



Beacon Office™

Administrator Manual

Version - 2.5(1)

Radianta Inc.

September 2008

Table of Contents

Contents

<i>Introduction</i>	3
What is Beacon Office	3
How to Use This Guide	3
Conventions	3
<i>Beacon Office Overview</i>	4
<i>Beacon Office Director</i>	5
Signing Into Beacon Office Director	5
<i>Beacon Office Director Main Page</i>	6
<i>Beacon Office Administration Settings</i>	7
<i>Beacon Office Systems Configuration Settings</i>	8
Clock out Reminder Duration	8
Time Entry Login Timeout	9
Administrator Password	9
Multicast Address Setup	10
Personal Queue Setup	10
<i>Beacon Office User Permissions and Roles</i>	11
Establishing and Assigning Roles	12
Establishing User Permissions	14
<i>Emergency Alert</i>	18
<i>Appendix A: Beacon Office Database Rebuild</i>	22
<i>Appendix B: Beacon Office User Synchronization</i>	22
<i>Summary</i>	23

Introduction

Welcome to Beacon Office! Beacon Office is the preeminent office productivity suite available for the Cisco Unified Application Environment. By integrating personal call control and communications management tools, Beacon Office enables employees to be more productive. Whether it is call-back capabilities or personal queuing, Beacon Office has something for every professional. Also, there are a host of other important features in our full Beacon Office version. To learn more about Beacon Office, just visit our website at www.radianta.com. However you decide to use Beacon Office, or our more powerful Beacon Office Premium, we are certain that their features will help your business streamline its communications.

What is Beacon Office

Beacon Office works in conjunction with Cisco Unified Application Environment (CUAE) and leverages Cisco Unified Communications Manager (CUCM) to provide a host of personalized communications utilities. These tools can be used to make every employee's experience with CUCM even more feature rich and valuable. Some of the tools are available with a Cisco IP phone-based user interface and some are available with a computer-based interface accessible from your personal computer.

How to Use This Guide

This guide will show you to how to operate the Beacon Office suite of features. Administrators who wish to understand and manage the installation and configuration of Beacon Office are encouraged to read the Beacon Office Administration Guide. To get started, begin with the section regarding Beacon Office Overview on the next page.

Conventions

When using this guide, you will find simple tips, notes, and warnings after each section of this guide as shown in Table 1.

Table 1

Title	Description
Notes	Informs you of items to pay attention to while working within Beacon Office.
Warnings	Informs you of items to be aware of while working within Beacon Office.

Beacon Office Overview

With applications built to enhance the Cisco Unified Communications platform, Beacon Office allows you to use personal communications tools. This suite consists of applications that can be accessed using either a Cisco IP phone or the Beacon Office Director through a web interface as part of Beacon Office Director. This guide will review the following personal communication application tools within Beacon Office Director. Beacon Office Director is the main administrative page that supports all Beacon Office user features. Beacon Office Director provides tools for all messaging, recording, scheduling and communications management as described below:

Table 2

Communications Tool	Description
Call Notes	Beacon Office Call Notes allows you to create text messages or use existing text messages that can be posted to a screen of a Cisco IP phone while a call is made.
Call Recording	Beacon Call Recording enables you to access the application through the Cisco IP Phone Services key so that you can record an active call, maintain, playback and delete recordings.
Call Back	Beacon Office Call Back enables you to interact with coworkers effectively. When a called party is busy or unreachable, callers may initiate a call back request from their phone. The called party is notified and gives the called party capabilities of tracking and responding to these call back requests.
Phone Lock	Beacon Office Phone Lock enables you to control access to Cisco IP phones by locking phones to prevent general outbound calling and unwanted access to personal directories, call records and other services. In addition, you can enable Phone Lock to automatically lock any phone according to a set schedule. Note - Unlocking a phone is as simple as entering an individual's Cisco Unified Communications Manager credentials. During locked mode, however, administrators have the flexibility to allow phones to dial emergency numbers if desired.
Extension Mobility Web	Beacon Office allows you to connect a PC to any Cisco IP phone and invoke Extension Mobility from a web screen. Extension Mobility Web requires the user to enter the target phone's extension—no additional information is required.
Dialer	Beacon Office Dialer allows you call a list of phone numbers and dial outbound calls and play pre-recorded messages to each number reached. The Dialer is a great tool for users who must broadcast a single message to multiple destinations both within the network and out over the public switch telephone network (PSTN).
Timecard	Beacon Office Timecard enables IP phones to become a time clock device. Employees can sign in and out for work anywhere there is a phone, relieving congestion at centralized time clock stations. Note - Logging information is easily exported from the associated database into third party time-tracking applications
Paging	Commence Paging by sending a text, text-to-speech, recorded message, or live pages simultaneously to any Cisco IP phone on your network. All types of pages except "live" can be immediate, scheduled, or automatically recurring.
Personal Queue	As numerous calls ring in, Personal Queue enables you to view calls in a visual queue on your PC workstation. Controls are provided by Personal Queue enabling you to play custom queue hold messages, music and to inject custom messages such as, "I'll be right there - just need to finish something up" while the caller is in the queue. The system will allow you to streamline daily communications by caller details to decide which call takes priority and answering or managing the messaging accordingly.
Emergency Alert	When a particular dialing pattern is detected, for example a 911 emergency call, Beacon Office Emergency Alert automatically sends messages to designated IP phones and email addresses. Message information includes caller number, name, called number and IP phone location information.

Beacon Office Director

Beacon Office Director is the primary interface for Beacon Office. Beacon Office Director, a web-based utility, allows users to personalize their configuration, record voice messages, create pre-defined text messages and trigger key applications within the suite. Beacon Office Director is also the primary interface for system administrators. From here, administrators can perform several key tasks such as assigning end user licenses and features.

Signing Into Beacon Office Director

As mentioned, Beacon Office Director is a web-based utility. The URL is of the following form: <http://<server>/beaconoffice/> where <server> is the IP address or hostname of your CUAE application server.

If you specified a custom port address for Beacon Office during installation or otherwise have a non-standard installation, the alternate address is of the form <http://<server><port>> where <server> is the IP address or hostname of your CUAE application server and <port> is the administration port specified during installation. Once connected, you should see a login screen as shown in Figure 1: **Beacon Office Director Log-In Prompt**

Note – The default, the value is 8082. It is strongly recommended that you use the default value and address Director as described in the preceding paragraph.



Figure 1: Beacon Office Director Log-In Prompt

Warning - Enter "Administrator" as the Username and the Password which was set during installation. Do not check the **Login to Extension Mobility** check box – this feature is discussed in the *Beacon Office User Manual* document. Once you have entered your log-in credentials click on the **Login** button.

Beacon Office Director Main Page

Once you have logged into Beacon Office Director you will be presented with the Beacon Office Director main page for administrators. From here you will have access to all of the key administrative functions of Beacon Office. This section will familiarize you with the main page. Key functions of the page are show in Figure 2: **Beacon Office Director Main Page**.

