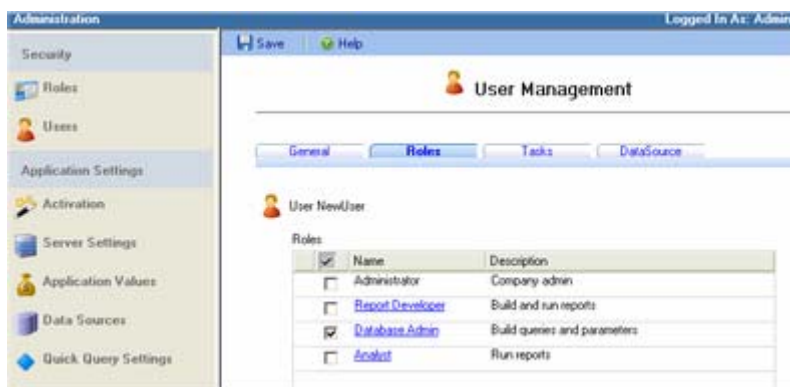
When adding a new User you will need to provide a logon id, name, and domain if the "Windows" Authentication radio button is selected. If you decide to add a user that will be a part of an application group ***the user id will be the password until your first logon attempt. In other words, the user id and password will initially be the same.*** The User will be required to provide a new password immediately following their first log-on. The "Reset Password" link resets the user's password to the logon ID.

Through "Security Access", the administrator has the ability to Grant or Deny Cizer.Net access to the User, should it become necessary to temporarily block a User, without having to completely delete them from the system.



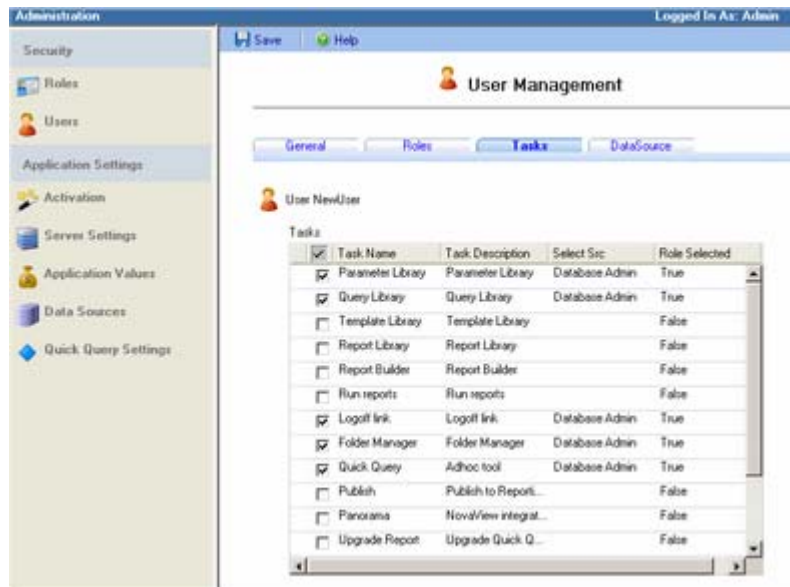
### 2.3.9.2 Roles Tab

The Roles tab allows the administrator to place a user within a particular role/group. Rights associated with the role will dictate access granted to the user who belongs to the role. See Section 2.3.10; "Manage Application Roles", for more detail on this topic.



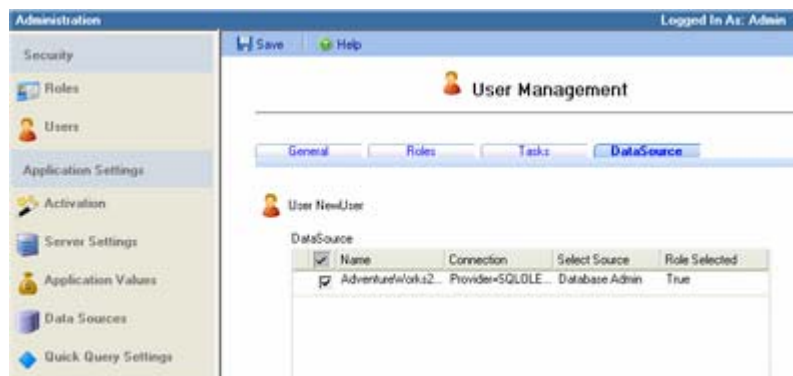
### 2.3.9.3 Tasks Tab

The Tasks tab allows the administrator to grant either all or certain rights that are associated with the Role. If there is a Role Task that you do not want to provide the user, remove the associated check mark and click "Save".





