UC for Enterprise (UCE) Desktop Client/Agent (UNIVERGE UC700)

Installation Guide

NEC Corporation

Liability Disclaimer

Contents

Figures

Tables

1

Introduction

The *UNIVERGE UC700 Installation Guide* provides the information you need to install and configure the UC700 application.

Chapter Topics
- *UC700 Overview*
- *How This Guide is Organized*

UC700 Overview

UNIVERGE UC700 combines contacts, rich presence, communication history, instant messaging, call control, optional mobility, voice conferencing, and collaboration into one powerful, easy to manage solution. The UC700 provides an intuitive interface that combines unified communications functionality in a single application.

Your presence and status may be easily shared with fellow UC700 users, MC550 mobility clients (R2 and greater), and users of NEC's soft phone, Dterm, MH250, and DT750/INASET phones.

Based on your status, you may implement rules for groups of contacts so that people can reach you in the most effective and appropriate method possible.

Limitations

Please note the following limitations for UC700.

- UC700 does not display the destination name correctly when the destination user, who belongs to a different PBX, transferred the call to an external number.

Example: *User A (PBX 1) calls User B(PBX 2) via CCIS*

User B (blind) transferred the call to external number

User A should see the external number in the call control window, but displays User B

- In a 3-way conference with CCIS network case, the initiating user can see the user name of both participants, but participants can only see the user name of the initiating caller.

Example: *User A (Initiator:PBX 1), User B (PBX 1) and User C (PBX 2) are in a 3-way conference*

User A can see all participants in the call control window but User C can see only User A information; because User B belongs to a different PBX

How This Guide is Organized

Chapter 1
Introduction

This chapter provides an overview of the UC700 Client application and the chapter layout of the UNIVERGE UC700 Client Getting Started Guide. Also, included in this chapter are the known limitations for UC700.

Chapter 2
UNIVERGE UC700 Server Installation

This chapter provides the step-by-step procedures to install the UC700 Server software.

Chapter 3
UNIVERGE UC700 Client Software Installation

This chapter lists the procedures required to install the UC700 Client application as a standalone desktop application or as a toolbar working in conjunction with Microsoft Outlook.

Chapter 4
Configuring OW5000 to Support UC700 Clients

This chapter describes the functions and associated screen displays for configuring the UC700 in OW5000 Administrator.

Chapter 5
Configuring OW5000/UC700 to Support ACD Integration

This chapter describes the configuration process needed for the UC700 when integrated with ACD.

Chapter 6
Configuring OW5000 SSL Support for UC700 Clients

This chapter lists the procedures to set up SSL security support for communications between UC700 clients and the OW5000.

Chapter 7
Installing and Configuring Calendar Link

This lists the procedures to install and configure Calendar Link to support UC700 clients.

2

UNIVERGE UC700 Server Installation

This chapter provides step-by-step procedures used to install the UC700 server software. The procedures and other information are found in the following sections of this chapter.

Chapter Topics
- *Before Starting the Installation Procedure*
- *Installing UNIVERGE UC700*
- *Configuring UNIVERGE UC700*
- *Enabling Voice Conferencing*
- *Conference Bridge Configuration*
- *PBX Configuration—Voice Mail Pilot*
- *Uninstalling the UNIVERGE UC700*

Before Starting the Installation Procedure

Before installing the UC700 software, refer to the *Requirements* section in the *UNIVERGE OW5000 Getting Started Guide*. Verify that your system meets the Application Environment requirements for the OW5000 Platform and the specific application software you purchased.

> *The UNIVERGE OW5000 Platform must be installed prior to installing the UC700 Server.*

IMPORTANT

To install the UNIVERGE UC700 server software:

- You must be logged into the computer where the software is to be installed.
- You must have Administrator rights to the computer.
- Table 2-1 provides a list of software and hardware requirements for the UC700 server that must be met.

Table 2-1 *Additional Requirements*

Operating System
Microsoft Windows Server 2003 R2 SP2 or later 32bit/64bit Microsoft Windows Server 2008 32bit/64bit Microsoft Windows Server 2008 R2 (latest Service Pack and Critical Updates)
Processor
Dual Core 1.8GHz or faster
Memory
2 GB RAM.
Hard Drive Space (available before installation)
10 GB or more available space
Web Server
Microsoft Internet Explorer 6.0, 7.0 and 8.0 (latest Service Pack and Critical Updates) for Windows
Note: *IIS requires installation of the current security patches located at windowsupdate.microsoft.com.*
.NET Framework
.NET Framework 3.5 SP1

Installing UNIVERGE UC700

Follow the steps below to install the UNIVERGE UC700.

> **NOTE**
> *If you wish to install without rebooting the server following the completion of the install, then you must first stop the OW5000 UCConference Manager service. Otherwise, you will be asked to reboot the server following the install.*

Step 1   Place the OW5000 DVD into the **DVD-ROM drive**. On most computers Autorun automatically starts the installation when you load the DVD. If Autorun is not enabled on the computer, though, you must do the following:

—After placing the 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 Main menu, select the link to launch the installer for UNIVERGE UC700 Server. Figure 2-1 displays.

Figure 2-1 *UC700 Server—Welcome dialog*

Step 3 Click **Next**. Figure 2-2 displays.

Figure 2-2 *Choose Destination dialog*

Step 4   Do one of the following:

—To install to the default folder, click **Next**.

—To select a different location, click **Change**. Figure 2-3 displays.

Figure 2-3 *Change Destination Folder dialog*

Step 5   Do one of the following:

—Select the desired folder from the drop-down list.

—Create a new folder by clicking the new folder icon.

Step 6   Click **OK**. Figure 2-4 displays.

Figure 2-4 *Ready to Install dialog*

Step 7   Click **Install**. Figure 2-5 displays.

Figure 2-5 *Installing UC700 dialog*

—After the files are installed, Figure 2-6 displays.

Figure 2-6 *Installation Complete dialog*

Step 8   Click **Finish** to complete the installation.

Step 9   If requested by the installer, reboot the server.

Configuring UNIVERGE UC700

UC700 uses the OAI Server to manage all calls, PBX Configurations, Dialing Rules, and Monitored Numbers. The OAI Server must be properly configured for the UC700 to function. Refer to the *UNIVERGE OW5000 Configuration Guide* for more information.

UC700 also uses the OW5000 Application Message Service (AMS) for notification of incoming and outgoing calls, status changes, and voice mail notification.

After installing the UC700, you can view the **Client Settings** and **General Settings** using the Admin web site. Refer to *Logging into OW5000 Administrator* below.

Logging into OW5000 Administrator

Each time you work with OW5000 Administrator, log in with your OW5000 login ID and password. If this is the first time you are logging in to the OW5000 Administrator, use the default login ID admin and the default password for admin is admin.

When you have finished using the application, you can either log out or just close your browser.

Step 1 From the desktop, click the **Start** button and then select **All Programs** > **NEC OW5000** > **Platform** > **OW5000 Administrator**. An OW5000 Administrator Login dialog box displays (Figure 2-7).

Figure 2-7 *OW5000 Admin Login screen*

Step 2 Enter your login ID in the **Login ID** field.

*The login ID is **admin**.*

NOTE

Step 3 Enter your password in the **Password** field.

*The first-time password for admin is **admin**.*

NOTE

Step 4 Click **Login** to display the OW5000 Administration page.

Figure 2-8 *OW5000 Admin page*

Step 5 Select **Unified Communications > UC700**. A UC700 Client Settings Tab dialog displays (Figure 2-9).

Figure 2-9 *UC700 Client Settings Tab dialog*

This page displays available licenses for UC700 and a list of currently logged in users. You can click on any heading to change the contents from ascending to descending order.

Step 6 Click **General Settings**. Figure 2-10 displays.

Figure 2-10 UC700 General Settings Tab dialog

Step 7   In the **Allow clients to search for employees in** drop-down list, select to allow only their own company, or all companies.

Step 8   In the **Display Home Phone** field and the **Display Mobile Phone** field, select Always, Based on Contact Rules, or Never.

Step 9   In the **Ping Interval (Minutes)** field, enter the number of minutes between pings.

Step 10   Click **Apply** to save the changes or **Cancel** to exit without saving the changes.

Enabling Voice Conferencing

Follow the steps below to configure voice conferencing.

Step 1   Click the **Conference Configuration** tab. Figure 2-11 displays.

Figure 2-11 UC700 Conference Configuration Tab dialog

Step 2   In the **Enable UC700 Conferencing** drop-down box, select **Enabled**.

Step 3   In the **Conferencing Server Port Number** field, type the port number of the UC700 conference server. The default is **8731**.

Step 4   Click **Apply**.

Conference Bridge Configuration

PBX Configuration

The following restrictions or options are available.

- 8, 16, or 32 ports for conference bridges are available.
- The conference bridge should be programmed for **Meet-Me Conference**.
- Conference bridge port members must be programmed as Hunt Group (ASHU/L/N or ASHC/L/N or ASHP/L/N).

UC700 provides a visual voice conference feature that works with the PBX conference bridge. Use the following steps to configure the conference bridge.

Step 1   From the OW5000 Administrator page (Figure 2-8), follow the path **OW5000 > Platform > Conference Bridge** to set up a Conference Bridge for UC700. Figure 2-12 displays.

Figure 2-12 *Conference Bridge dialog*

Step 2   Click **Add New Bridge** to set up a Conference Bridge for UC700. Figure 2-13 displays.

Figure 2-13 *Conference Bridge—Add New dialog*

> **Step 3**   Enter the **Bridge Name** and select the **Tenant** number from the drop-down list. **Is Host Controlled** should be set if this bridge is used by the UC700 Voice Conference feature. If this parameter is checked, the bridge name is displayed in UC700.

Figure 2-14 Conference Bridge—Ports

> *Even if the added port numbers are listed on the page, these numbers are not saved until the data is saved.*
>
> **NOTE**

> **Step 4**   Enter the conference bridge ports one by one using the **Ports** field.

> **Step 5**   Click **Set Pilot Number** on the bridge port member that is the pilot number users call to join the bridge.

> **Step 6**   Do one of the following:
>
> —Click **Apply** to save the conference bridge without exiting the dialog box.
>
> —Click **Done** to save the conference bridge and exit the dialog box.
>
> —Click **Cancel** to exit the dialog box without saving the conference bridge.

PBX Configuration—Voice Mail Pilot

To support the UC700 Voice Mail feature on an Incoming pop up, you must configure a reserved number, and a voice mail pilot number using the OW5000 Administrator Control Panel. You may also be required to set up a Redirect Number.

Adding a Reserved Number

To set up a reserved number for voice mail, follow the steps below.

Step 1   Follow the path, **OW5000 > Platform > PBXs** to set up a Voice Mail Pilot number for UC700. Figure 2-15 displays.

Figure 2-15   OW5000 Administrator—PBX Configuration—PBX List page

Step 2   Click the **Pencil** icon of the target PBX. A PBX Settings screen displays.

Step 3   Select the **Reserved Numbers** tab to display Figure 2-16.

Figure 2-16   PBX Configuration—Reserved Number dialog

Step 4   Click the **Add New Monitored Number** button. Figure 2-17 displays.

Figure 2-17   Add Reserved Number dialog

Step 5 Enter the reserved **Number** and select the **Tenant** number from the drop-down list. Set the Monitored Number as the **Reserved Type** and Oai Server as the **Application**.

Step 6 Do one of the following:

—Click **Apply** or **Apply & Add New** to save the voice mail pilot number without exiting the dialog box.

—Click **Done** to save the voice mail pilot number and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the voice mail pilot number.

Adding a Voice Mail Pilot Number

A voice mail pilot number is required to redirect an incoming call to voice mail. Follow the steps below to set the voice mail pilot number:

Step 1 Select the **Voice Mail Pilot Numbers** tab from the PBX Configuration dialog box (Figure 2-16).

This action displays a Voice Mail Pilot Numbers dialog box (Figure 2-18), allowing you to add or edit one or more voice mail pilot numbers.