The Beacon Office Director Main Page is divided into two sections as follows:

Main/Settings – Beacon Office Director allows quick access to key Beacon Office administration settings.

Menu/Beacon Office News – The right pane of Beacon Office Director is used to access links and invoke all Beacon Office web-based functions.



Figure 2: Beacon Office Director Main Page

Beacon Office Administration Settings

The rest of this document focuses on all of the administrative settings of Beacon Office. All settings are accessed in the same manner by clicking on the **Settings** tab on the Beacon Office Director main page in either the left or right panes. Figure 3: **Beacon Office Administrative System Settings Page** illustrates the available settings. Three key administrative functions are available. **System Settings** contains critical settings needed for Beacon Office to function properly. **User Permissions** allows administrators to establish user permissions and roles. Each is discussed next in this guide.

Main Settings Log out

Settings

User Permissions
System Settings

System Settings

Clockout Reminder Duration minutes

Time Entry Login Timeout minutes

PQ Operator Forward Number

PQ Voicemail Prefix

Old Administrator Password (Leave blank to keep old password)

New Administrator Password (Leave blank to keep old password)

Confirm New Password (Leave blank to keep old password)

Multicast Address Setup

Action	Name	Multicast Address	Port
Add new multicast address			
	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 3: Beacon Office Administrative System Settings Page

Beacon Office Systems Configuration Settings

This section outlines the operation of all Beacon Office systems configuration parameters. To access the systems configuration page, simply click on the **Systems Settings** submenu on the left pane of Beacon Office Director, or click on the **Systems Setting** tab at the top of Beacon Office Director. The resulting screen is illustrated in Figure 4: **Systems Settings Main Screen**. From this screen we can modify several parameters.

Figure 4: Systems Settings Main Screen

Clock out Reminder Duration

The Beacon Office Time Card application is a basic time and attendance application that can be accessed from Cisco IP phones. In many cases, not only do companies wish to track employee time on the job site, they also want to be notified if employees are exceeding standard shift duration. For example, corporate management would like to be notified if an employee clocks out for a shift that exceeds eight hours. The **“Clockout Reminder Duration”** allows Administrators to set this notification threshold. If an employee clocks in and then tries to clock out at a time that exceeds this duration, the employee will be prompted to confirm the time or enter the proper clock out time and management will be notified in the Time Card reports that a Clockout reminder was triggered for this event.

Note - To modify the Clockout Reminder Duration parameter, simply enter the appropriate duration, in minutes, in the field to the right of **“Clockout Reminder” Duration** field label.

Time Entry Login Timeout

As part of Beacon Office TimeCard, employees utilize Cisco IP phones to enter clock in and clock out times. This activity requires that an employee log into the application, as described in detail within the *Beacon Office User Manual* document. This login activity presents a specialized screen on the Cisco IP phone. For security purposes, the **Time Entry Login Timeout** parameter allows administrators to automatically timeout that screen after a specific period of time, requiring employees to again login for authentication.

Note - To modify the Time Entry Login Timeout parameter, simply enter the appropriate duration, in minutes, in the window to the right of **Time Entry Login Timeout** field label.

Administrator Password

Another key parameter managed from this screen is the administrator password. To change the administrative password, type the current administrator password in the **Old Administrator Password** field. Next, type the modified password in the **New Administrator Password** field. Repeat typing the same modified password in the **Confirm New Password** field and click the **Apply Changes** button as shown in Figure 5: **Administrator Password Modification Screen**.

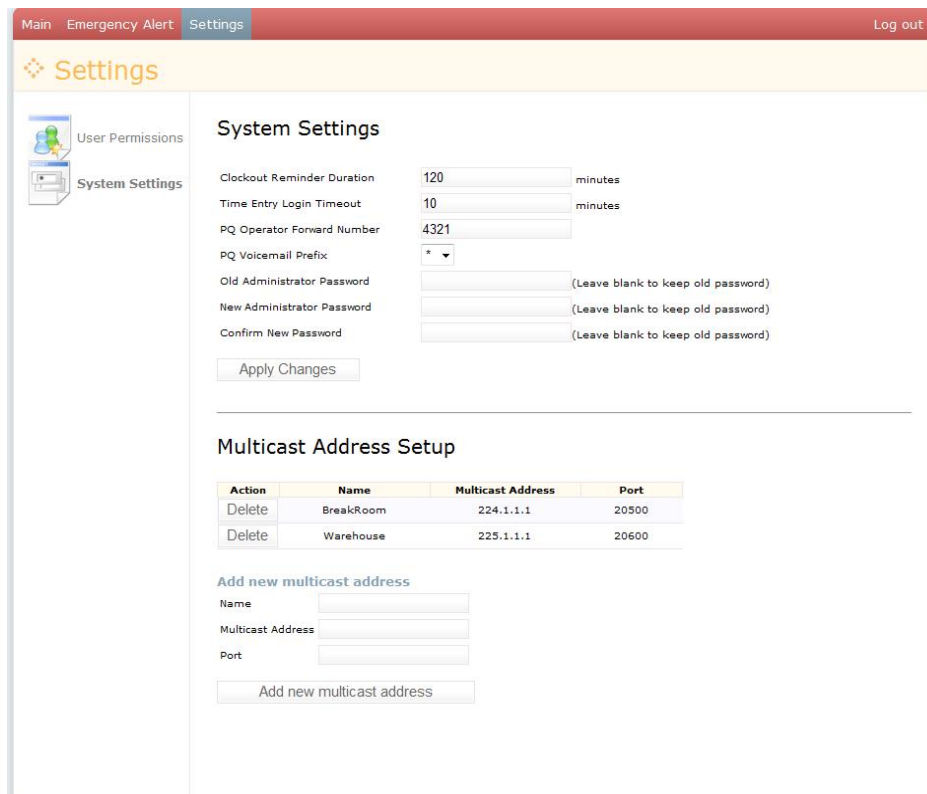


Figure 5: Administrator Password Modification Screen

Warning: To change the administrative password, enter the new password and confirm the password in the appropriate fields. Then, click the **Apply Changes** button. The system will prompt you if you're the passwords do not match.

Multicast Address Setup

Multicast Address Setup allows you to add one or more multicast speaker addresses for broadcasting. To add a multicast address, enter a name in the **Name** field. Next, enter a multicast IP address in the **Multicast Address** field. Last, enter the multicast **Port Number** field and then click the **Add New Multicast Address** to save. Once you have saved this information, the system will display each multicast address under the **Multicast Address** field as shown in Figure 5: **Administrator Password Modification Screen**.

Warning – Port addresses must be an even number and within a range of 20480 and 20000.