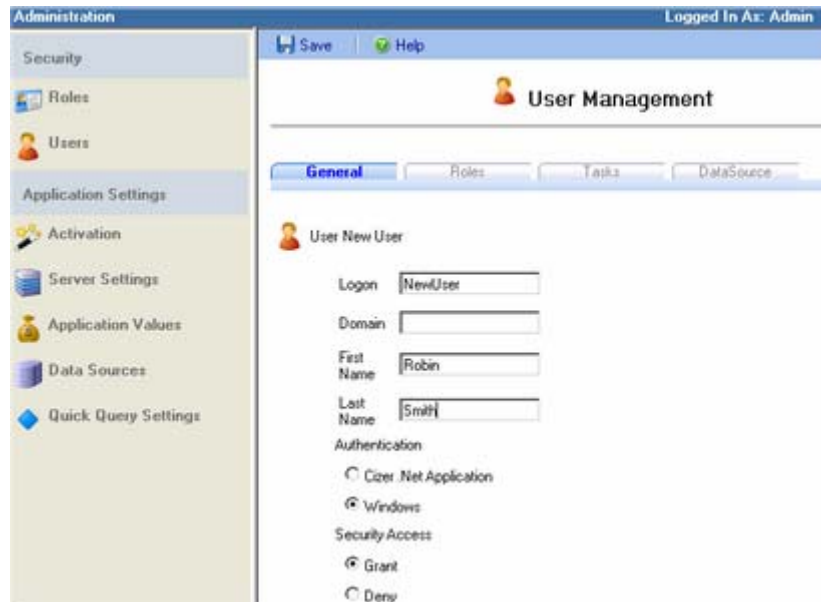
### 2.3.9.4 Data Sources

The Data Source tab allows the administrator to either grant or remove access to the individual data sources. To remove individual access to a data source, uncheck the box next to the appropriate data source. If you want to allow access to another data source, do so by selecting the checkbox next to the preferred data source.



### 2.3.9.5 Add a New User

1.  Click on "Users" in the control panel of the Admin screen. In the menu bar of the work area, click on  "Add New User".
2. At the General Tab, enter the User logon ID, first name, last name and select the appropriate radio buttons for Authentication and Security Access. If you select the "Windows" Authentication radio button, be sure to enter the appropriate domain in the text box that appears under the "Logon" text box.



3. You must first save the new user before you will be able to assign the user any roles, tasks or data sources.
4. Click on Roles. Select the Role(s) you wish to apply to the New User, or continue on to the Tasks tab.


*You can assign a New User to a predefined Role, and also add individual tasks to that User to elevate their capabilities beyond what their role membership provides. You can also remove individual tasks from a User that is assigned to a predefined Role to lower their capabilities provided by role membership.*

5. Click on Tasks; select the tasks you wish to be available to the New User. If you wish to select all tasks, click the check mark in the column header. Clear all checked items by selecting the grey box in the column header.

*You should not assign Administrator rights to any Role or User other than the actual Cizer.Net Administrator. If a user is assigned Administrator rights, they will have full access to the Cizer.Net Management Interface.*

6. Select the Data Source tab. Here you will see a list of all valid Data Sources defined within Cizer.Net. Select the appropriate Data Sources for this User.
7. Finally – **VERY IMPORTANT** – click "Save" on the menu bar of the work area. Failing to do so will result in a loss of all your changes.

### 2.3.9.6 Bulk Import Users

 Users can be bulk loaded into CNR by uploading a file that contains information about the user such as the User ID, First Name, Last Name, Authentication method and Role. The file must be a comma separated (delimited) file that contains the user information in the following format, with each line containing a carriage return at the end.

Proper Syntax:

*Login ID, First Name, Last Name, Authentication Type, Domain Name, Role*

NOTE: Quotes are **not** used around the entries ("Login ID", "First Name", etc.)

Authentication Types:

1 (Application): Does not check for Domain Name.

2 (Windows): Requires a Domain Name. When applying windows authentication, the Login ID must be the same as the user's network ID. The user will enter their network password at the login page rather than the application password.



Example of Windows Authenticated User:

*JSmith, John, Smith, 2, Cizer, Administrator*

Example of Application Authenticated User:


*JSmith, John, Smith, 1, , Administrator*

*Note: A space must represent the Domain Name for application authentication.*


Business Rules applied during upload/import:

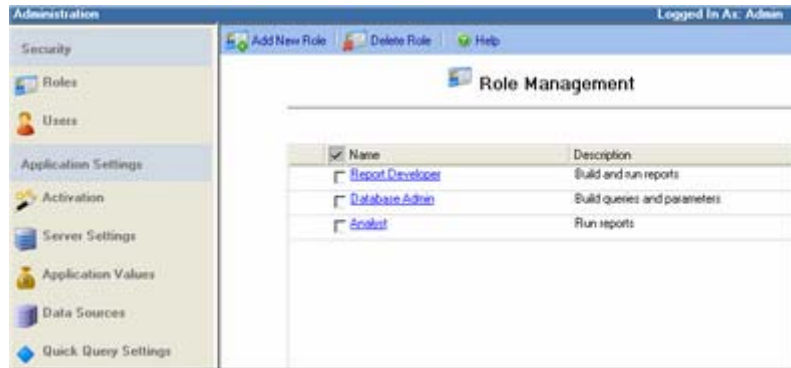
1. The length of the item in a row must be six. If there are first or last names with commas, the record will encounter an error.
2. The first item (Logon ID) must not be omitted. Any blank ID will be rejected. Logon IDs cannot contain the following reserved characters ; ? : @ & = + \$ , \ \* < > | " / , and cannot consist exclusively of dots.
3. If the Authentication Type is 2 (Windows) then a Domain Name must be provided.
4. *The role must already exist in the system.* If the user is assigned to a role that does not exist in the system, an error will occur. The Role is case sensitive and has to match exactly how it is stored in CNR. It is possible, but not recommended, to have two roles with the same exact name and case. In this case, the Bulk Import user will take the first one that is returned.
5. If a duplicate Logon ID is provided, the row will be rejected.
6. Processing of the file will continue up to 2 minutes. If the file has not completely processed by 2 minutes, the application provides an error that indicates the last line processed. You must delete all lines before and including the last line processed before uploading the file again.