Figure 2-18 *Voice Mail Pilot Numbers dialog*

Step 2 Click **Add New Pilot Number**. Figure 2-17 displays.

Figure 2-19 *Add New Pilot Number*

Step 3 Enter the number to reserve for UC700 voice mail routing in the **Pilot Number** field.

Step 4 Do one of the following:

—Click **Apply** to save the voice mail pilot number without exiting the dialog box.

—Click **Done** to save the voice mail pilot number and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the voice mail pilot number.

Step 5   To change the default voice mail pilot number, click **Set Default** next to the pilot number to be the new default pilot number.

—The default pilot number displays in bold face.

—The default pilot number is used when a client does not specify the voice mail pilot number.

Step 6   To delete a **Voice Mail Pilot Number**, click the trash can icon.

Adding a Redirect Number

A Redirect Number is required when using a contact rule. To add a Redirect Number, follow the steps below.

Step 1   Click the Pencil icon next to the selected PBX, then click the **Reserved Numbers** tab. Figure 2-20 displays.

Figure 2-20 PBX Settings—Add New Monitored Number dialog

Step 2   Click the **Add New Monitored Number** button. Figure 2-21 displays.

Figure 2-21 Add New Monitored Number dialog

Step 3   Enter the **Number** and **Tenant**. Select Monitored Number for the **Reserved Type**, and Un-Assigned for the **Application**.

Step 4 Do one of the following:

— Click **Apply** or **Apply & Add New** to save the Redirect number without exiting the dialog box.

— Click **Done** to save the voice mail pilot number and exit the dialog box.

— Click **Cancel** to exit the dialog box without saving the voice mail pilot number.

Incoming Call Assistant

Follow the steps below to assign a Redirect Number to the PBX.

Step 1 Go to **OW5000 > Applications > Incoming Call Assistant**.

Step 2 Select the **PBX Settings** tab to display an Enable Incoming Call Assistant dialog box (Figure 2-22).

Figure 2-22 *Enable Incoming Call Assistant dialog*

Step 3 Check the **Selected** check box.

Step 4 Click **Apply** to save the information.

Step 5 Select the **Redirect Configurations** tab and then click **Add New Redirect Configuration**. Figure 2-23 displays.

Figure 2-23 *Assign Redirect Number to PBX dialog*

Incoming Call Assistant Redirect Configuration Manager

PBX: Atlanta
Redirect Number 47510

Done   Cancel

Step 6 Select the **PBX** and **Redirect Number**, assigned earlier on the PBX configuration page, from the drop-down list (Figure 2-23).

Step 7 Do one of the following:

—Click **Done** to save the information and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the voice mail pilot number.

Uninstalling the UNIVERGE UC700

The UC700 software can be uninstalled using the Windows operating system **Add/Remove** software function in the Windows Control Panel.

To uninstall the software, in the Add/Remove dialog box, select **UC700** and then click **Remove**. Follow the displayed instructions and remove all components when prompted. For more information, refer to the Windows documentation for the version of Windows installed.

3

UNIVERGE UC700 Client Software Installation

This chapter provides step-by-step procedures for installing the UC700 Client software. It includes these topics:

Chapter Topics
- *Client System Requirements*
- *UC700 Desktop Client Installation*
- *UC700 Outlook Toolbar Installation*

Client System Requirements

Refer to Table 3-1 for a list of system requirements for the UC700 client installation before installing the UC700 Client software.

NOTE *UC700 Client must be installed on a Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 7.*

Table 3-1 *UC700 Desktop Client System Requirements*

Operating System
Microsoft Windows XP Professional x86 with Service Pack 3
Microsoft Windows XP Professional x64 with Service Pack 2
Microsoft Windows Vista x86 or x64 with Service Pack 1
Microsoft Windows 7 x86 or x64
Processor
1.0 GHz or faster
(2 GHz or faster recommended)
Memory
1 GB RAM (or more)

Hard Drive Space (available before installation)
20 MB for install (uses 9 MB of space after install)

Additional Hardware and Software
Graphics card with support for Microsoft DirectX 9.0 graphics with Windows Vista Display Driver Model (WDDM) Driver (even on XP), 128 MB of graphics RAM or more, Pixel Shader 2.0 in hardware, 32-bits per pixel

Web Browser
Microsoft Internet Explorer 6.0 or higher (latest Service Pack and Critical Updates) for Windows

Monitor
1024 x 768 or higher-resolution 24-bit color

.NET Framework
Microsoft.NET Framework 3.5 SP1 (pre-installed)

Microsoft Outlook
For UC700 Desktop Client Outlook Status Integration: Outlook 2003 or 2007 (32 or 64 bit)
For UC700 Toolbar Client: Outlook 2003 or 2007

Windows Media Player
Windows Media Player 11 or higher (listed in Windows update as an optional update). Applies to XP users only. The appropriate media player is already provided for other OSes.

Windows Media Player is used for voice mail playback, so only the default codecs in Windows is supported. (See *Supported Windows Audio Formats (WAV)*). Other codecs can be supported if the administrator purchases them from their owners and installs them on the client computers.

Supported Windows Audio Formats (WAV)

- 11,025Hz 16bit PCM
- 8,000Hz 16bit PCM
- 11,025Hz 8bit PCM
- 11,025Hz u-Law
- 8,000Hz 8bit PCM
- 8,000Hz u-Law
- 11,025Hz 4bit ADPCM
- 8000Hz 4bit ADPCM
- 11,025Hz GSM6.10
- 8000Hz Mp3
- 8,000Hz GSM6.10
- 8,000Hz DSP Group TrueSpeech
- 8000Hz Mp3 8k

UC700 Desktop Client Installation

This section explains how to install the UC700 Desktop Client for standalone use. It also explains how to launch the UC700 Desktop Client from the System Tray and establish initial connection settings. The following topics are included in this section.

- *UC700 Desktop Client Installation Steps*
- *Launching the UC700 Desktop Client*

UC700 Desktop Client Installation Steps

The steps for installing the standalone UC700 Desktop Client are as follows:

Step 1   Type the host name or IP address of the OW5000 in Internet Explorer to access the installation execute file for the machine you are currently using. Use the following format:

http://<hostname>/uc700

where **<hostname>** is the name or IP address of your OW5000 server. This information will be provided to you by your system administrator. Figure 3-1 displays.

Figure 3-1   *UNIVERGE UC700 Main Page*

Step 2   Click **Downloads**. The download options on the page displays.

Step 3   Click **DOWNLOAD UC700 DESKTOP CLIENT**.

Step 4   Click **Run** when prompted to start the installation immediately, or click **Save** to save the download so you can start the installation later.

Step 5   If you clicked **Save** to save the download for installation later, when you are ready to install the toolbar, double-click the **uc700.setup.exe** file.

Step 6   Click **OK**.

—If .NET Framework 3.5 SP1 is not installed on your machine, Figure 3-2 displays.

Figure 3-2 *UC700—InstallShield Wizard Completed—Interrupted dialog*

—If this occurs, click **Install** and then download and install the Microsoft .NET Framework 3.5 SP1 installation execute file (**dotnetfx35.exe**) from http://www.microsoft.com before restarting the UC700 Desktop Client install.

—If .NET Framework 3.5 SP1 or later is installed on your machine, continue to Step 7.

Figure 3-3 *UC700—InstallShield Wizard—Welcome dialog*

Step 7   Click **Next**. Figure 3-4 displays.

Figure 3-4 *UC700—InstallShield Wizard—Custom Setup dialog*

Step 8   Select the program features you want to install by clicking the icon next to a particular feature. The options are:

—**UC700 Desktop Client for Windows**—Used to install the feature components and subfeature components required to run the UC700.

—**Outlook Status Integration—** Used to install integration components for Microsoft Outlook, permitting you to automate your status through calendar events.

—**Language Pack Additions**—Used to localize UC700 for a specific language. (Not supported at this time.)

NOTE

*To install the components to a different destination folder, click **Change** and select the new folder location.*

Step 9   Click **Next**. Figure 3-5 displays.

Figure 3-5 *UC700—InstallShield Wizard—Ready to Install the Program dialog*

Step 10   Click **Install**.

—The installation begins. It may take a few seconds to install the software. Once the software is installed, Figure 3-6 displays.

Figure 3-6 *UC700—InstallShield Wizard Completed dialog*

Step 11 Check the **Launch UC700** check box.

Step 12 Click the **Finish** button. Figure 3-7 displays.

Launching the UC700 Desktop Client

To launch the UC700 Desktop Client:

Step 1 Right-click the **UC700** system tray icon and then select **Login** from the popup menu (see Figure 3-7).

Figure 3-7 *UC700 System Tray Icon—Open*

—If the UC700 Client icon is not present in the System Tray you can follow this path to start UC700:

Click **Start > All Programs > NEC > UC700**. Figure 3-8 displays.

Figure 3-8 *UC700 Client Login dialog*

Step 2 Fill in these fields:

—**Use Windows Authentication**: If the **Username** and **Password** are to be authenticated by Windows, check this box.

> **NOTE** *Windows Authentication requires configuration in OW5000 Administrator of the UC700 user to support this feature. Please refer to "Person Management Configuration" on page 4-3.*

—**Username**: Your user login identifier associated with the server. The **Username** must match the **Login ID** specified when the user was created using the OW5000 Administrator's User Management function.

—**Password**: Password associated with the login identifier. The **Password** must match the password value specified when the user was created using the OW5000 Administrator's User Management function.

—**Remember Password**: If you do not want to reenter the password each time you log in, check this box. This option is recommended.

—**Automatically Log in at Startup** (Figure 3-8): If you check this box, you are not prompted for the **Username** and **Password** and are instead logged in automatically each time you start UC700.

—**Start UC700 on Windows Startup** (Figure 3-8): If you check this box, you are not prompted for the **Username** and **Password** and are instead logged in automatically each time you start Windows.

—**Server**: This is the DNS name for the server or the server's IP address. The **Server** value must match the name of the machine where the UC700 server is installed.

—**Use SSL**: Do not check this option unless instructed to do so by your system administrator. This option provides an added layer of security that requires the administrator to set up encryption in the system.

—Click the **Help About button** for information on the current client version, to view UC700 Online Help, and to view the server status.
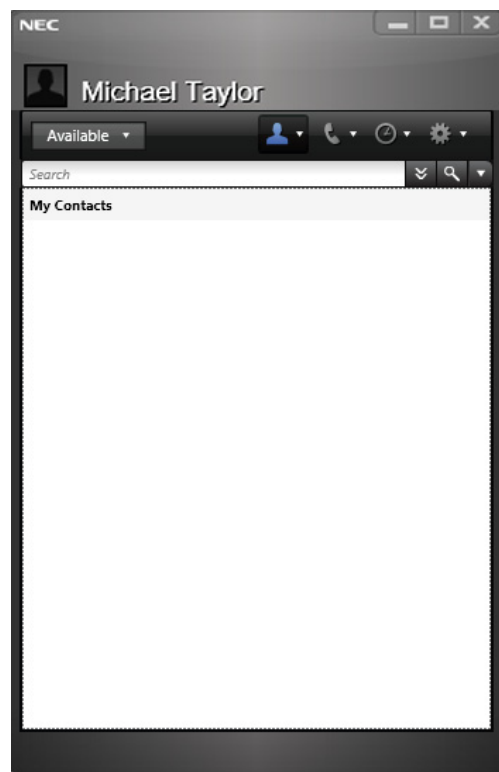
NOTE

The About screen, shown in Figure 3-8, is only present when selected.

Step 3 Click the **Login** button. Figure 3-9 displays.

NOTE

The first time a user logs into the UC700 Client, it can take 30 seconds or longer to load.

Figure 3-9 *UC700 Client Window*

—The UC700 Client installation is now complete.

Step 4   To close the UC700 Client window, click **Exit (X)**.

REFERENCE

For more information on using the Client software, refer to the UNIVERGE UC700 Getting Started Guide or the UNIVERGE UC700 Online Help system.

