UC for Enterprise (UCE) Emergency On-Site Notification (E-OSN)

Installation Guide

N E C NEC Corporation

September 2010
NDA-31053 Issue 2

Liability Disclaimer

NEC Corporation reserves the right to change the specifications, functions, or features, at any time, without notice.

NEC Corporation has prepared this document for the exclusive use of its employees and customers. The information contained herein is the property of NEC Corporation and shall not be reproduced without prior written approval from NEC Corporation

NEAX and Dterm are registered trademarks of NEC Corporation.

© 2010 NEC Corporation

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brand or product names are or may be trademarks or registered trademarks of, and are used to identify products or services of, their respective owners.

Contents

Introduction 1-1

Overview 1-1

How This Guide is Organized 1-1

Installation 2-1

Before Installing UCE Emergency On-Site Notification 2-1
- UCE Emergency On-Site Notification Limitations and Disclaimers 2-1
- Licensing 2-2
- Server Requirements 2-2
- SQL Server Report Service 2-2
- Client and PBX Requirements 2-3

Installing the UCE Emergency On-Site Notification Application 2-3

Installing the E-OSN Client 2-6

Installing SQL Server Report Service 2-9

Configuring the Reporting Services for SQL 2005 2-9
- Loading the SQL Service Report Service 2-15

Configuring the Reporting Services for SQL 2008 2-19
- Service Account 2-20
- Web Service URL 2-22
- Database 2-23
- Report Manager URL 2-30
- Loading the SQL Service Report Service 2-32

Configuring the Reporting Services for SQL Services 2008 R2 2-36
- Service Account 2-37
- Web Service URL 2-39
- Database 2-40
- Report Manager URL 2-46
- Loading the SQL Service Report Service 2-47

Configuration 3-1

Login Authorization 3-1
Selecting Desired User Role 3-2

Route Configuration 3-3
Adding/Editing UCE Emergency On-Site Notification Routes 3-3

Emergency Notification Administration 3-5
Emergency Notification Client Settings 3-6
E-OSN Workstations 3-8
Notification Configuration 3-11
Reports 3-15
System Test 3-18
Trunk Monitor Status 3-21

Email Notification 3-22

MA4000 Location Data Sync 3-24

Figures

Figure	Title	Page
2-1	E-OSN Welcome Dialog Box	2-4
2-2	Ready to Install Dialog Box	2-5
2-3	Installing Message Center Dialog Box	2-5
2-4	Installation Complete Dialog Box	2-6
2-5	File Download - Security Warning	2-7
2-6	Emergency Notification Client Welcome Dialog Box	2-7
2-7	E-OSN Client Ready to Install	2-8
2-8	E-OSN Client Installing	2-8
2-9	Install Shield Wizard Complete	2-9
2-10	2005 Reporting Services Configuration	2-10
2-11	2005 Instance Selection dialog box	2-10
2-12	2005 Report Server Status dialog box	2-11
2-13	Report Server Virtual Directory Settings dialog box	2-11
2-14	2005 Report Manager Virtual Directory dialog box	2-12
2-15	Task Status dialog box	2-12
2-16	Database Connection dialog box	2-13
2-17	New SQL Server Connection Dialog	2-14
2-18	Database Connection Confirmation dialog box	2-15
2-19	2005 Role Assignment dialog box	2-16
2-20	2005 New Role Assignment dialog box	2-16
2-21	2005 Settings dialog box	2-17
2-22	2005 Reports Confirmation dialog box	2-18
2-23	2008 Reporting Services Configuration	2-19
2-24	2008 Instance Selection dialog box	2-19
2-25	2008 Report Server Status dialog box	2-20
2-26	2008 Service Account dialog	2-21
2-27	2008 Web Service URL dialog box	2-22
2-28	Confirmation dialog box	2-23
2-29	2008 Report Server Database dialog box	2-24
2-30	Change Database—Action dialog box	2-25
2-31	Change Database—Database Server dialog box	2-26
2-32	Test Connection Confirmation dialog box	2-26
2-33	Change Database—Database dialog box	2-27
2-34	Change Database—Credentials dialog box	2-28
2-35	Change Database—Summary dialog box	2-28

2-36 Change Database—Progress and Finish dialog box . . . 2-29
2-37 Report Server Database—Database option . . . 2-30
2-38 2008 Report Manager URL dialog box . . . 2-31
2-39 2008 SQL Server Reporting Services Home . . . 2-31
2-40 2008 SSRS Properties Page . . . 2-32
2-41 2008 New Role Assignment dialog box . . . 2-33
2-42 2008 Settings dialog box . . . 2-33
2-43 2008 Reports Confirmation dialog box . . . 2-34
2-44 Reports Home page . . . 2-34
2-45 2008 R2 Reporting Services Configuration . . . 2-36
2-46 2008 R2 Instance Selection dialog box . . . 2-36
2-47 2008 R2 Report Server Status dialog box . . . 2-37
2-48 2008 R2 Service Account dialog . . . 2-38
2-49 2008 R2 Web Service URL dialog box . . . 2-39
2-50 2008 R2 Web Service URL—Confirmation dialog box . . . 2-40
2-51 Report Service Database . . . 2-40
2-52 Change Database—Action dialog box . . . 2-41
2-53 Change Database—Database Server dialog box . . . 2-42
2-54 Test Connection Confirmation dialog box . . . 2-42
2-55 Change Database—Database dialog box . . . 2-43
2-56 Change Database—Credentials dialog box . . . 2-43
2-57 Change Database—Summary dialog box . . . 2-44
2-58 Change Database—Progress and Finish dialog box . . . 2-45
2-59 Report Server Database—Database option . . . 2-45
2-60 2008 R2 Report Manager URL dialog box . . . 2-46
2-61 2008 R2 SQL Server Reporting Services Home . . . 2-47
2-62 2008 R2 Role Assignment dialog box . . . 2-47
2-63 2008 R2 New Role Assignment dialog box . . . 2-47
2-64 2008 R2 New Role Assignment Datafill . . . 2-48
2-65 2008 R2 Settings dialog box . . . 2-48
2-66 2008 R2 Reports Confirmation dialog box . . . 2-49
2-67 Report Manager—Home . . . 2-49
3-1 User Type Selection . . . 3-2
3-2 Route/Trunk Management . . . 3-3
3-3 Add/Edit Route/Trunk Management dialog box . . . 3-4
3-4 Add/Edit Route/Trunk confirmation . . . 3-5
3-5 E-OSN Administration application . . . 3-6
3-6 E-OSN Client Settings . . . 3-7
3-7 E-OSN Workstation Configuration . . . 3-8
3-8 E-OSN Client Workstations . . . 3-9
3-9 Add/Modify New Workstation . . . 3-9
3-10 Notification Configuration . . . 3-12
3-11 Group Management . . . 3-12
3-12 Add a New Group . . . 3-13
3-13 Editing a Group . . . 3-14

3-14 Add Email by Person 3-14
3-15 Adding a new Email Prompt 3-15
3-16 Contact Method 3-15
3-17 Reports 3-16
3-18 Report Filters and Criteria 3-17
3-19 Emergency On-Site Call History Generated Report 3-17
3-20 Link Failure Notification 3-19
3-21 Successful Emergency Call Test 3-20
3-22 Trunk Monitor Status 3-21
3-23 Path to Email Notifications 3-22
3-24 Email Notification 3-23
3-25 SHOW NENA DAtA 3-25
3-26 Expanded NENA DATA 3-26

Tables

Table	Title	Page
2-1	VS-32 Requirements for Conference.	2-3
3-1	Emergency Call Test Field Descriptions	3-20

1

Introduction

The *UCE Emergency On-Site Notification (E-OSN) Installation Guide* provides the information you need to install and configure the E-OSN application.

The following topics are included in this chapter:

Chapter Topics

- *Overview*
- *How This Guide is Organized*

Overview

The UCE Emergency On-Site Notification (E-OSN) feature monitors a specific trunk group for outbound calls and then generates notifications to individuals within an organization as to the nature of the call, the calling station/user, and the physical location of the call.

This feature also notifies people in multi-room buildings of the arrival of emergency personnel and premise emergency situations. They can then properly direct the emergency responders to the correct location with the highest level of efficiency, thereby cutting the response time and limiting their own liability.

How This Guide is Organized

Chapter 1
Introduction
This chapter outlines how to use the manual including the organization and chapter layout of the UCE Emergency On-Site Notification (E-OSN) Installation Guide.

Chapter 2
Installation
This chapter describes the installation process of the UCE Emergency On-Site Notification (E-OSN).

Chapter 3
Configuration
This chapter provides the steps and information needed to start and configure the E-OSN.

2

Installation

This chapter describes the installation process and requirements for the UCE Emergency On-Site Notification (E-OSN).

Chapter Topics

- *Before Installing UCE Emergency On-Site Notification*
- *Installing the UCE Emergency On-Site Notification Application*
- *Installing the E-OSN Client*
- *Installing SQL Server Report Service*
- *Configuring the Reporting Services for SQL 2005*
- *Configuring the Reporting Services for SQL 2008*
- *Configuring the Reporting Services for SQL Services 2008 R2*

Before Installing UCE Emergency On-Site Notification

This section describes the required components that must be in place before installing the E-OSN application.

IMPORTANT

You must read the following UCE Emergency On-Site Notification Limitations before proceeding.

UCE Emergency On-Site Notification Limitations and Disclaimers

- In a fusion PBX network, there is a limitation of being able to select notification groups by PBX because OW5000 requires all extensions to be entered under the main fusion node.
- In certain situations, E-OSN may not be able to properly deliver notifications due to external applications or hardware. For example, not being able to disable the screen saver to pop on an E-OSN Client, PC sound not enabled or working for audio notification, SMTP mail server not configured or working to receive e-mail notification.
- The dialed emergency number may not be available in all situations.
- The originating calling party caller ID may not be available if the out-bound emergency trunk is CCIS to the caller.
- The originating calling party information will not be available if the station does not exist in the OW5000 database.
- In a non-unique numbering plan, where the calling party's extension is not unique in the OW5000 database, the Callers name and location

will not be displayed and the Route trunk Info will not contain the PBX name. Email notifications will not be sent.

- In a remote trunking situation (CCIS trunks) where the caller's emergency trunk is not on the same PBX as the caller's station, the notified group will be the caller's PBX group not the trunk's.
- In order to join a call in progress, an E-OSN Workstation must be configured on the PBX the caller originated from (with valid prime line and emergency line).
- E-OSN Audit log reports will not contain information on the person or user performing **Listen In**, **Conference**, or **Acknowledge** when picking up the emergency line. The only piece of information that will be logged is the E-OSN workstation name (description) that was used to monitor or conference the call. If the E-OSN Client was logged into the E-OSN workstation for that Dterm, then the E-OSN user information is available.
- If a caller originates an emergency call from a subline, the subline must be correctly mapped to the prime line in the OW5000 database in order to display the originating caller information.
- OW5000 does not allow assigning route 0.The 2000 IPS PBXs accept route 0 - the rest of PBXs (2400, SV7000, etc) do not. If an IPS has route 0 set in the PBX, E-OSN will not be able to monitor the trunks from that route. Do not use route 0 as an emergency route because E-OSN will not be able to monitor that route for emergency calls.

Licensing

Please refer to the *UNIVERGE OW5000 Installation Guide* for details on license installation and configuration.

If no license is available for the OW5000, the UCE Emergency On-Site Notification service will be available for 30 days in trial mode or until a license system is connected.

If the connection to the license service is disconnected or unavailable, the application continues to run in a grace period for 30 days. After 30 days, the application will no longer run. During the grace period, the E-OSN Client will alert the user that the application is in the grace period and that the license connection should be restored.

Server Requirements

The E-OSN has no additional requirements that differ from the OW5000 Server requirements. Please refer to the *UNIVERGE OW5000 Installation Guide* for more information.

SQL Server Report Service

The SQL Server Report Service must be installed in order to run reports in UA5200 applications. For more information, refer to"Installing SQL Server Report Service" on page 9.

Client and PBX Requirements

E-OSN Client can be installed and operated on the following operating systems, with minimum PC requirements defined by each system:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2003 or 2008 Server
- Microsoft Windows 7

The following PBX platforms support E-OSN:

- SV8500 Family: IPX, SV7000, and SV8500
- SV8300 Family: IPS and SV8300

Table 2-1 *VS-32 Requirements for Conference*

VS-32 Type	FlasRom Name	Min Rev
SN8075 (VSEA-A)	SP-3789 SP-3834	Prog-A 4A
SN8111 (VSEB-A)	SP-3834	Prog-B 5A
SN8132 (VSED-A)	SP-3834 SP-3901	7A 00.08
MG-VS32VA	SP-3891 SP-3901	6A 00.08
SCA-VS32VA	SP-3891 SP-3901	6A 00.08

NOTE

NEC legacy conference bridges support silent monitor and do not need to be upgraded.

Installing the UCE Emergency On-Site Notification Application

This application can be installed from the UCE DVD as part of the OW5000 application list. Perform the following steps to install the E-OSN application.

Step 1 Place the UCE DVD into the computer's DVD-ROM drive. On most computers, setup will automatically start when the DVD is loaded. If Autorun is not enabled on the computer, then do the following:

—After placing the UCE DVD into the computer's DVD-ROM drive, open Windows Explorer and double-click the **DVD-ROM drive** icon.

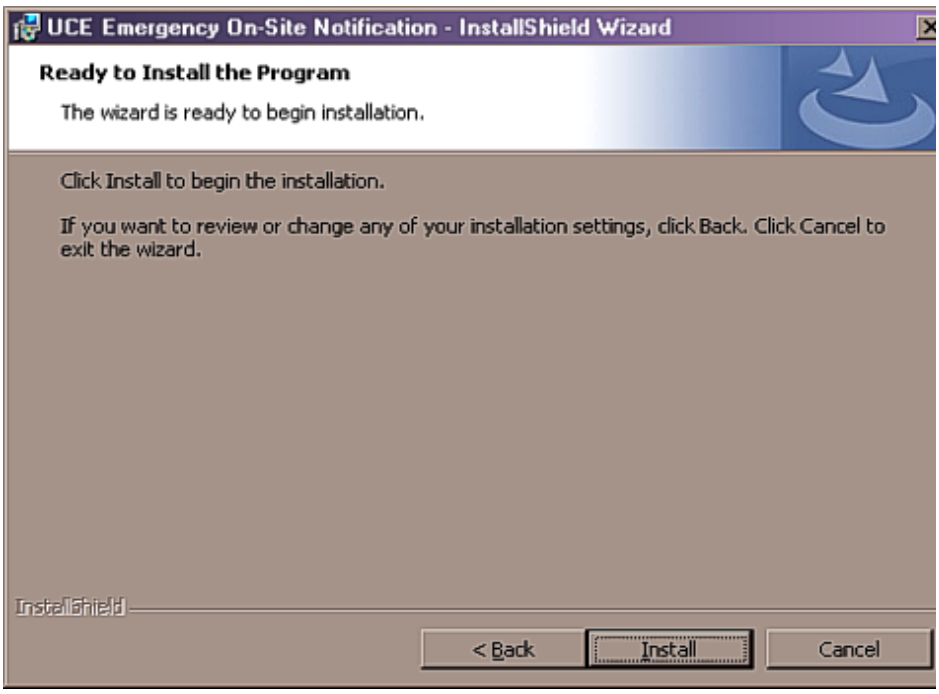
—In the DVD-ROM file list, double-click the **Setup.exe** file.

Step 2 From the Master Installation Menu, choose the **UCE Emergency On-Site Notification** option to start the installation process. A Preparing to Install screen displays briefly then a Welcome Message Center dialog box, (Figure 2-1) displays.

Figure 2-1 *E-OSN Welcome Dialog Box*

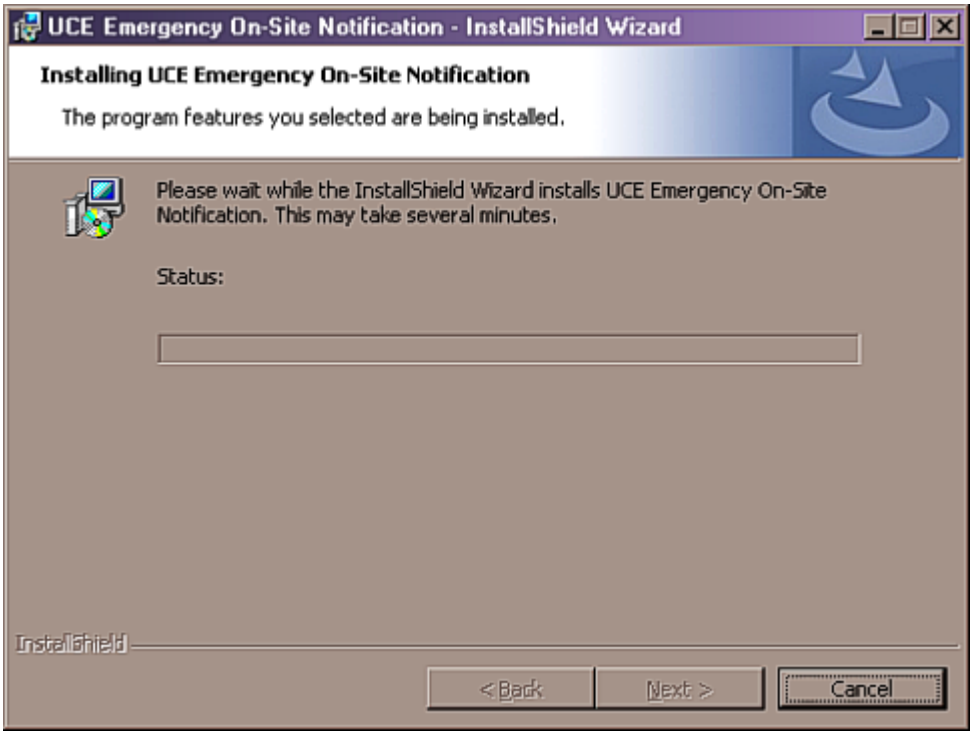
Step 3 Click **Next**. A Ready to Install screen briefly displays, then A Ready to Install dialog box, (Figure 2-2) displays.

Figure 2-2 *Ready to Install Dialog Box*



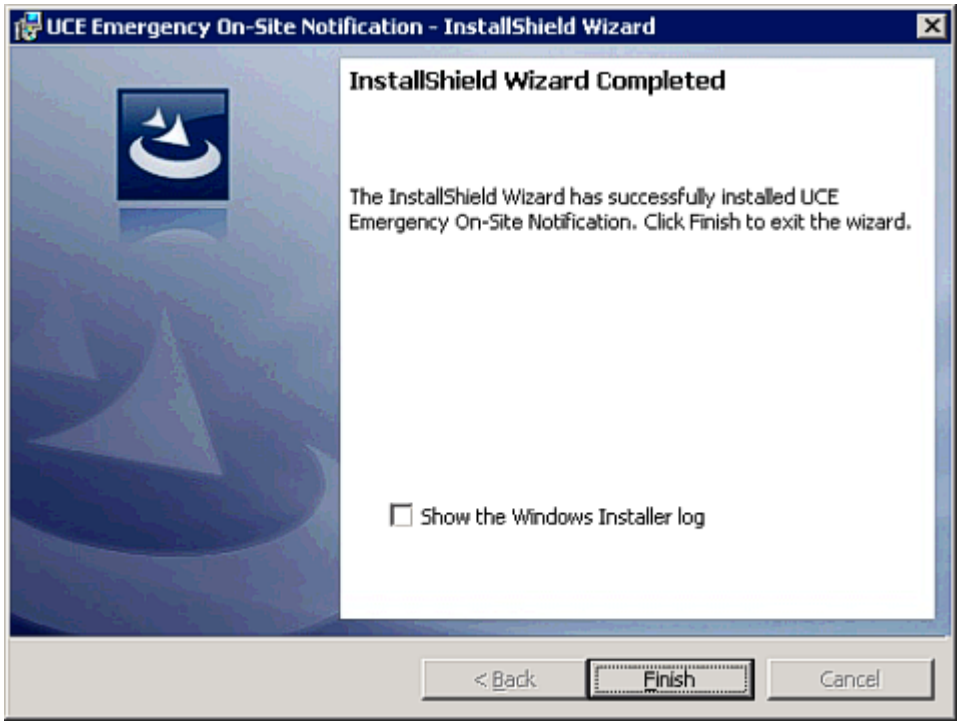
Step 4 Click **Install**. An Installing Message Center dialog box, Figure 2-3 displays.

Figure 2-3 *Installing Message Center Dialog Box*



Step 5 Click **Next** when installation stops. An Installation Complete dialog box, Figure 2-4 displays.

Figure 2-4 *Installation Complete Dialog Box*



Step 6 Click **Finish** to complete the **UCE Emergency On-Site Notification** installation.

Installing the E-OSN Client

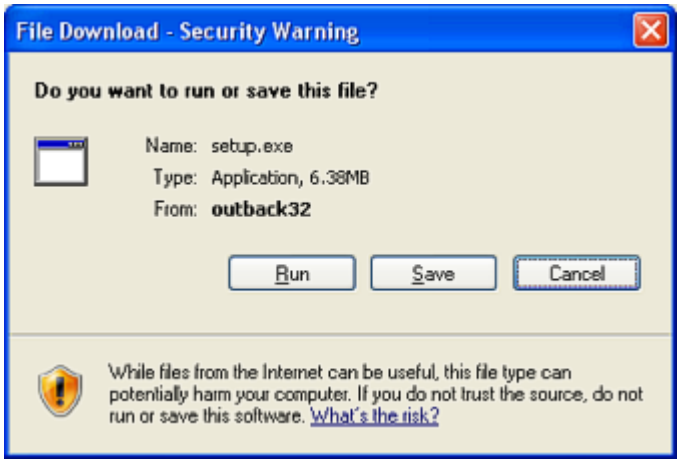
The UCE Emergency On-Site Notification Client is a Windows application used for receiving Emergency Notification events and is downloaded from a URL. The download also includes the installer file to upgrade the remote client.

On each startup of the E-OSN Client, the client application verifies that the version being started is the same version as the client deployed on the server. If the version is older, it prompts for an upgrade. This ensures that the end user will never be running an older version or an out of sync database. The older version upgrades without the need for manual un-install or re-entry of information.

Use the steps below to install the application from a Server. The web site to download the E-OSN Client is always **http://<machine name>/eosn/setup.exe**, where **<machine name>** is the name of the server where the UCE Emergency On-Site Notification application was installed.

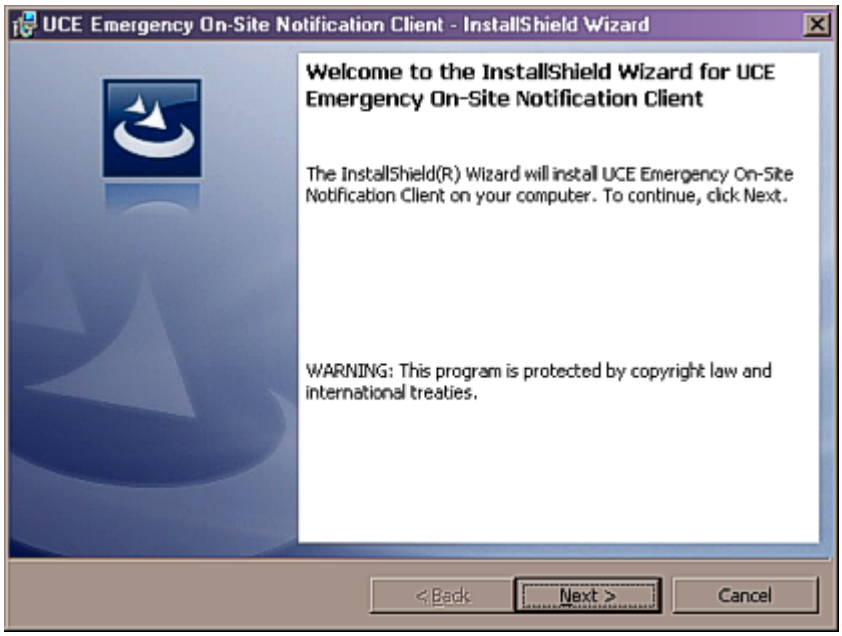
Step 1 Place the following URL in your Web browser **http://<machine name>/eosn/setup.exe**. A **File Download - Security Warning** dialog box, (Figure 2-5) displays. From here you can either run the program, save it to your PC for later installation, or cancel the installation.

Figure 2-5 *File Download - Security Warning*



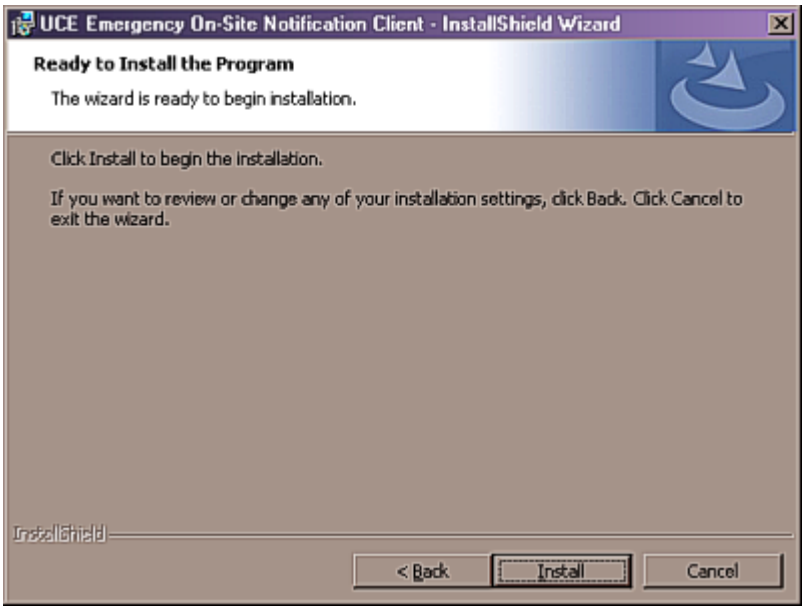
Step 2 Click **Run**. A **Preparing to Install** screen briefly appears then an **Install Shield Welcome** Screen, (Figure 2-6) displays.