Uploading Your Prepared Comma Delimited File:

 Select "Bulk Import Users" from the menu bar of the work area. The Bulk Import Users page displays with a "File Name" text box for entering the name and file path, or browsing to the location of the prepared file. Once the file is entered, click "Upload". Cizer reads the entire file one line at a time to make sure the expected syntax is correct and verifies that each line complies with all the business rules before adding the users to the database. If the syntax of a line being imported does not match the expected format, an error will be listed in the browser after all the records have processed.

### 2.3.10 Manage Application Roles

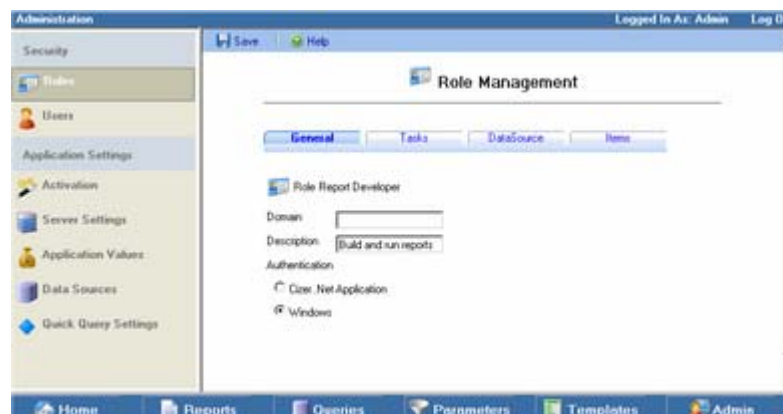
 The Role Management Section allows the administrator the ability to create, edit and delete roles that are assigned different rights and privileges. Windows Roles may also be added, allowing all Windows users, logged into that particular domain, access to Cizer.Net without having to add the users individually.



Toolset Items		
	<b>Add New Role:</b>	See Section 2.3.10.5; "Add a New Role".
	<b>Delete Role:</b>	Deletes Role when associated checkbox is marked. <b>Note: No warning message is displayed; role is immediately deleted.</b>
	<b>Help:</b>	Access on-line help.

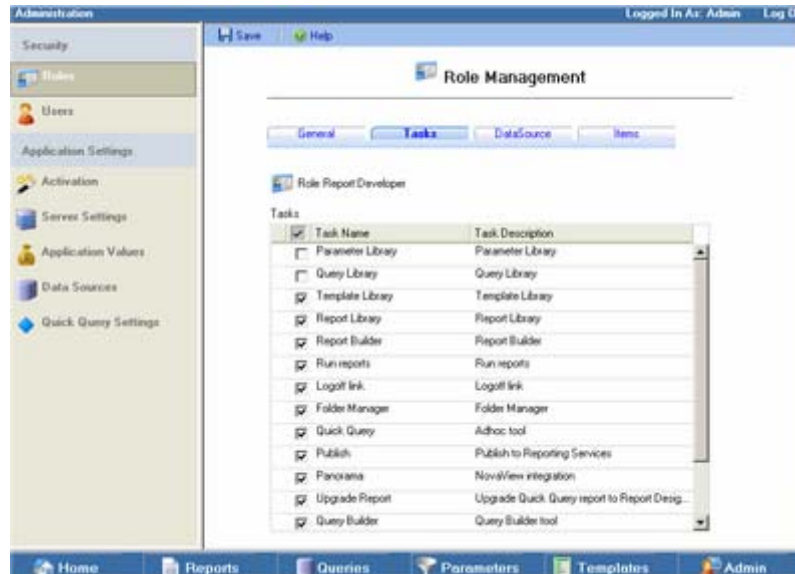
#### 2.3.10.1 General Tab

The General tab stores the description of the Role, as well as the method by which security is authenticated. If the "Windows" authentication radio button is selected, a "Domain" text box will display above the "Description" text box.



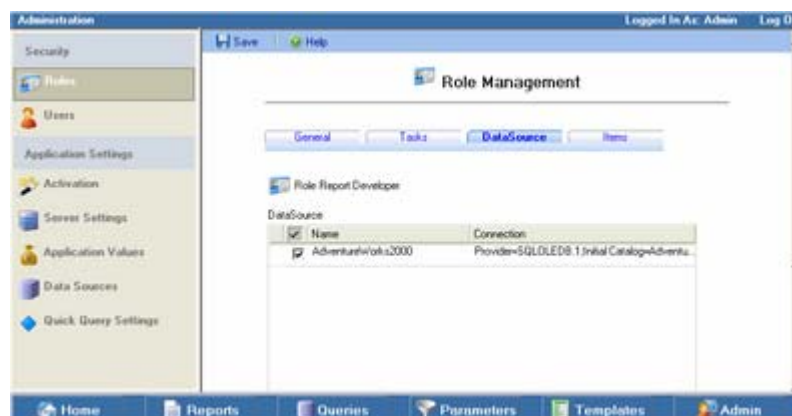
### 2.3.10.2. Tasks Tab

The Tasks tab allows the administrator to grant either all or certain rights that are associated with the Role. If there is a task that you do not want to provide to the Role, simply remove the check mark and click "Save".