UC700 Outlook Toolbar Installation

The UC700 Outlook Toolbar is used to perform UC700 functions when using Outlook. This section describes how to install the UC700 Outlook Toolbar. It also explains how to initially access UC700 using the toolbar, how to establish connection settings, and how to access Online Help for more information about using UC700 with Outlook. The following topics are included in this section

- *UC700 Outlook Toolbar Installation Steps*
- *Logging in to UC700 Using the Outlook Toolbar*
- *UC700 for Microsoft Outlook Online Help*

UC700 Outlook Toolbar Installation Steps

The steps used to install the UC700 toolbar for use with Outlook are very similar to those used to install the UC700 Desktop Client version. The steps below are used to install the toolbar.

Step 1   Type the host name or IP address of the OW5000 in Internet Explorer to access the installation execute file for the machine you are currently using. Use the following format:

http://<hostname>/uc700

where **<hostname>** is the name or IP address of your OW5000 server. This information will be provided to you by your system administrator. The **UNIVERGE UC700 Main Page** displays.
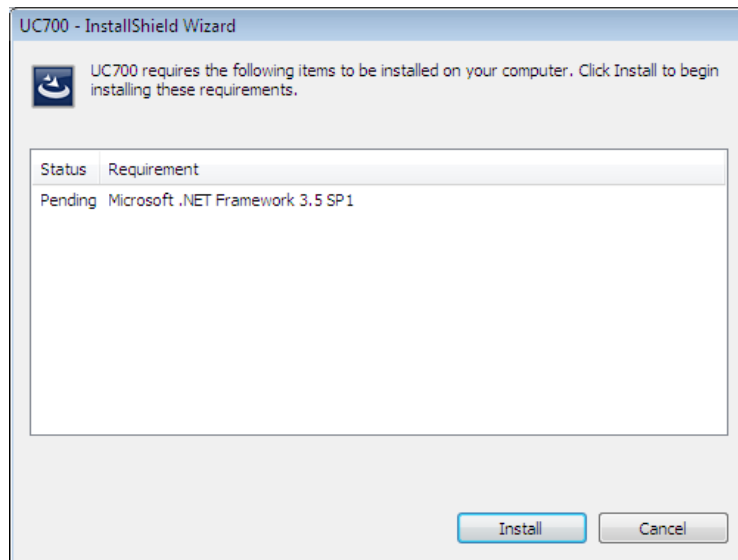
Step 2   In the upper-right corner, click the **Downloads** link. The download options on the Main Page displays.

Step 3   Click **DOWNLOAD UC700 CLIENT FOR MICROSOFT OUTLOOK®**. A form displays asking whether you want to run the installation now or save the installation .exe to run later.

Figure 3-10 *UNIVERGE UC700 Main Page*

Step 4   Click **Run** when prompted to start the installation immediately, or click **Save** to save the download so you can start the installation later.

Step 5   If you clicked **Save** to save the download for installation later, when you are ready to install the toolbar, double-click the **uc700.toolbar .setup.exe** file. A form displays that is used to start the installation.

Step 6   Click **OK**.

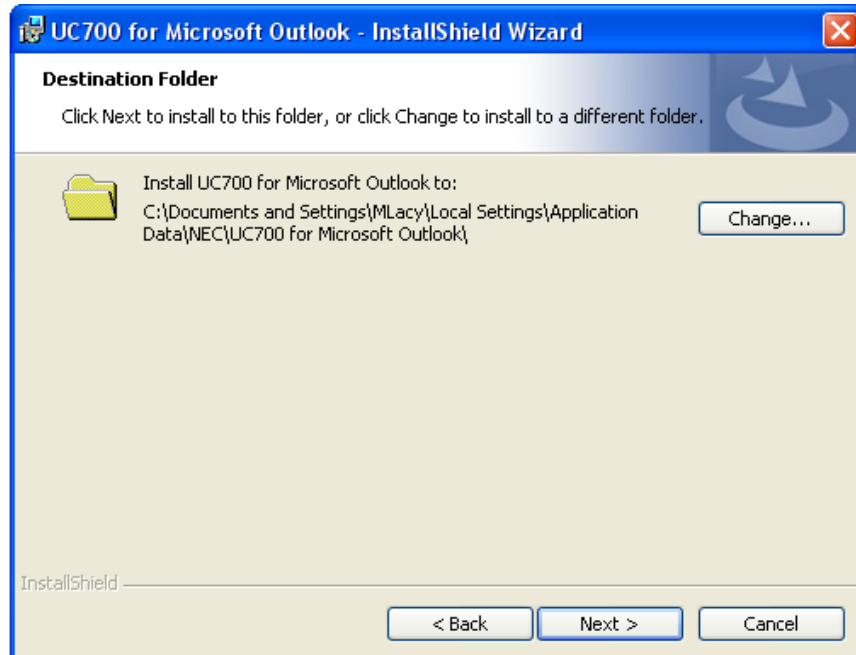—If .NET Framework 3.5 SP1 is not installed, Figure 3-11 displays.

Figure 3-11 *UC 700—InstallShield Wizard Completed—Interrupted dialog*

—If this occurs, click **Install** to end this installation procedure. Download and install Microsoft .NET Framework 3.5 SP1 (**dotnetfx35.exe**) from http://www. microsoft.com.

—After installing Microsoft .NET Framework 3.5 SP1, you can restart the toolbar installation.

—If .NET Framework 3.5 SP1 or later is already installed, a **Preparing to Install** message displays briefly, and then Figure 3-12 displays. Proceed to Step 7.

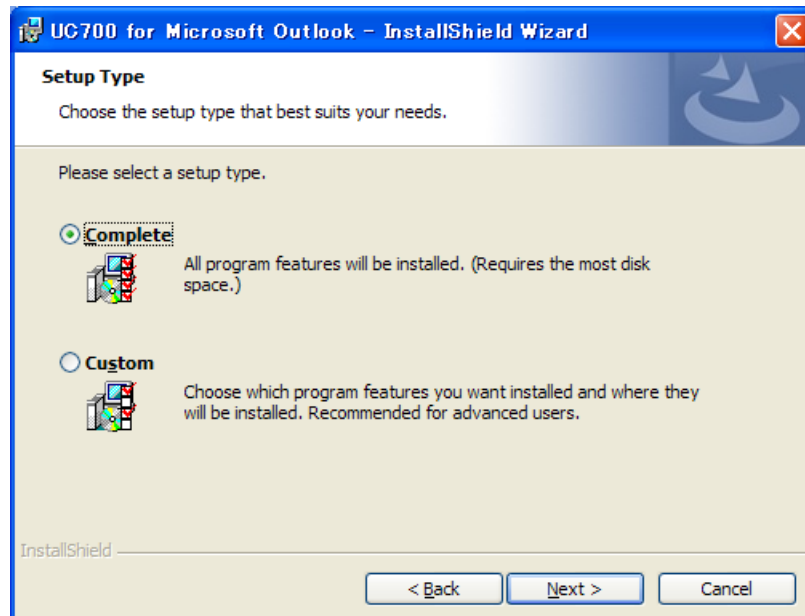***Figure 3-12*** *UC700 for Microsoft Outlook—Welcome dialog*

Step 7   Click **Next**. Figure 3-13 displays.

Figure 3-13 *UC700 for Microsoft Outlook—Destination Folder dialog*
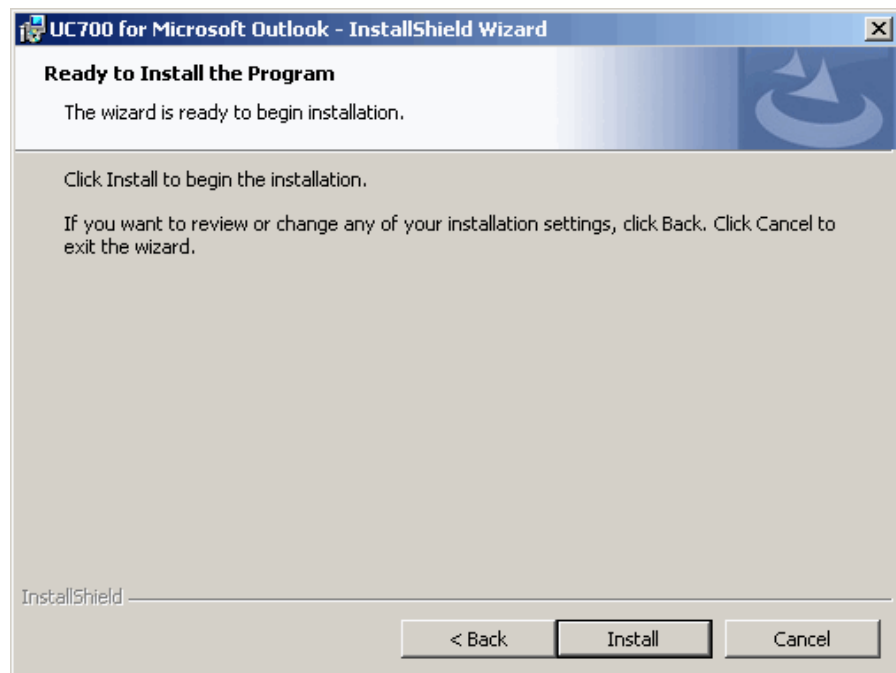

Step 8   Click **Next** to accept the default installation folder and proceed to step, or click **Change** and indicate the new installation folder location. Figure 3-14 displays.

Figure 3-14 *Setup Type dialog box*

Step 9   Select **Complete** and then click **Next**. Figure 3-15 displays.

Figure 3-15 *UC700 for Microsoft Outlook—Ready to Install the Program dialog*
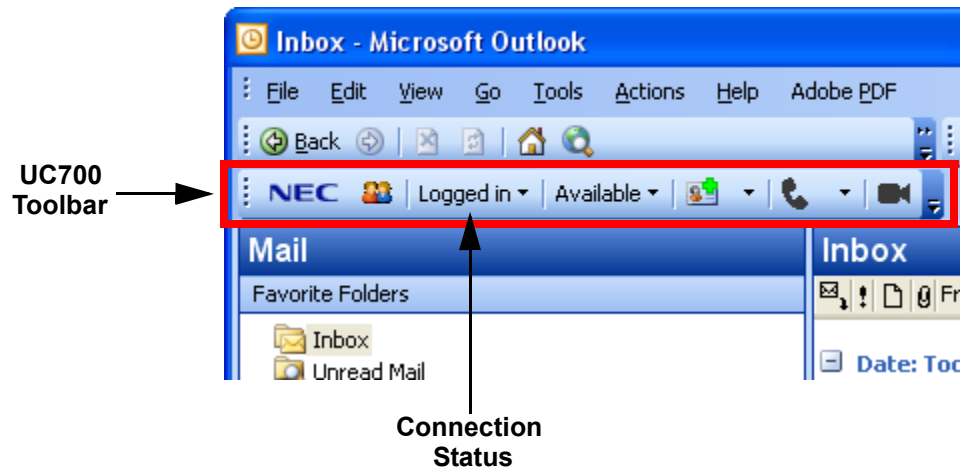

Step 10   Click **Install**.

—The installation starts. Wait while the installation program unpacks and installs the files.

—Once the installation finishes, Figure 3-16 displays.

Figure 3-16 *UC700 for Microsoft Outlook Completed dialog*

Step 11   Click **Finish**.

—This completes the installation. Outlook automatically loads and the new toolbar can been seen in the upper-left corner of the Outlook screen (see Figure 3-17).