Figure 2-6 *Emergency Notification Client Welcome Dialog Box*



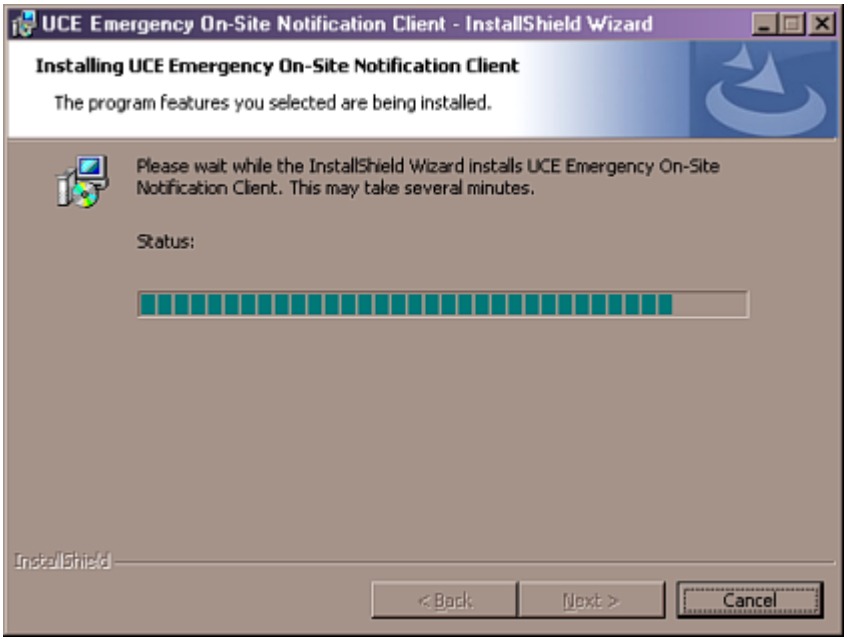
Step 3 Click **Next**. (Figure 2-7) displays.

Figure 2-7 *E-OSN Client Ready to Install*



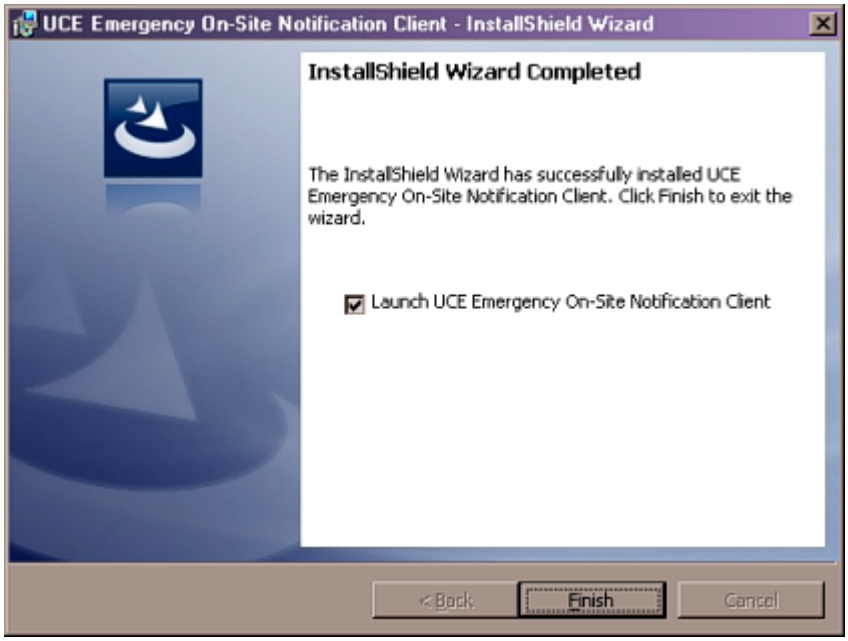
Step 4 Click **Install**. (Figure 2-8) displays.

Figure 2-8 *E-OSN Client Installing*



Step 5 Click **Next** when installation stops. An Installation Complete dialog box, (Figure 2-9) displays.

Figure 2-9 *Install Shield Wizard Complete*



Step 6 To immediately launch the UCE E-OSN Client, check the **Launch UCE Emergency On-Site Notification Client** box or leave blank to launch later. Click **Finish**.

Installing SQL Server Report Service

IMPORTANT

If you already have the Full version of SQL installed, you do not need to run the SQL Server Advanced Services SP2 upgrade. The Full SQL already comes with the upgrade.

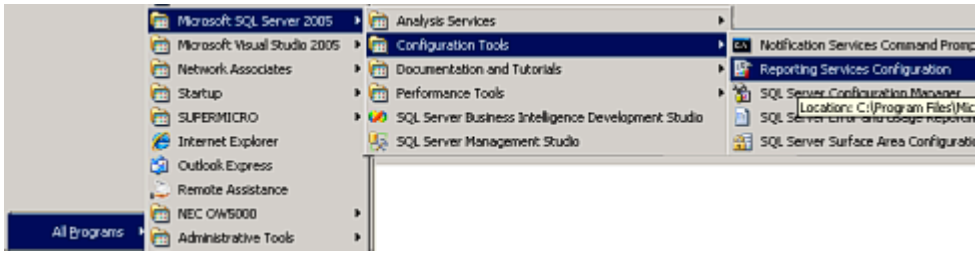
If you have SQL Express installed you must upgrade to SQL Advanced Services to get SQL Server Report Service.

Refer to the *OW5000 Installation Guide* for information on installing SQL Express.

Configuring the Reporting Services for SQL 2005

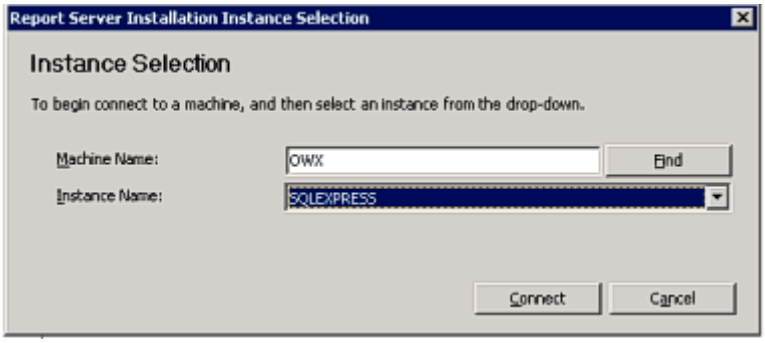
Step 1 Open the Reporting Services Configuration Tool by following the path, **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration Manager** (Figure 2-10).

Figure 2-10 *2005 Reporting Services Configuration*



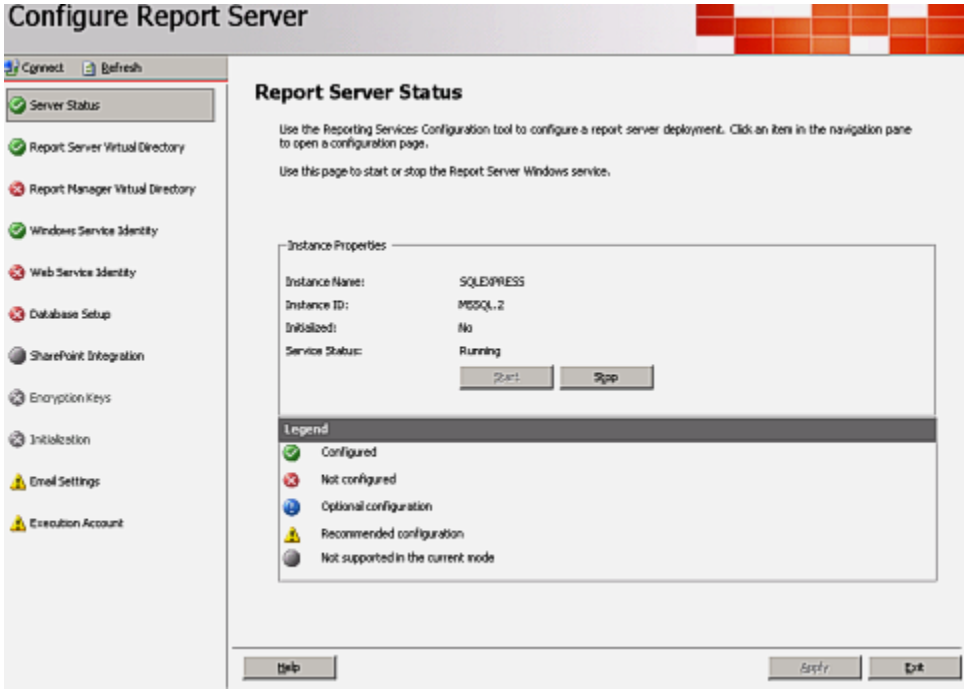
An Instance Selection dialog box displays (Figure 2-11).

Figure 2-11 *2005 Instance Selection dialog box*



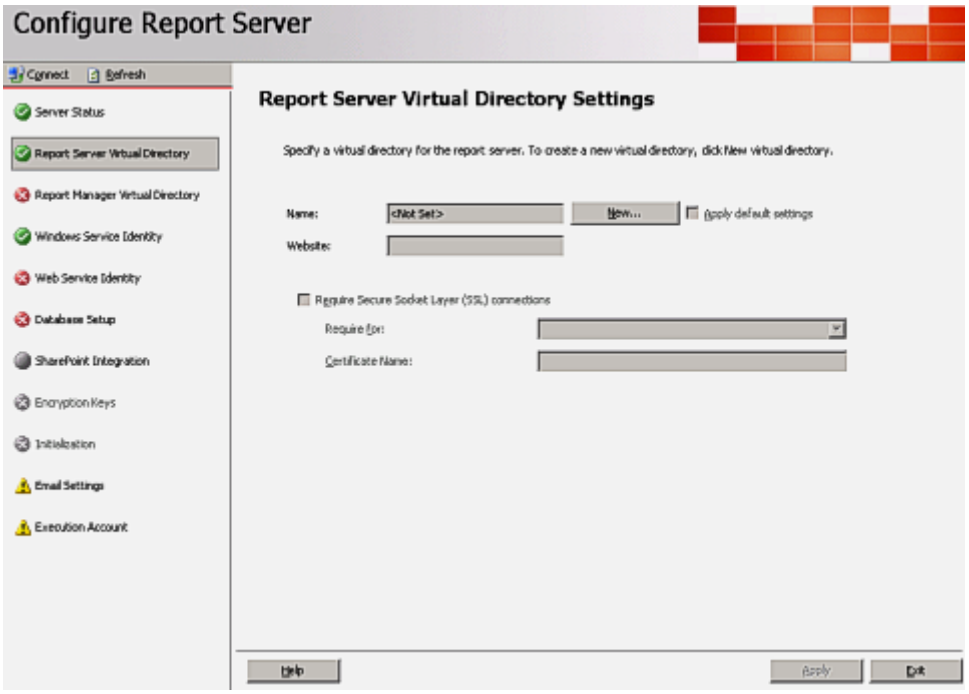
Step 2 Click **Connect**. If this is an upgrade, a Report Server Status dialog box displays (Figure 2-12).

Figure 2-12 *2005 Report Server Status dialog box*



Step 3 Click **Report Server Virtual Directory**. A Report Server Virtual Directory Settings dialog box displays (Figure 2-13).

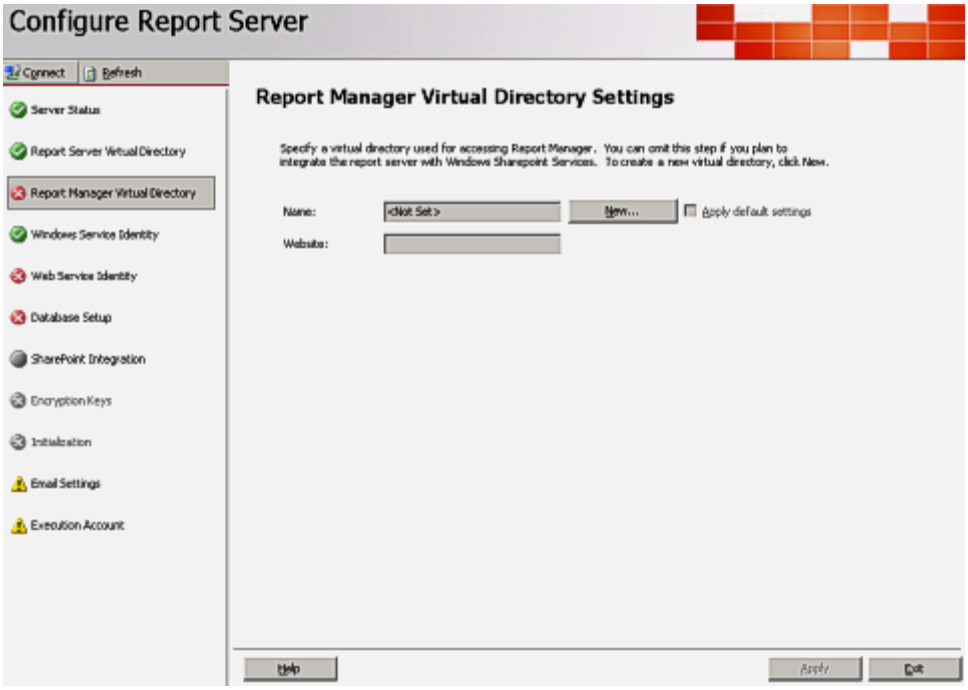
Figure 2-13 *Report Server Virtual Directory Settings dialog box*



Step 4 Click **New**. Accept the default values and then click **OK**.

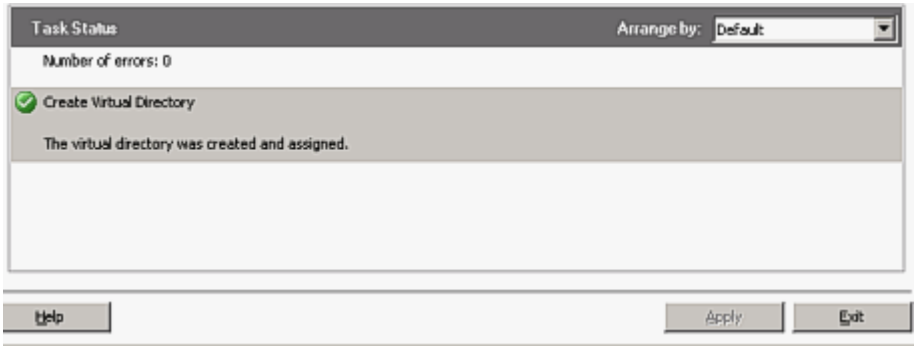
Step 5 Click **Report Manager Virtual Directory**. A Report Manager Virtual Directory dialog box displays (Figure 2-14).

Figure 2-14 *2005 Report Manager Virtual Directory dialog box*



Step 6 Click **New**. Accept the default values and then click **OK**. A Task Status dialog box displays (Figure 2-15) confirming the directory was successfully created.

Figure 2-15 *Task Status dialog box*

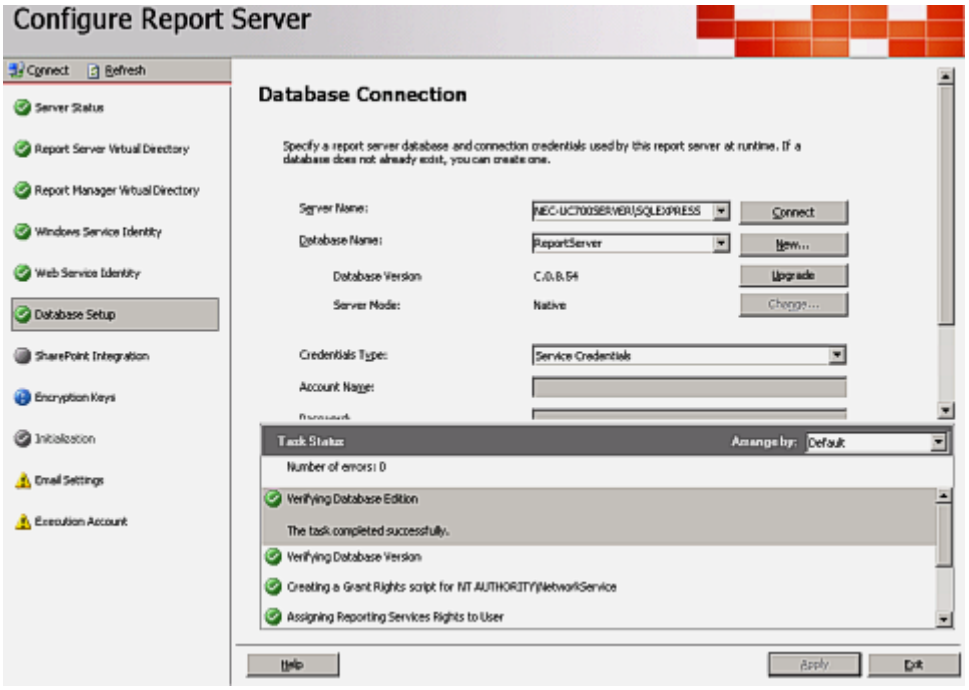


Step 7 If **Windows Service Identity** is marked with a green check mark, no changes are needed. If it is not marked with a green check mark, click Windows Service Identity and click **Apply** to accept the default values.

Step 8 Click **Web Service Identity**, click **New**, accept the default values and then click **Apply**.

Step 9 Select **Database Setup** to display a Database Connection dialog box (Figure 2-16).

Figure 2-16 *Database Connection dialog box*



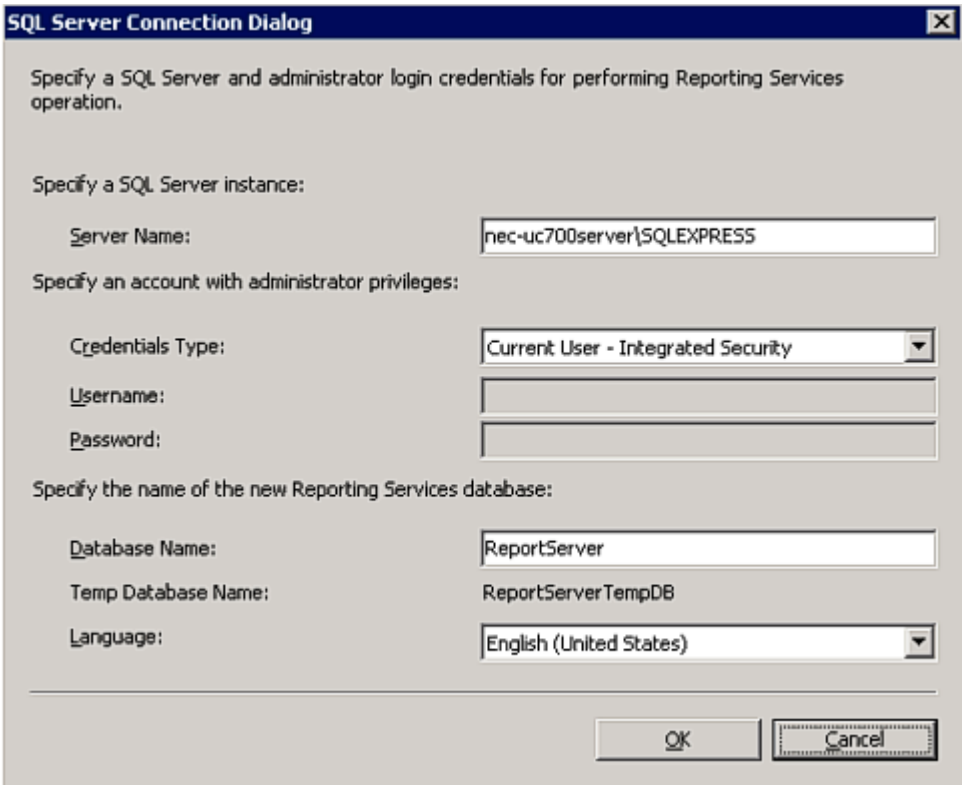
Step 10 Edit the **Server Name** field to read "<MACHINE NAME>\SQLEXPRESS" instead of "LOCALHOST\SQLEXPRESS".

NOTE

If the full version for SQL is being used, then ***\SQLEXPRESS*** *will not be a part of the name unless some other named instance for the database was used.*

Step 11 Create a new Database Name by clicking **New**. A New SQL Server Connection Dialog displays (Figure 2-17).

Figure 2-17 *New SQL Server Connection Dialog*

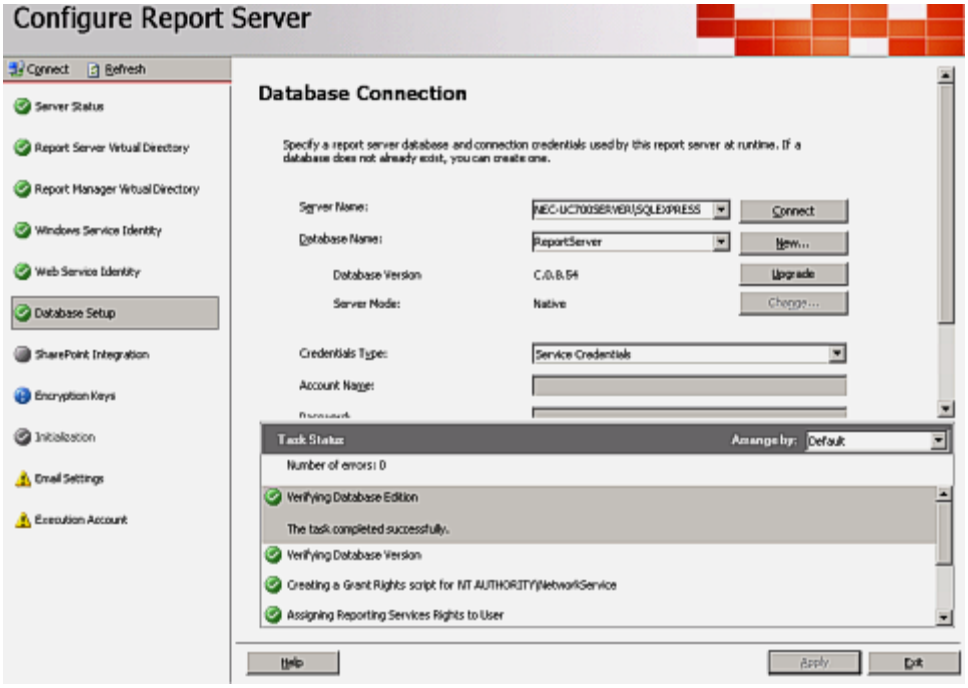


Step 12 Rename the new Reporting Service **ReportServer**. Use the defaults from the new database dialog.

Step 13 Press the **Connect** button (Figure 2-16) to verify the database connectivity. If connectivity fails, verify that the SQL Server OW5000 is installed and is accessible. Also, verify that the **Server Name** field is correct.

Step 14 Click **Apply**. A Database Connection Confirmation dialog box displays (Figure 2-18).

Figure 2-18 *Database Connection Confirmation dialog box*



Step 15 Click **Exit**.

Loading the SQL Service Report Service

Step 1 Open a Web Browser and type the URL: ***//<Server Name>/Reports***

Step 2 If the page fails to load, a configuration file must be manually edited by following the procedure below:

—Browse to **C:\Program Files\Microsoft SQL Server\MSSQL.X\Reporting Services\ReportManager**. Find the file named **RSWebApplication.config**.

Multiple MSSQL folders may appear, such as MSSQL.1, MSSQL.2, and MSSQL.3. Browse through all of them until you find one that has a **Reporting Services** sub folder.

—Open the config file with NotePad and find the line containing **<ReportServerVirtualDirectory></ReportServerVirtualDirectory>**.

Modify the line by inserting the Virtual Directory Name **ReportServer** in the field. The line will now appear as follows:

—<ReportServerVirtualDirectory>ReportServer</ ReportServerVirtualDirectory>

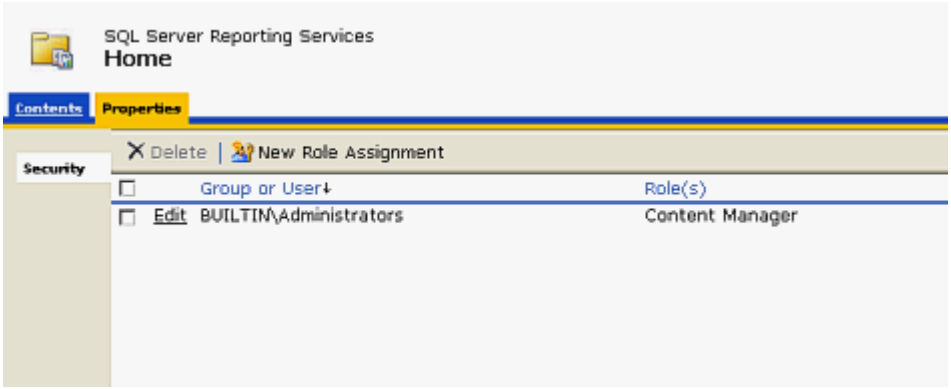
Step 3 Save and close the configuration file.

Step 4 Retry opening the URL ***//<Server Name>/Reports***. A web page opens displaying the **Home** level.

NOTE *If the web pages does not open, verify that IIS is running on your server.*

Step 5 Click **Properties** to display a Role Assignment dialog box (Figure 2-19).

Figure 2-19 *2005 Role Assignment dialog box*



Step 6 Click **New Role Assignment**. A New Role Assignment dialog box displays (Figure 2-20).

Figure 2-20 *2005 New Role Assignment dialog box*

Step 7 Enter **NT AUTHORITY\NETWORK SERVICE** in the **Group or user name** field. This field is case sensitive.

Step 8 Check the following check boxes:

—Browser

—Content Manager

—Publisher

Step 9 Click **OK**.

Uploading OW5000 Reports

You must log on to the OW5000 Administrator in order to upload reports. Refer to the *UNIVERGE OW5000 Configuration Guide* for information on how to log on to the OW5000 Administrator. When you have finished, you can either log out or just close your browser.

Step 1 Once you are logged on to OW5000 Administrator, follow this path to open the Report Setting configuration options: **OW5000 > Settings > General Settings**. A Settings dialog box displays (Figure 2-21).

Figure 2-21 *2005 Settings dialog box*

Step 2 Verify that the reporting services URL reads as follows: **http://<Machine Name>/ReportServer**.

Step 3 Click **Upload Reports**. A Reports Confirmation dialog box displays (Figure 2-22).

Figure 2-22 *2005 Reports Confirmation dialog box*

Step 4 If a confirmation dialog box does not display, verify that the **NT AUTHORITY\NETWORK SERVICE** account was correctly added to the Home level in the Report Manager web page by doing the following.

— Go to the Report Manager web page **//<Server Name>/Reports**. Verify the sub directory OW5000 was created under **Home**.