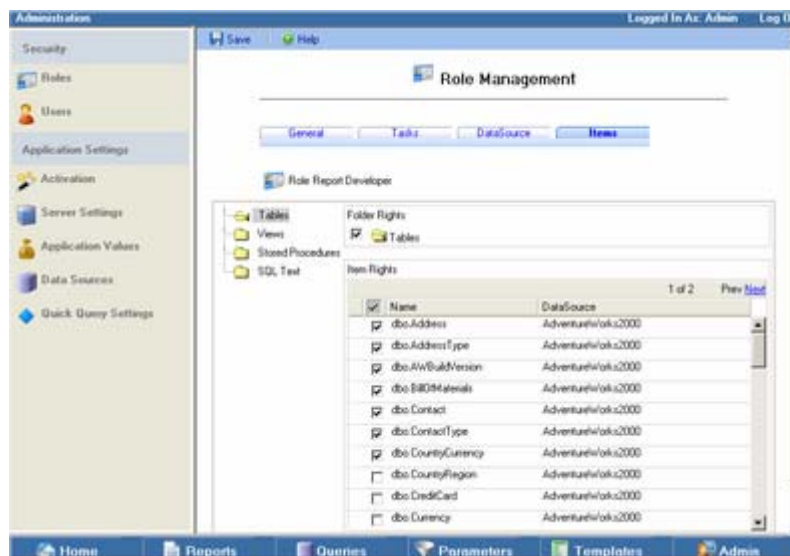
### 2.3.10.3 DataSources Tab

The Data Source tab allows the administrator to either grant or remove Role access to a data source. The data sources **MUST BE ADDED FIRST** in the Data Source Section of Application Settings. To allow access to a data source, check the box next to the preferred data source.




### 2.3.10.4 Items Tab

Roles can be assigned access to some, all or none of the Tables, Views and Stored Procedures in your database for use in Quick Query or Query Builder. Only Table and View items are accessible in Query Builder. SQL Text allows the user to manually enter SQL statements in Quick Query. Select the checkbox next to the Folder and Item(s) the Role should have access to. Select the check mark in the column header to check all the items within the selected folder at once. Clear all checked items by selecting the grey box in the column header.



### 2.3.10.5 Add a New Role

1.  Click on "Roles" in the control panel of the Admin screen. In the Role Management work area, click on "Add New Role".
2. At the General Tab, give the role a name and a description. Choose the Authentication method, entering the appropriate domain in the text box that appears under the "Name" text box if you select the "Windows" Authentication radio button to add a Windows Role.
3. Click "Save".
4. Click on Tasks; select the tasks to be available to the New Role.

*You should not assign Administrator rights to any Role or User other than the actual Cizer.Net Administrator. If a User is assigned Administrator rights, either individually or through a Role, they will have full access to the Cizer.Net Management Interface.*

5. Click on the Data Source tab. Here you will see a list of all valid Data Sources defined within Cizer.Net. Select the appropriate Data Sources for this New Role.
6. Select the Items tab. A tree displays with folders labeled Table, Views, Stored Procedures and SQL Text. Open each folder and select the folder and items within the folder that the New Role should have access to in order to create reports in Quick Query. *Users will only be able to see the items you have granted to them.*
7. Finally – **VERY IMPORTANT** – click "Save" on the menu bar of the work area. Failing to do so will result in a loss of all your changes.

## 2.4 Cizer.Net Management Interface: Application Settings

### 2.4.1 Activation



The Activation section gives you information about Cizer.Net and also activates the product with an activation key. A temporary activation key is delivered to the email address supplied in the software download form. Copy the key into the Activation Key Text Box and click the Save button. If you are utilizing a web farm setup, be sure to select the desired server name from the Server drop down menu to enter the correct activation key to its corresponding server.

The version of Cizer.Net installed on your server(s) will be available in the Activation Screen, along with the **Product Key**. The product key is specific to the server where Cizer.Net is installed. ***The Product Key will be needed by Cizer Support to generate a permanent activation key.*** Note that in a web farm set up, the product key will change depending on the server you've been directed to by network load balancing.

After you enter a new Activation Key into the space provided, remember to click the Save button. If for any reason the Activation Key is incorrect, an error will display after a failed attempt at saving.

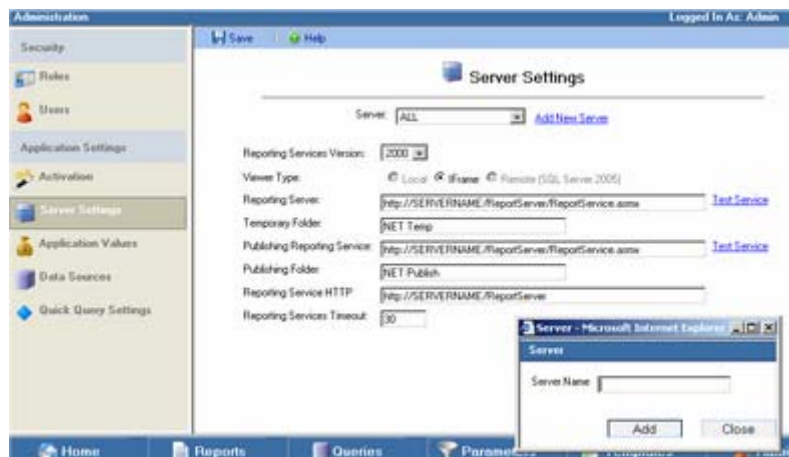
If you are accessing CNR through a hosted application, the Application screen will not be available to you.