Personal Queue Setup

Beacon Office Personal Queue allows a user to forward calls from their personal queue to one of three extensions. For example, a caller who is placed in a user's personal queue will hear the user's custom pre-recorded message. This custom pre-recorded message may provide the caller with one or all of the following options:

Press "0" – transfers the caller to the pre configured operator extension. This extension is configured by inputting the desired operator extension into the **PQ Operator Forward Number** field as shown in Figure 6: **System Settings PQ Setup Screen**.

Press "1" - transfers the caller directly to the user's voicemail box. Ensure that your Cisco voice gateway and Cisco Unified Communications Manager call routing is configured to route calls with a desired prefix (such by a *) directly to a user's voicemail box. For example, if your Cisco Unified Communications infrastructure were configured to look for a * as the desired prefix, a transfer to *1234 would transfer the call directly into extension 1234's voicemail box. Once your Cisco voice gateway and Cisco Unified Communications Manager are properly configured, you may select the prefix used for "direct to voicemail dialing" in the **PQ Voicemail Prefix** drop down menu shown in Figure 6: **System Settings PQ Setup Screen**.

Press "2" – transfers the caller to a personalized extension the user determines; for example, a secretary. See the Beacon Office Personal Queue section in the Beacon Office User Guide V 2.5 (1) for further information on setting up this option.

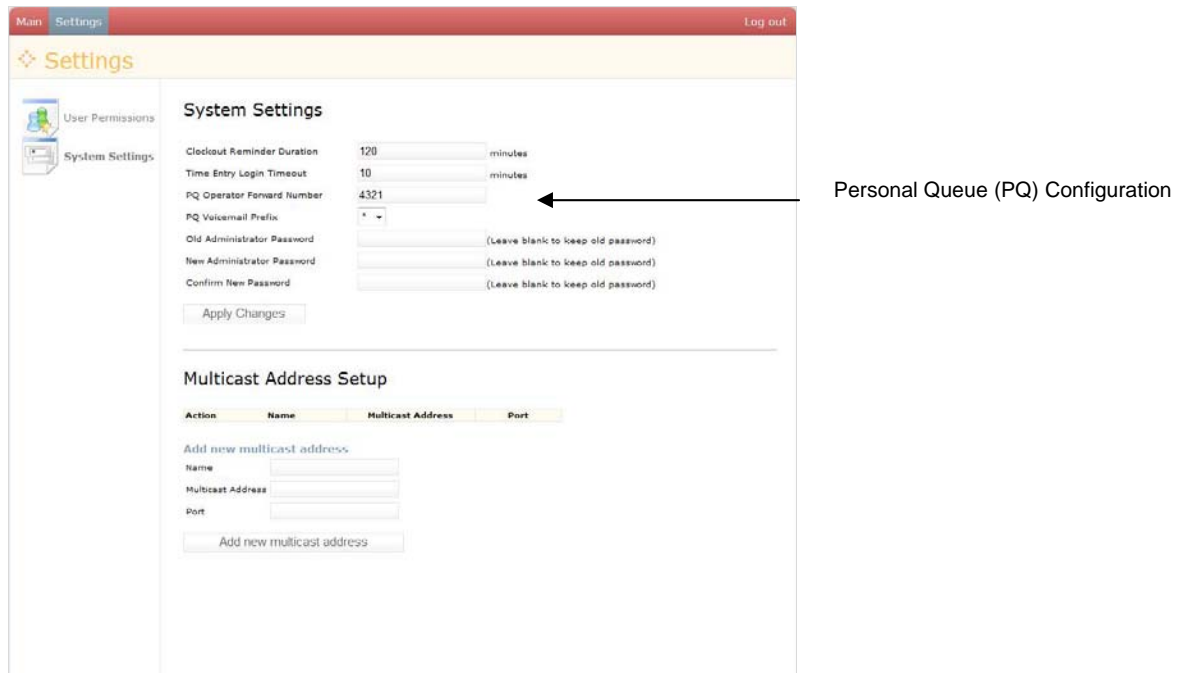


Figure 6: System Settings PQ Setup Screen

Beacon Office User Permissions and Roles

This section outlines the operation of all Beacon Office user configuration parameters. To access the user Permissions page, click on the **User Permissions** option on the left pane of Beacon Office Director. The resulting screen is illustrated in Figure 7: **User Permissions Main Screen**.

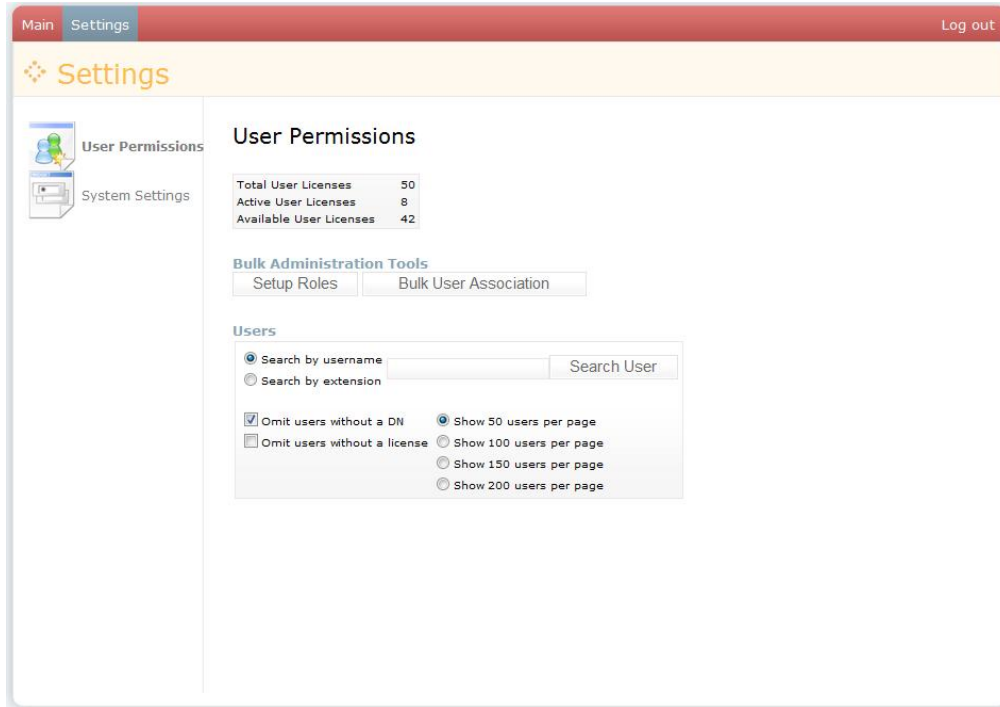


Figure 7: User Permissions Main Screen

From this screen you can create and assign roles such as Administrator or User, and you can assign licenses and access to specific Beacon Office features. Beacon Office automatically creates a list of available users from the Cisco Unified Communications Manager database. The following sections outline steps to configure user capabilities.