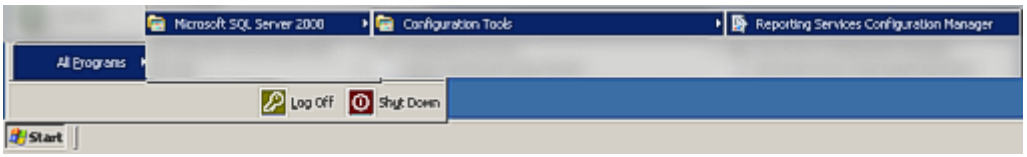
— Click **OW5000**, and then click **Admin**. All reports that OW5000 currently deploys and supports will display. All future reports will be uploaded to this location anytime the Upload button is pressed in Admin, assuming that the report to upload is residing in the reports deployment folder. The default deployment folder is **C:\Program Files\NEC\OW5000\Administrator\ReportFiles**.

Reports can now be generated for applications using SSRS reports.

Configuring the Reporting Services for SQL 2008

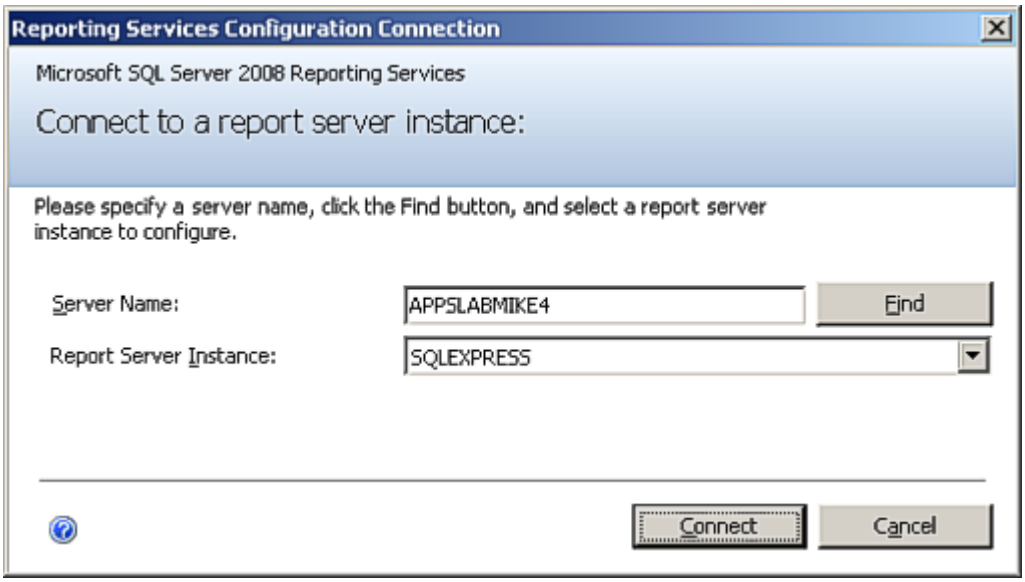
Step 1 Open the Reporting Services Configuration Tool by following the path, **Start > All Programs > Microsoft SQL Server 2008 > Configuration Tools > Reporting Services Configuration Manager** (Figure 2-23).

Figure 2-23 *2008 Reporting Services Configuration*



An Instance Selection dialog box displays (Figure 2-24).

Figure 2-24 *2008 Instance Selection dialog box*

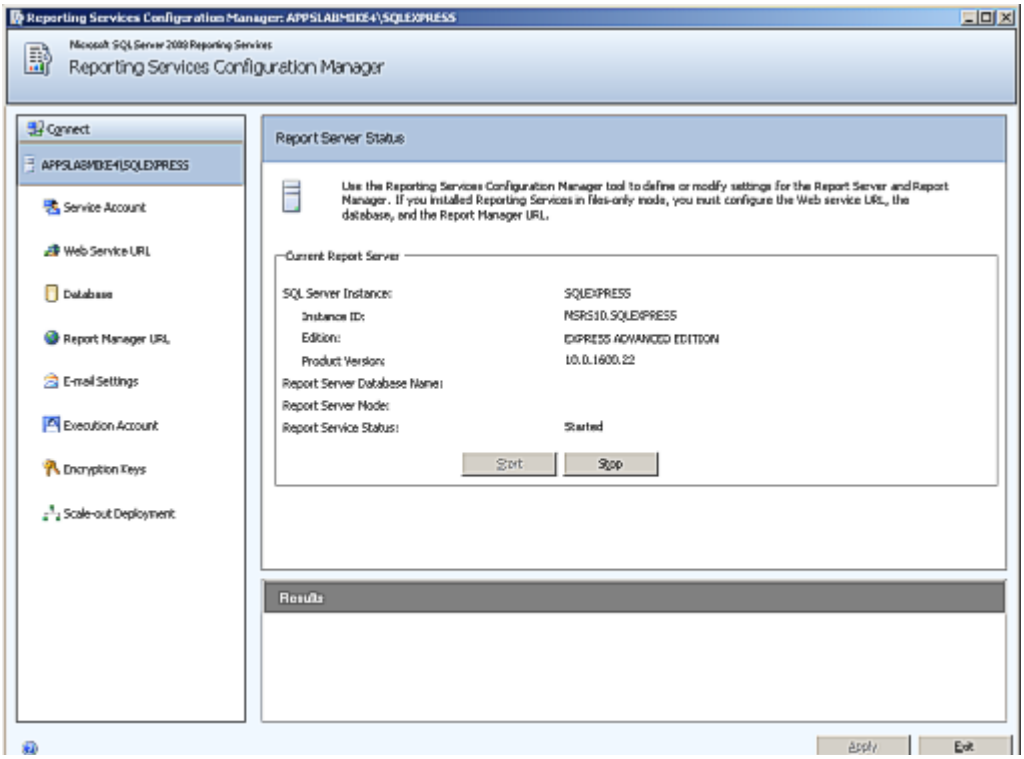


Step 2 Specify a **Server Name**, select a **Report Server Instance,** and then click **Connect**. A Report Server Status dialog box displays (Figure 2-25).

NOTE

*If **Report Server Instance** is greyed out, re-run the SQL installation and ensure that the Report Server component is installed.*

Figure 2-25 *2008 Report Server Status dialog box*



NOTE

*If the If the **Stop** button is greyed out, the Report Server is not connected. Click the **Start** button.*

The following topics are included for Configuring Reporting Services for SQL 2008:

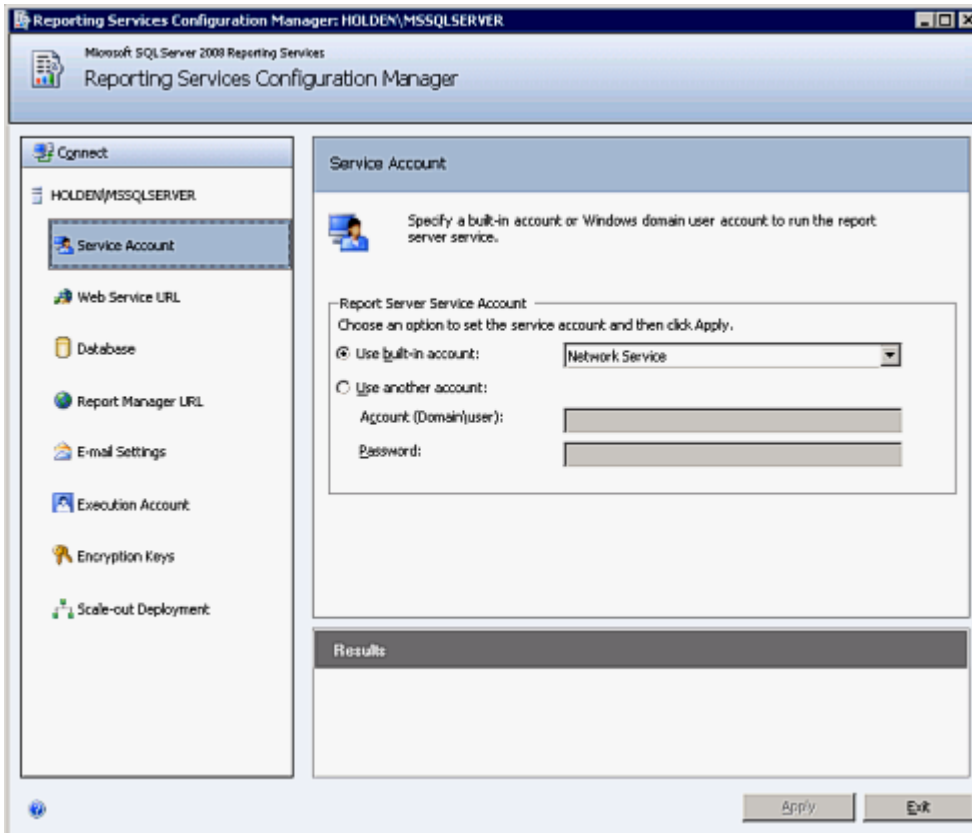
- *Service Account*
- *Web Service URL*
- *Database*
- *Report Manager URL*

Service Account

Service Account identifies which account will run the report server service. The server account is selected during SQL installation.

To verify the account, select **Service Account** from the **Reporting Services Configuration Manager** dialog window. Figure 2-26 displays.

Figure 2-26 *2008 Service Account dialog*



The default value for **Use built-in account** is **Network Service**.

NOTE

*The **Service Account** window is for verification purposes only. It is recommended that the **Use built-in account** value not be changed from the default.*

Once verified, no further action is required.

In order to change the bullt-in account type, you must have an encryption key. It is recommended that you create a backup of the Report Server Database before selecting any account other than the default.

IMPORTANT

*If the **Use built-in account** field is changed, the following error message may appear.*

"The report server cannot decrypt the symmetric key used to access sensitive or encrypted data in a report server database. You must either restore a backup key or delete all encrypted content. Check the documentation for more information. (rsReportServerDisabled)"

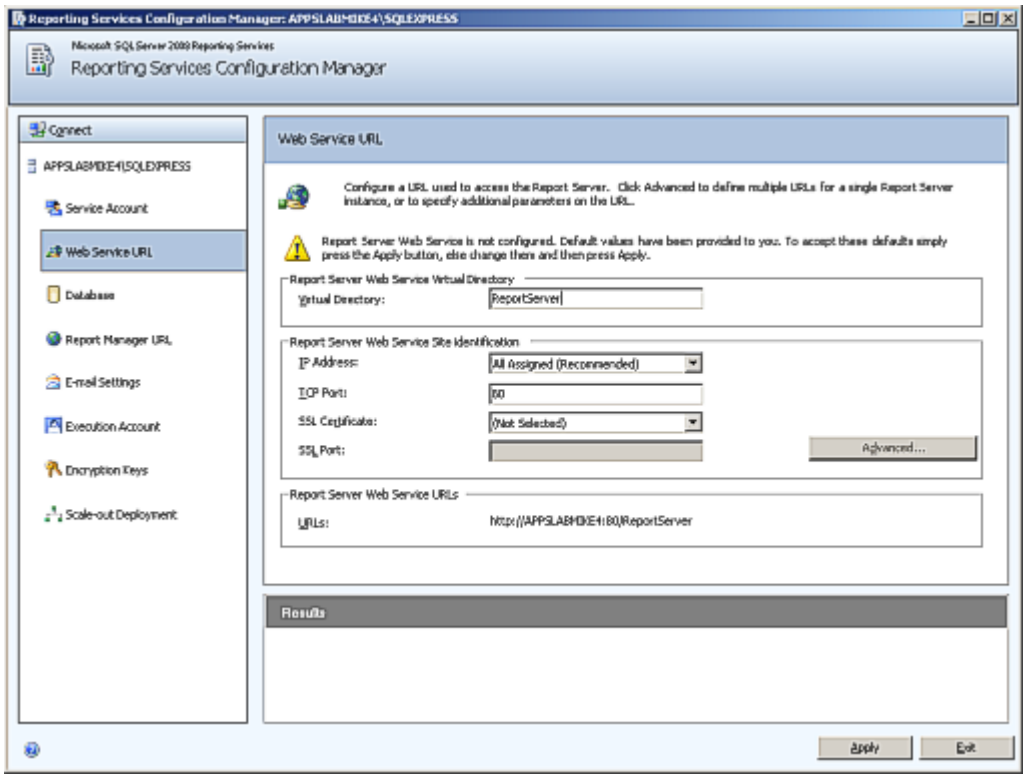
If you receive this error, the Service login account has changed and a new encryption key file is needed to validate the new account. You should restore a symmetric key only if it is the same key that is currently used to encrypt and decrypt data in the report server database. If you restore a symmetric key that is not valid, you will no longer be able to access sensitive data. In this case, you must delete and re-create the key. Refer to documentation from Microsoft SQL Server on restoring encryption Key files. If the key file is not available, then go to the Encryption section and delete the current key file and re-do all steps.

Web Service URL

Follow the steps below to configure a URL to access the Report Server.

Step 1 From the **Reporting Services Configuration Manager** dialog box, select **Web Service URL**. Figure 2-27 displays.

Figure 2-27 *2008 Web Service URL dialog box*



NOTE

The Web Service URL dialog box is populated with data identified during the SQL installation. If no changes are needed, it is recommended that you accept the default settings. If you accept the default settings, no further action is needed.

If you need to make changes, notify your System Administrator and proceed with the steps below.

Step 2 Enter a name for the Virtual Directory. This allows you to specify the virtual directory name for the Report Server Web service. You can only have one virtual name for each Report Server Web service instance on the same computer.

NOTE

*If the default value for **Virtual Directory** is **ReportServer_SQLEXPRESS**, it is recommended that you change it to **ReportServer** by removing the **_SQLEXPRESS** portion (to match the last qualifier of the default Report Server URL seen in OW5000 Settings).*

Step 3 Select an **IP Address** from the drop-down list. It is normally OK to accept the default value, **All Assigned**.

Step 4 Enter the **TCP Port number**. The default is 80.

Step 5 Click **Apply**. A confirmation dialog box, Figure 2-28 displays.

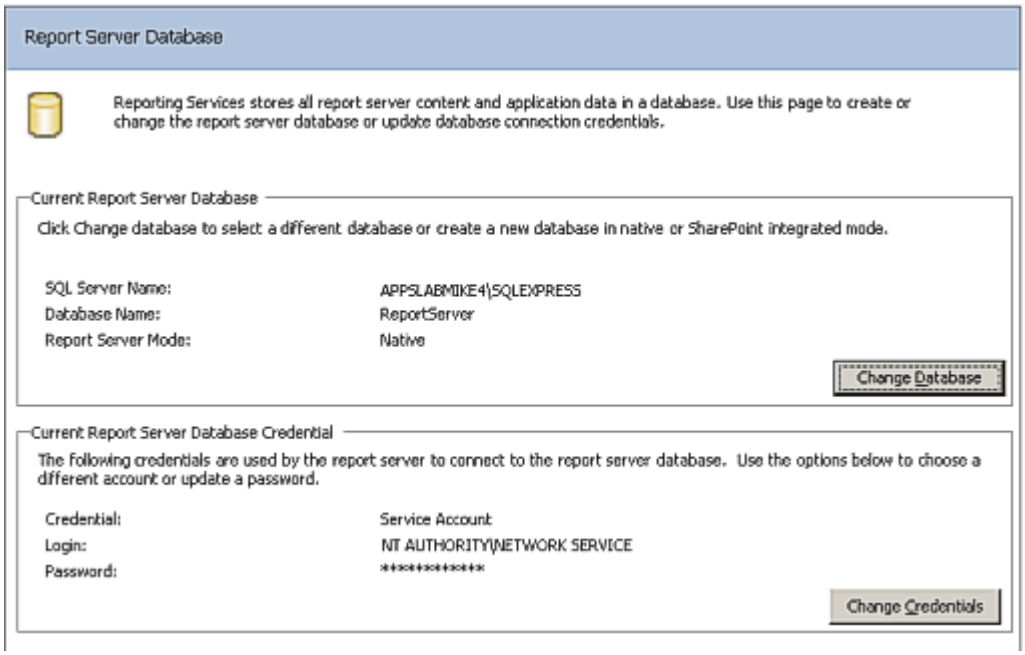
Figure 2-28 *Confirmation dialog box*

For information on Advanced settings, refer to ***Microsoft's SQL Server 2008 SQL Server Setup Help, Web Service URL (Reporting Services Configuration) Online Help***.

Database

The **Report Service Database** stores all report content and application data and is accessed under **Database** on the **Reporting Services Configuration Manager** dialog window (Figure 2-29). Use the **Report Service Database** dialog window to verify report server database settings.

Figure 2-29 *2008 Report Server Database dialog box*

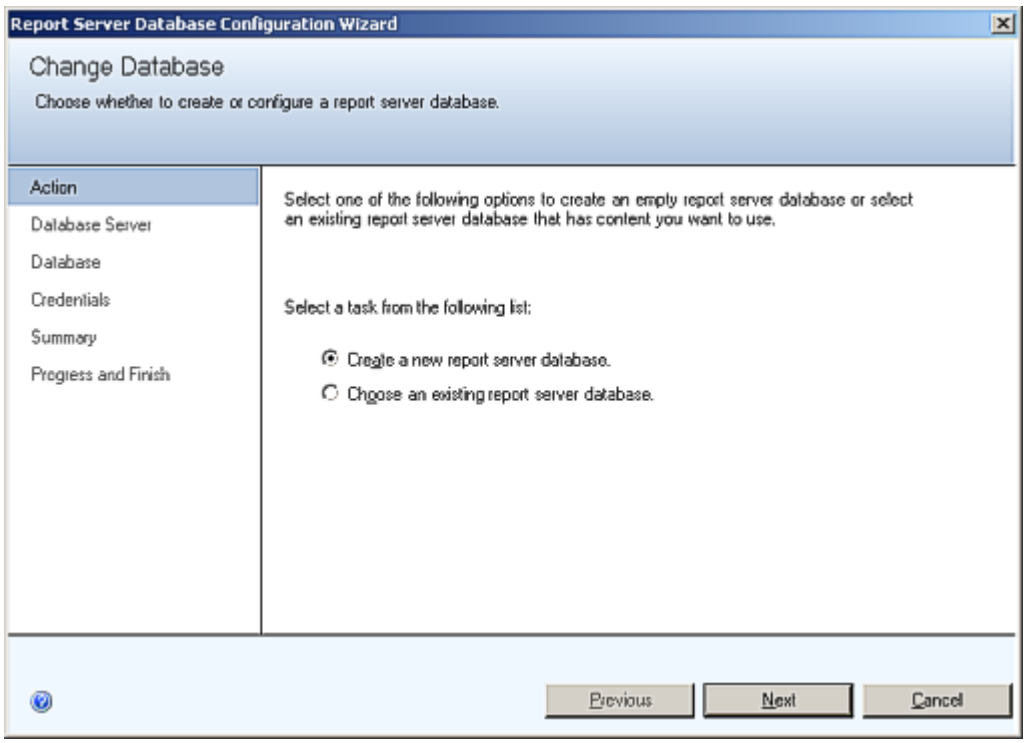


NOTE

The fields in the ***Report Server Database*** *dialog box are populated during SQL installation. If SQL Installation was performed correctly, no changes to this page are necessary.*

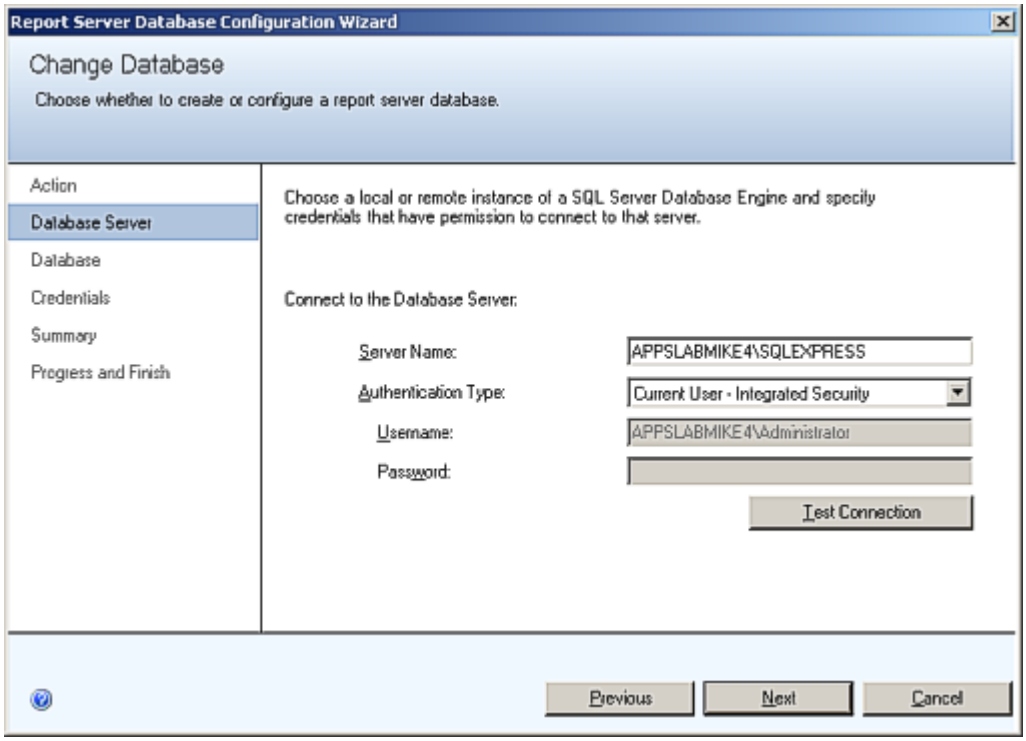
Step 1 If the fields in Figure 2-29 are blank, click **Change Database**. A Change Database—Action dialog box displays (Figure 2-30).

Figure 2-30 *Change Database—Action dialog box*



Step 2 Click **Next**. A Change Database—Database Server dialog box displays (Figure 2-31).

Figure 2-31 *Change Database—Database Server dialog box*



Step 3 Click **Test Connection**. Figure 2-32 displays.

Figure 2-32 *Test Connection Confirmation dialog box*

Step 4 If the test is not successful, edit the Server Name to match the instance name and try again.

NOTE

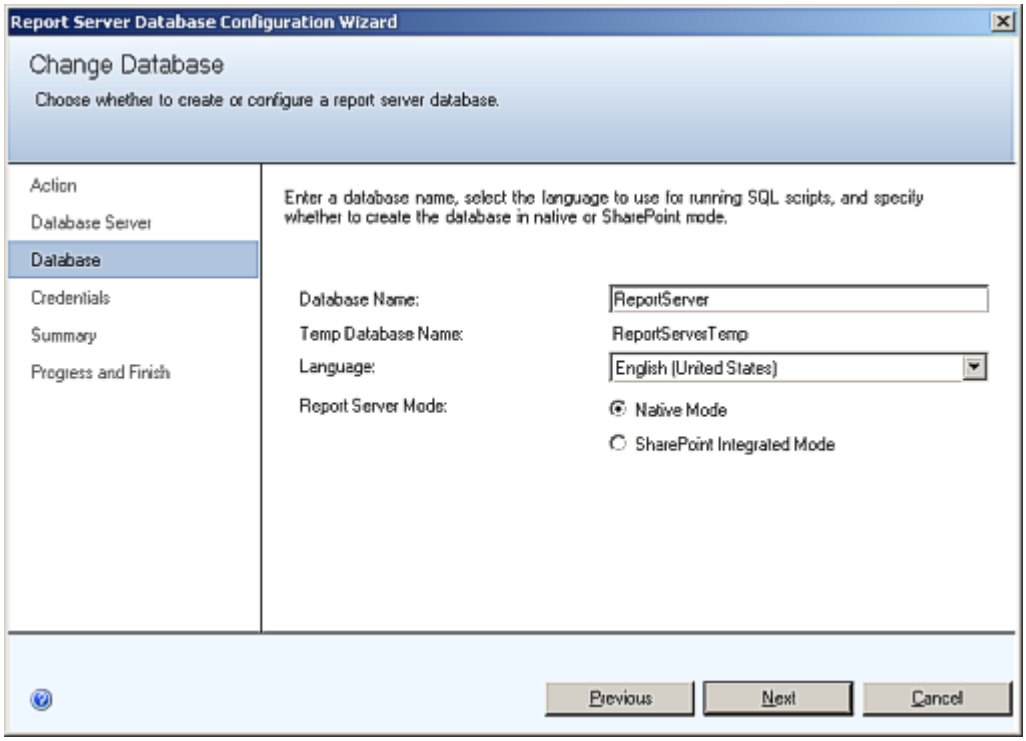
Depending on the SQL edition you are using and how it was installed, one of the following should allow a successful connection:

<hostname>
<hostname>\<instance name>
.\<instance name>

If you are in doubt as to whether or not a successful Test Connection is connecting to the correct SQL instance, try using Microsoft SQL Server Management Studio to connect to the value you have specified here. You should not only be able to connect, but also examine the Databases to find the OW5000 database residing there. (It's technically OK, however, to install the Report Server Database within a different instance of SQL than that where the OW5000 database resides.)

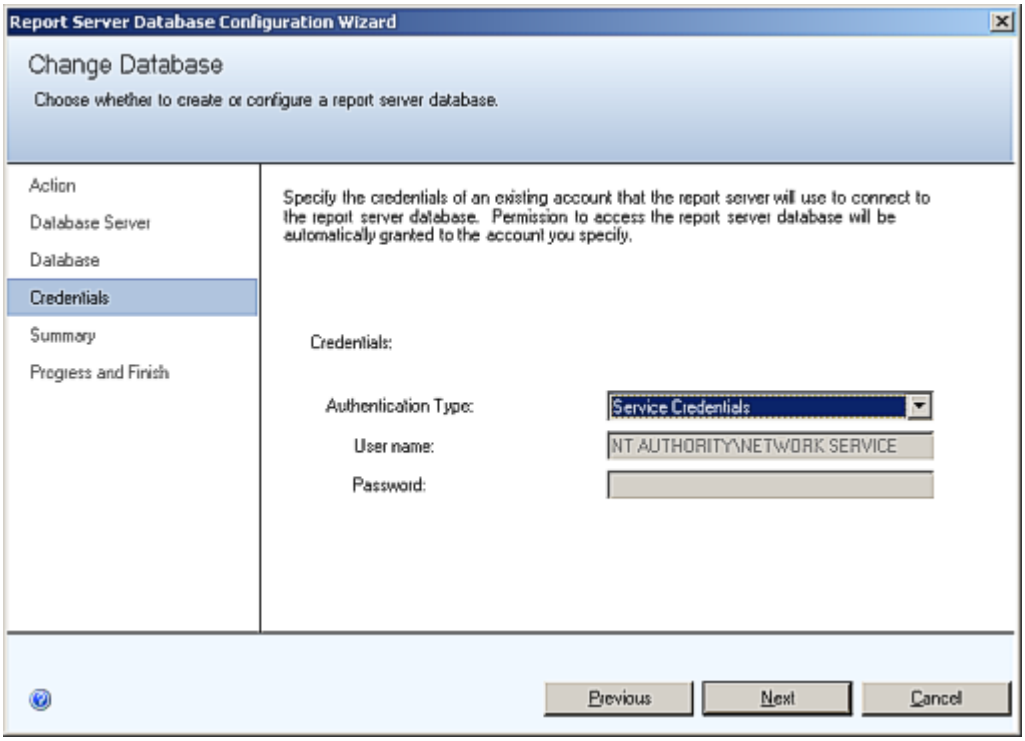
Step 5 Click **Next**. A Change Database—Database dialog box displays (Figure 2-33).