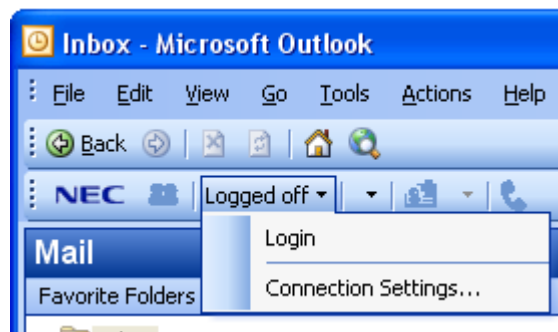*Figure 3-17* *UC700 Outlook Toolbar example*

Logging in to UC700 Using the Outlook Toolbar

To log in to UC700 using the Outlook Toolbar, you must establish connection settings first. To establish connection settings and log in to UC700, follow the steps below.
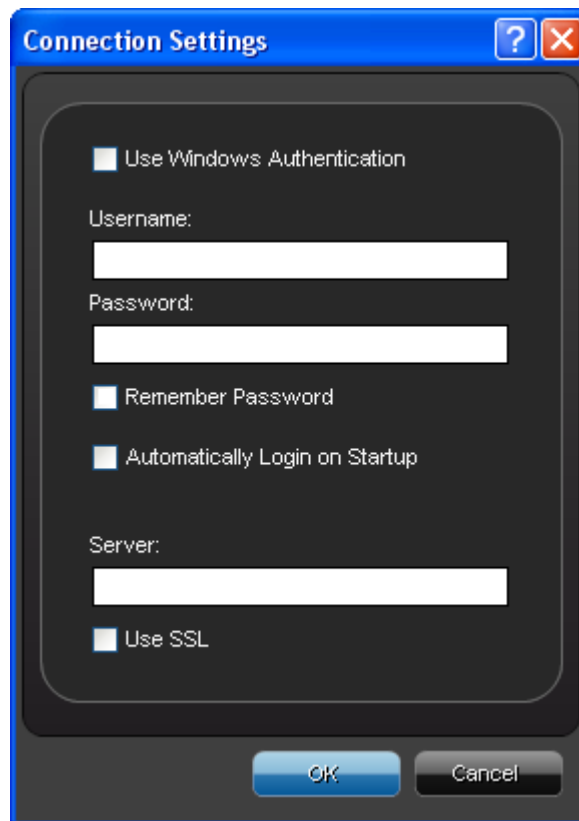
Step 1   Bring up Outlook and click the down-arrow next to the **Logged off** button. A menu displays, as shown in Figure 3-18.

Figure 3-18 *UC700 Logged Off Status dialog*

Step 2   Click the **Connection Settings** option. Figure 3-19 displays.

Figure 3-19 *UC700 Connection Settings dialog*

Step 3   Fill in these fields:

—**Use Windows Authentication**: If the **Username** and **Password** are to be authenticated by Windows, check this box.

NOTE

To enable this function, the user must be configured in OW5000 Administrator. Refer to "Person Management Configuration" on page 4-3 for more information.

—**Username**: Your user login identifier associated with the server. The **Username** must match the **Login ID** value specified when the user was created using the OW5000 Administrator's User Management function.

—**Password**: Password associated with the login identifier. The **Password** value must match the password specified when the user was created using the OW5000 Administrator's User Management function.

—**Remember Password**—If you do not want to reenter the password each time you log in, check this box. This option is recommended.

—**Automatically Log in on Startup** (Figure 3-19)—If you check this box, you are not prompted for the **Username** and **Password** and are instead logged in automatically each time you open Outlook. This option is recommended.

—**Server**—This is the DNS name for the server. The **Server** value must match the name of the machine where the UC700 Server is installed.

—**Use SSL**—Do not check this option unless instructed to do so by your system administrator. This option provides an added layer of security that requires the administrator to set up encryption in the system.

Step 4   Click **OK**. This stores the settings for use the next time you log in. The UC700 Connections Settings dialog box disappears.

Step 5   Log into the system by clicking the **Logged off** menu, then selecting the **Login** option. The system logs you in.

—The **Logged off** menu changes names to **Logged in**.

—The **Availability** menu displays and the toolbar options go from grayed-out and unselectable to colored and usable.

The first time a user logs in to UC700, it can take 30 seconds or longer to load the software. Subsequent logins are much faster.

NOTE

UC700 for Microsoft Outlook Online Help

If you need instructions for performing UC700 functions from Outlook, access the helps system. To access the help system, follow the steps below.

Step 1   Click **Help** on the Outlook menu.

Step 2   Click the **UC700 for Microsoft Outlook Help** option. The online help system displays.

4

Configuring OW5000 to Support UC700 Clients

This chapter provides the procedures needed to configure the UNIVERGE OW5000 for use with UC700.

This chapter assumes that the OW5000 Platform, OW5000 Access Server, and the UC700 Server are installed.

NOTE

Chapter Topics
- *Logging into OW5000 Administrator*
- *Person Management Configuration*
- *User Management Configuration*

The UNIVERGE OW5000 must be configured to support the UC700 client software and to add UC700 users. A UC700 user must have UC700 privileges, a Primary Extension, and an Employee or Physician role in the UNIVERGE OW5000 Corporate Directory.

To configure UNIVERGE OW5000 to support UC700, use the OW5000 Administrator. It provides a graphical user interface that can be used to modify OW5000 user account information, PBX configurations, and database entries.

Logging into OW5000 Administrator

Each time you work with OW5000 Administrator, log in with your OW5000 login ID and password. If this is the first time you are logging in to the OW5000 Administrator, use the default login ID **admin** and the default password for the admin login, which is also **admin**.

When you have finished using the application, you can either log out or close your browser. To log in, follow the path below.

Step 1 Click the **Start** button and then select **All Programs > NEC OW5000 > Platform > OW5000 Administrator**. Figure 4-1 displays.

Figure 4-1 *OW5000 Administrator Login dialog*

Step 2 Enter the default login identification and password.

Step 3 Click **Login**. Figure 4-2 displays.

Figure 4-2 *OW5000 Administrator Control Panel dialog*

Person Management Configuration

UC700 Client software users must be added to the OW5000. They must be given a security role and assigned a primary contact method. These additions are made using the **OW5000 Administrator Control Panel**.

Adding a User

To add a UC700 Client software user to the OW5000, select **OW5000 > Directory > People** (Figure 4-3). Figure 4-4 displays.
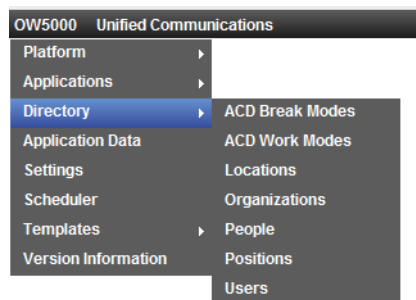
Figure 4-3 *OW5000 Directory Menu*

Figure 4-4 *OW5000 Administrator—Person Management*

Step 1   Click **Add New Person** to define a Person who will be using the UC700 Client. Figure 4-5 displays.

Figure 4-5 Person Management—Add User

Step 2   Fill in the required fields. The required fields for all UC700 Client users are:

—**Last Name**: Last Name of the person you are adding.

—**First Name**: First name of the person you are adding.

Step 3   If your are implementing Instant Messaging for UC700 users, you must fill in these fields for each UC700 user. UC700 requires 2 types of URI as listed below:

—**SIP URI**: used for presence. UC700 gets presence information through PSGW, so the SIPAccessServer must be PSGW server. (By default, PSGWLocal is created during the OW5000 installation process.)

—**IM URI**: used for instant messaging. UC700 uses Access Server for Instant messaging, so the IM Access Server must be Access Server. If Access Server has not been installed, install and configure at least

one Access Server. Refer to the OW5000 Installation Guide and the OW5000 Configuration Guide for more details.

—**SIPUA Group**: (optional) If the Access Control feature is required, select the proper SIPUA group from the drop-down list. A SIPUA Group must be assigned from **OW5000 > Platform > Access Control** before Person management. Refer to the OW5000 Configuration Guide for more details. SIPUA Group configuration of the UC700 is supported in the US only.

> **NOTE**
>
> *SIP URI/IM URI is a Uniform Resource Identifier (URI) used by UC700 user. This identifier is similar to an e-mail account, and acts similar to an e-mail account or phone number in locating the user for instant messaging traffic. This identifier must be entered in the format user@host, where user is the username of the UC700 user, and host is the host name of the user's computer where he or she receives instant messages. (Examples: Carl.Price@tropia.com, edgar@fiznet.com, servicedept@potomobile.biz). The host name can be a domain (DNS) name of the host server or its IP address.*

> **NOTE**
>
> *If you want to see SP350 and/or NEC SIP terminal presence, the SIP URI must be the same as the Extension SIP URI assigned in the Extension Management page.*

> **NOTE**
>
> *AccessServer is not case sensitive.*

> **NOTE**
>
> *The SIP and IM URI must be unique. It is recommended you use the following format:*
>
> • Use **user@sip.host.whatever** for SIP URI.
>
> • Use **user@im.host.whatever** for IM URI.

Step 4   To add a **Photo**, enter the file name or click **Browse**. An "Add Photo" dialog box displays. Enter the file name of the desired photo or choose a different path to find the location and then click **Open**. The file name is added in the **Photo** field.

> **NOTE**
>
> *When adding a picture for a person to be viewed in the UC700 client, please be sure to put pictures in a folder accessible by the local service account on the OW5000 server. Do NOT select a path in a specific user's My Documents or My Pictures folder, for example. Instead, create a separate folder under the C or D drive.*

Step 5   Do one of the following:

—Click **Apply** to save the new user without exiting the dialog box.

—Click **Done** to save and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the information.

Edit or Delete a Person Entry

• To edit a person entry, select the **Pencil** icon next to the person's name (Figure 4-4). A form displays showing the person data. You can change the values in the dialog box and click **Done** to save.

• To remove a person entry, select the **Trashcan** icon next to the person's name (Figure 4-4)**.**

Adding a Role for a Person

While using Person Management, you can add a security role for a person. To add a security role:

Step 1   Click the **Roles** tab to display a Roles dialog box (Figure 4-6).

Figure 4-6   *Roles dialog*

Step 2   Click **Add Role** to display an **Add User Role** dialog (Figure 4-7).

Figure 4-7   *Add User Role dialog*

Step 3   Select **User** for the Role type for this Person.

NOTE

Fields which must be completed are designated with an asterisk (*).

IMPORTANT

UC700 ACD User Role is supported in the US only.

Step 4   Specify values for **Login ID**, **New Password** and **Confirm New Password**.

NOTE

The length of the password must be at least 8 characters long and include the following rules:
1 Uppercase letter (A-Z)
1 Lowercase letter (a-z)
1 Digit(0-9)
1 Special Character (excluding a space, square brackets, backslash, and single or double quotes)

Step 5   For Windows Authentication, enter your **NTLM Login ID**. The NTLM Login ID format is **domain\User ID** or **UserID** if the account is on the local machine.

IMPORTANT

UC700 User's function Automatically Login on Startup requires configuration of the NTLM Login ID.

Step 6   Click to enable the **UC700** user privilege and then select **UC700 User Role**. UC700 ACD User Role is supported in US only.

Step 7   Click **Done** after a **User role added** confirmation message appears (Figure 4-8). The UC700 User is now defined.

Figure 4-8 *User Role Added*

NOTE

When a UC700 User privilege is assigned to a user and then saved, the Employee role is created automatically.

Edit or Delete Roles

If the selected person already has a role assigned, you can edit or delete the role by clicking the **Pencil** icon or the **Trashcan** icon.

IMPORTANT

Removing an Employee or Physician role removes UC700 privileges.
Removing UC700 privileges deletes all personal information. For example, contact rules, buddy lists, and personal directories.

Adding an Employee Role

After selecting the name, click the **Roles** tab from the Person Management dialog (Figure 4-7). Select **Employee** from the drop-down role type list box to display an Employee Role Type dialog (Figure 4-9).

Figure 4-9 *Employee Roles—Add New dialog*

Step 1   Enter the **Employee ID**.

Step 2   Select the **Employee Position** from the drop-down list.

Step 3   Select the **Employee Type** from the drop-down list. For example, a Contractor, Permanent, or Part Time employee.