Please contact [support@cizer.com](mailto:support@cizer.com) if you have any questions.

### 2.4.2 Server Settings

The Server Settings section allows you to define your server(s), Reporting Services and viewer connections. In the case of a web farm setup, the name of each server on the web farm must be added through the "Add New Server" link. For the Reporting Services connections, be sure to replace "localhost" with the server name. The "Test Service" links should be used to ensure proper connection to the Reporting Services server. If the connection is unsuccessful, make sure Reporting Services has been configured properly and that all user names and passwords are correct.

If you are accessing CNR through a hosted application, the Server Settings screen will not be available to you.



Server Settings	
<b>Server:</b>	For web farms, select the name of the server you wish to configure, or select "All" to apply the same settings to all the servers in the web farm. Standalone installations need not enter their CNR server name through the "Add New Server" link; they may configure their server settings using "All", even though they are only using one server.
<b>Add New Server:</b>	For web farm setups, the name of each server on the web farm must be added through the "Add New Server" link.
<b>Reporting Services Version:</b>	None, 2000, 2005
<b>Viewer Type:</b>	Cizer.Net includes three viewer type options, IFrame, local and remote, each dependant on if, and what version of, SQL Server Reporting Services will be accessed.
<b>Reporting Server:</b>	Identifies the location of the Microsoft Reporting Services server, for example: <i>http://Reporting_Services_server_name/ReportServer/ReportService.asmx</i>
<b>Temporary Folder:</b>	Identifies the folder where all temporary files are stored.
<b>Publishing Reporting Service:</b>	Identifies the location of the Reporting Service (it should be the same location as the Reporting Server above).
<b>Publishing Folder:</b>	Identifies the folder where published reports are saved.
<b>Reporting Services Timeout:</b>	Value equals the number of seconds Microsoft Reporting Services will process a report before it times out.
<b>Reporting Service HTTP:</b>	Enter the Reporting Service HTTP.

### 2.4.3 Application Values



The Application Values section allows you to configure settings specific to the CNR application.

If you are accessing CNR through a hosted application, the Application Values screen will not be available to you.



Application Values	
<b>Max Filter Count:</b>	The maximum number of values displayed during a Quick Query Filter Lookup.
<b>Data Source Timeout:</b>	Value equals the number of seconds an application data source can be connected to the database before it times out.
<b>Image Path:</b>	Identifies the folder where images are saved. <i>Note: In web farms the image path is configured in the CNR web.config file, rendering this path entry invalid.</i>
<b>Log/Image Directory:</b>	Identifies the folder where log files and the Image folder are located.
<b>Password Expiration:</b>	Number of days before a new password expires.
<b>Windows Auto Logon:</b>	Select this checkbox to enable network authentication logon. See Section 2.4.3.1; "Using Windows Authentication" for further instructions.
<b>Enable Admin Account LockOut:</b>	Select this checkbox to limit Admin logon to three failed attempts.
<b>Query Governor Cost Limit:</b>	CNR estimates the number of seconds needed to process a query. If the number of seconds estimated is more than the Cost Limit value entered, CNR will not process the report. This helps avoid hanging the server when there is an overly large amount of data being returned.

If you are using a viewer that requires SQL Server Reporting Services and you wish to install Cizer.Net Reporting on a machine separate from Reporting Services, edit the URL path(s) to point to the correct location, and follow the steps in Section 1.3; "Advanced Configuration". Use the "Test Service" links to test your connection.

### 2.4.3.1 Using Windows Authentication

In addition to creating a Windows user in Cizer.Net and checking the Application Values "Windows Auto Logon" checkbox, two more steps are required for a Windows user to bypass the Cizer.Net Logon Screen:

1. Change impersonation in the web.config file(inetpub/wwwroot/cnr) from "false" to "true".

Ex. `<identity impersonate="true" />`



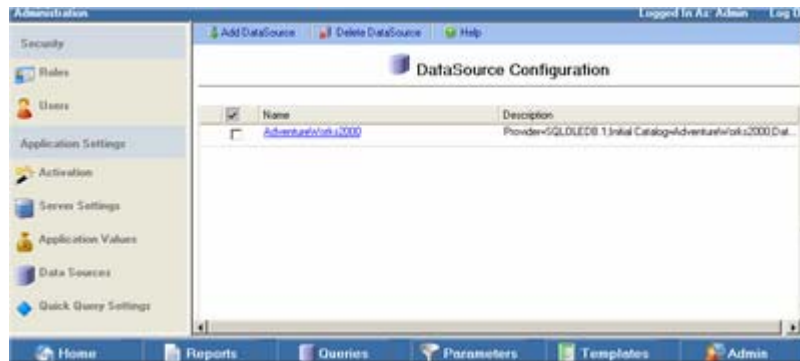
2. Make sure Anonymous Access is unchecked in IIS Directory Security.