Figure 2-33 *Change Database—Database dialog box*



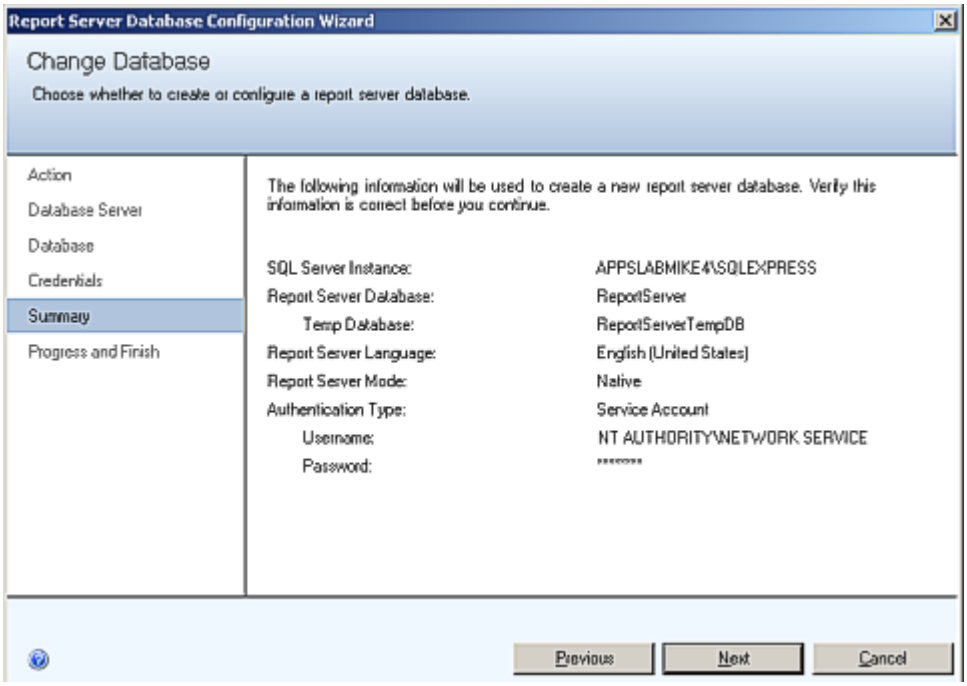
Step 6 Accept the defaults and click **Next**. A Change Database—Credentials dialog box displays (Figure 2-34).

Figure 2-34 *Change Database—Credentials dialog box*



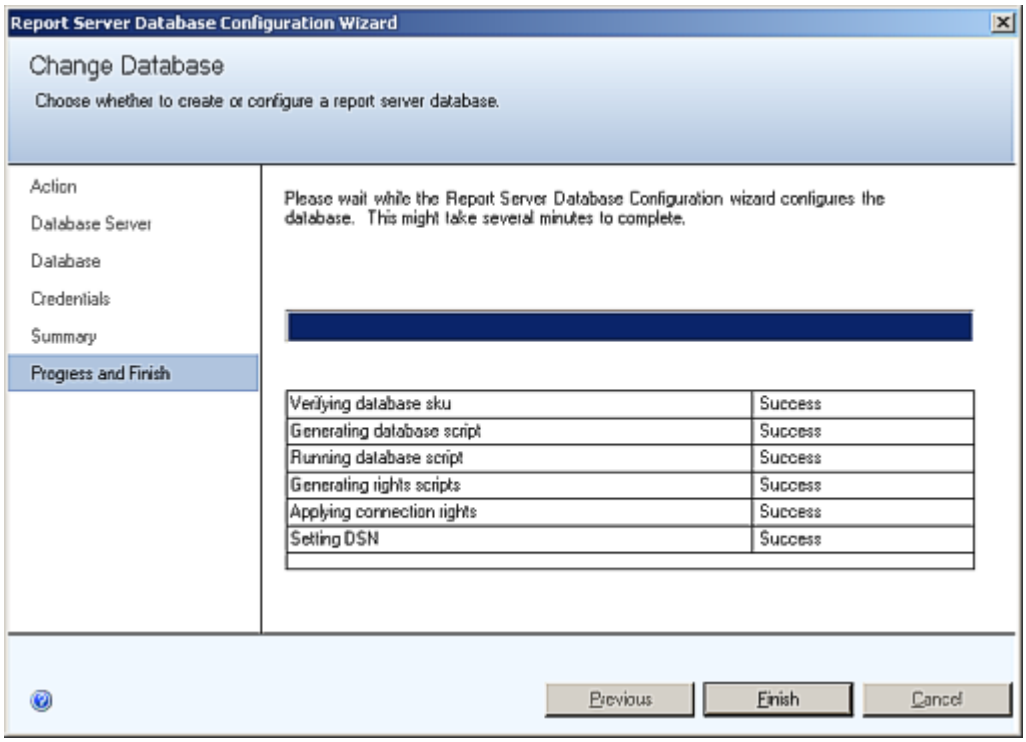
Step 7 Accept the default values and click **Next**. A Change Database—Summary dialog box displays (Figure 2-35).

Figure 2-35 *Change Database—Summary dialog box*



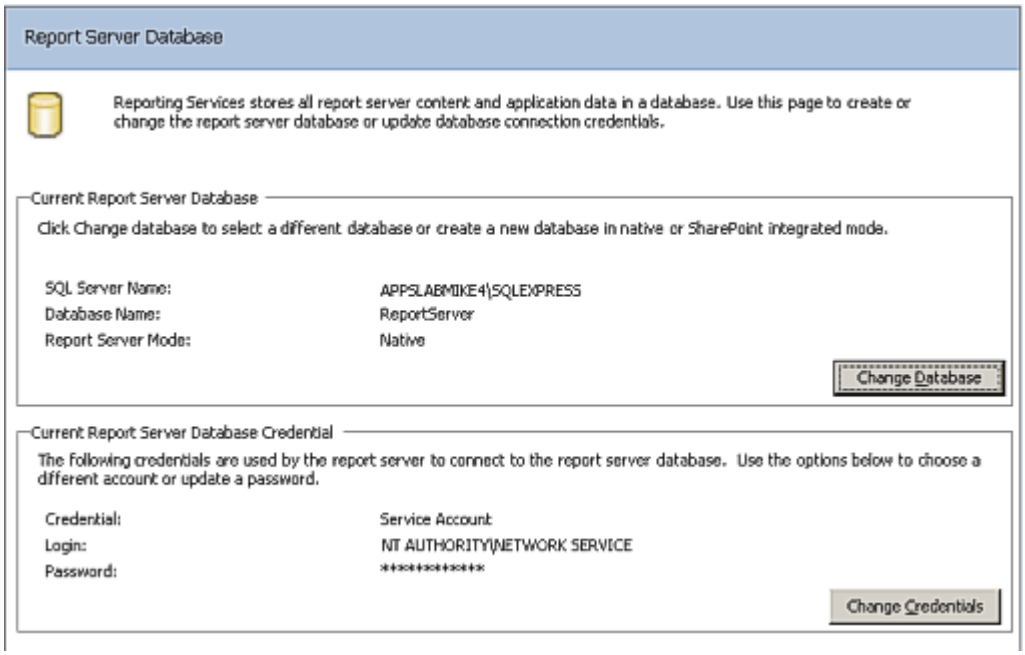
Step 8 Review the settings and click Next. The Change Database - Progress and Finish dialog box displays, Figure 2-36. (Wait for it to complete.).

Figure 2-36 *Change Database—Progress and Finish dialog box*



Step 9 Confirm that a status of **Success** is shown for each step, and then click **Finish**.

Figure 2-37 *Report Server Database—Database option*

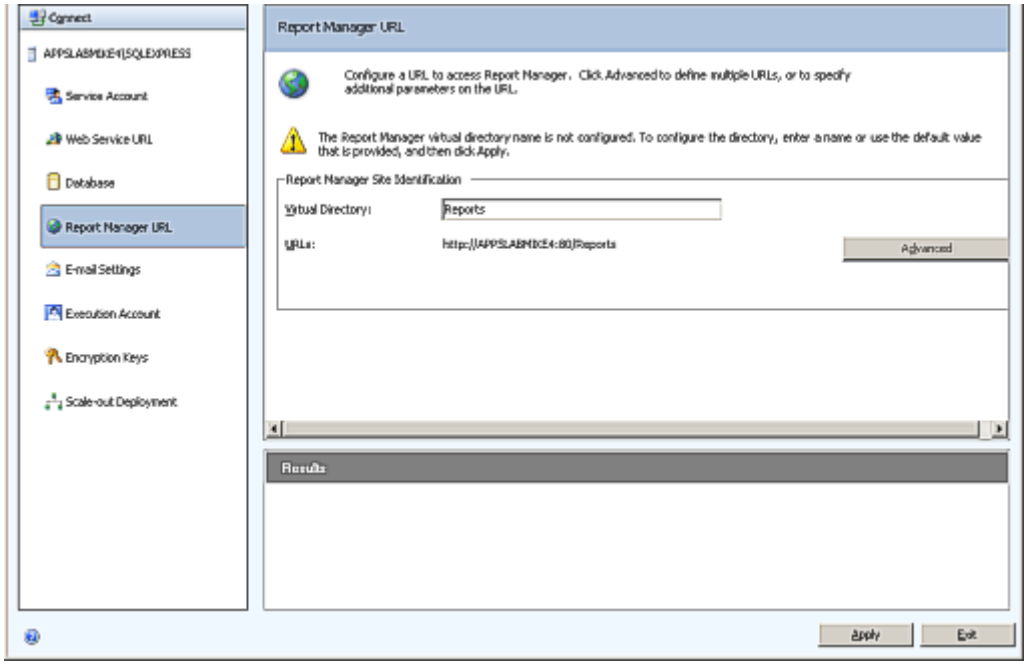


Report Manager URL

To access the Report Manager, you must configure a URL. Follow the steps below.

Step 1 Select **Report Manager URL** from the Report Server Status dialog box. Figure 2-38 displays.

Figure 2-38 *2008 Report Manager URL dialog box*



Step 2 Enter a value of **Reports** for the **Virtual Directory** name for **Report Manager Site Identification**.

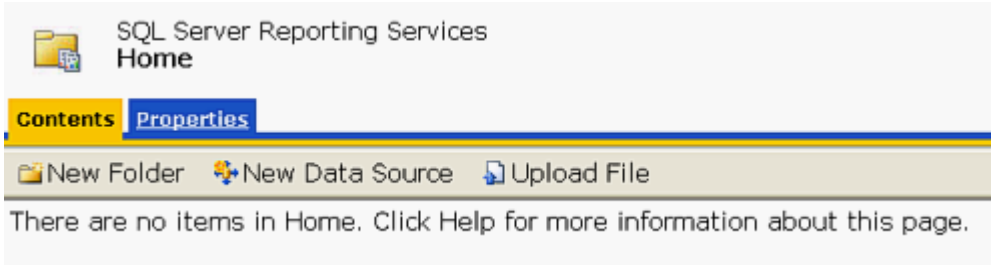
Step 3 Click **Apply**.

Step 4 Test the URL by clicking the link in the **URLs** section of the **Report Manager URL** window. If the URL is correct, Figure 2-39 displays. (It can take 60 seconds or longer for this page to open in your browser).

NOTE

If prompted, enter the User Name and Password of the person that has machine administrator privileges on that machine.

Figure 2-39 *2008 SQL Server Reporting Services Home*



Loading the SQL Service Report Service

Step 1 If the page fails to load, a configuration file must be manually edited by following the procedure below:

—Browse to **C:\Program Files\Microsoft SQL Server\MSSQL.X\Reporting Services\ReportManager**. Find the file named **RSWebApplication.config**.

Multiple MSSQL folders may appear, such as MSSQL.1, MSSQL.2, and MSSQL.3. Browse through all of them until you find one that has a **Reporting Services** sub folder.

—Open the config file with NotePad and find the line containing **<ReportServerVirtualDirectory></ReportServerVirtualDirectory>**.

Modify the line by inserting the Virtual Directory Name **ReportServer** in the field. The line will now appear as follows:

—<ReportServerVirtualDirectory>ReportServer</ ReportServerVirtualDirectory>

Step 2 Save and close the configuration file.

Step 3 Retry opening the URL ***//*<Server Name>/Reports**. A web page opens displaying the **Home** level.

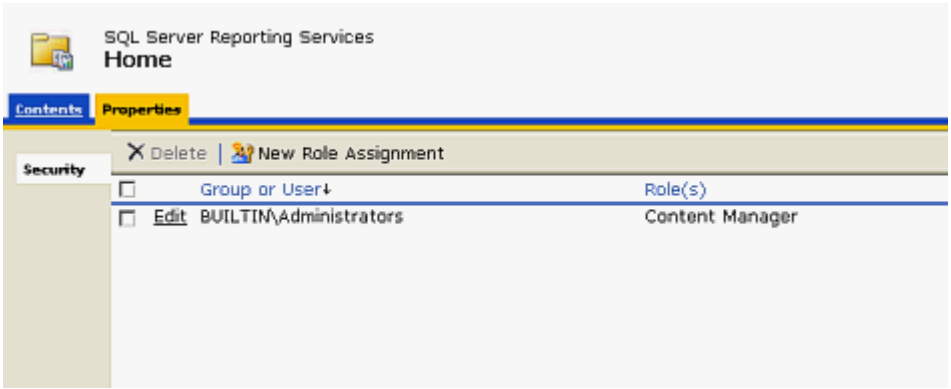
NOTE

If the web pages does not open, verify that IIS is running on your server.

If the web page opens, the following error might be displayed: ***This page might not function correctly because either your browser does not support scripts or active scripting is disabled****. If so, using Internet Explorer, go to* ***Tools*** *>* ***Internet Options*** *>* ***Security tab*** *>* ***Local Intranet****, click the* ***Sites*** *button, and add your Report Manager URL to the list of sites.*

Step 4 Click the **Properties** tab. Figure 2-40 displays.

Figure 2-40 *2008 SSRS Properties Page*



Step 5 Click **New Role Assignment**. A New Role Assignment dialog box displays (Figure 2-41).

Figure 2-41 *2008 New Role Assignment dialog box*

Step 6 Enter **NT AUTHORITY\NETWORK SERVICE** in the **Group or user name** field. This field is case sensitive.

Step 7 Check the following check boxes:

—Browser

—Content Manager

—Publisher

Step 8 Click **OK**.

Uploading OW5000 Reports

You must log on to the OW5000 Administrator in order to upload reports. Refer to the *UNIVERGE OW5000 Configuration Guide* for information on how to log on to the OW5000 Administrator. When you have finished, you can either log out or just close your browser.

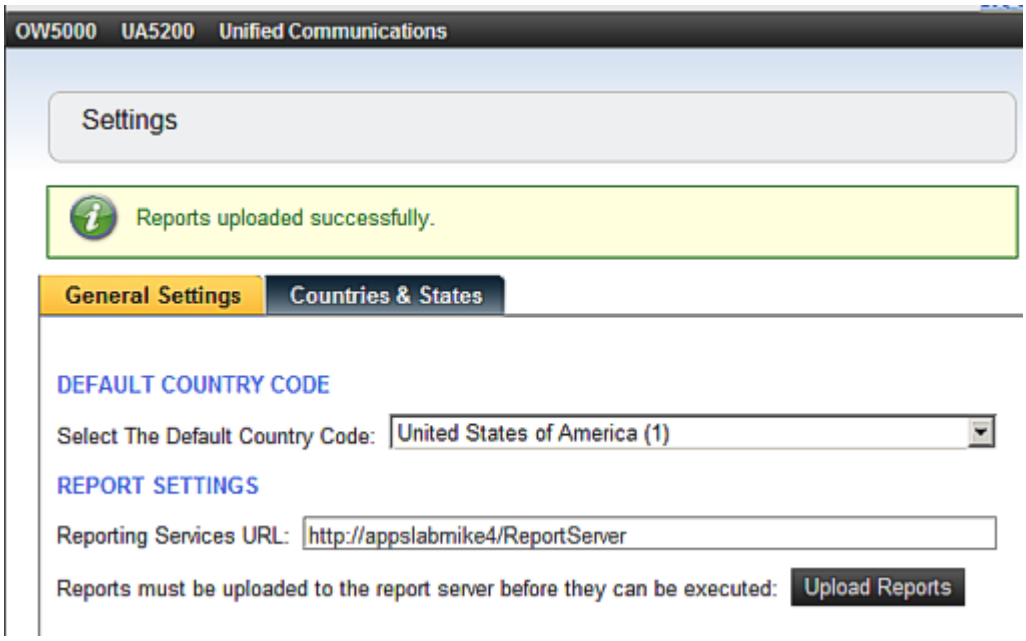
Step 1 Once you are logged on to OW5000 Administrator, follow this path to open the Report Setting configuration options: **OW5000 > Settings > General Settings**. A Settings dialog box displays (Figure 2-42).

Figure 2-42 *2008 Settings dialog box*

Step 2 Verify that the reporting services URL reads as follows: **http://<Machine Name>/ReportServer**.

Step 3 Click **Upload Reports**. A Reports Confirmation dialog box displays (Figure 2-43).

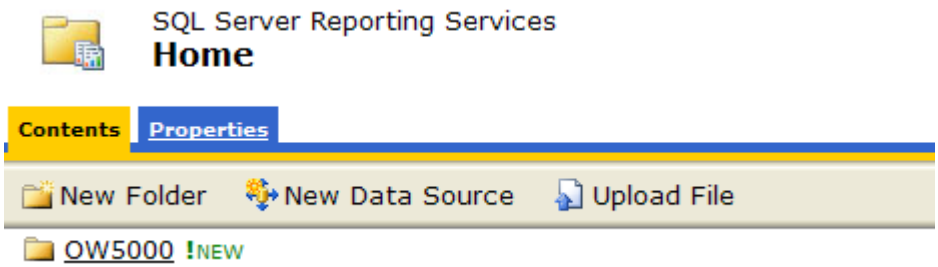
Figure 2-43 *2008 Reports Confirmation dialog box*



Step 4 If a confirmation dialog box does not display, verify that the **NT AUTHORITY\NETWORK SERVICE** account was correctly added to the Home level in the Report Manager web page by doing the following.

—Go to the Report Manager web page **//<Server Name>/Reports**. Figure 2-44 displays.

Figure 2-44 *Reports Home page*



—Verify the sub directory **OW5000** was created under the **Contents** tab.

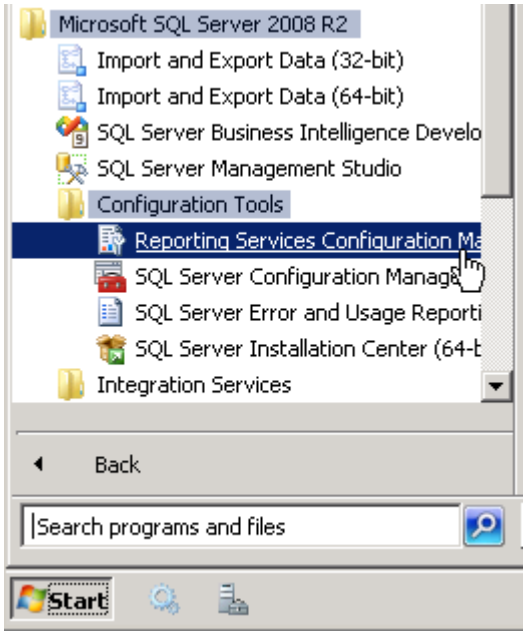
— Click **OW5000**, and then click **Admin**. All reports that OW5000 currently deploys and supports will display. All future reports will be uploaded to this location anytime the Upload Reports button is pressed in Admin, assuming that the report to upload is residing in the reports deployment folder. The default deployment folder is **C:\Program Files\NEC\OW5000\Administrator\ReportFiles**.

Reports can now be generated for applications using SSRS reports.

Configuring the Reporting Services for SQL Services 2008 R2

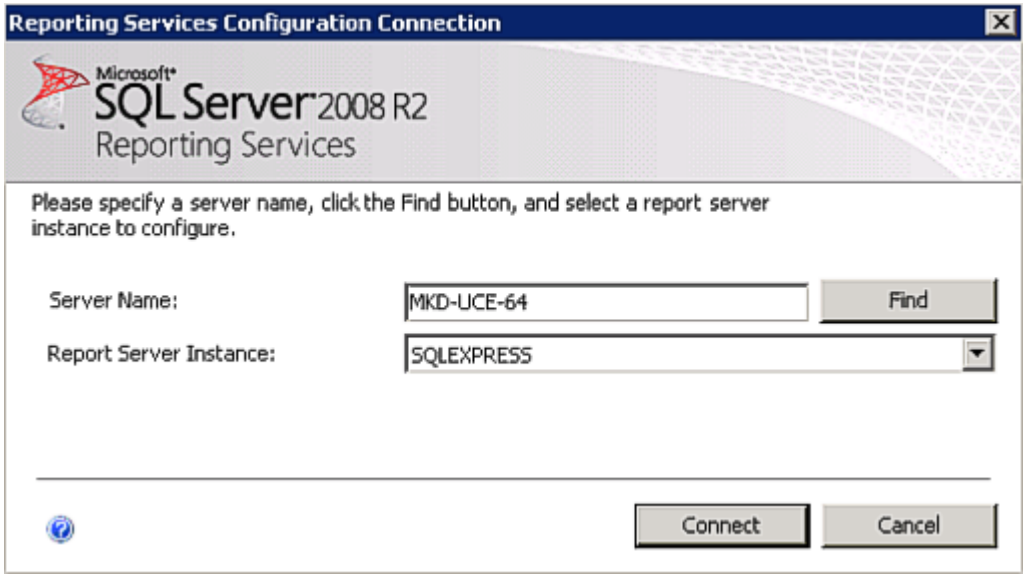
Step 1 Open the Reporting Services Configuration Tool: **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > Reporting Services Configuration Manager** (Figure 2-45).

Figure 2-45 *2008 R2 Reporting Services Configuration*



An Instance Selection dialog box displays (Figure 2-46).

Figure 2-46 *2008 R2 Instance Selection dialog box*

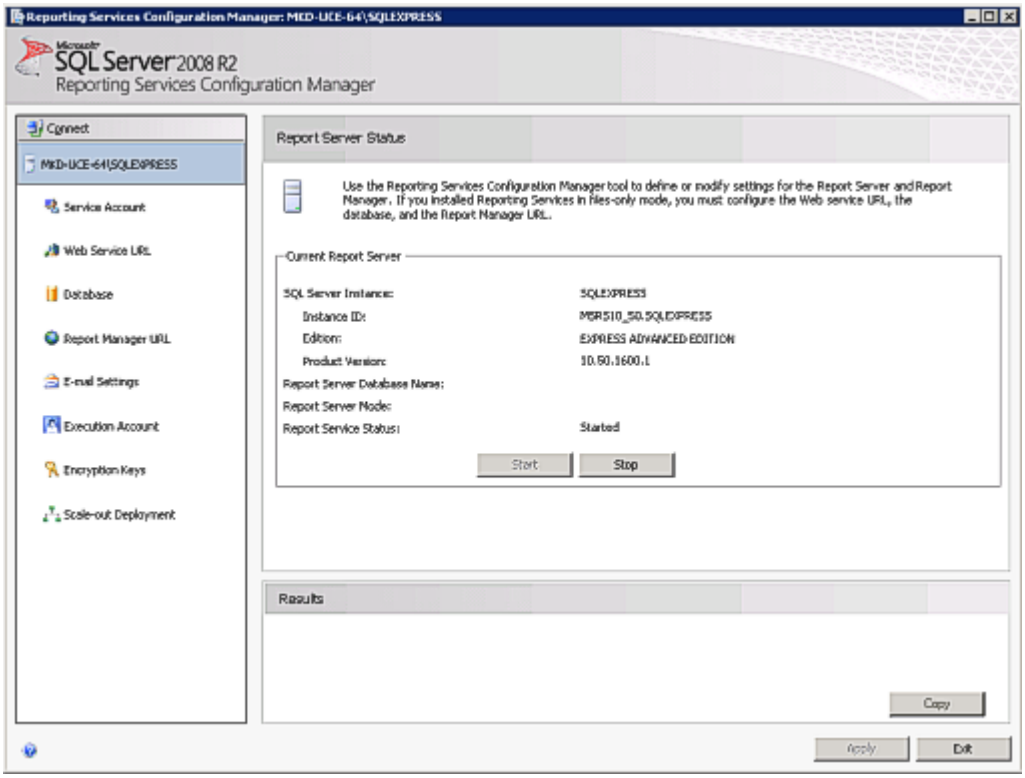


Step 2 Specify a **Server Name**, select a **Report Server Instance,** and click **Connect**. A Report Server Status dialog box displays (Figure 2-47).

NOTE

If Report Server Instance is grayed out, re-run the SQL installation and ensure that the Report Server component is installed.

Figure 2-47 *2008 R2 Report Server Status dialog box*



—If the **Stop** button is grayed out, the Report Server is not connected. Click the **Start** button.