Step 4   To set an **Organization** for this employee, click **Select** and then choose an organization. To remove an organization, click **Remove**.

Step 5   To set a **Location**, click **Select** and then choose a location. To remove a location, click **Remove**.

Step 6   Select the **Confidentiality Status** from the drop-down menu.

Step 7   Do one of the following:

—Click **Apply** to add the role and continue with the configuration.
—Click **Done** to save the information and close the dialog box.
—Click **Cancel** to exit without saving the changes.

Adding a Contact Method for a Person

While using Person Management, you can add a contact method for a person. To add a contact method:

Step 1   Click the **Contact Method** tab. Figure 4-10 displays.

Figure 4-10   *Contact Method dialog*

Step 2   If no Contact Methods are configured, click the **Add New Contact Method** button Figure 4-11 displays.

Figure 4-11   *Select Contact Method—Type dialog*

Step 3   Select the **Contact Method** type from the drop-down list.

Step 4   Select the **Priority** status from the drop-down list.

Step 5   Select the **PBX Name** from the drop-down list.

Step 6 Enter the **Extension** for this user role.

NOTE

Fields which must be completed are designated with an asterisk (*).

Primary Extension, Secondary Extension, and Tertiary Extension are available as a SIP Presence feature. Please refer to the OW5000 Configuration Guide to enable the SIP Presence feature.

NOTE

Person entries must have at least a primary extension. No other contact methods are required.

NOTE

The Contact Method dialog boxes may differ depending on the type of contact method you selected.

Adding an Address for a Person (Supported in US Market only)

While using Person Management, you can add addresses for a person. To add an address:

Step 1 Click the **Addresses** tab. Figure 4-12 displays.

Figure 4-12 *Address Information dialog*

Step 2 To add an address, click **Add New Address**. Figure 4-13 displays.

Figure 4-13 *Add Address Information dialog*

Step 3   Select the **Address Type** from the drop-down list.

NOTE

Fields which must be completed are designated with an asterisk (*).

Step 4   Select the Country/Region from the drop-down list.

Step 5   Enter information in the following fields:

—Street

—City

—State/Province

—Zipcode

Step 6   Do one of the following:

—Click **Apply** to add the address.

—Click **Done** to display the new entry.

—Click **Cancel** to exit without saving the information.

User Management Configuration

Selecting **Users** from the OW5000 Directory Menu (Figure 4-3) displays Figure 4-14. This option allows you to manage user information, and to add or change application and role privileges.

Figure 4-14 *User Management dialog*

Use the steps below to change passwords, application privileges, or to delete a user account.

Modifying a User Account

Use the following steps to modify an account.

Step 1 Select the **Pencil** icon next to the desired user from the list of displayed names (Figure 4-14), or enter data in the **Filter By** field and click **Search**.

Step 2 Enter the **Login ID**.

> **NOTE**
>
> *Fields which must be completed are designated with an asterisk (*).*

Step 3   Enter a new password in the **New Password** field.

NOTE

The length of the password must be at least eight characters long and include the following rules:

1 Uppercase letter (A-Z)
1 Lowercase letter (a-z)
1 Digit(0-9)
1 Special Character (excluding a space, square brackets, backslash, and single or double quotes)

Step 4   Enter the new password again in the **Confirm New Password** field.

Step 5   For Windows Authentication, enter the **NTLM Login ID** for the user. The NTLM Login ID format is **domain\User ID** or **UserID** if the account is on the local machine.

NOTE

This parameter is displayed only when the United States is selected as the Sales Region or if OW5000 Applications which are released in US market is installed.

Step 6   To disable the user role for any reason, click the check box **Login is disabled**.

Step 7   To set the password to never expire for the user, click the check box **Password never expires**.

Step 8   Select **UC700** as the application and then select the desired user role from the drop-down list.

Step 9   Click **Apply**.

Deleting a User Account

Step 1   Select the **Trashcan** icon next to the desired user from the list of displayed names (Figure 4-14), or enter data in the **Filter By** field and click **Search**. A delete confirmation dialog displays.

Step 2   Click **OK** to delete the user role for this person.

5

Configuring OW5000/UC700 to Support ACD Integration

UC for Enterprise (UCE) Agent is a separately licensed option that provides a unified communications desktop application for ACD agents. It enhances the capabilities of NEC's CallCenterWorX® ACD, which is part of the CCDesign® product suite. As an integral part of NEC's suite of applications, it combines all of the functionality of the UCE Desktop Client with the enhanced features designed specifically for agents.

The following topics are included in this chapter.

- *ACD Server Management*
- *ACD Configuration*

ACD Server Management

In order to provide ACD agent functionality for UC700 users, it is necessary to configure the ACD system(s) that will be connected to the server by the application. The OW Agent Service component establishes communication with any ACD that is configured.

The following topics are included in this section.

- *ACD Servers Configuration*
- *ACD Settings Configuration*
- *Agent Screen Pop Configuration*
- *ACD Break Modes Configuration*
- *ACD Split Modes Configuration*
- *ACD Work Modes Configuration*

Follow the steps below to configure ACD Server options.

Step 1   Log on to the OW5000 Administrator program. Once you are logged in to OW5000 Administrator, select **OW5000 > Applications > ACD**. Figure 5-1 displays.

ACD Servers Configuration

Figure 5-1 *ACD Server Management—ACD Servers dialog*

Follow the steps below to configure ACD Servers.

Step 1   Click **Add New ACD Server**. Figure 5-2 displays.

Figure 5-2 *ACD Servers—Add New dialog*

Step 2   Enter the **ACD Name**.

Step 3   Enter the ACD **IP Address** of the server. If this is for internal ACD, enter the IP address of the PBX.

Step 4   Enter the TCP Port used to connect to the ACD in the ACD **Port** Number box. This must be an integer between 1 and 65534 inclusive. The default value is 60030.

Step 5   Select the **PBX** from the drop-down list.

Step 6   Select **Apply** to save the changes or **Cancel** to exit the dialog box without saving the changes.

NOTE

The OWAgentService must be restarted after adding a new ACD.

ACD Settings Configuration

Selecting **ACD Settings** from the ACD Server Management dialog (Figure 5-1) displays an ACD Settings dialog (Figure 5-3).

Figure 5-3 *ACD Settings dialog*

Step 1   Enter the IP Address in the **OWAgentService IP Address** text box.

> **NOTE**
>
> *If the OWAgentService is on the same server, this field should be left blank.*

Step 2   Select **Apply** to save the changes or **Cancel** to exit the dialog box without saving the changes.

> **IMPORTANT**
>
> *To ensure proper ACD integration, the following options should be enabled (checked) in the **System Data** screen of the ACD MAT commands:*
>
> *- Infolink with Call ID*
> *- Infolink with Split Information*
> *- Expanded Infolink with Call ID*
>
> *Also choose the **Iq** rather than the **IQ** for the Incoming Call Msg field in the same screen. See Figure 5-4 .*

Figure 5-4 *ACD Settings*

Agent Screen Pop Configuration

The UC700 Agent Screen Pop feature is designed to integrate the UC700 with a customer's CRM application. In order for this to be accomplished, the CRM must be able to accept input from UC700 in the form of arguments (parameters). When an ACD call is presented to an agent, UC700 will launch a predefined application along with information about the call provided in these arguments. For example, the contact center may utilize a browser-based CRM application which would accept the callers CID information as a parameter and populate the agent's browser with specific information about the caller.

Selecting **Agent Screen Pop** from the ACD Server Management dialog window (Figure 5-1) displays an Agent Screen Pop dialog (Figure 5-5).

Figure 5-5 *Agent Screen Pop dialog*

The agent screen pops can be configured globally or on a per-split basis, to provide flexibility. The global configuration can either specify the screen pop settings to be used for all splits or for those splits which are not configured separately. The split configuration can be used if screen pops are only necessary for certain splits or if individual splits require different screen pop settings.

Global Screen Pop Configuration

Global screen pop configuration includes the application in the **Executable** field that will be opened when the call is presented to the agent. Additionally, arguments for that executable can be configured by selecting one of the drop-down options below:

- **Code**: Customer information associated with the call. This is commonly attached by an IVR.
- **Caller ID**: The telephone number of the caller.
- **Split**: The ACD split in which the calls are being answered.
- **Pilot**: The ACD pilot number where the call arrived into the system.
- **Login**: The answering agent's ACD login ID.

It is important to ensure that the arguments selected meet the requirements of your CRM application.

NOTE

Follow the steps below to configure a global screen pop.

Step 1   Select the Agent Screen Pop tab from the ACD Server Management main window. Global Screen Pop Configuration is at the top of the window. See Figure 5-6.

Figure 5-6 *Global Screen Pop Configuration*

Step 2   Configure the application in the **Executable** field that will be opened when the call is presented to the agent.

NOTE

It may be necessary to enter the full path in the Executable field. This depends on the path settings defined for the computer user.

Step 3   Enter the Executable's arguments in the **Arguments** field. The arguments can also be built using the drop-down menu field to the right of the **Arguments** field. See Figure 5-7.

Figure 5-7 *Arguments Drop-Down Menu*

Step 4   Once, a option is selected from the drop-down menu, click the **Insert** button to add the option to the executable's argument.

Step 5   Click **Apply** to save the Global Screen Pop Configuration, Figure 5-8 displays.

Figure 5-8   *Global Screen Pop Configuration Confirmation*

— Click **Cancel** to cancel the action.

Screen Pop Split Configuration

The split configuration is used if screen pops are only necessary for certain splits or if individual splits require different screen pop settings.

Follow the steps below to configure a split configuration.

Step 1   From the Agent Screen Pop tab, under **ACD Split Screen Pop Configuration**), select the ACD splits to be configured (Figure 5-9).

To narrow down the list of available ACD splits, use filtering. Filtering can be by **ACD Name**, **Split** or **Tenant Name**, and further defined with the following qualifiers from a drop-down menu.

- **Contains**
- **Ends With**
- **Equals**
- **Starts With**

Figure 5-9   *Screen Pop Split Configuration*

Step 2   Click on the **Pencil** icon next to the desired ACD split to be configured. Figure 5-10 displays.

Figure 5-10 *Agent Screen Pop dialog*

Step 3 Enter the Screen Pop information for this particular split.

—Configure the application in the **Executable** field that will be opened when the call is presented to the agent.

—Enter the Executable's arguments in the **Arguments** field. The arguments can also be built using the drop-down menu field to the right of the **Arguments** field.

Step 4 Once, a option is selected from the drop-down menu, click the **Insert** button to add the option to the executable's argument.

Step 5 Click **Apply** to apply the Screen Pop Split Configuration (Figure 5-10).

OR

Cancel to cancel the action.

ACD Configuration

Several ACD related components (Break Modes, Split Modes, and Work Modes) can be configured to provide more descriptive status information.

Follow the path below to configure the ACD.

Step 1 Log on to the OW5000 Administrator program. Once you are logged in to OW5000 Administrator, select **OW5000 > Directory**. Figure 5-11 displays.

ACD Break Modes Configuration

ACD supports nine break modes, numbered one through nine. A descriptive name can be assigned to each break mode so an agent doesn't need to know the meaning of each break mode number. The names are stored in the database allowing the UC700 client program to read them for display. The name assigned to each mode can be up to 32 characters in length.

Follow the steps below to configure ACD Break Modes.

Step 1 Select **ACD Break Modes** from the ACD Configuration—Main Menu (Figure 5-11). An ACD Break Modes dialog displays (Figure 5-12).

Figure 5-12 *ACD Break Modes dialog*

NOTE

UC700 does not use the **Set Default** option seen in Figure 5-12.

Step 2 To edit an ACD Break Mode, click the **Pencil** icon next to the desired Break Mode number. A Break Mode Description dialog displays (Figure 5-13).

Figure 5-13 *Break Mode Description dialog*

Step 3 Enter a description for the selected Break Mode in the text box.

Step 4 To delete an ACD Break Mode, click the **Trashcan** icon.