Establishing and Assigning Roles

Beacon Office allows administrators to create roles to assign the feature to Beacon Office users. To create roles, first select **Setup Roles** button as shown in Figure 7: **User Permissions Main Screen**. This action brings up screen illustrated in Figure 8: **Roles Setup Main Screen**.

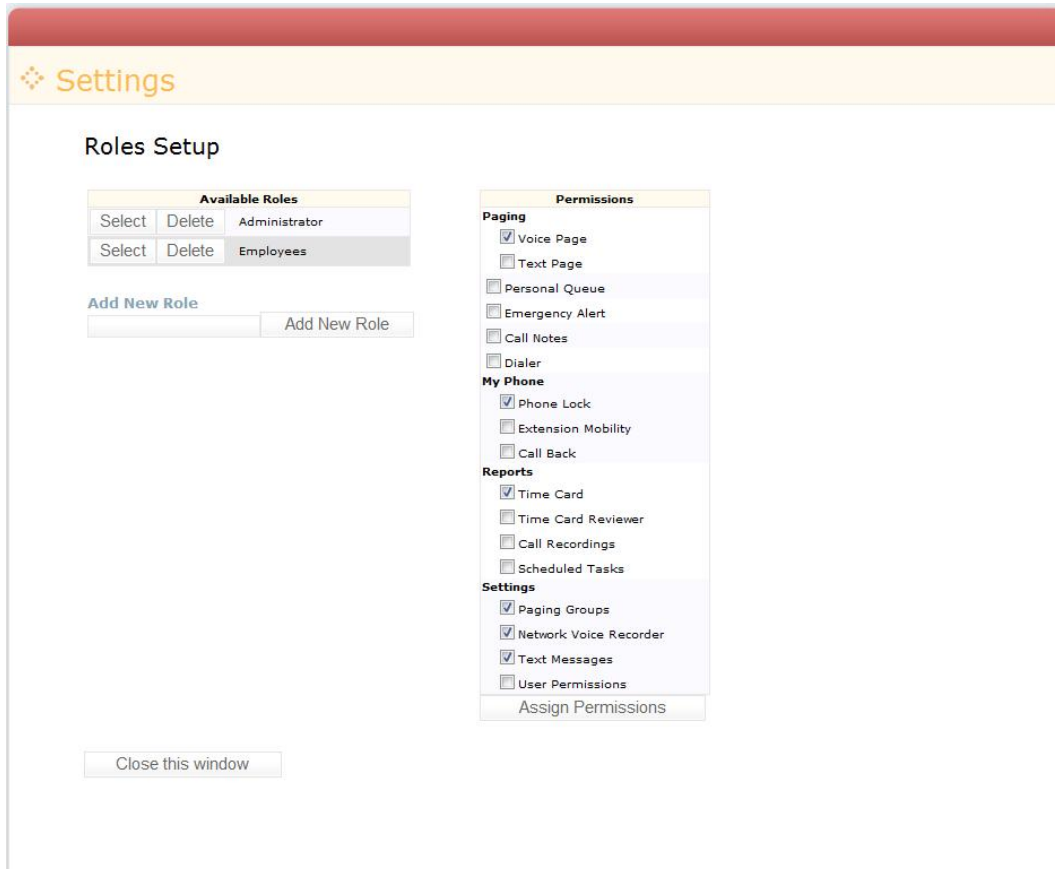


Figure 8: Roles Setup Main Screen

Next, type in the name of the new role in the **Add New Role** field, and then click on the **Add New Role** button. The new roll will appear in the Available Roles list. To manage this role, click **Select** next to the role. From here you can select the Beacon Office features that you wish to associate with the selected role

Note – The available role selected is highlighted indicating that it is the role being modified. The result is shown in Figure 8 for a new role called *Employees*.

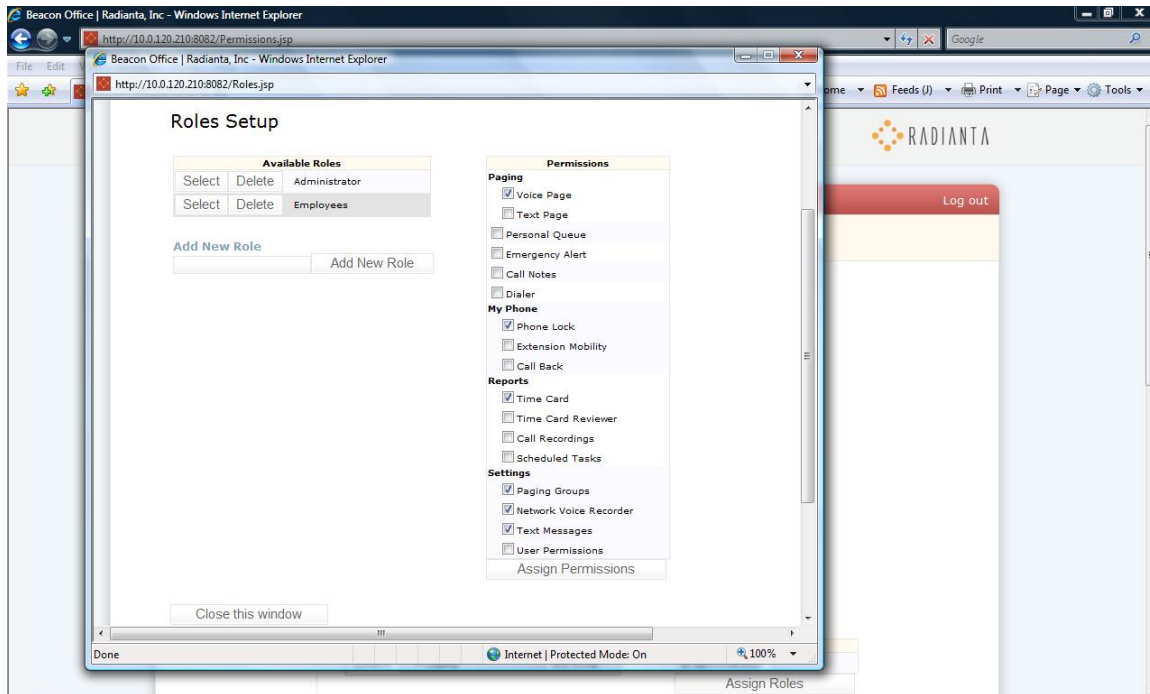


Figure 9: User Role Setup Configuration

Figure 9: **User Role Setup Configuration** shows voice and text paging capabilities within the Permissions window. These paging functions are part of Beacon Office Premium and may not be available on your version without an upgrade. Beacon Office Premium is available by contact Radianta at www.radianta.com.

It should also be noted that there are two key permissions that should be reserved for administrators only. They are **Emergency Alert** and **User Permissions**. **Emergency Alert** is an automated emergency notification mechanism that is discussed later in this document. **User Permissions** enables the user configuration menu.