### 2.4.4 Data Sources



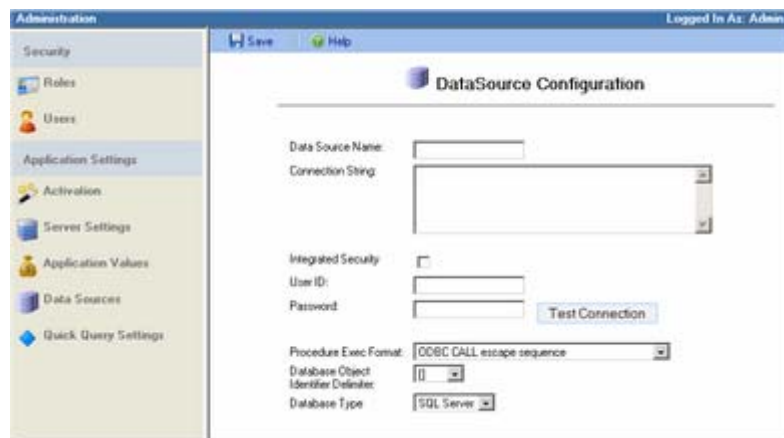
The Data Sources section allows you to connect to databases on any server in your network. If the correct connection string and user id/password are provided, you will be connected to the database you want to query.



**Note:** The AdventureWorks database connection is installed by default, but you must edit the Data Source in the connection string from "(local)" to the actual server name, and enter the correct User ID and Password in order to access the database.

#### 2.4.4.1 Adding and Managing Data Sources

1. From the menu bar, click on "Add DataSource".
2. Enter the Connection string, login and database information. The DataSource name you define in the Connection String will display in the End User Interface. See section 2.4.4.2; "Connection String Examples".
3. Test your connection before clicking on "Save All" to save the information you've entered.



**Integrated Security:** If the data source connection is using Windows Authentication, check the Integrated Security check box. You must use the "Trusted Connection" connection string when using Integrated Security. See section 2.4.4.2; "Connection String Examples".

The **Procedure Exec Format**, **Database Object Identifier Delimiter** and **Database Type** are defaulted to work with SQL Server ODBC database connections. This ODBC connection can also be used for OLE DB. If you are using another type of database connection, please select the appropriate connection in the drop-down menu.

### 2.4.4.2 Connection String Examples

Cizer.Net always uses an OLE DB connection string. Refer to the following examples when entering a connection string:

#### **Standard Security:**

```
Provider=SQLOLEDB;Data Source=Your_Server_Name;Initial Catalog=Your_Database_Name
```

#### **Trusted Connection:**

```
Provider=SQLOLEDB;Data Source=Your_Server_Name;Initial Catalog=Your_Database_Name;Integrated Security=SSPI;
```


*(use serverName\instanceName as Data Source to use an specific SQLServer instance, only SQLServer2000)*

#### **Connect via an IP address:**

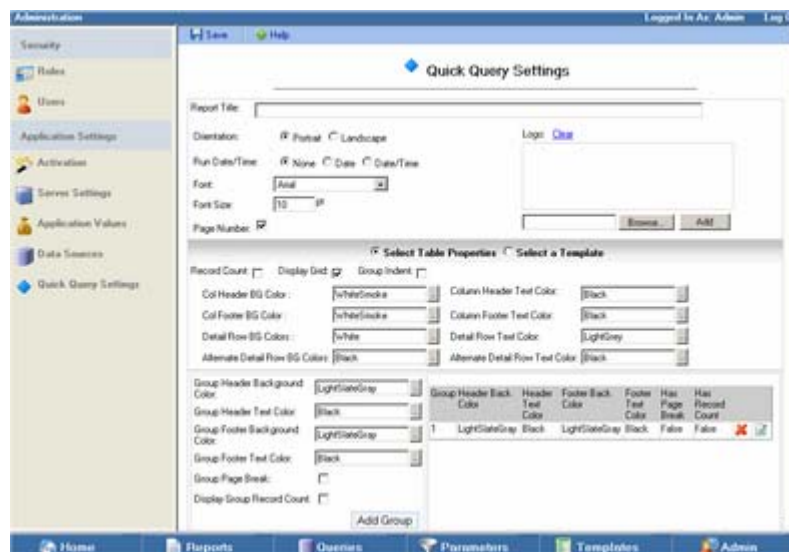
```
Provider=sqloledb;Data Source=Your_IP_Address;Network Library=DBMSSOCN;Initial Catalog=Your_Database_Name
```

*(DBMSSOCN=TCP/IP instead of Named Pipes, at the end of the Data Source is the port to use (1433 is the default))*



### 2.4.5 Quick Query Settings

 Businesses often require specific formatting of their reports to reflect company colors, font styles and design. Quick Query Settings allows configuration of default report and grouping formats to ensure a consistent look and feel of reports. After the Cizer.Net Reporting administrator configures the desired settings, Quick Query automatically applies the format when accessed by the end user.

To begin, click on "Quick Query Settings". Define details such as the layout and colors in the report, and other important information you would like to include that does not come from the database itself. Click "Save" to apply your settings.