Step 5 Do one of the following:

—Click **Apply** to save the information without exiting the dialog box.
—Click **Done** to save the information and exit the dialog box.
—Click **Cancel** to exit the dialog box without saving the changes.

ACD Split Modes Configuration

The ACD Split Mode feature allows a descriptive name to be assigned and displayed within the UC700 client when an ACD split has been forwarded to a particular ACD pilot number. Split call forwarding is usually invoked by a call center supervisor using the night key.

Follow the steps below to configure ACD Split Modes.

Step 1 Select **ACD Split Modes** from the ACD Configuration—Main Menu (Figure 5-11). Figure 5-14 displays.

Figure 5-14 *ACD Split Modes dialog*

NOTE

Day and Night modes are automatically provided and cannot be removed.

Adding a Split Mode

Step 1   Select **Add New Split Mode** to open Figure 5-15.

Figure 5-15   *Add New Split Mode*

ACD Split Modes

ModeName :

Description :

* ACD Name: Select an ACD

ACD Pilot Number :

Apply   Done   Cancel

Step 2   Enter the **Mode Name** for this split.

Step 3   Enter a **Description** in the text box to describe the Mode Name.

Step 4   Select an **ACD Name** from the drop-down list.

Step 5   Enter the **ACD Pilot Number** for the split.

Step 6   Do one of the following:

—Click **Apply** to save the information without exiting the dialog box.

—Click **Done** to save the information and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the changes.

Editing ACD Split Modes

Step 1   Select the **Pencil** ✎ icon next to the desired Split Mode name to edit (Figure 5-14). An ACD Split Modes—Edit dialog displays (Figure 5-16).

Figure 5-16 *ACD Split Modes—Edit dialog*

> **Step 2**   Make the necessary changes to all or any of the desired fields and then do one of the following.

> *The pilot numbers listed under the **Pilot Number** column is provided to assist you when adding or changing a pilot number. One of these numbers should be used in the **ACD Pilot Number** field.*

> —Click **Apply** to save the information without exiting the dialog box.
> —Click **Done** to save the information and exit the dialog box.
> —Click **Cancel** to exit the dialog box without saving the changes.

Deleting ACD Split Modes

Step 1   Select the **Trashcan** icon next to the desired ACD Split Mode name (Figure 5-14) to delete. A confirmation dialog box displays.

Step 2   Click **OK** to delete the Split Mode or **Cancel** to close the dialog box without deleting the Split Mode.

ACD Work Modes Configuration

The ACD supports 99 work modes, numbers 1 through 99. A descriptive name can be assigned to each work mode so an agent doesn't need to know the meaning of each work mode number. These names are stored in the database to allow the UC700 client program to read them for display. The name assigned to each mode can be up to 32 characters in length.

Step 1   Select **ACD Work Modes** from the ACD Configuration—Main Menu (Figure 5-11). An ACD Work Modes Configuration dialog displays (Figure 5-17).

Figure 5-17 *ACD Work Modes Configuration dialog*

NOTE *UC700 does not use the **Set Default** option seen in Figure 5-17.*

Step 2 To edit an ACD Work Mode, click the **Pencil** icon next to the desired Work Mode number. A Work Mode Description dialog displays (Figure 5-18).

Figure 5-18 *Work Mode Description dialog*

Step 3 Enter a description for the selected Work Mode in the text box.

NOTE ***Is VIP Wake-up Processing work mode** and **Is E-OSN Call Processing work mode** options are not used by UC700.*

Step 4 To delete an ACD Work Mode, click the **Trashcan** icon (Figure 5-17).

Step 5 Do one of the following:

—Click **Apply** to save the information without exiting the dialog box.

—Click **Done** to save the information and exit the dialog box.

—Click **Cancel** to exit the dialog box without saving the changes.

6

Configuring OW5000 SSL Support for UC700 Clients

The following topics are included in this chapter.

Overview

By default, the UC700 connection to the OW5000 server is not secured, meaning the data that flows between the UC700 and OW5000 is not encrypted. If one were able to capture data packets in this flow (a difficult proposition in an Ethernet switched environment, but not impossible), one could discover a UC700 user's login and password and view other data, such as Instant Message text. This may be a security problem in private LANs, depending on your organization's security policy and other safeguards put in place.

If your organization requires a secure UC700-to-OW5000 connection, the OW5000 server supplies the capability to use the Transport Layer Security (TLS) protocol to secure the connection. (TLS is also known as Secure Sockets Layer, or SSL).

Secure Sockets Layer (SSL) provides confidentiality for UC700 data, including the login and password, by encrypting the connection. In addition, SSL uses certificates, so that the UC700 client connects only to the correct OW5000 server.

Configuring SSL for OW5000 and UC700

The OW5000 can be configured for SSL connections or unsecured connections, but not both. If OW5000 is configured for SSL connections, the UC700 clients must be configured to connect using SSL.

The procedures that must be followed to configure SSL on the OW5000 and UC700 are:

Step 1   *Obtaining an OW5000 Server Certificate on Windows Server 2003*
or
Obtaining an OW5000 Server Certificate on Windows Server 2008

Step 2   *Installing the OW5000 Server Certificate on Windows Server 2003*
or
Installing the OW5000 Server Certificate on Windows Server 2008

Step 3   *Installing CA Certificates on Client PCs*

Step 4   *Replacing web.config file with SSL.web.config file*

Step 5   *Configuring UC700 Clients to Use SSL*

Step 3 is not necessary if a server certificate is obtained from a well-known CA, such a VeriSign. Microsoft Windows comes pre-installed with well-known CA certificates (also known as "trusted root CA certificates").

One can view these in Windows by opening **Internet Options > Content > Certificates > Trusted Root Certificate Authorities** as shown in Figure 6-1 and Figure 6-2.

Each of the above steps is described in more detail in the remainder of this chapter.

Figure 6-1   *Internet Options—Content*

Figure 6-2 *Trusted Root Certificate Authorities*

Obtaining an OW5000 Server Certificate

This section includes procedures on *Obtaining an OW5000 Server Certificate on Windows Server 2003* and *Obtaining an OW5000 Server Certificate on Windows Server 2008*.

Obtaining an OW5000 Server Certificate on Windows Server 2003

If the OW5000 platform is installed on Windows Server 2003, use the following procedure to create a new certificate request which can be sent to a Certificate Authority (CA) for processing. If successful, the CA sends back a file containing a validated certificate.

Follow the steps below to generate a certificate request.

Step 1   Start Internet Information Services (IIS) Manager.

Step 2   Expand the Server and select **Default Web Site** as shown in the figure.

Figure 6-3 *Default Web Site*

Step 3   Right-click **Default Web Site** and click **Properties**. Figure 6-4 displays.

Figure 6-4 *Default Web Site Properties*

Step 4   Click the **Directory Security** tab.

Step 5   In the **Secure communications** section, click the **Server Certificate** button to launch the Web Server Certificate Wizard (Figure 6-5).

Figure 6-5 *Server Certificate Button*

Step 6   Click **Next**. Figure 6-6 displays.

Figure 6-6 *Server Certificate*

Step 7   Click the **Create a New Certificate** radio button, then click **Next**. Figure 6-7 displays.

Figure 6-7 *Delayed or Immediate Request*

Step 8   Click the **Prepare the request now, but send it later** radio button, then click **Next**. Figure 6-8 displays.

Figure 6-8 Name and Security Settings

Step 9   In the **Name** field, type a user-defined name for the certificate, such as "ow5000." The name is not used in the certificate. It is a name administrators can use for the certificate.

Step 10   Accept the default bit length for the key in the **Bit length** field by clicking **Next**. Figure 6-9 displays.

Figure 6-9 Organizational Information

Step 11   In the **Organization** field, type an organization's name.

Step 12 In the **Organizational unit** field, type an organizational unit, such as a department name. Click **Next** to display Figure 6-10.

NOTE *The CA verifies the Organization and Organization unit values. In addition, users see these names when deciding whether to accept the certificate. Make sure the data you enter in these fields are accurate.*

Figure 6-10 *Your Site's Common Name*

Step 13 In the **Common name** field, type a common name for the OW5000 and click **Next**. Figure 6-11 displays.

— If the OW5000 has a DNS name of "ow5000.abc-corp.com," and internal users can resolve the DNS name to an IP address, specify the DNS name in the **Common name** field. You may need to make sure the internal DNS servers have an entry for the OW5000 server.

— Alternatively, if your OW5000 has a NetBIOS name of "ABC-OW5000," and users can resolve the NetBIOS name to an IP address, you can specify the NetBIOS name in the **Common name** field.

NOTE *The Common Name becomes a part of the certificate. It is the name used when configuring the UC700 **Server** field for connection to the OW5000 server. The Common Name entered here and the UC700 **Server** field must match or the UC700 client will not be able to connect to the OW5000.*

Figure 6-11 Geographical Information

> **Step 14**   Enter the **Country/Region**, **State/province** and **City/locality**, then click
> **Next**. Figure 6-12 displays.

Figure 6-12 Certificate Request File Name

> **Step 15**   Enter a file name and location for the certificate request. Click **Next**.
> Figure 6-13 displays.

Figure 6-13 *Request File Summary*

Step 16 After reviewing the summary, click **Next**. Figure 6-14 displays.

Figure 6-14 *Completion message*

Step 17 Click **Finish**. The certificate request can now be sent to a CA for verification and processing.

—Your IT department can send the request to an internal CA to sign. Microsoft and OpenSSL are two examples of internal CAs. The advantage of using an internal CA is cost, because the signed certificate is free. The disadvantage is the internal CA's root certificate must be installed on each client PC.

—Alternatively, the IT department can use a well-known external CA to sign the certificate request. VeriSign and Entrust are examples of external CAs. The advantage of using a well-known CA is that the client PCs will already have the CA's certificate installed and one can

skip the procedure, *Installing CA Certificates on Client PCs*. The disadvantage is the cost to purchase a CA-signed certificate.

— If verification and processing is successful, the CA sends back a certificate, which is contained in a file. You can continue to the next procedure to install the certificate on the Web server.

Obtaining an OW5000 Server Certificate on Windows Server 2008

If the OW5000 platform is installed on Windows Server 2008, use the following procedure to create a new certificate request which can be sent to a Certificate Authority (CA) for processing. If successful, the CA sends back a file containing a validated certificate.

Follow the steps below to generate a certificate request.

Step 1   Start Internet Information Services (IIS) Manager.

Step 2   Navigate to the server node in the left pane, as shown in Figure 6-15, and double-click **Server Certificates** in the middle pane. Figure 6-16 displays.

Figure 6-15 *Server Certificates dialog*

Figure 6-16 *Create Certificate Request dialog*

>   **Step 3**   Select **Create Certificate Request...** in the right pane. Figure 6-17
>   displays.

Figure 6-17 *Certificate Name Properties dialog*

>   **Step 4**   Fill out the information to go into the certificate.

>   —In the **Common name** field, type a common name for the OW5000.

>   If the OW5000 has a DNS name of **ow5000.abc-corp.com**, and
>   internal users can resolve the DNS name to an IP address, specify the
>   DNS name in the Common name field. You may need to make sure

the internal DNS servers have an entry for the OW5000 server.

Alternatively, if your OW5000 has a NetBIOS name of **ABC-OW5000**, and users can resolve the NetBIOS name to an IP address, you can specify the NetBIOS name in the Common name field.

NOTE

*The Common Name becomes a part of the certificate. It is the name used when configuring the UC700 **Server** field for connection to the OW5000 server. The Common Name entered here and the UC700 **Server** field must match or the UC700 client will not be able to connect to the OW5000.*

—In the **Organization** field, type an organization's name.

—In the **Organizational unit** field, type an organizational unit, such as a department name.

NOTE

The CA verifies the Organization and Organization unit values. In addition, users see these names when deciding whether to accept the certificate. Make sure the data you enter in these fields are accurate.

—Enter the **City/locality**, **State/province**, **Country/Region** and then click **Next**. Figure 6-18 displays.