Once the appropriate permissions for this role have been established, click the **Assign Permissions** button. This new role will be available when configuring specific users. Additional roles can be created as required using the same steps noted above.

Establishing User Permissions

Beacon Office allows administrators to assign specific features to specific users as appropriate. To begin this process, search by user's name or extension, then select **Users** from the search results. Beacon Office Director will display the list of available users drawn from the Cisco Unified Communications Manager database or you may add a list by clicking the Bulk User Association button. To assign particular features to a user click **Select** next to the user's name. This action brings up a screen as shown in Figure 10: **Assigning User Roles and Permissions Screen**.

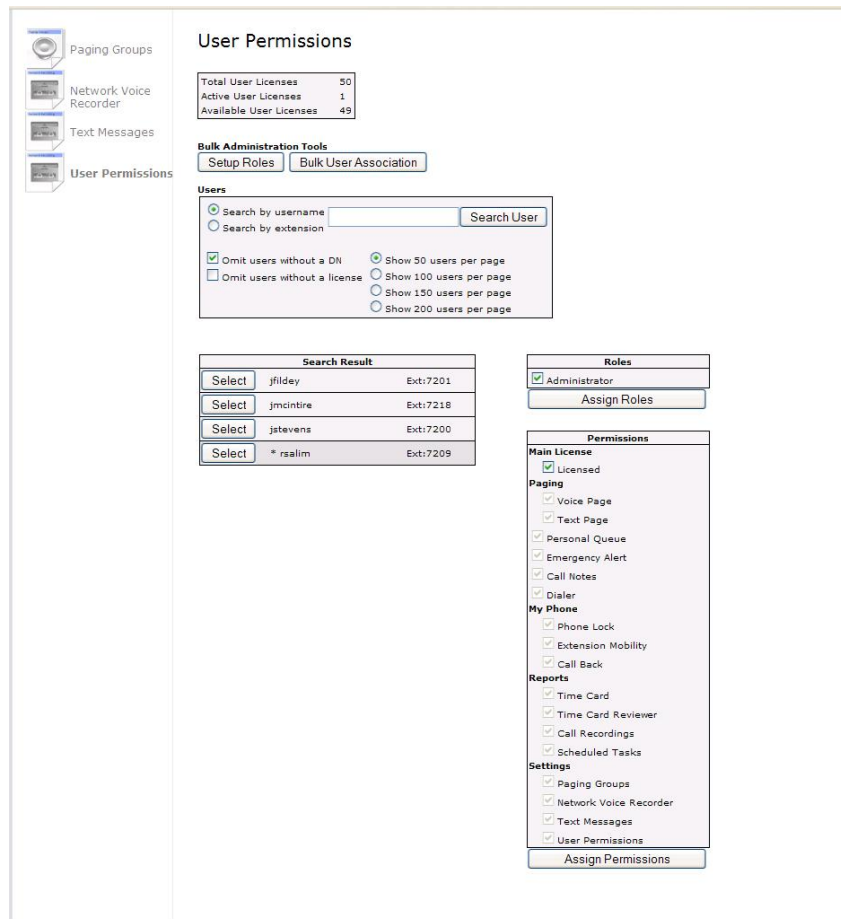


Figure 10: Assigning User Roles and Permissions Screen

In order to assign feature permissions to a user, that user must first be licensed. The Beacon Office CUAE bundle comes with a default number of licenses (50). Additional licenses can be purchased from Radiana by visiting www.radiana.com. The total number of licenses, including the number assigned and available, is listed at the top of the page. To assign a license to a user, click the check box next to **Licensed** in the **Permissions** in the **Main License** field and then click **Assign Permissions** button. Licensed users will have an asterisk, "*", next to their name in the **Search Result** user list as shown in Figure 11: **Assign Permissions Options**. From here you will be presented with check boxes next to each available feature, as shown in Figure 12: **Manual Permissions Assignment**.

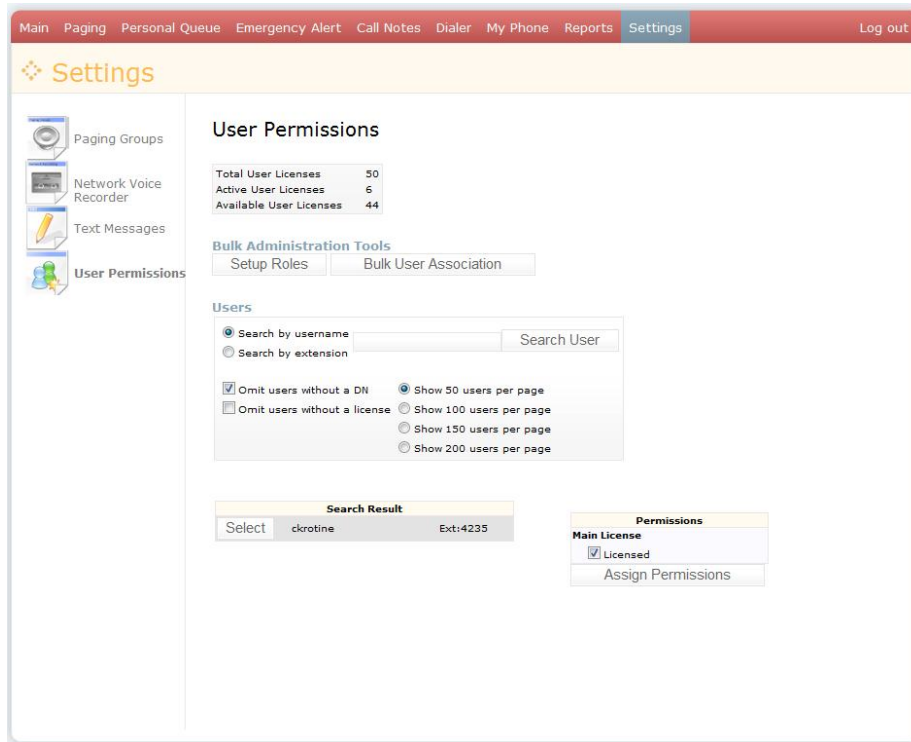


Figure 11: Assign Permissions Options

There are two options available to chief administrators to assign permissions to licensed users. First, you may individually select permissions by clicking on the check box next to each of the appropriate features, as illustrated in Figure 12: **Manual Permissions Assignment** where the user, line, has access only to Call Tag, Phone Groups Setup and Text Message Setup features.