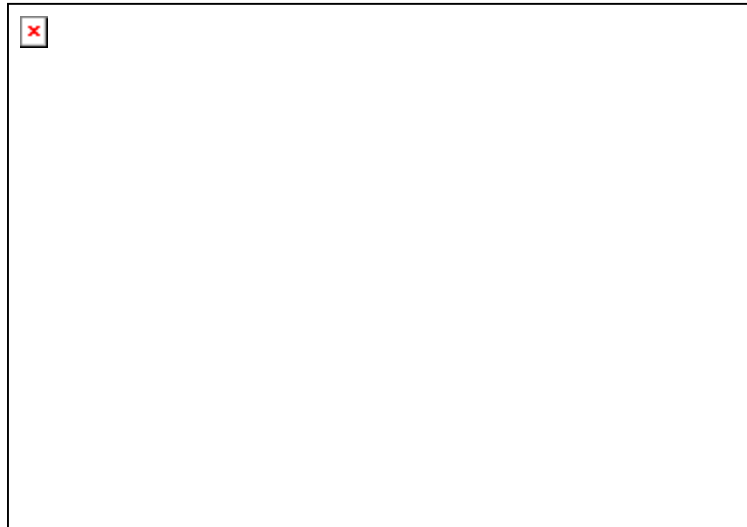


Quick Query Formatting Options	
<b>Add Group:</b>	Create individually formatted groupings by selecting the desired group settings and clicking "Add Group". The formatted group is now listed on the right, with a group number assigned. Each new group added is assigned a subsequent number. When configuring a Quick Query report, the first grouping added displays the first group format listed in the Quick Query Settings. If there are more groupings in the report than there are group formats listed in Settings, the additional groupings acquire the last group format configured in Quick Query Settings.
<b>Column Header and Footer Background Colors:</b>	Choose a background color for the Column Header or Footer. Standard web color names and hexadecimal values are accepted. The ellipsis button to the right of the text box displays the three-tab color palette window, where you can choose any of the standard "web-safe" colors, a variety of named colors, or design a color using the red, green and blue custom sliders.
<b>Column Header and Footer Text Color:</b>	Choose a text color for the Column Header or Footer. Standard web color names and hexadecimal values are accepted. The ellipsis button to the right of the text box displays the three-tab color palette window, where you can choose any of the standard "web-safe" colors, a variety of named colors, or design a color using the red, green and blue custom sliders.
<b>Detail Row and Alternate Detail Row Background and Text Colors:</b>	Choose background and text colors for the Detail Rows. Standard web color names and hexadecimal values are accepted. The ellipsis button to the right of the text box displays the three-tab color palette window, where you can choose any of the standard "web-safe" colors, a variety of named colors, or design a color using the red, green and blue custom sliders. The second Detail Row Colors will be the color of the alternating row.

<b>Display Grid:</b>	When checked, grid lines will show in the report to separate the rows and columns of data. This option holds if the report is printed as well.
<b>Display Group Record Count:</b>	Adds a group record count for the group.
<b>Font:</b>	Choose a Font from the drop-down list. All column headers and detail rows of the report will display in the chosen font.
<b>Font Size:</b>	Type a Font Size into the text box. All column headers and detail rows of the report will display in the chosen font size.
<b>Group Header Background and Text Color:</b>	Choose background and text colors for the Group Header(s). Standard web color names and hexadecimal values are accepted. The ellipsis button to the right of the text box displays the three-tab color palette window, where you can chose any of the standard "web-safe" colors, a variety of named colors, or design a color using the red, green and blue custom sliders.
<b>Group Footer Background and Text Color:</b>	Choose background and text colors for the Group Footer(s). Standard web color names and hexadecimal values are accepted. The ellipsis button to the right of the text box displays the three-tab color palette window, where you can chose any of the standard "web-safe" colors, a variety of named colors, or design a color using the red, green and blue custom sliders.
<b>Group Indent:</b>	In Detail reports, when checked, the report detail rows will be indented a couple spaces beneath each group description.
<b>Group Page Break:</b>	When checked, inserts a page break after each record grouping.
<b>Logo:</b>	Insert a company logo or other .jpg, .gif or .png file by utilizing the "Browse" and "Add" buttons. The image will appear at the top left of the report. Remove the image by clicking the "Clear" link.
<b>Orientation:</b>	Choose the "Portrait" or "Landscape" radio button for the preferred page layout. "Portrait" is selected by default.
<b>Page Number:</b>	When checked, the page number will display at the bottom right of each page of the report.
<b>Record Count:</b>	When checked, the total number of all records is displayed at the top right of the report. Group record counts appear in the group header, after the group name, as (Count: X).
<b>Report Title:</b>	Type a title for your report into this text box.
<b>Run Date/Time:</b>	Choose the "None", "Date" or "Date/Time" radio button for the desired display on the page footer. "None" is selected by default.
<b>Select Table Properties:</b>	Displays table property formatting options.
<b>Select a Template:</b>	Displays a list and preview of saved Table Templates.
	Delete the saved formatted group.
	Edit the saved formatted group.

## Appendix A: Report URL Call Extension

The Report URL Call extension provides Cizer customers with a powerful engine for integrating their custom applications with Cizer.Net Reporting. This reporting extension allows customer applications to request report information from the Cizer web service and then run reports using a simple URL request. Encrypted tokens are utilized to secure connections between the customer application and the Cizer web service.



1. The customer application requests an authentication token from the Cizer custom security extension using the current user logon id.
2. The customer application requests a report list for the current user by calling the Cizer web service using the authentication token. The Cizer web service returns a list of reports and a secure session token for each report.
3. The customer application uses the report list to build hyperlinks based upon the report session tokens. A user click of a link will automatically authenticate the user to CNR and run the selected report.

### **Business Rules:**

1. Custom security authentication token expires after 10 minutes.
2. Web service report session token expires after 10 hours.
3. Report list returned from web service is restricted by CNR logon id.
4. Each report item contains a different session token.
5. The following reports can be run with a URL call:
  - a. Quick Query
  - b. CNR
  - c. Panorama
  - d. External
6. URL call report display:
  - a. Quick Query reports are displayed in the Quick Query module and are not automatically run.
  - b. CNR reports, with parameters, are displayed in the parameter panel and are not automatically run.
  - c. CNR reports, without parameters, are automatically run.
  - d. External reports are automatically run.