The following topics are included in this section:

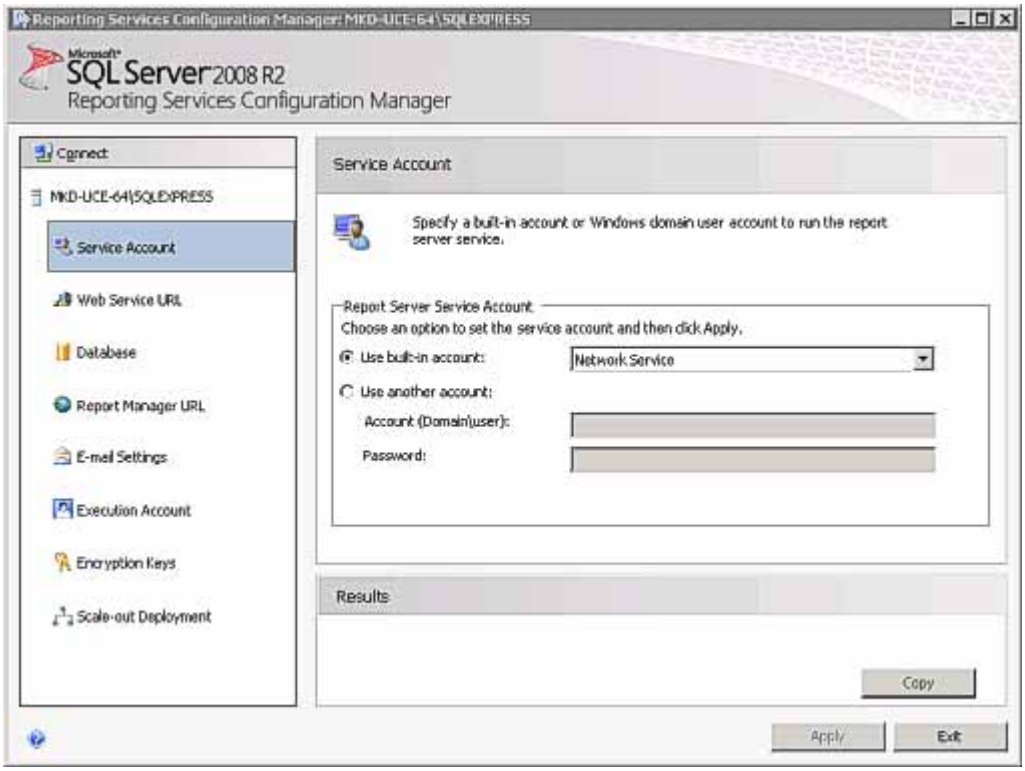
- *Service Account*
- *Web Service URL*
- *Database*
- *Report Manager URL*

Service Account

Service Account identifies which account will run the report server service. The server account is selected during SQL installation.

To verify the account, select **Service Account** from the **Reporting Services Configuration Manager** dialog window. Figure 2-48 displays.

Figure 2-48 *2008 R2 Service Account dialog*



The default value for **Use built-in account** is **Network Service**.

NOTE

*The **Service Account** window is for verification purposes only. It is recommended that the **Use built-in account** value not be changed from the default.*

Once verified, no further action is required.

In order to change the bullt-in account type, you must have an encryption key. It is recommended that you create a backup of the Report Server Database before selecting any account other than the default. See .

IMPORTANT

*If the **Use built-in account** field is changed, the following error message may appear.*

"The report server cannot decrypt the symmetric key used to access sensitive or encrypted data in a report server database. You must either restore a backup key or delete all encrypted content. Check the documentation for more information. (rsReportServerDisabled)"

If you receive this error, the Service login account has changed and a new encryption key file is needed to validate the new account. You should restore a symmetric key only if it is the same key that is currently used to encrypt and decrypt data in the report server database. If you restore a symmetric key that is not valid, you will no longer be able to access sensitive data. In this case, you must delete and re-create the key. Refer to documentation from Microsoft SQL Server on restoring encryption Key files. If the key file is not available, then go to the Encryption section and delete the current key file and re-do all steps.

Web Service URL

In order to access the Report Server, the Web Service URL must be configured. Use the Web Service URL page to configure or modify the URL used to access the report server. A URL reservation will be created based on the URL you specify.

Follow the steps below to configure a URL in order to access the Report Server.

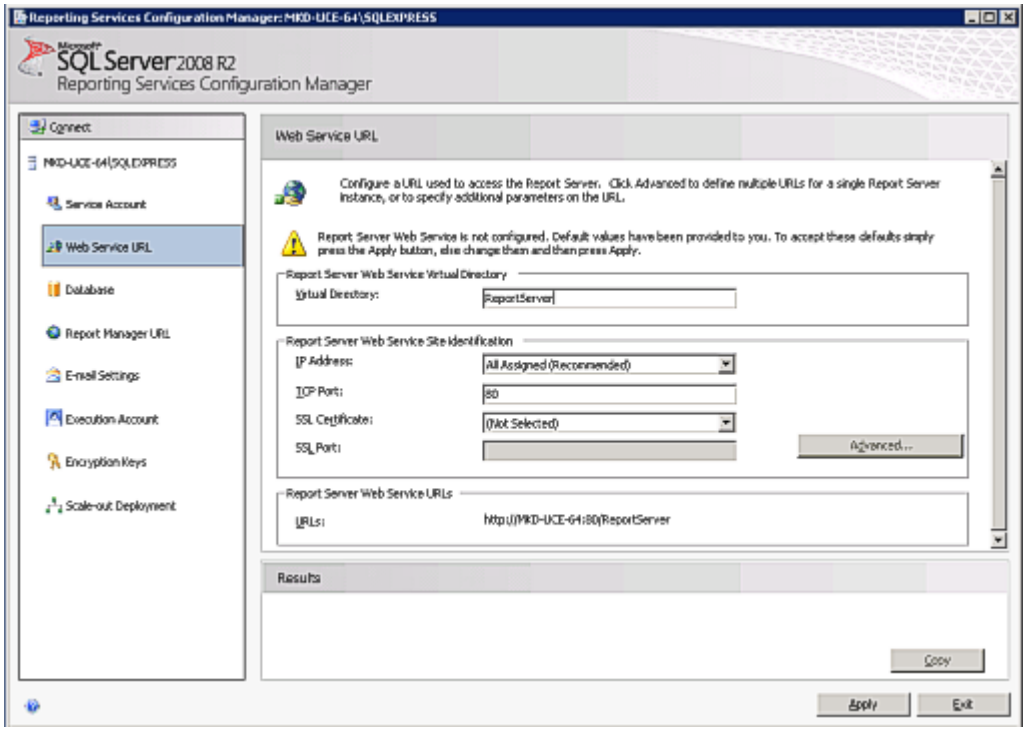
Step 1 From the left panel of the **Reporting Services Configuration Manager** dialog window, select **Web Service URL**. Figure 2-49 displays.

NOTE

The Web Service URL dialog box is populated with data identified during the SQL installation. If no changes are needed, it is recommended that you accept the default settings. If you accept the default settings, no further action is needed for this procedure.

If you need to make changes, notify your System Administrator and proceed with the steps below.

Figure 2-49 *2008 R2 Web Service URL dialog box*



Step 2 Enter a name for the **Virtual Directory**. This allows you to specify the virtual directory name for the Report Server Web service. You can only have one virtual name for each Report Server Web service instance on the same computer.

Step 3 Select an **IP Address** from the drop-down list. It is normally OK to accept the default value, **All Assigned**.

Step 4 Enter the **TCP Port Number**. The default is 80.

Step 5 Click **Apply**. Figure 2-50 displays.

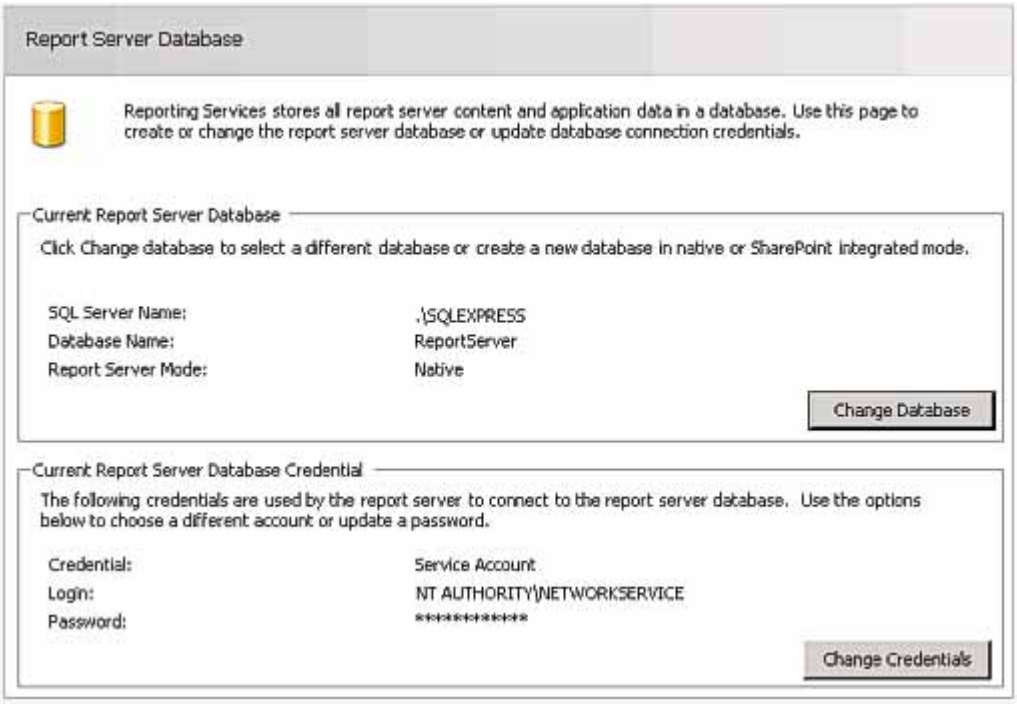
Figure 2-50 *2008 R2 Web Service URL—Confirmation dialog box*

For information on **Advanced** settings, refer to ***Microsoft's SQL Server 2008 R2 Reporting Services Configuration Manager Online Help***.

Database

The **Report Service Database** stores all report content and application data and is accessed under **Database** on the **Reporting Services Configuration Manager** dialog box. Use the **Report Service Database** dialog box to verify report server database settings.

Figure 2-51 *Report Service Database*

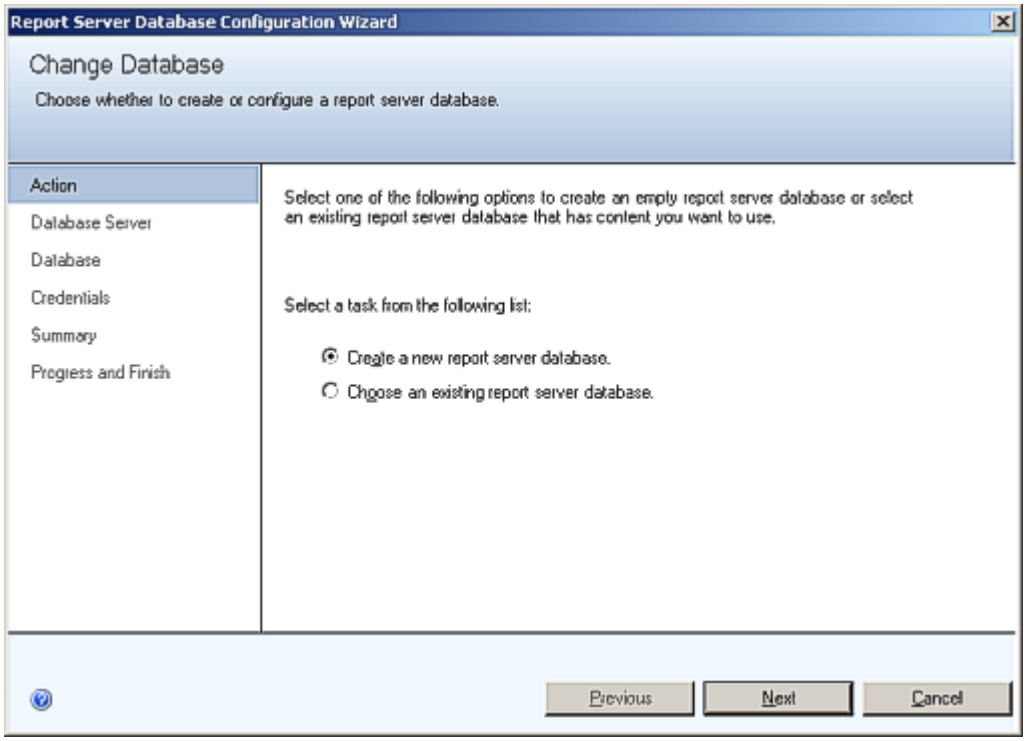


NOTE

*The fields in the **Report Server Database** dialog box are populated during SQL installation. If SQL Installation was performed correctly, no changes to this page are necessary. If the fields are blank on the Report Server Database dialog, follow the steps below.*

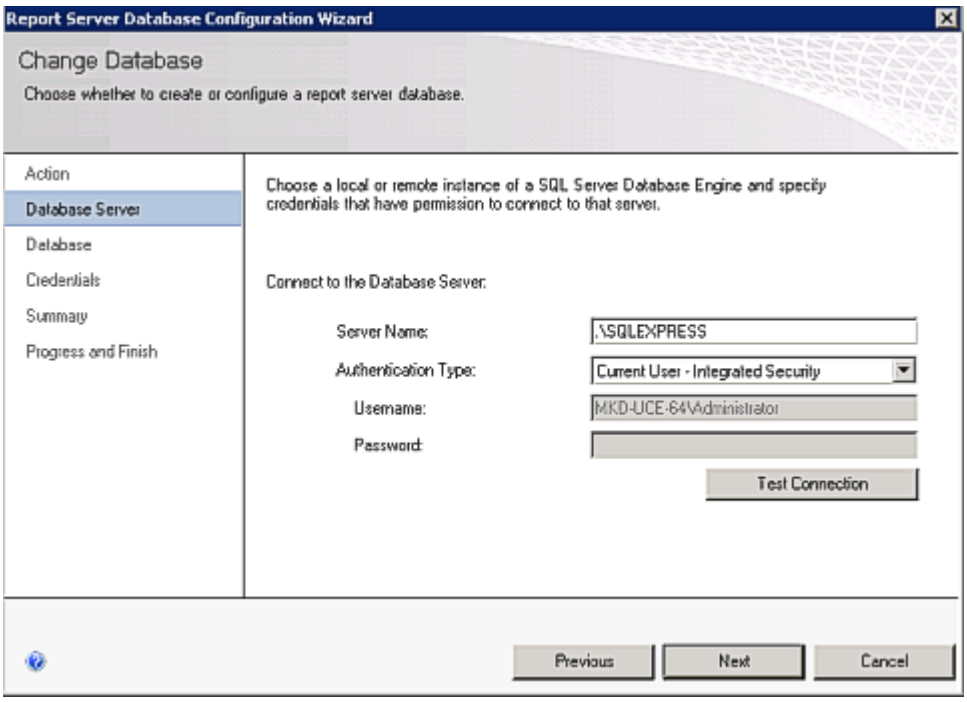
Step 1 If the fields in the Report Server Database dialog are blank, click **Change Database**. A Change Database—Action dialog box displays (Figure 2-52).

Figure 2-52 *Change Database—Action dialog box*



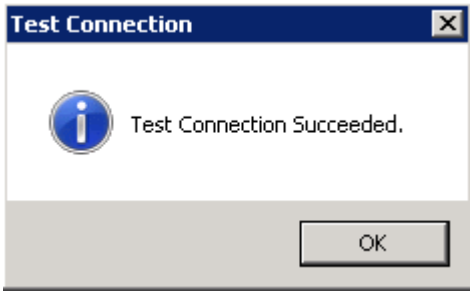
Step 2 Click **Next**. A Change Database—Database Server dialog box displays (Figure 2-31).

Figure 2-53 *Change Database—Database Server dialog box*



Step 3 Click **Test Connection**. Figure 2-32 displays.

Figure 2-54 *Test Connection Confirmation dialog box*



Step 4 If the test is not successful, edit the Server Name to match the instance name and try again.

NOTE

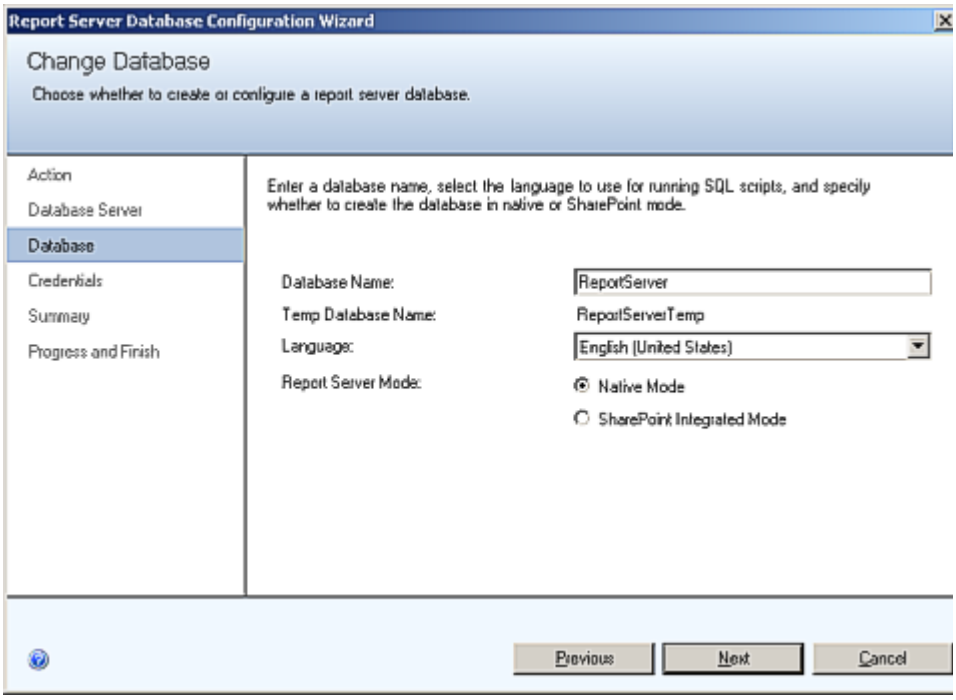
Depending on the SQL edition you are using and how it was installed, one of the following should allow a successful connection:

<hostname>
<hostname>\<instance name>
.\<instance name>

If you are in doubt as to whether or not a successful Test Connection is connecting to the correct SQL instance, try using Microsoft SQL Server Management Studio to connect to the value you have specified here. You should not only be able to connect, but also examine the Databases to find the OW5000 database residing there. (It's technically OK, however, to install the Report Server Database within a different instance of SQL than that where the OW5000 database resides.)

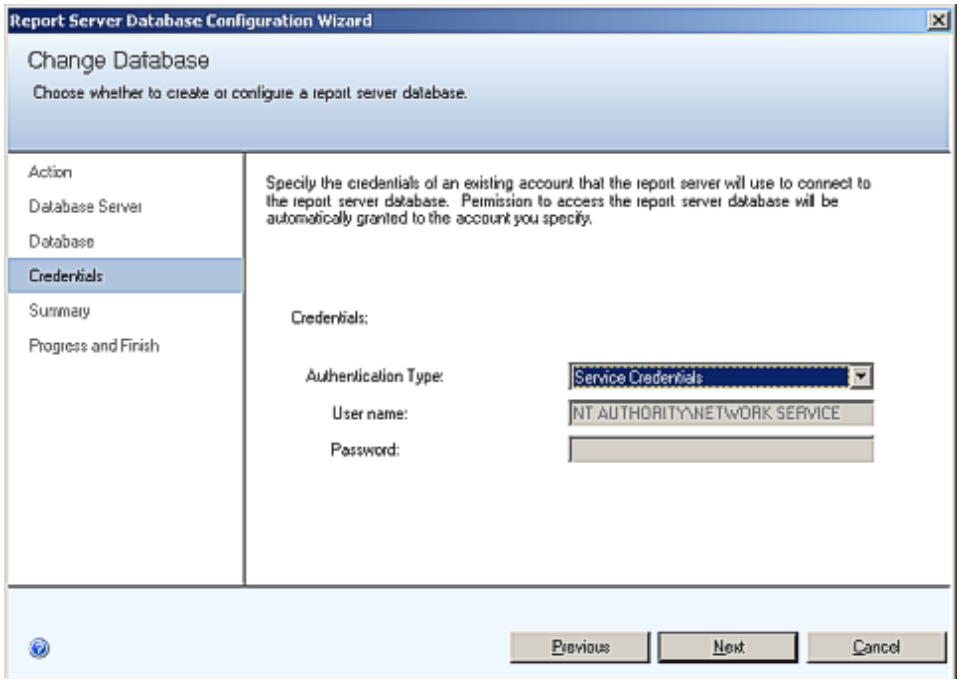
Step 5 Click **Next**. A Change Database—Database dialog box displays (Figure 2-33).

Figure 2-55 *Change Database—Database dialog box*



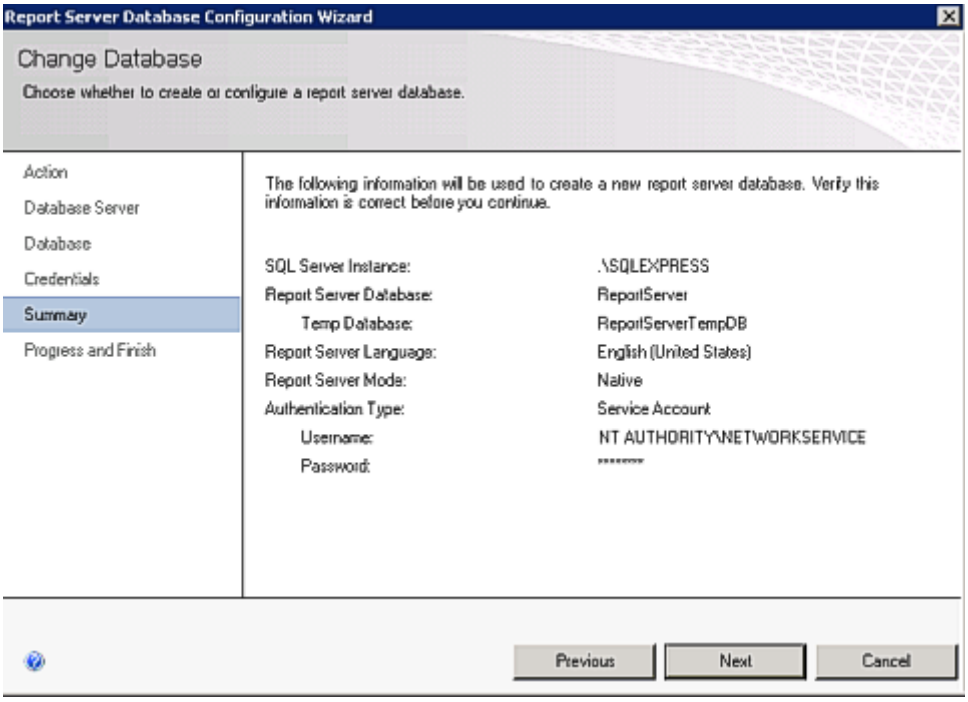
Step 6 Accept the defaults and click **Next**. A Change Database—Credentials dialog box displays (Figure 2-34).

Figure 2-56 *Change Database—Credentials dialog box*



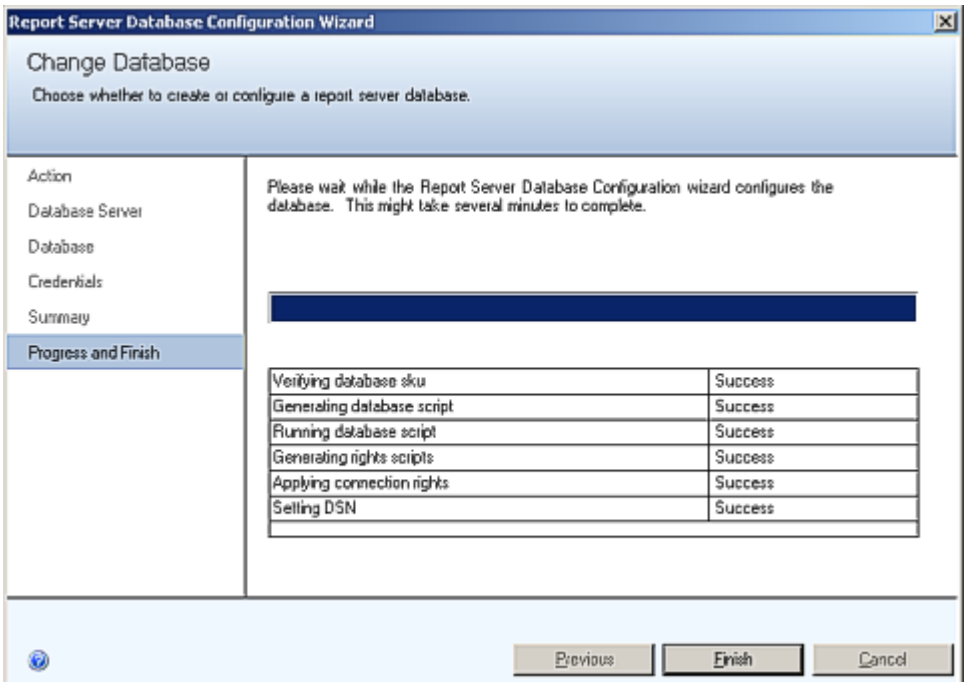
Step 7 Accept the default values and click **Next**. A Change Database—Summary dialog box displays (Figure 2-35).

Figure 2-57 *Change Database—Summary dialog box*



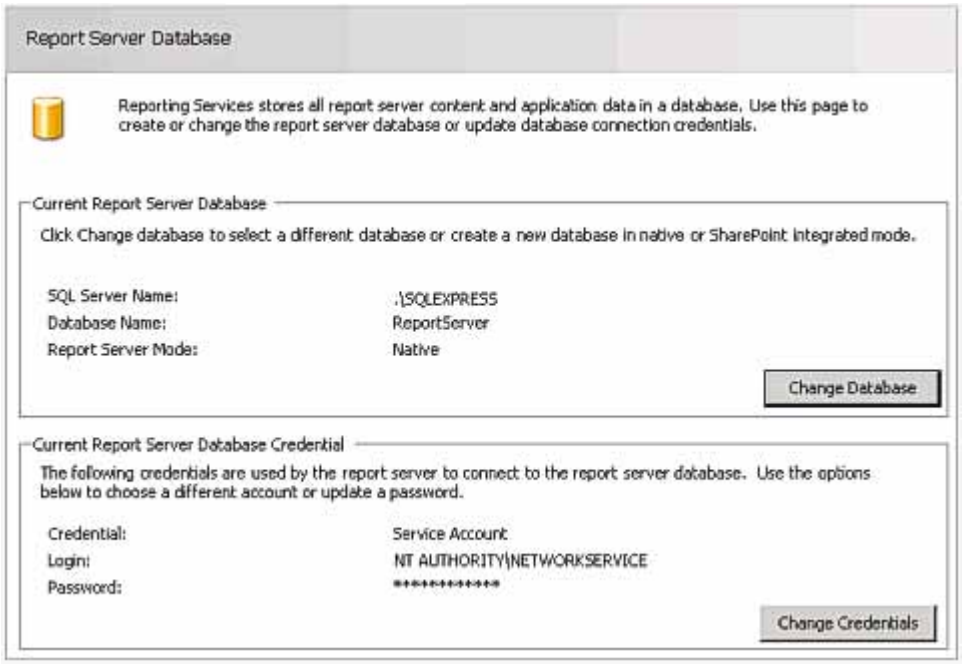
Step 8 Review the settings and click **Next**. A Change Database—Progress and Finish dialog box displays (Figure 2-36). Wait for it to complete.