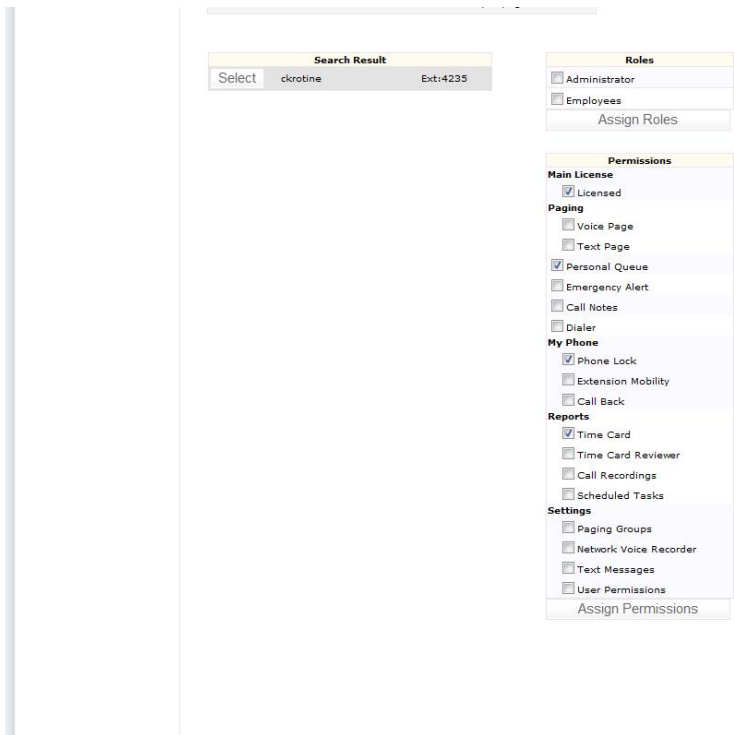


Figure 12: Manual Permissions Assignment

The second option utilizes roles that were configured in earlier sections of this document. To assign features based upon roles, simply license the user as before, click the check box next to the appropriate role and click the **Assign Roles** button. This will highlight the features assigned to the role, in this case *Users*, for this particular user. Permissions configured using roles assignment will be checked and grayed. An example is illustrated in Figure 13: **Permissions Assigned By Roles**.

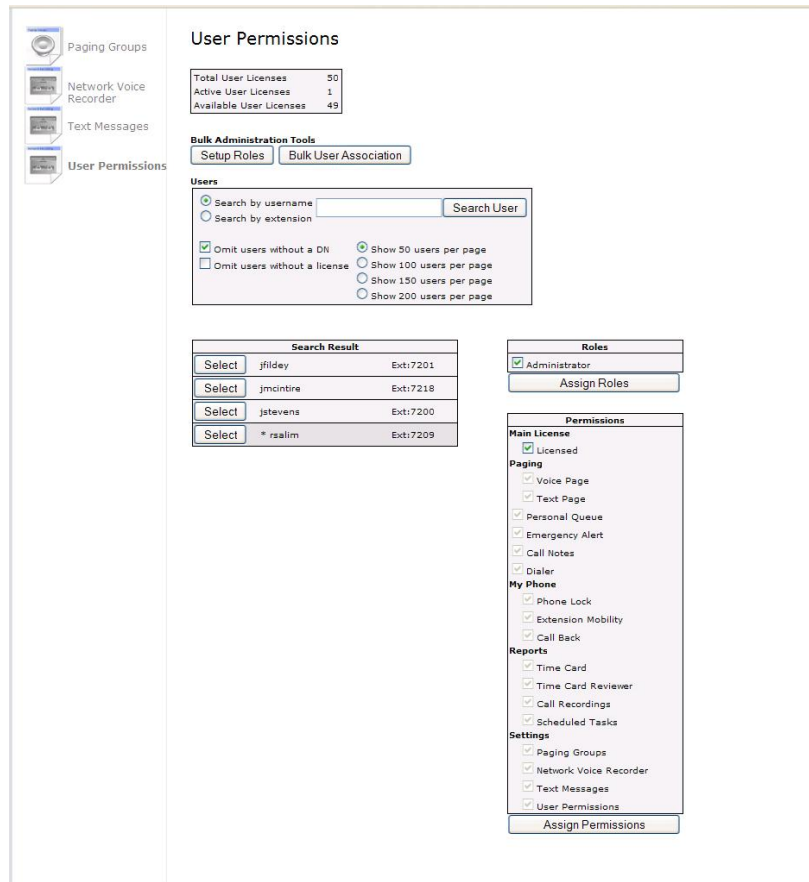


Figure 13: Permissions Assigned By Roles

Note - You can assign permissions to access features in addition to the features defined in a user's role, but you cannot unselect features if they were added as part of a role. If you need to assign features to users that are different from defined roles, you must configure them manually as described earlier.

At this point, once the role has been assigned and the desired features checked, click the **Assign Permissions** button.

Note - You can look at the features enabled for any licensed user by clicking the **Select** link next to the user's name.

Emergency Alert

In the Beacon Office Director relegated to the administrator, is the configuration of the Emergency Alert feature. As noted at the beginning of this guide, Emergency Alert enables the system to trigger automated messages based upon the keying of a specific digit string by a user. In general, this string would be a 911 call routing messages to Security or first responders, but the system will allow administrators to define messages that are triggered for any specific leading digit string.

In order to configure Emergency Alert a user, such as the administrator, must be licensed and have permissions for the Emergency Alert feature. Follow the guidelines in the last section to ensure that you have the appropriate permissions. After gaining the permission for Emergency Alert, you can click on the **Settings** button and notice that **Emergency Alert** has been added to both panes of the window, as shown in Figure 14: **Settings with Emergency Alert**.

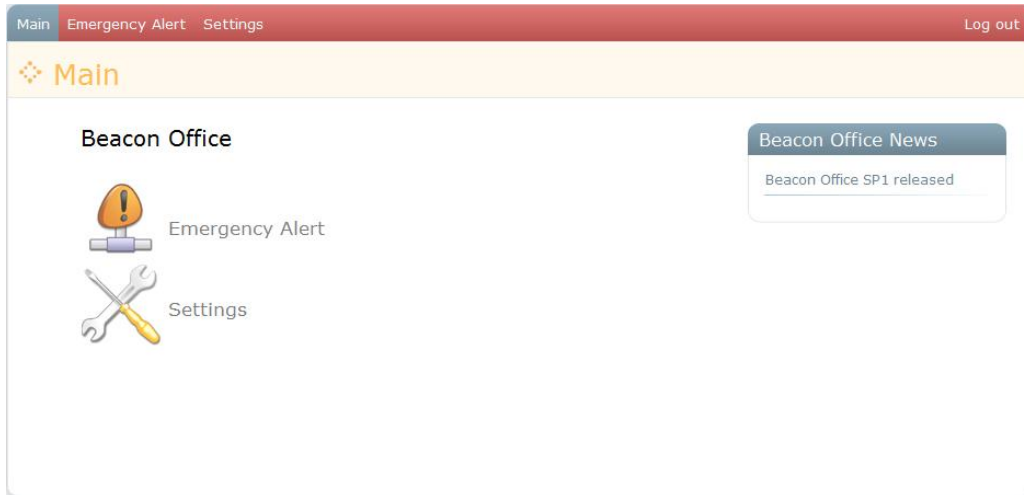


Figure 14: Settings with Emergency Alert

To access Emergency Alert, click on the buttons in either the left or right panes bringing up the main Emergency Alert page shown in Figure 15: **Emergency Alert Main Page**.