7. Web service returns the following report properties:
  - a. Name
  - b. Token (URL report call)
  - c. Description
  - d. Author
  - e. Create timestamp
  - f. Last update timestamp
  - g. Report type (Quick Query, CNR)
  - h. Favorite (yes or no)
  
8. Use case is valid for the following Cizer security authentication models:
  - a. Cizer
  - b. Windows
  - c. Windows Roles
  - d. Security extension

A sample application is included along with the URL Call Extension web-service that shows how the web-service can be called from an external application.

## Appendix B: Configuration with Panorama NovaView

Several configuration and administration steps are required in order to utilize Panorama NovaView with Cizer.Net Reporting.

### Internet Information Services:

1. Disable Anonymous Access.
2. Enable Windows Authentication.

### Cizer.Net Reporting web.config file:

1. Line 9: Remove comment tags. Change "NovaViewServer" value to equal the name of your NovaView server:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="exceptionManagement" type="Microsoft.ApplicationBlocks.ExceptionManagement.ExceptionManagerSectionHandler,
  </configSections>
  <appSettings>
    <add key="CizerConnectionString" value="server=CIZERNETSERVERNAME;uid=sa;pwd=*****;initial Catalog=CizerNet" />
    <add key="RSPProvider" value="Provider=SQLOLEDB" />
    <add key="NovaViewServer" value="NOVAVIEW_SERVER_NAME" />
  </appSettings>
  <!-- exception management -->
  <exceptionManagement>
    <publisher mode="on" assembly="Cizer.ExceptionManagement" type="Cizer.ExceptionManagement.TextFileExceptionPublisher" />
  </exceptionManagement>
</system.web>
```

<!--<add key="NovaViewServer" value="SERVER\_NAME">--> to  
<add key="NovaViewServer" value="NOVAVIEW\_SERVER\_NAME">

2. Line 58: Change "identity impersonate" value to "true".

```
<authentication mode="windows" />
<!--
  identity Attributes:
    impersonate="[true|false]" - Impersonate windows user
    userName="windows user account to impersonate" | empty string implies impersonate the LOGON U
    password="password of above specified account" | empty string
-->
<identity impersonate="true" />
<!--<identity impersonate="true" userName="domain\newaccount" password="newaccount" />-->
<!-- AUTHORIZATION
  This section sets the authorization policies of the application. You can allow or deny access
  to application resources by user or role. wildcards: "*" mean everyone, "?" means anonymous
  (unauthenticated) users.
-->
```

### Cizer.Net Administration:

Users and Roles must be added to Cizer.Net utilizing Windows Authentication. See section 3.3.9.6; "Add a New User" and section 3.3.10.5; "Add a New Role".

## Index

- .
- .net, 1, 5
- A**
  - access, 34
  - activation, 16, 31, 32
  - add, 35
  - admin, 16, 17, 23, 28
  - administrator, 16
  - adventureworks, 35
  - anonymous, 34
  - application, 23, 28, 33
  - authentication, 18, 33, 34
  - authorization, 18
  - auto, 33
- B**
  - bulk, 27
- C**
  - catalog, 36
  - configuration, 13, 39, 41
  - connection, 36
  - count, 33
  - CQQ, 37
- D**
  - database, 35
  - datasource, 25, 29, 35
  - datasources, 35, 36
  - delete, 35
  - delimiter, 35
  - directory, 34
- E**
  - exec, 35
  - expired, 20
  - extention, 39
- F**
  - filter, 33
  - folder, 33
  - form, 18
  - format, 35
- G**
  - general, 24, 28
  - groups, 37
- H**
  - http, 33
- I**
  - IFrame, 4
  - IIS, 1, 5, 34
  - import, 27
  - inactive, 21, 22
  - integrated, 35
  - invalid, 20
  - IP, 36
  - items, 30
- K**
  - key, 16, 31, 32
- L**
  - level, 19
  - local, 1, 2
  - locked, 21
  - lockout, 33
  - login, 15
  - logo, 15
  - logon, 33
- M**
  - max, 33
- N**
  - new, 26, 30, 35
  - NovaView, 41
- O**
  - object, 35
  - ODBC, 35
  - OLEDB, 35
- P**
  - Panorama, 41
  - password, 16, 20, 21, 22
  - portal, 15
  - procedure, 35
  - product, 31
  - provider, 36
- R**
  - remote, 5, 6
  - requirements, 1, 5
  - reset, 22
  - role, 30
  - roles, 16, 18, 24, 28, 29, 30
  - row, 19
- S**
  - samples, 36
  - security, 16, 17, 18, 19, 34, 36
  - settings, 37
  - SharePoint, 13
  - SQLOLEDB, 36
  - string, 36
- T**
  - tasks, 25, 29
  - Tech Support Line, ii
  - template, 37
  - temporary, 33
  - timeout, 33
  - trusted, 36
- U**
  - URL, 33
  - URLcall, 39
  - user, 22, 24, 25, 26
  - users, 16, 18, 23, 27
- V**
  - values, 33
  - viewer, 1, 2, 4, 5, 6
- W**
  - webfarm, 2, 4, 6, 13
  - windows, 18, 33, 34