Figure 2-58 *Change Database—Progress and Finish dialog box*



Step 9 Confirm that a status of **Success** is shown for each step, and then click **Finish**.

Figure 2-59 *Report Server Database—Database option*

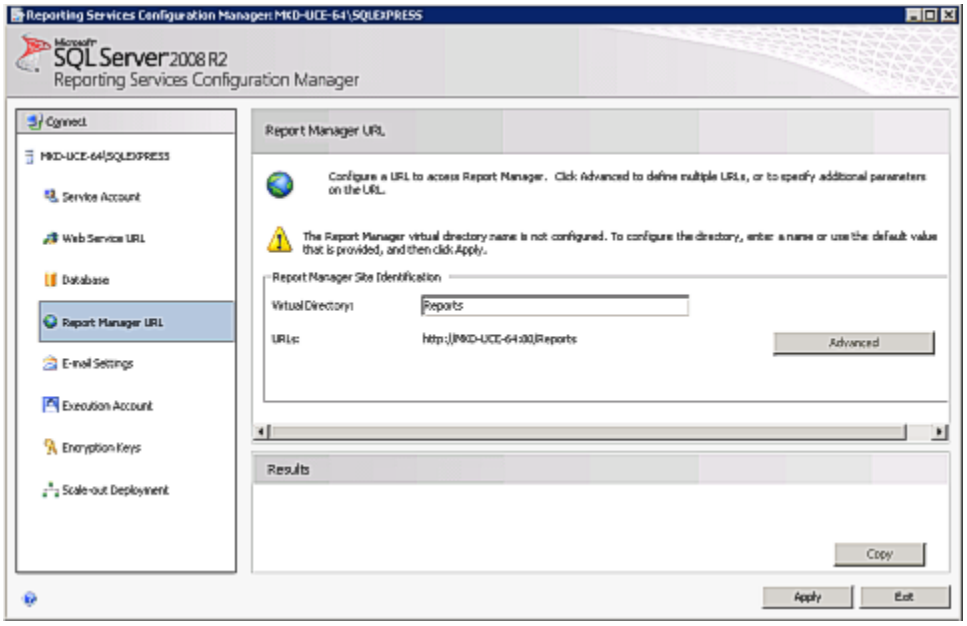


Report Manager URL

Use the Report Manager URL page to configure or modify the URL used to access Report Manager. Report Manager listens on the same IP address and port as the Report Server Web service. By default, the Report Manager URL inherits the prefix, IP address, and port of the Report Server **Web Service URL**. If you configured Report Manager to point to a different Report Server Web service, you must modify the Report Manager URL settings. Follow the steps below.

Step 1 Select **Report Manager URL** from the **Reporting Services Configuration Manager** dialog box. Figure 2-60 displays.

Figure 2-60 *2008 R2 Report Manager URL dialog box*



Step 2 Enter a value of **Reports** for the **Virtual Directory** name for the Report Manager Site Identification.

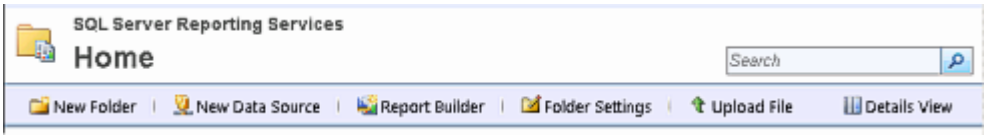
Step 3 Click **Apply**.

Step 4 Test the URL by clicking the link in the **URLs** section of the **Report Manager URL** window. If the URL is correct, Figure 2-61 displays. (It can take 60 seconds or longer for this page to open in your browser.)

NOTE

If prompted, enter the User Name and Password of the person that has machine administrator privileges on that machine.

Figure 2-61 *2008 R2 SQL Server Reporting Services Home*



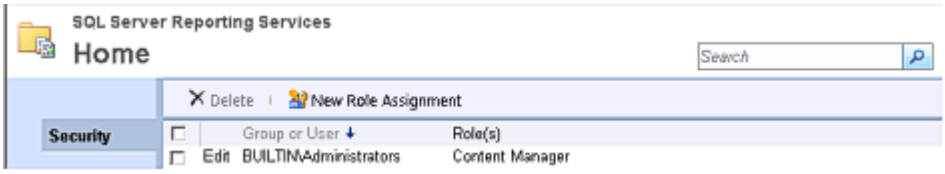
NOTE

If the web page does not open, verify that IIS is running on your server.If the web page opens, the following error might be displayed: ***This page might not function correctly because either your browser does not support scripts or active scripting is disabled.*** *If so, using Internet Explorer, go to* ***Tools*** *>* ***Internet Options*** *>* ***Security tab*** *>* ***Local Intranet****, click the* ***Sites*** *button, and add your Report Manager URL to the list of sites.*

Loading the SQL Service Report Service

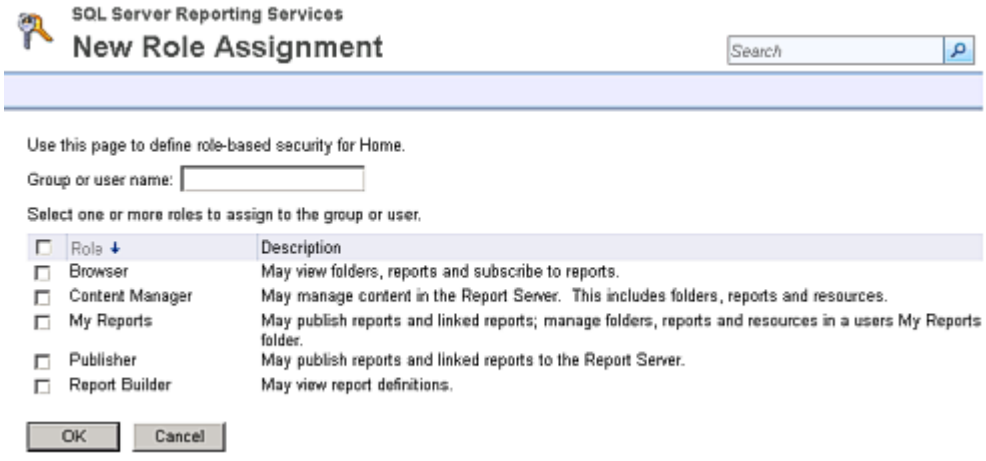
Step 1 Click **Folder Settings** (Figure 2-61) to display a Role Assignment dialog box (Figure 2-62).

Figure 2-62 *2008 R2 Role Assignment dialog box*



Step 2 Click **New Role Assignment**. A New Role Assignment dialog box displays (Figure 2-63).

Figure 2-63 *2008 R2 New Role Assignment dialog box*



Step 3 Enter **NT AUTHORITY\NETWORK SERVICE** in the **Group or user name** field. This field is case sensitive.

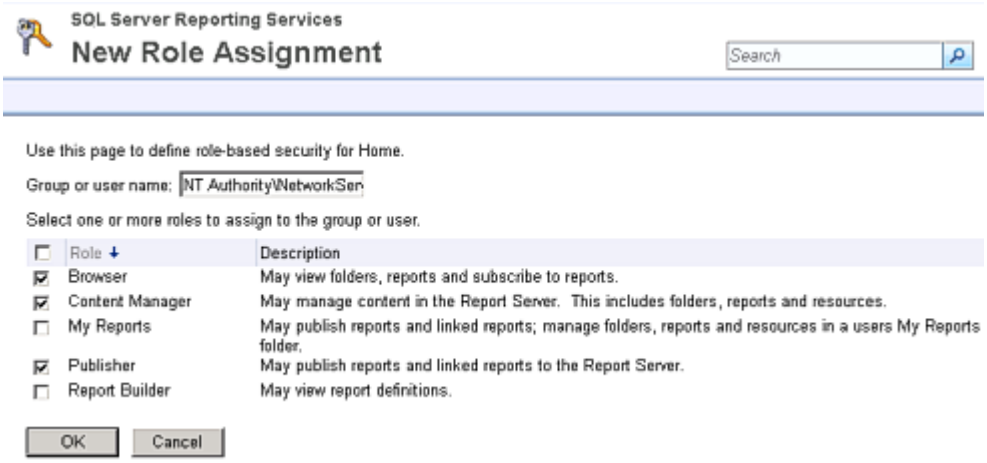
Step 4 Check the following check boxes, as shown in Figure 2-64.

—Browser

—Content Manager

—Publisher

Figure 2-64 *2008 R2 New Role Assignment Datafill*



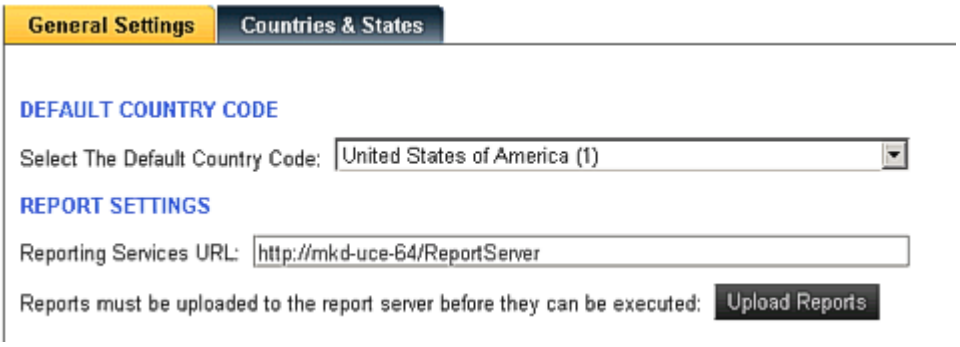
Step 5 Click **OK**.

Uploading OW5000 Reports

You must log on to the OW5000 Administrator in order to upload reports. Refer to the *UNIVERGE OW5000 Configuration Guide* for information on how to log on to the OW5000 Administrator. When you have finished, you can either log out or just close your browser.

Step 1 Once you are logged on to OW5000 Administrator, follow this path to open the Report Setting configuration options: **OW5000 > Settings > General Settings**. A Settings dialog box displays (Figure 2-65).

Figure 2-65 *2008 R2 Settings dialog box*



Step 2 Verify that the reporting services URL matches the Virtual Directory value in the Reporting Services Configuration Manager. The default is **http://<Machine Name>/ReportServer**.

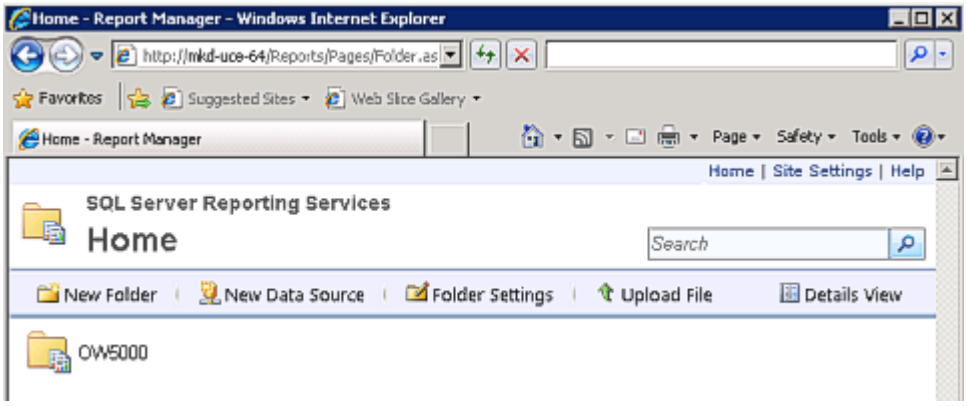
Step 3 Click **Upload Reports**. A Reports Confirmation dialog box displays (Figure 2-66).

Figure 2-66 *2008 R2 Reports Confirmation dialog box*

Step 4 If a confirmation dialog box does not display, verify that the **NT AUTHORITY\NETWORK SERVICE** account was correctly added to the Home level in the Report Manager web page by doing the following.

—Go to the Report Manager web page ***//<Server Name>/Reports***. Figure 2-67 displays.

Figure 2-67 *Report Manager—Home*



— Verify the sub directory **OW5000** was created under **Home**.

—Click **OW5000**, and then click **Admin**. All reports that OW5000 currently deploys and supports will display. All future reports will be uploaded to this location anytime the Upload button is pressed in Admin, assuming that the report to upload is residing in the reports deployment folder. The default deployment folder is **C:\Program Files\NEC\OW5000\Administrator\ReportFiles**.

Reports can now be generated for applications using SSRS reports.

3

Configuration

The functions and associated screen displays for configuring the UCE Emergency On-Site Notification (E-OSN) application are described in this chapter.

Before configuring the E-OSN application, a user with OW5000 Administrator access rights must log in to the OW5000 Administrator application and create a user with E-OSN Administrator privileges. Once a user is given E-OSN Administrator access rights, that user can log in to OW5000 Administrator and configure the E-OSN application. Through the OW5000 Administrator, you select routes to be monitored and designate those routes as emergency notification routes. You also designate personnel to receive emergency notification events. From the OW5000 you can also create Emergency Call History reports. When you have finished configuring the application, you can either log out or just close your browser.

This chapter provides the procedures for starting and configuring the E-OSN application and UCE Emergency On-Site Notification Client (E-OSN Client). Procedures are located in the following sections:

Chapter Topics

- *Login Authorization*
- *Route Configuration*
- *Emergency Notification Administration*
- *Email Notification*
- *MA4000 Location Data Sync*

Login Authorization

The following user roles are available for the UCE Emergency On-Site Notification application.

- Emergency On-Site Notification Administrator - selecting this role allows you to login to OW5000 Admin and configure E-OSN options. You must also have OW5000 Admin authorization. The E-OSN Administrator has the same functionality as an Emergency On-Site Notification User.
- Emergency On-Site Notification User - an E-OSN User can log into an E-OSN Client and is able to view emergency calls, perform **Listen In**, **Conference**, and **Acknowledge**.

- Emergency On-Site Notification Observer - an E-OSN Observer can log into an E-OSN Client and is able to view emergency calls, but is not able to perform **Listen In**, **Conference**, or **Acknowledge**.

Selecting Desired User Role

Follow the steps below to select the desired user role.

Step 1 Navigate to **OW5000** > **Directory** > **Users**. On this screen, select the user to be given Emergency On-Site Notification privileges by clicking on the **Pencil** icon next to the name.

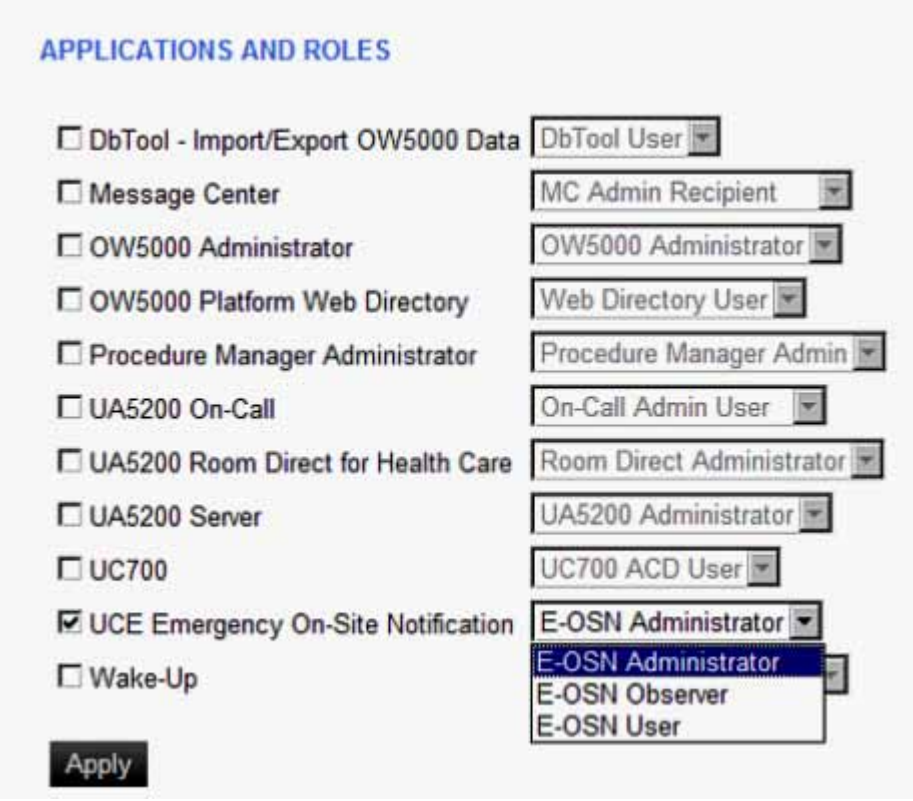
Step 2 Scroll down to the section **APPLICATIONS AND ROLES**.

Step 3 Click on the check box next to **UCE Emergency On-Site Notification** and select the desired user type from the drop list, Figure 3-1.

NOTE

An E-OSN Administrator must also have OW5000 Administrator access rights; otherwise, the E-OSN Admin will not be able to properly configure the system.

Figure 3-1 *User Type Selection*



Step 4 Click the **Apply** button.

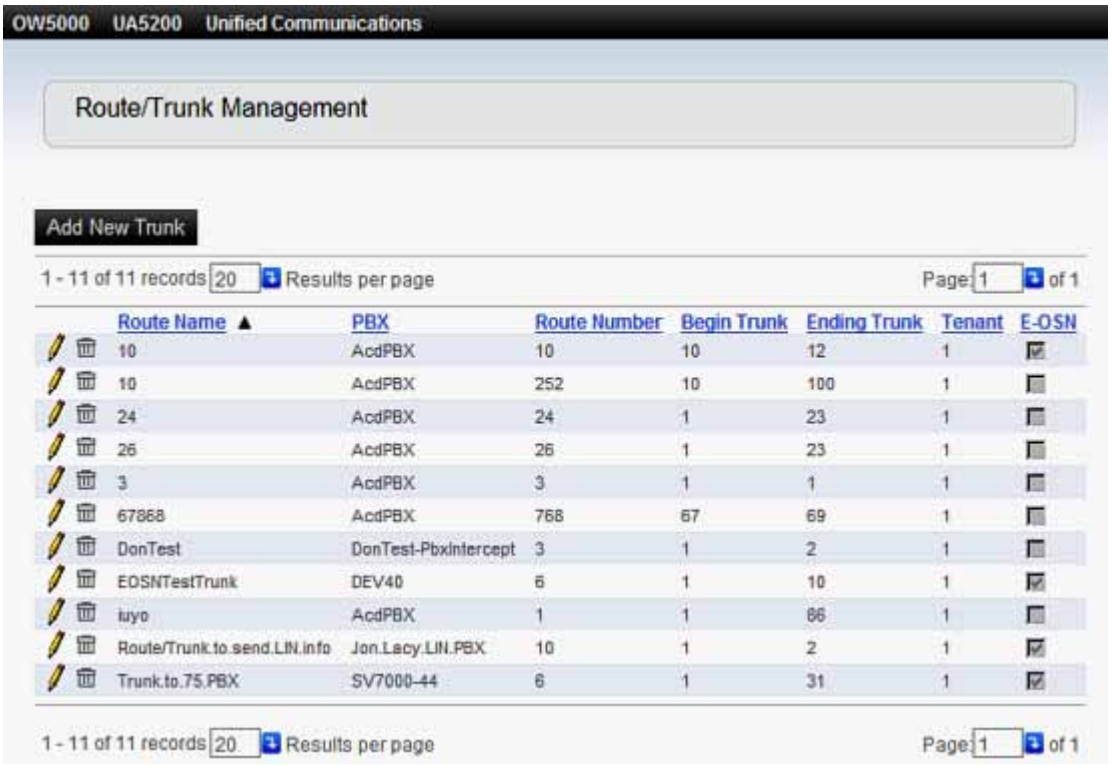
Route Configuration

Configuring a route and assigning a name to it uniquely identifies incoming calls on this route for users of Attendant applications.

The main Route/Trunk Management screen, Figure 3-2, is accessed from **OW5000** > **Platform** > **Routes/Trunks** and contains a list of all existing Routes. A check box in the E-OSN check box column identifies the route as an Emergency On-Site Notification route. The E-OSN check box is visible when Emergency On-Site Notification is properly licensed and the logged in user has Emergency On-Site Notification Administrator privileges.

Marking a route as an Emergency On-Site Notification Route allows the system to monitor the route and report all activity on the route as an emergency call.

Figure 3-2 *Route/Trunk Management*



Adding/Editing UCE Emergency On-Site Notification Routes

Perform the following steps to add or edit an UCE Emergency On-Site Notification Route.

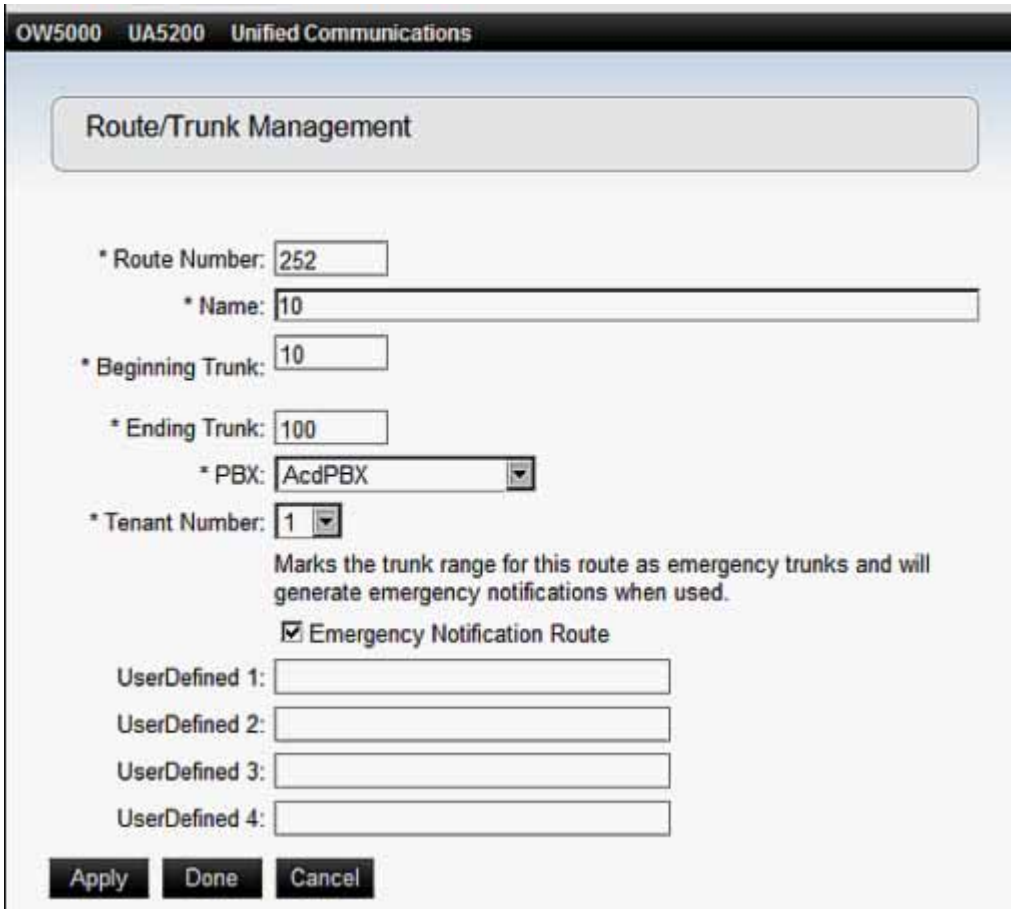
Step 1 To edit a Route and designate it as an Emergency Notification route, browse to **OW5000** > **Platform** > **Routes/Trunks**.

Step 2 Select the Route to be changed by clicking on the **Pencil** icon. A screen, Figure 3-3, opens displaying information for that Route. A check in the box under **UCE Emergency On-Site Notification** identifies the route as an UCE Emergency On-Site Notification route. Absence of a check in the box indicates the route is not an UCE Emergency On-Site Notification route.

NOTE

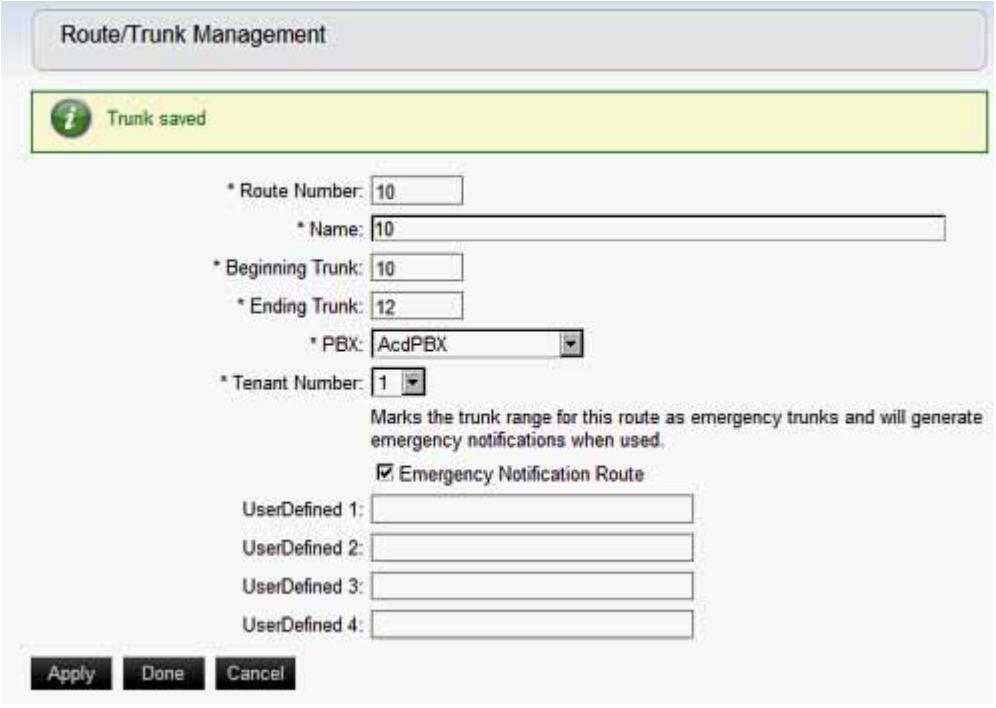
OW5000 does not support route 0 as a valid route. Route 0 should not be used as an emergency route in a PBX since E-OSN will not be notified when an emergency call is made on that route.