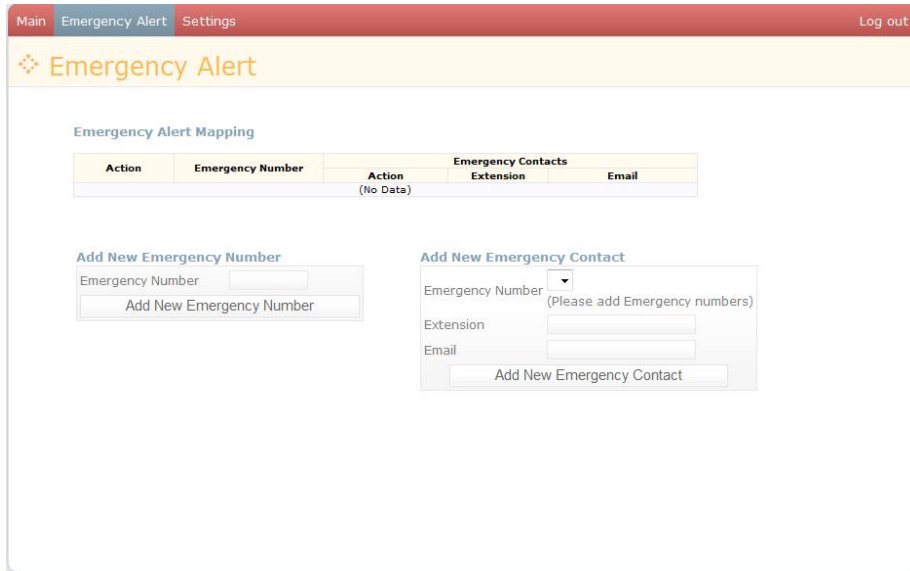


Figure 15: Emergency Alert Main Page

To begin configuring Emergency Alert, type the digit string that will trigger the desired messaging and enter a number in the **Emergency Number** field and click **Add New Emergency Number**. For example, we use the strings 9911 and 7711 which now appears in the **Emergency Number** window shown in Figure 16: **Emergency Alert Dial String**.

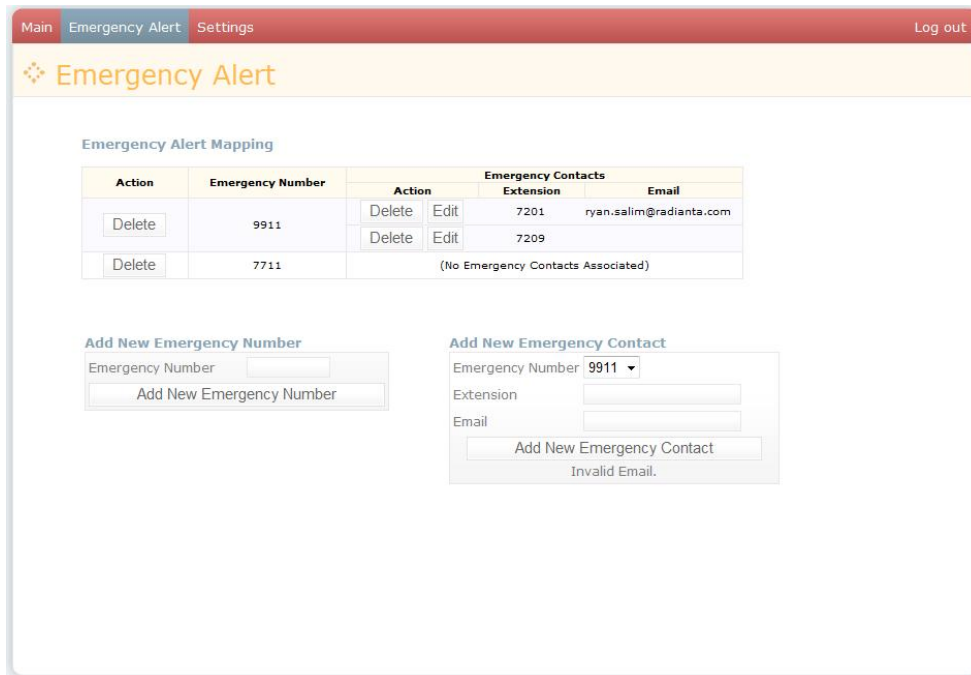


Figure 16: Emergency Alert Dial String

Now you can begin to associate alerts to specific destinations. First, select the appropriate emergency number from the drop down box next to **Emergency Number**. To send an automated message to a Cisco IP phone, type the extension of the phone in the box next to **Extension**. To trigger an automated email, type the email address in the field next to **E-mail**. Once you have selected either an extension, e-mail or both, click the **Add** button directly under **E-mail**. You can add additional destinations by selecting the emergency number and typing additional extensions and e-mail addresses. An example of a configured Emergency Alert feature is shown in Figure 17: Configured Emergency Alert Feature.

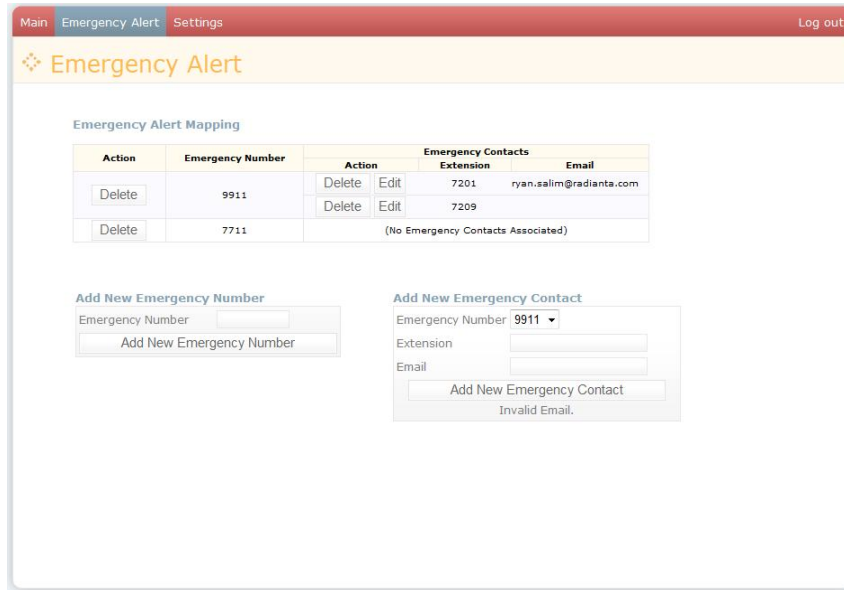


Figure 17: Configured Emergency Alert Feature

Note - In this example, if 911 is dialed by a user, their call will be directed to 911 emergency services. In addition, a message will be displayed on the Cisco IP phones configured to receive the alert as shown in Figure 18: **Emergency Alert Cisco IP Phone Notification**.