Figure 6-18 *Cryptographic Service Provider Properties dialog*

Step 5 Accept the default Cryptographic Service Provider properties and click **Next**. Figure 6-19 displays.

Figure 6-19 *File Name dialog*

Step 6   Enter a file name and location for the certificate request, and then click **Finish**.

The certificate request can now be sent to a CA for verification and processing.

—Your IT department can send the request to an internal CA to sign. Microsoft and OpenSSL are two examples of internal CAs. The advantage of using an internal CA is cost, because the signed certificate is free. The disadvantage is the internal CA's root certificate must be installed on each client PC.

—Alternatively, the IT department can use a well-known external CA to sign the certificate request. VeriSign and Entrust are examples of external CAs. The advantage of using a well-known CA is that the client PCs will already have the CA's certificate installed and one can skip the procedure *Installing CA Certificates on Client PCs*. The disadvantage is the cost to purchase a CA-signed certificate.

Installing the OW5000 Server Certificate

This section includes procedures on *Installing the OW5000 Server Certificate on Windows Server 2003* and *Installing the OW5000 Server Certificate on Windows Server 2008*.

After submitting the OW5000 certificate request to a CA, the CA should return a server certificate for the OW5000. The next procedure is to install the certificate on the OW5000 server.

Installing the OW5000 Server Certificate on Windows Server 2003

Follow the steps below to install the certificate on the OW5000 server.

Step 1   Start Internet Information Services (IIS) Manager.

Step 2   Expand the server and select **Default Web Site** as shown in Figure 6-20.

Figure 6-20 *Default Web Site*

Step 3   Right-click **Default Web Site** and click **Properties**. Figure 6-21 displays.

Figure 6-21 Default Web Site Properties

Step 4   Click the **Directory Security** tab. Figure 6-22 displays.

Figure 6-22 Server Certificate Button

Step 5   In the **Secure communications** section, click the **Server Certificate** button to launch the Web Server Certificate Wizard (Figure 6-23).

Step 6   Click **Next** to move past the welcome dialog. Figure 6-23 displays.

Figure 6-23 *Pending Certificate Request*

Step 7   Click **Process the pending request and install the certificate**, and then click **Next**. Figure 6-24 displays.

Figure 6-24 *Process a Pending Request*

Step 8   Type the path and file name of the file that contains the response sent from the CA and then click **Next**. Figure 6-25 displays.

Figure 6-25 *SSL Port*

Step 9   Accept the Default SSL port, 443, by clicking **Next**. Figure 6-26 displays.

Figure 6-26 *Certificate Summary*

Step 10   After reviewing the summary, click **Next**. Figure 6-27 displays.

Figure 6-27 *Completion message dialog*

Step 11   Click **Finish**.

The certificate is now installed on the web server. To test that the certificate is working, attempt to access OW5000 using a web browser. For example, you can attempt to connect to a URL such as https://ow5000.abc-corp.com/uc700. If the page displays, the certificate was installed successfully. If the server certificate was not signed by a well-known CA, a warning message displays indicating that a problem exists with the OW5000's certificate. Do not be concerned with the warning message because the next procedure used to install the CA certificate on the PCs makes the warning message go away.

Installing the OW5000 Server Certificate on Windows Server 2008

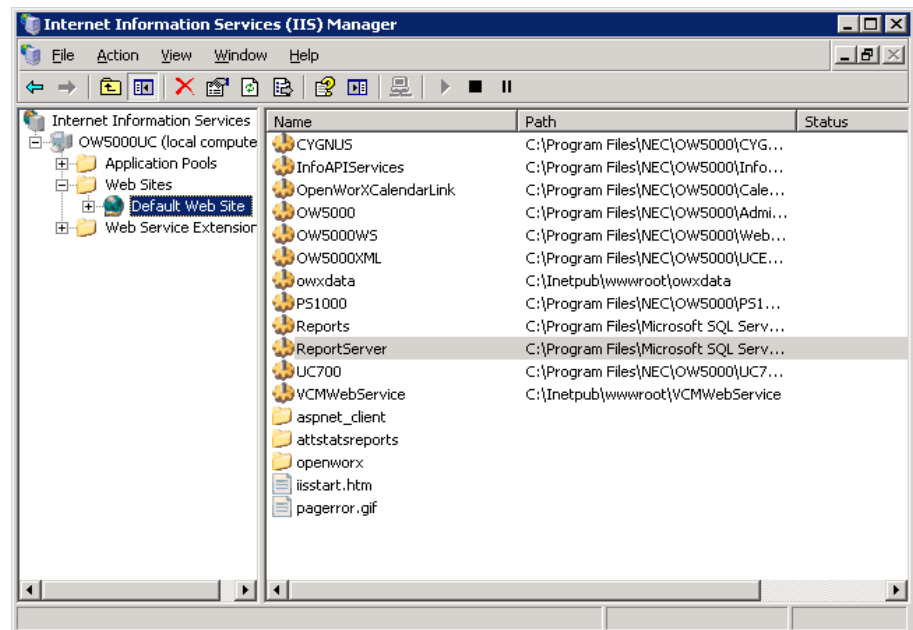After submitting the OW5000 certificate request to a CA, the CA should return to you a server certificate for the OW5000. The following procedure installs this server certificate on the OW5000 server.

Follow the steps below to install the certificate on the OW5000 server.

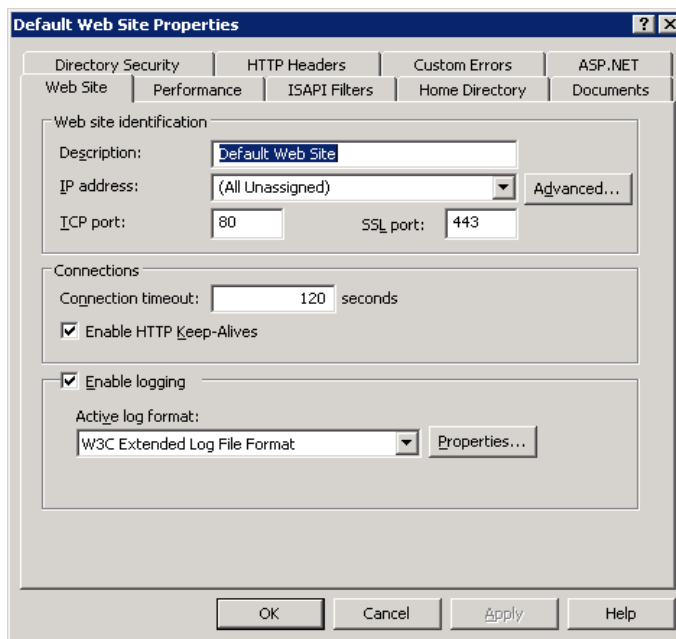*Step 1*   Start Internet Information Services (IIS) Manager.

Step 2   Navigate to the **Server Certificates** page as described in the previous section. Figure 6-28 displays.

Figure 6-28 *IIS Manager—Server Certificates*

> **Step 3**   Select **Complete Certificate Request** in the right pane. Figure 6-29 displays.

Figure 6-29 *Complete Certificate Request*

> **Step 4**   Enter the path and file name of the file that contains the response from the CA. Type any meaningful short description as the **Friendly name** for the certificate, then click **OK**. Figure 6-30 displays.

Figure 6-30 *IIS Manager—Server Certificates*

The middle pane now displays the certificate you installed.

Step 5   Navigate to the **Default Web Site** in the left pane, as shown in Figure 6-31.

Figure 6-31 *Default Web Site*

Step 6   Click on **Bindings...** in the right pane. Figure 6-32 displays.

Figure 6-32 *Default Web Site—Bindings*

> ***Step 7*** Click **Add** to display Figure 6-33.

Figure 6-33 *Add Bindings dialog*

> ***Step 8*** Select **https** from the **Type** field and accept the default **IP address** and **Port**. Select the SSL certificate from the drop-down list (choose the Friendly name you created), and then click **OK**. Figure 6-34 displays.

Figure 6-34 *Site Bindings Added dialog*

> ***Step 9*** You will see the additional site binding, **https** in the blinding list. Click **Close**.
>
> A certificate is now installed on the default web server and is available for use by the UC700 application.
>
> You may test that the certificate is working by opening a web browser session to the OW5000 via HTTPS. For example you may attempt to connect to a URL such as https://ow5000.abc-corp.com/uc700. If the page displays, the certificate has been installed successfully. If the server certificate you installed was not signed by a well-known CA then

you will get a warning that there is a problem with the OW5000's certificate. Do not be concerned with this warning because the next step will describe installing the CA certificate on PCs so that this warning will go away and so that UC700 clients can connect to the OW5000.

Installing CA Certificates on Client PCs

Each PC that runs a UC700 client must have the Trusted Root Certificate installed on it before UC700 can connect to the OW5000 using SSL. If the OW5000 server certificate installed is signed by one of the well-known trusted CAs, such as VeriSign, you may not need to perform this step because Windows pre-installs CA certificates from well-known and trusted CAs.

If the OW5000 server certificate installed earlier was signed by a CA internal to your organization, you must install the CA's certificate on each UC700 PC.

> **NOTE**
>
> *It is also useful to install the CA certificate on each PC used for OW5000 administration.*

There are a couple of ways to install the CA certificate on UC700 PCs. One is manually, as described below.

If you have a large population of UC700 PCs to install, manually going to each PC may be quite burdensome. A second method is to push the CA Certificate to all PCs in an Active Directory domain by adding it to a Group Policy object. This method is described by Microsoft at http://technet.microsoft.com/en-us/library/cc738131.aspx.

For the manual method, you or each client user must retrieve a CA certificate file from the CA. The following procedure installs this CA certificate on the UC700 PCs.

Step 1   Place the CA certificate file on the UC700 PC. To do this you can use one of these methods:

   —E-mail the CA certificate to each user with instructions for installing it.

   —E-mail each user with instructions for retrieving the CA certificate from a Windows Certificate Authority website.

   —An administrator inserts a thumb drive containing the CA certificate.

Step 2   Figure 6-35 displays a CA certificate file named certnew.cer on the desktop of a UC700 PC. Wherever the file is on the PC, double-click it.

Figure 6-35 *Certificate Icon*

— Double-clicking the file name or file icon displays a prompt asking whether you want to open the file.

Step 3 Click **Open** in response to the prompt. Certificate information displays (Figure 6-36). You can browse through the information about the certificate.

Figure 6-36 *Certificate Information Screen*

Step 4 Click **Install Certificate**. This action launches the Certificate Import Wizard (Figure 6-37).

Figure 6-37 *Certificate Import Wizard*

Step 5   Click **Next**. Figure 6-38 displays.

Figure 6-38 *Certificate Store*

Step 6   Click **Place all certificates in the following store**, and then click **Browse....** Figure 6-39 displays.

Figure 6-39 *Certification Store Selection*

Step 7   Select **Trusted Root Certificate Authorities**, click **OK** and then click **Next**.

Figure 6-40 *Certificate Import Wizard Completion Screen*

Step 8   Click **Finish**. A warning message displays (Figure 6-41).

Figure 6-41 Security Warning Message

Step 9   Click **Yes**. This action displays a message indicating that the import was successful.

Step 10   Click **OK**. This completes the procedure to install the certificate on the PC.

Replacing web.config file with SSL.web.config file

On the OW5000 server, in the C:\Program Files\NEC\OW5000\UC700\web directory on 32-bit Windows Server, or the C:\Program Files (x86)\NEC\OW5000\UC700\web directory on 64-bit Windows Server, the **Web.config** and **SSL.web.config** files can be found, as shown in the Figure 6-42 and Figure 6-43.

Figure 6-42 32-bit Windows Server UC700 Web Folder

Figure 6-43 *64-Windows Server UC700 Web Folder*

The SSL.web.config file is the same as Web.config except that a few additional lines are added that instruct the OW5000 to accept only SSL connections. To configure the OW5000 for UC700 SSL connections, you must swap the configuration files. Use these steps to swap the files:

Step 1   Rename **web.config** to **NoSSL.web.config**.