Figure 3-3 *Add/Edit Route/Trunk Management dialog box*



Step 3 Make desired change and click **Apply**. A confirmation screen displays, Figure 3-4.

Figure 3-4 *Add/Edit Route/Trunk confirmation*



NOTE When designating a route as an E-OSN route, ensure that the associated PBX is selected as a PBX for the OW5000 application called OAI Server. If OAI Server is not selected to get an OAI Association to that PBX, then a warning displays.

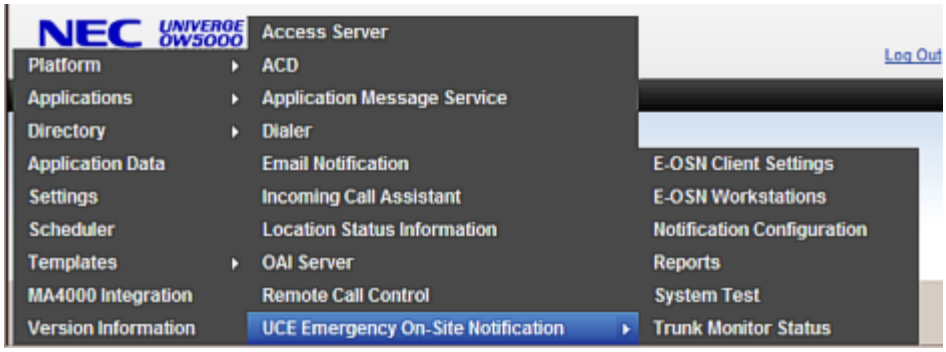
NOTE The TelEvent service must be restarted in order to have the new E-OSN route monitored.

Emergency Notification Administration

To access the UCE Emergency On-Site Notification application, browse to **OW5000** > **Applications** > **UCE Emergency On-Site Notification.** This provides the following administration options, Figure 3-5.

- E-OSN Client Settings
- Notification Configuration
- Reports
- System Test
- Trunk Monitor Status

Figure 3-5 *E-OSN Administration application*



NOTE

These menu options are only visible when UCE Emergency On-Site Notification is properly licensed and the user has UCE Emergency On-Site Notification Administrator privileges.

Emergency Notification Client Settings

The E-OSN Client can be configured to use Windows login or OW5000 User Role login. Use E-OSN Client Settings to configure the parameters for the E-OSN Client. Client Settings are accessed from **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **E-OSN Client Settings.** These parameters include:

- **Login method**
  - — Windows Login (Default) (NTLM)
  - — OW5000 login
- **Suppress Screen Saver**
  - — Enabled- (Default) On receipt of notification, send "mouse move" to make screen saver go away.
  - — Disabled - On receipt of notification do not attempt to make screen saver go away.

NOTE

Some screen saver systems may not respond and continue to block dialog pop attempts.

- **Alert Sound**
  - — Pick one from a list of audio file names for the E-OSN Client to play upon receipt of emergency notification call.
  - — The client comes installed with 10 "built in" wave files out of the box. The built in file names are listed in the **Alert Sound** drop down box, allowing you to choose which file to use.

NOTE

Preview alert sounds using the System Test for Emergency Calls. An E-OSN Client will play the configured sound when the test call is received.

- **Allow Listen In**
  - — Enabled - (Default) E-OSN Users are allowed to perform **Listen In** actions using their E-OSN Clients and/or their configured workstation Dterms.
  - — Disabled - E-OSN Users are not allowed to perform **Listen In** actions, from either their E-OSN Client or from their configured workstation Dterms.

NOTE

Listen In provides the ability to silently monitor an emergency call in progress.

- **Allow Conference**
  - — Enabled - E-OSN Users are allowed to perform conference actions using their E-OSN Clients and/or their configured workstation Dterms.
  - — Disabled - E-OSN Users are not allowed to perform conference actions from either their E-OSN Clients and/or their configured workstation Dterms.
- **Default Phone Action** describes the action executed when handling emergency calls via the configured workstation Dterms.
  - — **Listen In** (Default) - When joining an emergency call using the phone, the E-OSN User will silently listen to this call. This option is not available when **Listen In** is not selected.
  - — **Conference** - When joining an emergency call using the phone, the E-OSN User will enter into a conference with this call. This option is not available when **Conference** is not selected.

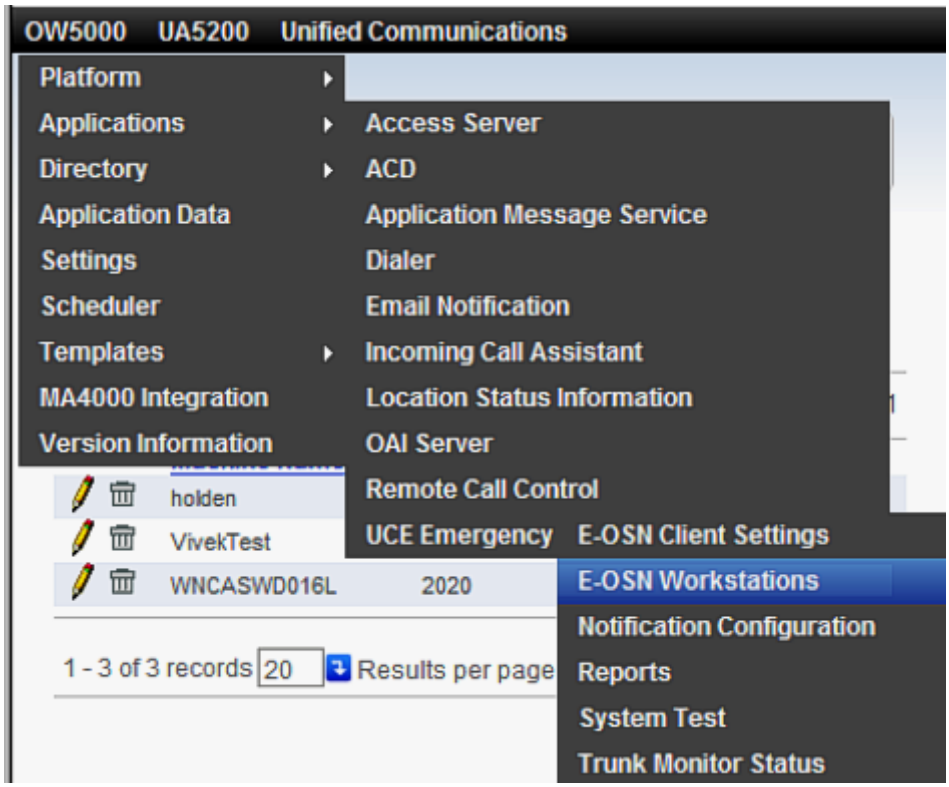
These settings apply to all E-OSN Client instances. Figure 3-6 provides an example of the E-OSN Client Settings screen.

Figure 3-6 *E-OSN Client Settings*

E-OSN Workstations

In order to use the E-OSN Client in combination with a Dterm extension (thus being able to perform **Listen In** and **Conference**), an E-OSN workstation must be configured for each machine that is running the E-OSN Client. Access the E-OSN workstation's configuration page from **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **E-OSN Workstations**, see Figure 3-7.

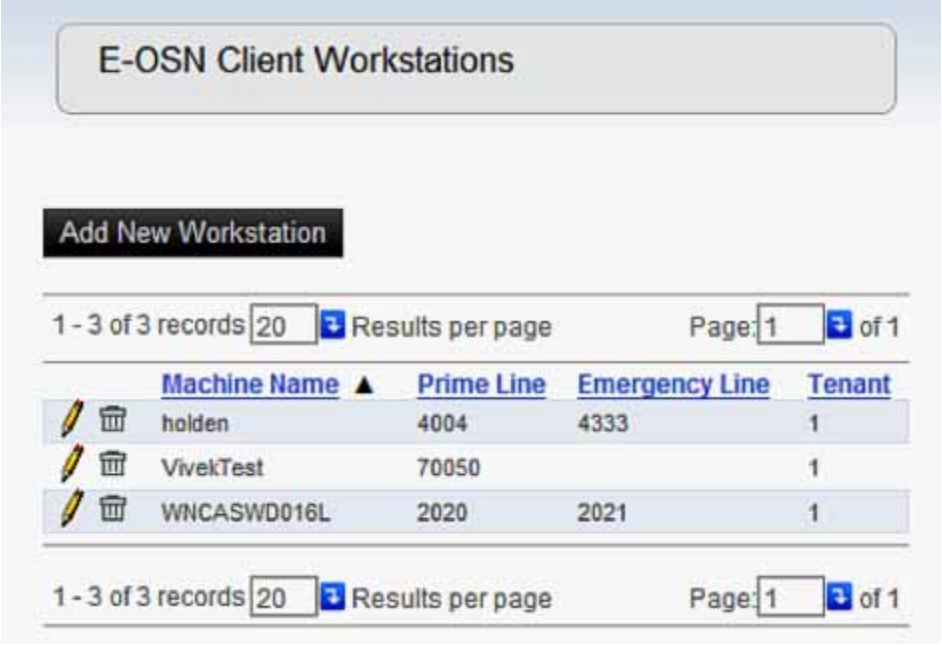
Figure 3-7 *E-OSN Workstation Configuration*



The main screen under **E-OSN Client Workstations** is depicted in Figure 3-8. To add a new workstation item, click the **Add New Workstation** button. The grid under this button contains a list of already configured workstations. This grid contains the following items:

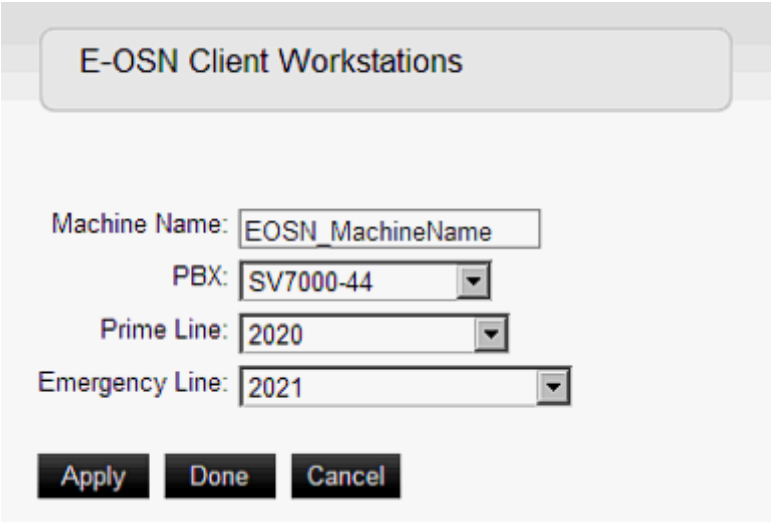
- Modify icon (pencil) - modifies an existing workstation
- Delete icon (trashcan) - deletes an existing workstation
- Machine Name - name of the PC that will run the E-OSN Client
- Prime Line - extension number used as prime line
- Emergency Line - extension number used as emergency line (subline)
- Tenant - tenant number for prime line/emergency line

Figure 3-8 *E-OSN Client Workstations*



Pressing **Add New Workstation** or the modify icon (the pencil icon) opens a new page where the administrator can define the **Machine Name**, the **PBX**, the **Prime Line** and the **Emergency Line**, see Figure 3-9.

Figure 3-9 *Add/Modify New Workstation*



The PBX can be picked from a drop down list populated with PBXs that are selected to be monitored by the Oai Server application. Choosing the PBX populates the Prime Line and Emergency Line drop down boxes

with extensions from that PBX, which can be used as prime line or emergency line.

NOTE

The emergency line must be defined in the PBX and in OW5000 Admin as a subline for the Dterm that uses the above mentioned prime line as main line. This subline should be labeled “Emergency Line on E-OSN Workstation's Dterm”.

The **Machine Name** can be entered only when a new workstation is created (related text field is disabled when modifying an existing workstation). Normally this field has to take the name of an existing PC. There are some situations when the machine has to take a fictive name, as depicted in the Note below.

NOTE

Customers must configure one E-OSN Workstation (with valid prime line and emergency line) for any PBX if they want the ability to join the call in progress on any PBX. The machine name does not have to be valid if it is not intended to run an E-OSN Client. Only the Dterm prime line and emergency line (subline) need to be valid. This will help when a single security guard station needs to be able to support a building with multiple PBX's. In that case, the customer will need to drop multiple Dterms near the main E-OSN Workstation so that the guard can still monitor/ conference into an emergency call regardless of which PBX it originated from. It is recommended that the name of the fictive E-OSN Workstation be a descriptive name, such as "Building A Emergency Line".

In the event the configured E-OSN workstation PCs are not usable (e.g. due to network problems), the following backup ringing and emergency call processing options are provided.

Backup Ringing

- The Dterms of the configured **E-OSN Workstations** page sounds the Alert chime and displays the text "Emergency Call" whenever there are new, unacknowledged calls in progress.
- After adding a new workstation using the **E-OSN Workstations** page, when new, unacknowledged calls in progress occur, the Dterm of the newly added workstation sounds the Alert chime and displays the text "Emergency Call".
- After removing an existing workstation using the **E-OSN Workstations** page, when there are new, unacknowledged calls in progress, the Dterm of the removed workstation stops chiming and it no longer displays the text "Emergency Call".

Emergency Call Processing

- When the security guard takes the prime line off-hook, the E-OSN Server application executes the default phone action (as defined in E-OSN Client Settings page), from the configured emergency line (subline) to the originating emergency caller.
- The security guard switches lines from the prime to the emergency line by pushing the flashing line and is placed into the emergency call.
- Picking up the receiver counts as an acknowledgement for the call that is joined.
- The line used to join the emergency calls should be labeled as the emergency line by the customer.

Notification Configuration

Notification Configuration is where an administrator goes to add E-OSN Client authorization and e-mail notification for emergency calls.

If an emergency call seizes a trunk that is in the Failed state, emergency notifications will not be sent.

When emergency routes are first defined, they will not display until the "OWTelephony Event Notification" service is restarted. The first time there is an attempt to monitor the trunks, the monitor status for those trunks displays.

The system does not attempt to re-monitor a trunk if it failed to be monitored at startup. If a trunk configuration is later fixed, the

Emergency Call Distribution List Creation

Emergency call notification recipients are configured by groups. Each group is associated with one or more PBX origination points.

The following illustrates an example of this concept. A customer's OW5000 Server has PBX connections to a PBX in Dallas, TX and Chicago, IL. A group called Dallas is configured to receive emergency call events from an extension in the Dallas PBX and a group called Chicago is configured to be notified of emergency calls from the Chicago PBX. A third group which is made up of the customer's management team is added to the default "All PBX Emergency Calls" to be notified of an emergency call originating from any PBX.

A recipient does not need to be in a particular PBX to be added to a group. E-OSN recipients can have locations or Email addresses anywhere. This way, the end-user can segment who gets notified based on call origination.

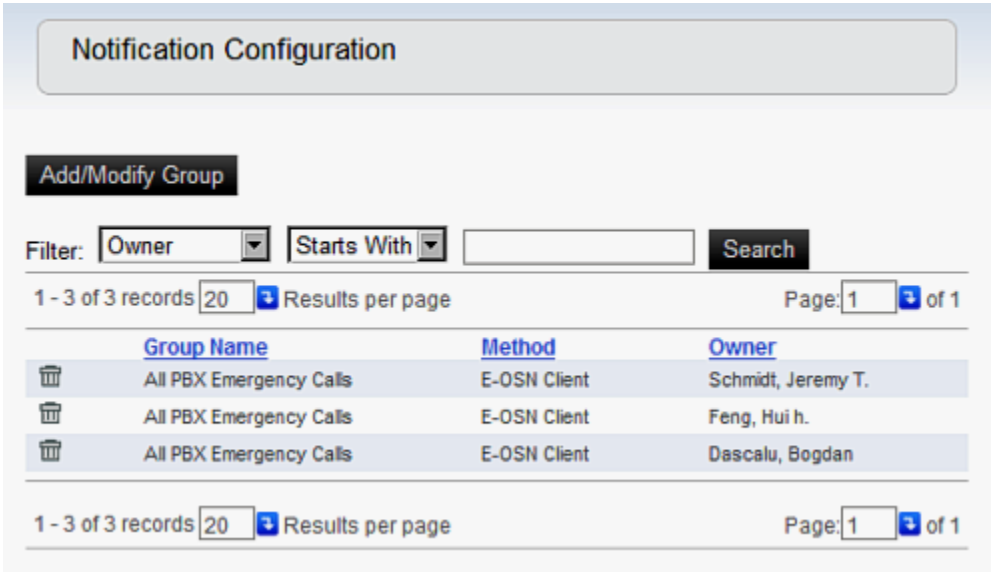
The main screen under **Notification Configuration**, Figure 3-10 provides a list of already selected Email addresses and E-OSN Client users and administrators along with the following:

- Delete icon (trash can)
- Group Name
- PBX Name
- Method
- Owner (if applicable)

NOTE

Methods are either by e-mail or as an E-OSN client.

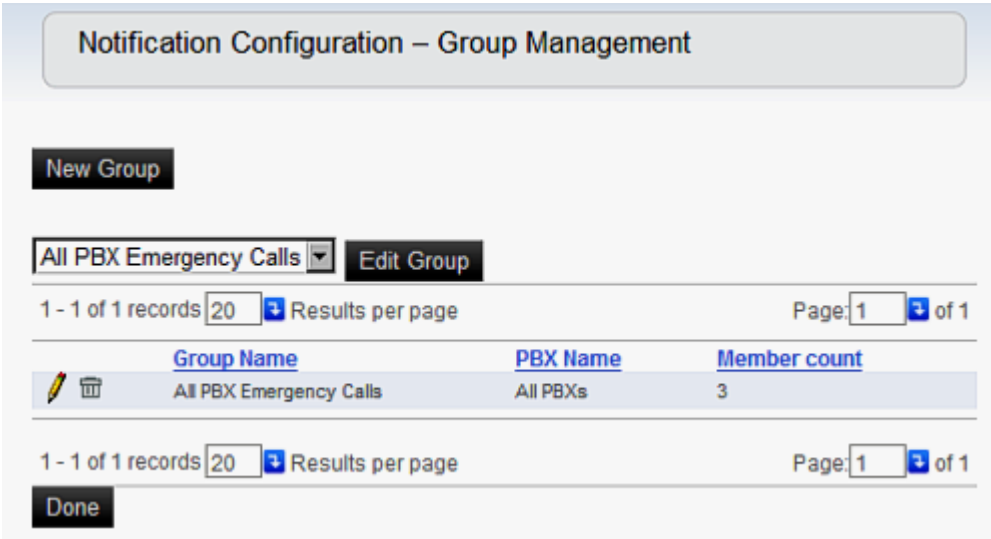
Figure 3-10 *Notification Configuration*



The **Add / Modify Group** button allows you to create and modify group names and manage recipients of a group. Clicking this button opens the Notification Configuration - Group Management page, Figure 3-11. This page shows the following:

- Pencil icon - allows editing of existing group.
- Trash can icon - deletes existing group.
- Group Name
- PBX Name
- Member Count - total number of Email addresses and E-OSN clients that will be notified in this group.

Figure 3-11 *Group Management*



E-OSN comes with a default group called "All PBX Emergency Calls". This group cannot be deleted.

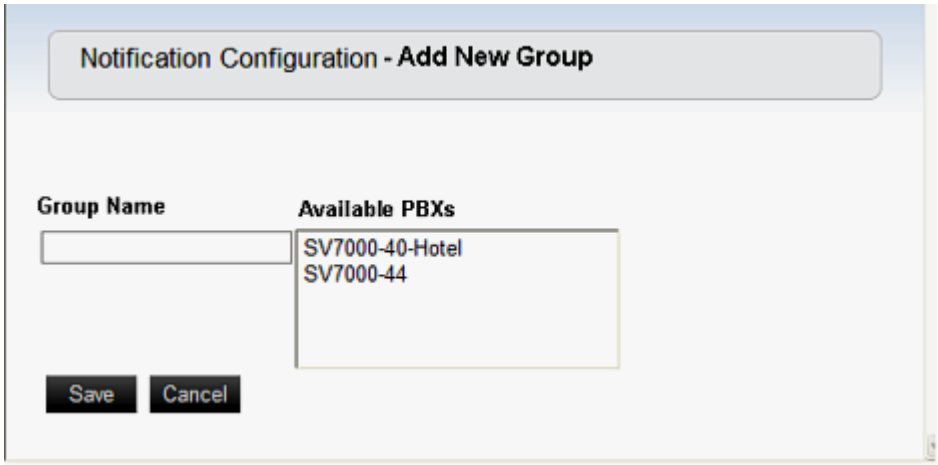
Adding a Group

Perform the following steps to add a new group.

Step 1 Navigate to **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **Notification Configuration**.

Step 2 To add a new group, click the **New Group** button. Identify a new group name and select the associated PBX from a drop-down list, Figure 3-12.

Figure 3-12 *Add a New Group*



Step 3 Click the **Save** button. The screen returns to the Add/Modify Group page with the new group visible.

Editing a Group

Perform the steps below to edit a group.

Step 1 Navigate to > **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **Notification Configuration**.

Step 2 Click **Add/Modify Group** button. the **Notification Configuration - Group Management** screen opens.

Step 3 There are two ways to edit a group.

—Pick a group from the drop down list and click the **Edit Group** button.

—Find an entry in the grid with the group name that matches the group you wish to edit and click on the **Pencil** icon.

A **Notification Configuration – Edit** (group name) screen opens, Figure 3-13.

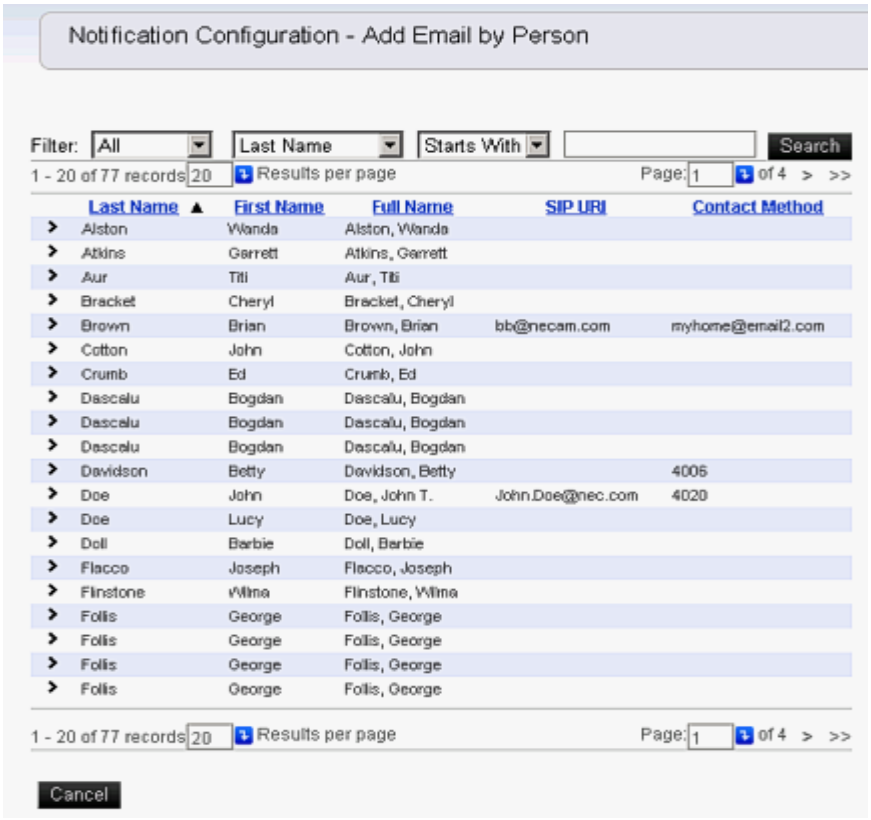
Figure 3-13 *Editing a Group*

Step 4 From this screen, you can delete a group member using the Delete (Trash Can) icon, add a new Email address to the group or individual, add an E-OSN user to the group, add or remove a Group PBX, and rename the group.

To add a new Email address to the group, type the Email address in the **Email Address** text box, then click **Add**.

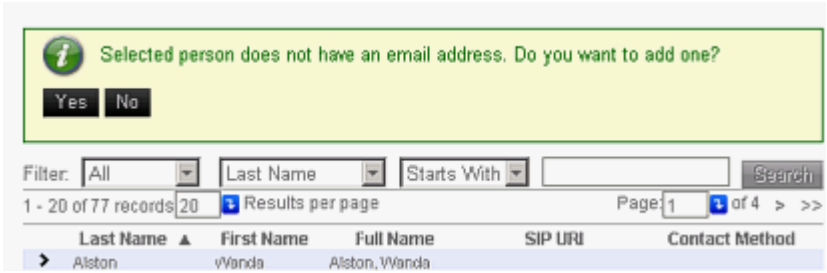
To add a new Email Address for an individual, click **Add Email by Person.** Figure 3-14 displays.

Figure 3-14 *Add Email by Person*



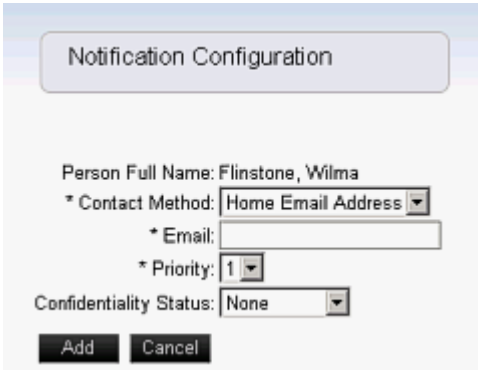
Step 5 Click the **>** next to the name of the person getting a new Email contact method. Figure 3-15 displays.

Figure 3-15 *Adding a new Email Prompt*



Step 6 Click **Yes**. Figure 3-16 displays.

Figure 3-16 *Contact Method*



Step 7 Enter the information and click Add. Figure 3-13 displays.