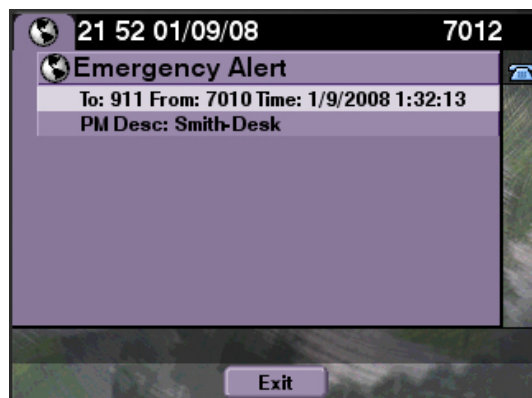


Figure 18: Emergency Alert Cisco IP Phone Notification

In addition, an automated email will be triggered to the appropriate addresses as shown in Figure 19: **Emergency Alert E-Mail Notification**.

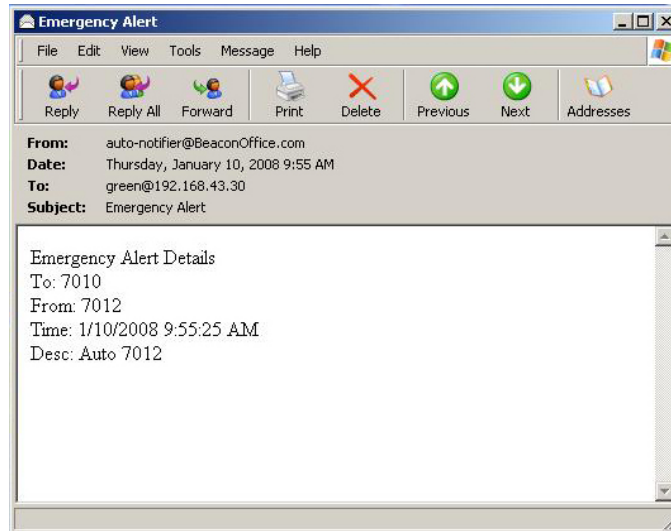


Figure 19: Emergency Alert E-Mail Notification

In each case, the source and destination information is displayed, allowing appropriate people within your organization to be immediately informed in the case of a specific situation, such as an emergency.

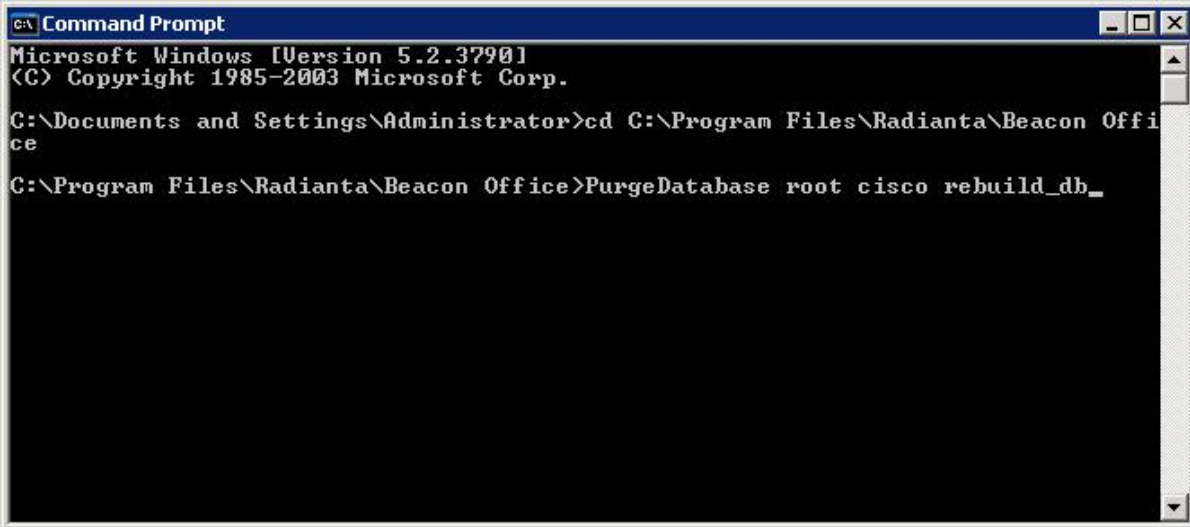
Appendix A: Beacon Office Database Rebuild

Sometimes it is necessary for an Administrator to rebuild the Beacon Office database. For example, an Administrator might want to point Beacon Office to another CallManager. This section of the Admin guide provides instructions for wiping and reconstructing the database.

To rebuild the database, open a command prompt and navigate to the Beacon Office installation directory. From there you can execute the `purgedatabase` command which performs the actual deleting and recreating of the database. As you can see in Figure 20, there are three parameters that can be passed to `purgedatabase` (each should be separated with a space):

1. MySql username
2. MySql password (this is the same MySql password that was provided in the Beacon Office install)
3. `rebuild_db` (this instructs `purgedatabase` to recreate the database after it's deleted. If this parameter is left out, the database is dropped, but not recreated)

Note: Executing the `purgedatabase` command will delete any data that is currently contained in the Beacon Office database. Please use this command with care.



```
C:\> Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd C:\Program Files\Radiana\Beacon Office
C:\Program Files\Radiana\Beacon Office>PurgeDatabase root cisco rebuild_db_
```

Figure 20

Appendix B: Beacon Office User Synchronization

Beacon Office gets all its user information from Call Manager. Whenever a new user is added or changed in Call Manager, it will be detected and added to Beacon Office when the next synchronization is performed.

By default, Beacon Office synchronizes with Call Manager once an hour. This value can be configured by changing the "Sync Timer" value in the "Beacon Office Global Settings" provider configuration page.

An on-demand sync may be performed through the "Invoke Extension" button under the "Radianta.Cuae.Providers.GlobalSettings.StartSync" extension in the "Beacon Office Global Settings" provider configuration page.

The synchronizer does not automatically delete Beacon Office users that no longer exist in Call Manager. If there is a need to cleanup "orphaned" Beacon Office users, use the "Invoke Extension" command under "Radianta.Cuae.Providers.GlobalSettings.StartReverseSync" in the "Beacon Office Global Settings" provider configuration page to clean up the user database.

Summary

This guide is designed to assist system administrators with the licensing and configuration of users within Beacon Office. As noted at the beginning of this guide, administrators who wish to understand how to install and configure Beacon Office should consult the guide, *Installing and Configuring Beacon Office – CUAE Bundle*. End users wishing to understand how to use features within Beacon Office should consult the *Beacon Office User Manual*.

We are always interested in your feedback, including additional features that you would like to see. Feel free to email us at support@radianta.com.