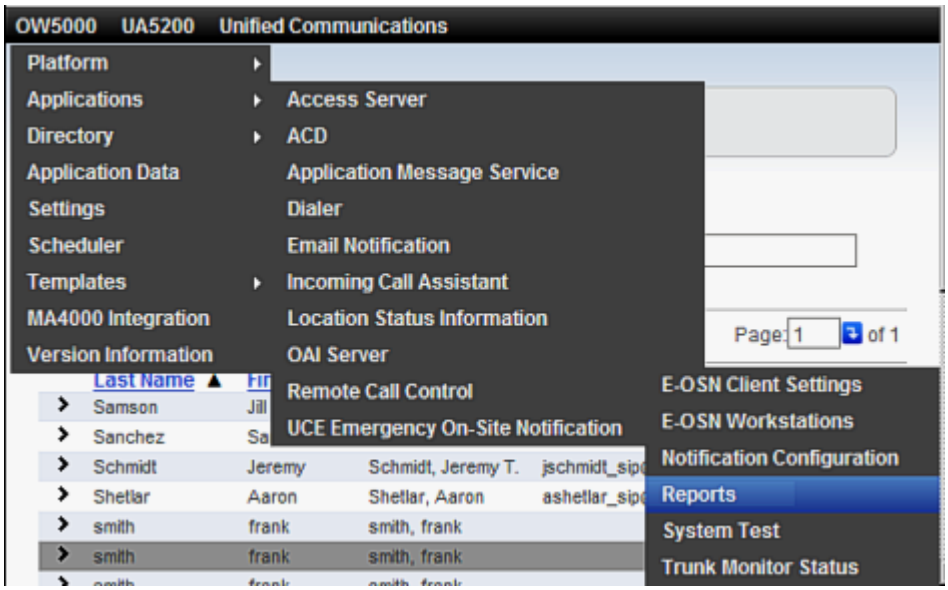
Step 8 Click **Done** when finished.

If a person has multiple Email contact methods, the Admin is given the opportunity to select from the list. A person can be selected multiple times for different Emails. They will be displayed multiple times in the edit group grid.

Reports

Emergency calls are recorded in the OW5000 database. OW5000 provides an Emergency On-Site Notification report for emergency-related audit information, including a time line for each call. It also provides call information, location, notifications sent, and acknowledgements. The Reports function is accessed from **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **Reports** (Figure 3-17).

Figure 3-17 *Reports*



Emergency On-Site Notification reports are based on SQL Reporting Services (SSRS). For more information see Chapter 2, “Installing SQL Server Report Service”.

Generating an Emergency Call History Report

E-OSN Reports support Report Grouping. The Report Grouping option is Event Date.

The report filters on date and time. There is an option to include or exclude test emergency calls in the report. Follow the steps below to generate an Emergency Call History report

Step 1 Navigate to **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **Reports.**

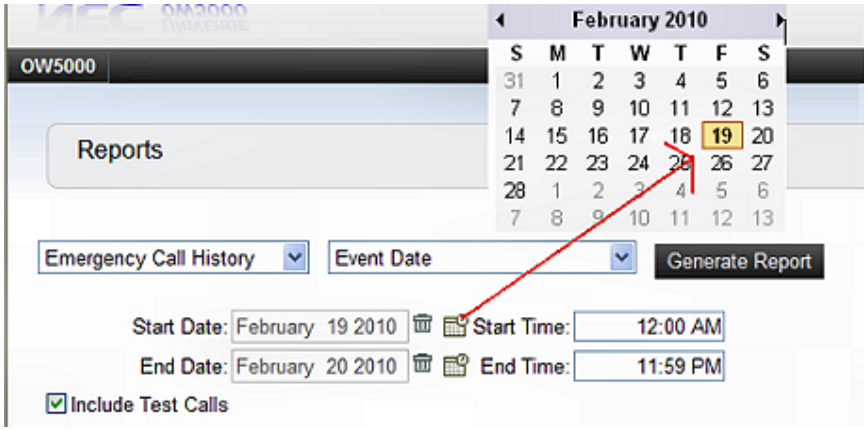
Step 2 Select the **Report Type** and **Report Grouping** from the drop down lists.

Step 3 Click on the **Calendar** icon to select the desired start and end date of calls to be included in the report. Use the **Trash Can** icon to clear the dates.

Step 4 Input the start and end times to correlate to the dates.

Step 5 To include Test Calls in the report, check the **include Test Calls** box. Leave the box empty if Test Calls are not to be included. See Figure 3-18.

Figure 3-18 *Report Filters and Criteria*

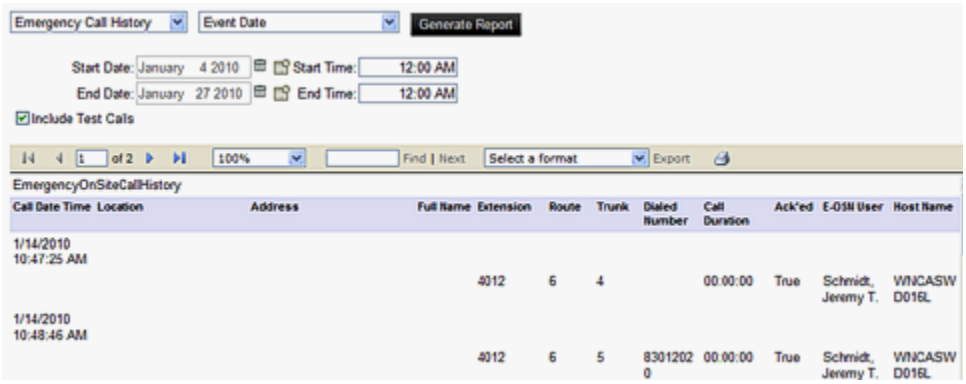


Print and export features follow standard SRSS capabilities. Emergency calls are recorded in the database with the following information:

- Date and time call was initiated
- Location data for calling phone (location hierarchy)
- Address for the calling location
- Person making the call (if associated with the calling phone)
- Extension and route/trunk used for making the call
- Emergency number dialed (example: 911)
- Call duration (calculated from trunk seizure and trunk release time)
- Acknowledgement status
- E-OSN user who acknowledged the call (if acknowledged)
- Machine name used by E-OSN client when acknowledged

Figure 3-19 below represents an Emergency On-Site Call History Generated Report.

Figure 3-19 *Emergency On-Site Call History Generated Report*



NOTE

For optimal printing and viewing of data, exporting to MS Excel or MS Word is recommended.

System Test

Notifications and configuration can be tested by generating test emergency events. The tests must be initiated by the Administrator and are logged and notified as normal, but are clearly marked as "**TEST**".

The System Test page allows an E-OSN Administrator to conduct a system test using all notification systems, including E-OSN Client and Email. It also allows for testing of all E-OSN application events including:

- Emergency Call Link Failure
- Emergency Call Link Connected
- Emergency Call Service Stopped
- Emergency Call Service Started
- Emergency Call Event
- Emergency Trunk Monitor Failure
- License Failure Warning
- License Failure Grace Period End

NOTE

An Email notification distribution list must be created before the link failure test can be executed. Distribution List, Email Subject and Email body will be empty until this configure is done.

Performing a System Event Test

Perform the following steps to conduct a System Event test.

Step 1 Navigate to **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **System Test**. The System Test page displays with two tabs: **Link Failure** and **Emergency Call** .

Step 2 Click on the **Link Failure** tab.

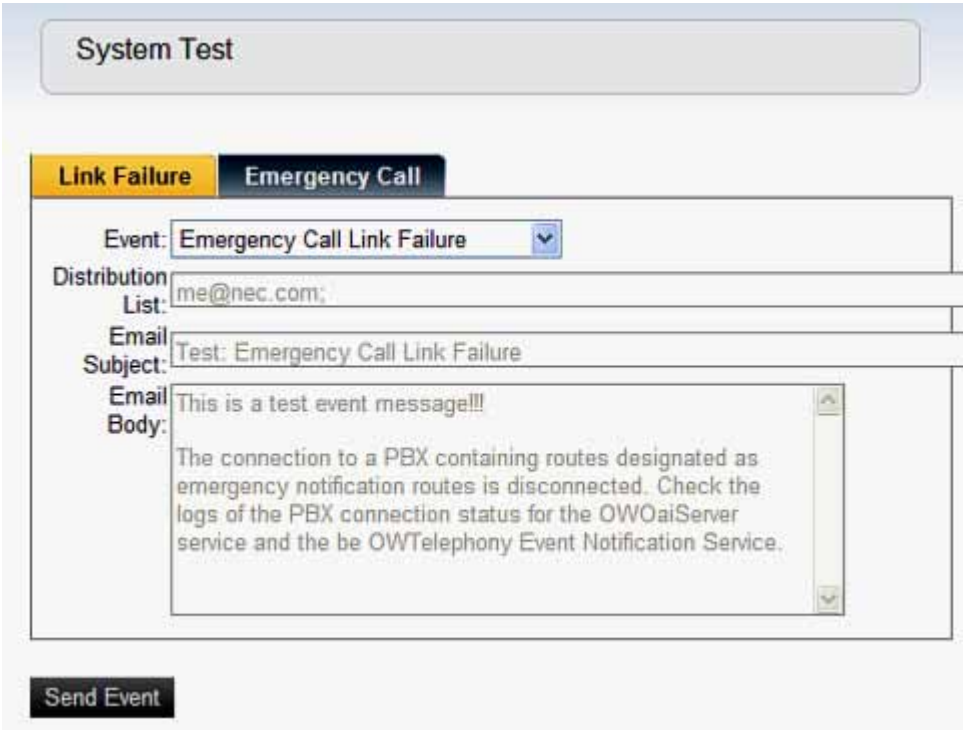
Step 3 Select the event type to test from the **Event** drop-down list.

Step 4 Click on the **Send Event** button. An e-mail is sent to the displayed Distribution List and a notification is sent to all E-OSN Clients. The E-OSN Clients will display the message as a test event. The test event will continue to be displayed on the E-OSN Client until a test message is sent to turn it off. For Example, an Emergency Call Link Failure

notification would need an Emergency Call Link Connected message to be sent to turn it off. See Figure 3-20.

NOTE *Any information related to the event selected displays as read-only.*

Figure 3-20 *Link Failure Notification*



Performing an Emergency Call Test

Emergency calls are tested from the **Emergency Call** tab on the **System Test** window. Fields marked with an asterisk are mandatory. The Emergency call test is a test of the notification system that does not use live phones or PBX trunks. This procedure tests the part of the system at the point where E-OSN has been notified by the PBX of an emergency call and the database is updated with the call information. This test system simulates the updating of the database and exercising all notifications that are executed as a result of a emergency call log entry to the database.

To test the telephony aspect of the emergency call system, coordination should be arranged with the local emergency service providers for making a live test call.

Perform the following steps to conduct an Emergency Call test.

Step 1 Navigate to **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **System Test > Emergency Call**.

Step 2 Enter the applicable information into the fields on the **Emergency Call** tab. Table 3-1 provides a description of the fields.

Step 3 Click on the **Send Event** button. Figure 3-21 represents a successful emergency call test.

Figure 3-21 *Successful Emergency Call Test*

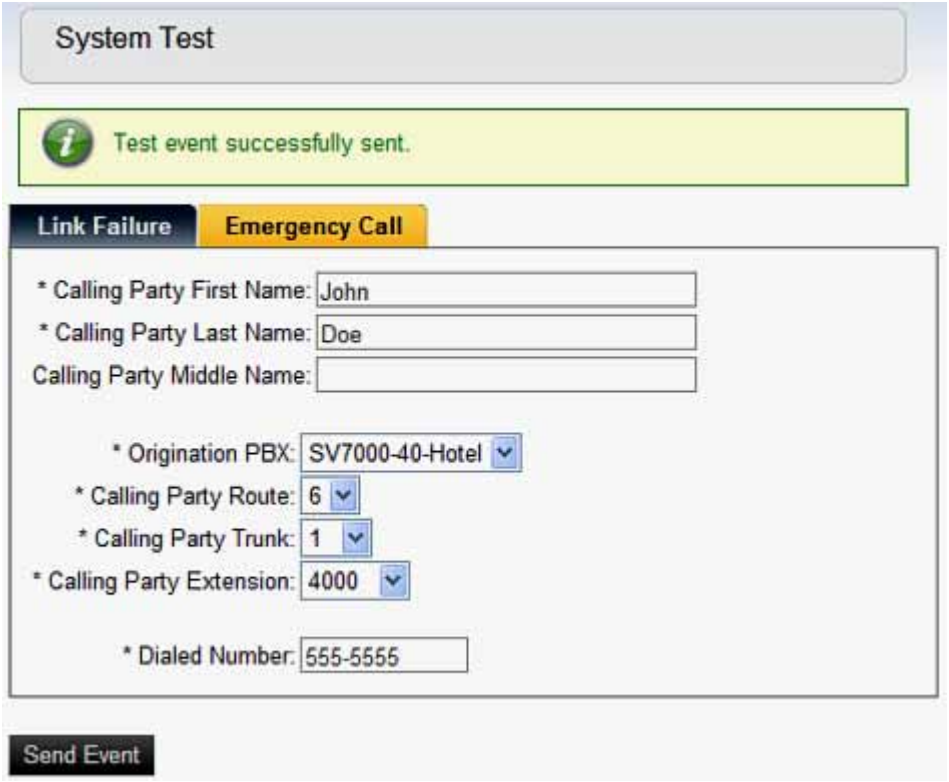


Table 3-1 *Emergency Call Test Field Descriptions*

Field	Description
Calling Party First Name Calling Party Last Name	Mandatory fields representing the first and last name of the person that initiates the emergency call. These are free form type fields.
Calling Party Middle Name	Field representing the middle name of the person initiating the emergency call. This field is not mandatory.
Origination PBX	A drop-down list of all PBXs containing emergency routes. Selecting a location automatically fills in the Calling Party Route, Calling Party Trunk, and the Calling Party Extension fields.
Calling Party Route	Contains all emergency routes that are defined for the current PBX. This is autofilled when the Origination PBX is selected.
Calling Party Trunk	Contains all the emergency trunks that are defined for the selected route. This is autofilled when the Origination PBX is selected.
Dialed Number	Number being called.

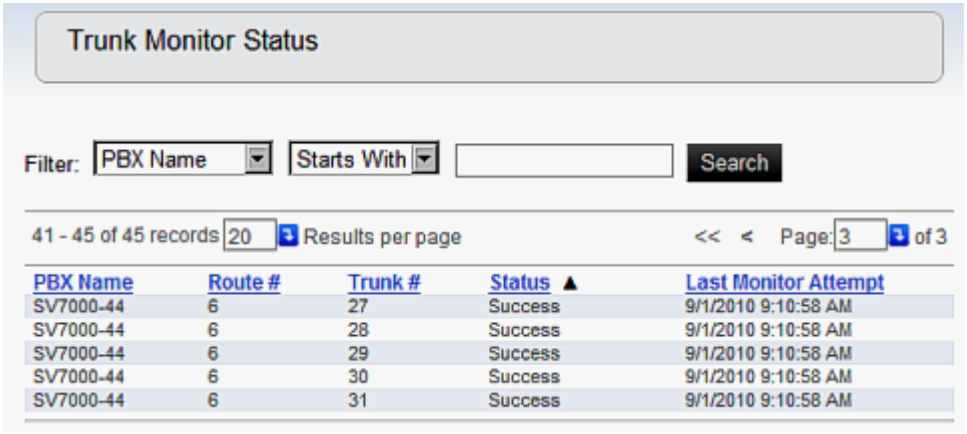
Trunk Monitor Status

This screen allows an administrator to quickly see the failed/success monitor status of all emergency trunks. To access this screen, navigate to **OW5000** > **Applications** > **UCE Emergency On-Site Notification** > **Trunk Monitor Status**. The following information displays:

- PBX name
- Route #
- Trunk #
- Status
- Last Monitor Attempt

The information can be sorted on any field. The default sort is on the Status field with failed trunks listed first. The information can also be filtered on PBX Name, Route Number, and Status. See Figure 3-22 for an example of the Trunk Monitor Status page.

Figure 3-22 *Trunk Monitor Status*



The Status field indicates whether or not the trunk has successfully been monitored. The four possible outcomes are:

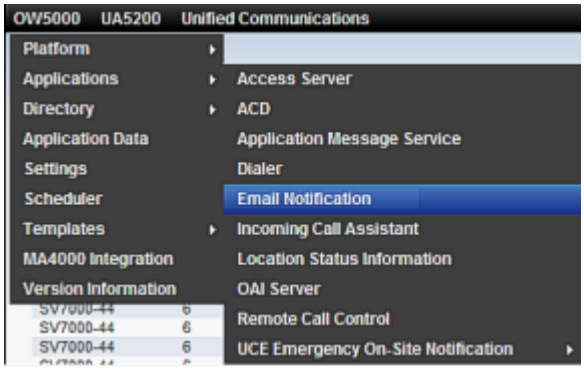
- Success - This status means the trunk was successfully monitored.
- Failed - This status means the trunk failed to be monitored.
- Stopped - This status means that the “OWT Telephony Event Notification” service has stopped running and is no longer monitoring the emergency trunks.
- Initialized - Briefly displays. This the state of a trunk just before a monitor attempt is about to occur.

Email Notification

Email Notification allows a user with OW5000 Administrator access right privileges to configure Email Notifications.

The **Email Notification** application is found under **OW5000 > Applications > Email Notification** in the OW5000 Administrator, Figure 3-23.

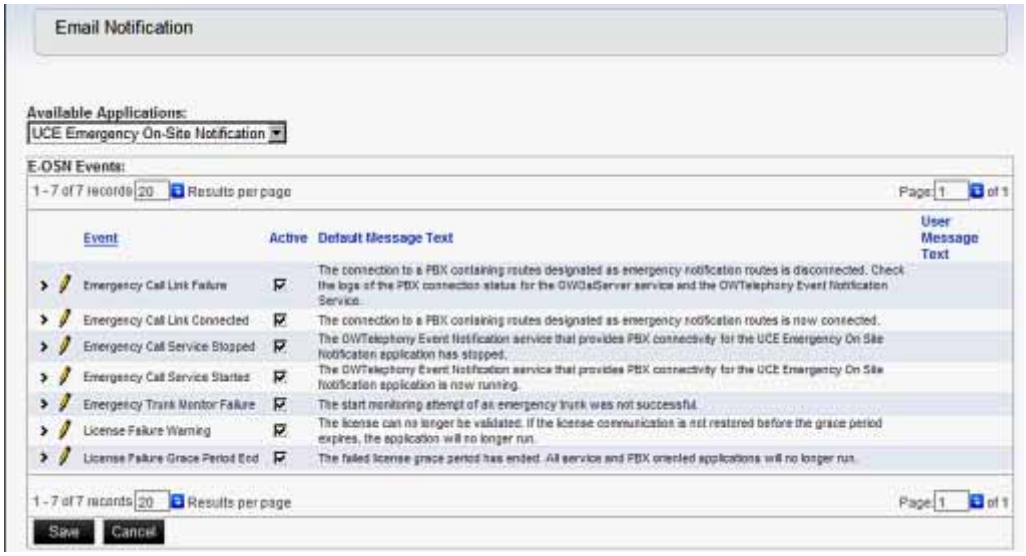
Figure 3-23 *Path to Email Notifications*



When UCE Emergency On-Site Notification is installed, the application name becomes visible in the "Available Applications" list box and when selected, the following E-OSN Events display. This is shown in Figure 3-24.

- Emergency Call Link Failure
- Emergency Call Link Connected
- Emergency Call Service Stopped
- Emergency Call Service Started
- Emergency Trunk Monitor Failure
- License Failure Warning
- License Failure Grace Period End

Figure 3-24 *Email Notification*



The Email Notification screen lists the applications available for Email Configuration in a drop down list. The events are listed along with the associated **Default Message Text**. Clicking the **Pencil** icon next to each event allows **User Message Text** to be appended to the **Default Message Text** that comes with the application.

Change in System Status Event Notifications

These notifications are sent by email through the Email Notification distribution lists based on an application event. They also display through the E-OSN client in a status bar.

For applications with PBX connections such as an OWTelephony Event Notification, these applications trigger link failure notifications when a problem occurs.

When E-OSN is installed, any of the following events can bring about a Change in System Status Notification:

- Emergency Call Link Failure -The OWTelephony Event Notification connection to the PBX(s) containing E-OSN routes is disconnected. If an OAI connection not containing E-OSN routes is disconnected, no event notification occurs.
- Emergency Call Link Connected - The OWTelephony Event Notification re-establishs connection to the PBX.
- Emergency Call Service Stopped - OWTelephony Event Notification is intentionally shutdown.
- Emergency Call Service Started - OWTelephony Event Notification service is restarted.

MA4000 Location Data Sync

NOTE *MA4000 should be installed and configured according to MA4000 documentation.*

Extensions for emergency services support are entered into the MA4000 and stored in the selected National Emergency Number Association (NENA) format.

NENA (http://www.nena.org/) is an organization whose mission is to foster the technological advancement, availability, and implementation of a universal emergency telephone number system.

MA4000 currently supports two NENA XML formats, version 2.1 and version 3.1. MA4000 stores the location data for an extension in one of these formats.

OW5000 DBSync is a service in OW5000 platform which synchronizes certain MA4000 data fields such as PBX, Extensions, Users, Organizations, Voice Mail boxes, etc., into the OW5000 database. MA4000 serves as the master repository for this data and DBSync synchronizes this data real-time into OW5000.

MA4000 will send a notification to DBSync for Extension update whenever the location data changes for the Extension. OW5000 DBSync will handle this notification and re-synchronize the location data to the OW5000 database.

This extension location data will be used by the E-OSN Client and e-mail notifications to provide details about an emergency call.

To review MA4000 imported extension location data, login to OW5000 Administrator and navigate to **OW5000 > Platform > Extension** and search for an extension that had location data imported.

Select the **SHOW NENA DATA** drop list (Figure 3-25) to display the values that were imported from MA4000. Figure 3-26 provides an example of expanded data.

Figure 3-25 *SHOW NENA DAtA*

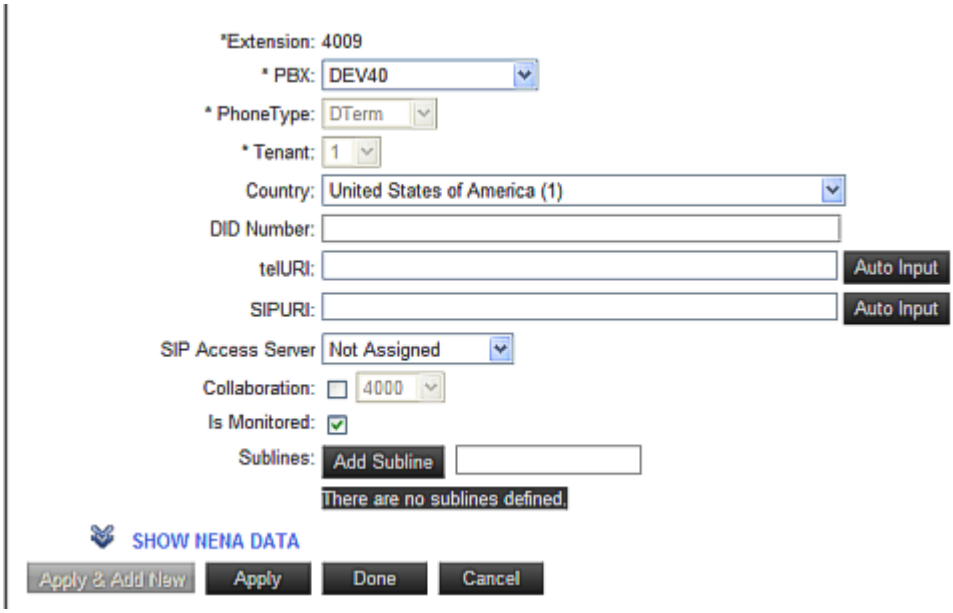
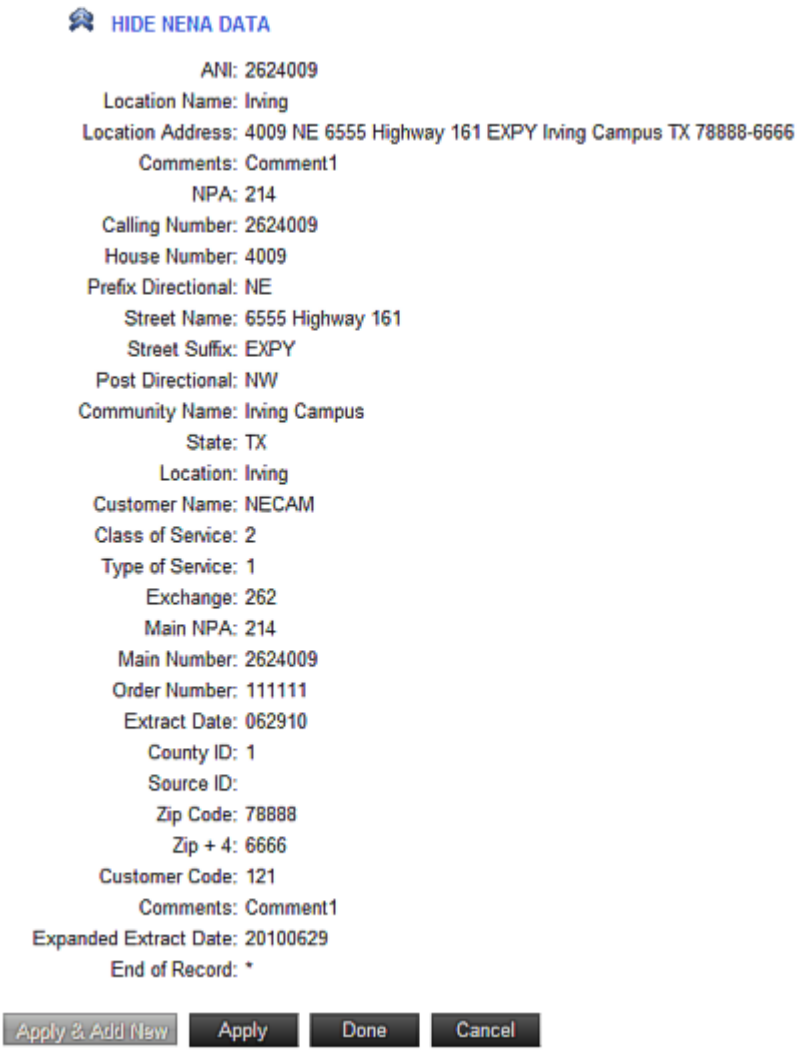


Figure 3-26 *Expanded NENA DATA*



For additional information or support on this NEC Corporation product, contact your NEC Corporation Representative.

N E C NEC Corporation

UCE Emergency On-Site Notification (E-OSN) Installation Guide

NDA-31053, Issue 2