Step 2   Rename **SSL.web.config** to **web.config**.

Configuring UC700 Clients to Use SSL

To configure the UC700 Clients to log in using SSL:

Step 1   The **Server** box should contain the DNS or NetBIOS name of the OW5000 server. It must match the common name that was placed into the server certificate during the first procedure. It should not be an IP address or any other name, or the UC700 cannot successfully connect the OW5000.

Step 2   Check the **Use SSL** box as shown in Figure 6-44.

Step 3   Supply the remaining login credentials and click **Login.** The user has a secure SSL connection to the OW5000 when the login completes.

Figure 6-44 *UC700 Client Login*

7

Installing and Configuring Calendar Link

This chapter gives the procedures for installing and configuring Calendar Link to allow UC700 users to set up and use Calendar Link.

Chapter Topics
- *Calendar Link Overview*
- *Installing Calendar Link on the Exchange Server*
- *Configuring Calendar Link*

Calendar Link can be configured to integrate with multiple Microsoft Exchange® servers; however, one Microsoft Exchange server can be supported by only one OW5000 server.

Before installing Calendar Link to the Exchange server, make sure the following requirements are met:

- Microsoft Windows Server 2003 32-bit and Windows Server 2008 64-bit
- Microsoft Exchange Server 2003 and 2007
- IIS is installed
- .Net Framework 3.5
- Supports 32-bit and 64-bit OS and Exchange

Calendar Link Overview

Calendar Link integrates UC700 to the Microsoft Exchange Server's Calendar, and updates the OW5000 database with the Calendar Event's schedule and their status.

Microsoft Outlook supports the statuses; Busy, Out-of-Office, Tentative and Free. OW5000 user status changes are only for Calendar events that are set to busy or out-of-office. Calendar Link adds support for UC700 status directly in Outlook, which can be modified at any given time.

Calendar Link uses Scheduler on OW5000 to change the status when Calendar Event is active.

Installing Calendar Link on the Exchange Server

Follow the steps below to install Calendar Link.

Step 1 Place the OW5000 DVD into the **DVD-ROM drive**. On most computers Autorun automatically starts the installation when you load the DVD. If Autorun is not enabled on the computer, though, you must do the following:

—After placing the OW5000 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 Main menu, select a link to launch the installer for UC700 Calendar Link (32-bit) or UC700 Calendar Link (6- bit). Figure 7-1 displays.
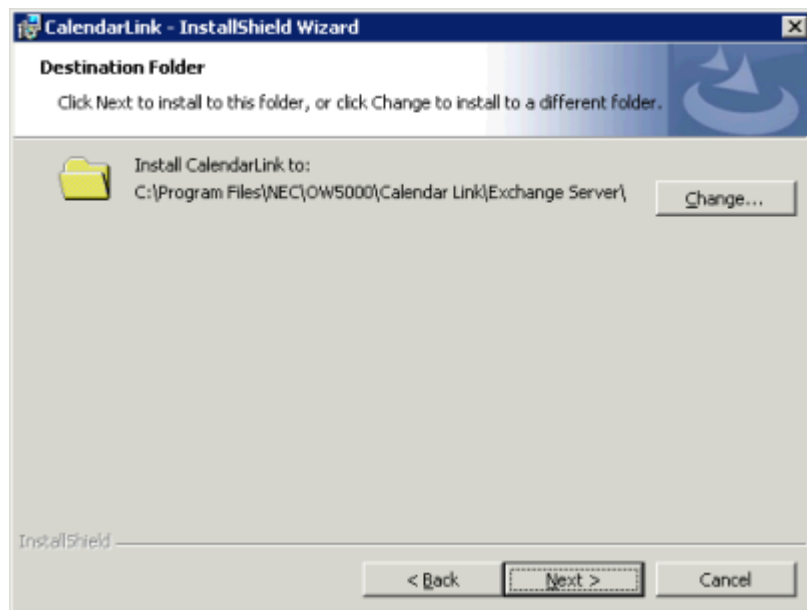
Figure 7-1 *Calendar Link Preparing to Install dialog*

—Once the initial preparation is complete, Figure 7-2 displays.

Figure 7-2 *Calendar Link Welcome dialog*

Step 3   Click **Next**. Figure 7-3 displays.

Figure 7-3 *Calendar Link Destination Folder dialog*

> **Step 4**   Click **Next**. Figure 7-4 displays.

Figure 7-4 *Calendar Link Configuration Information dialog*

Step 5   Enter the following information:

— **Exchange User Name**: The user name for the Exchange server. A new user can be created for CalendarLink configuration.
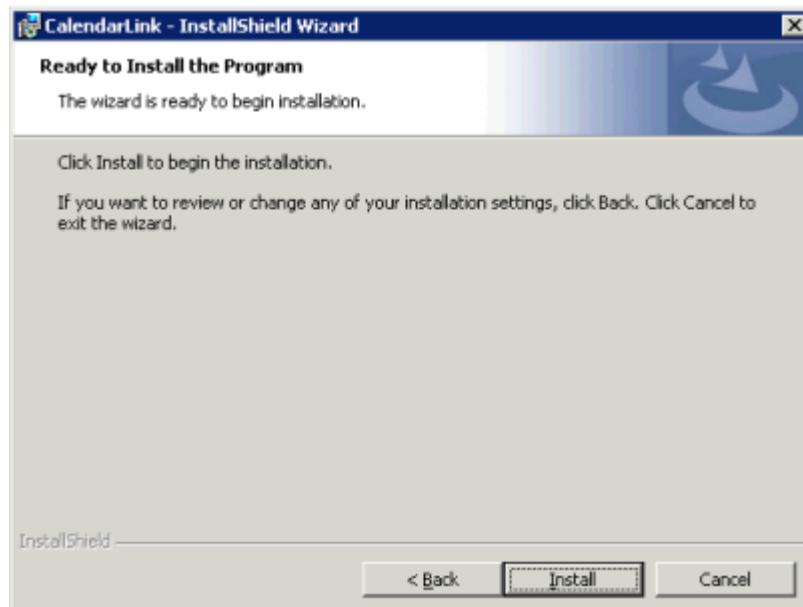
NOTE   *If the user belongs to a different domain, the user name should be fully qualified to include the domain information.*

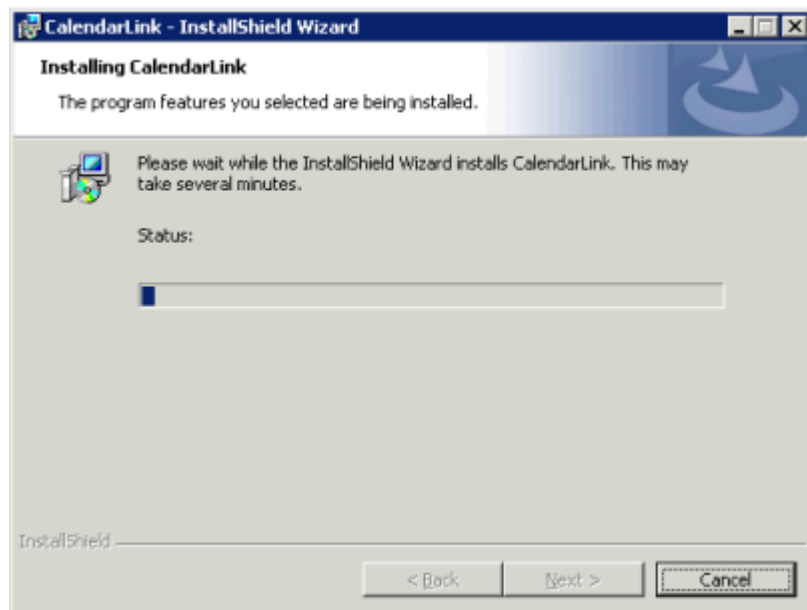— **Exchange Password**: The password for the Exchange User Name.

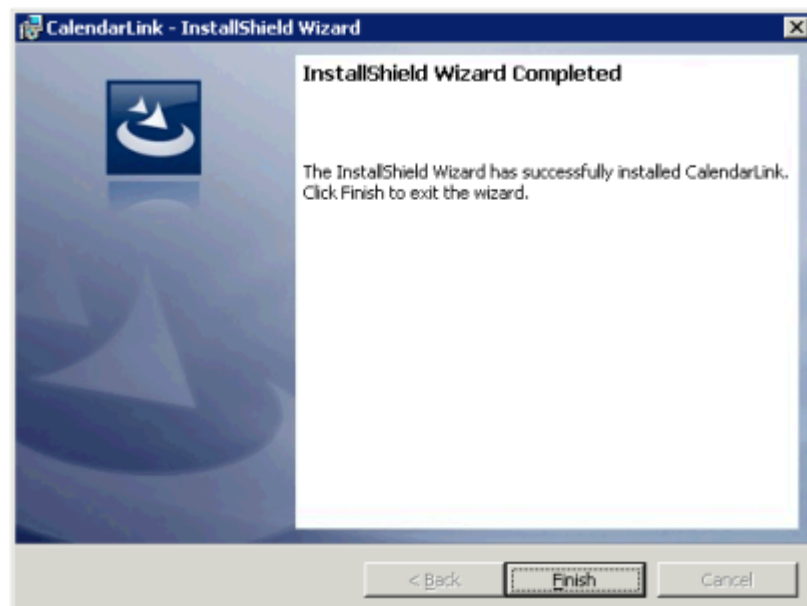— **OW5000 Server Name**: The name assigned to the server that OW5000 resides on.

Step 6   Click **Next**. Figure 7-5 displays.

Figure 7-5 Calendar Link Ready to Install dialog

Step 7   Click **Install**. Figure 7-6 displays briefly, then Figure 7-7 displays.

Figure 7-6 *Installation Status dialog*

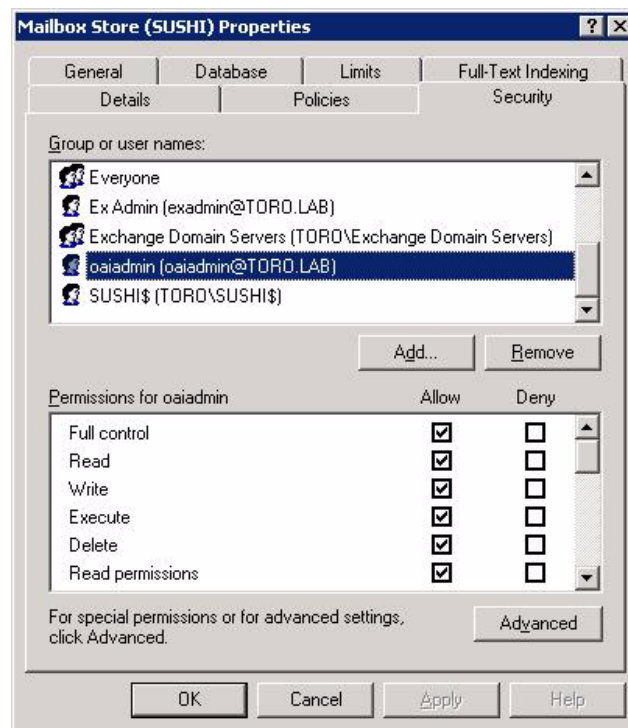***Figure 7-7*** *Installation Complete dialog*

Step 8   Click **Finish** to complete the installation of Calendar Link on the Exchange Server.

—After you have completed the installation process, set the permissions for the admin Exchange Server admin in the Mailbox store properties.

Configuration for Microsoft Exchange Server 2003

Step 1   From the Microsoft Exchange System Manager, select the server on which you installed the Calendar Link application and then right-click **Mailbox Store** and select **Properties**.

Step 2   Click on the **Security** tab and select the Exchange Server Admin User, which was entered in Step 5 above (Figure 7-4). Select the Full-Control permissions, as shown in Figure 7-8.

Figure 7-8 *Mailbox Store Properties dialog*
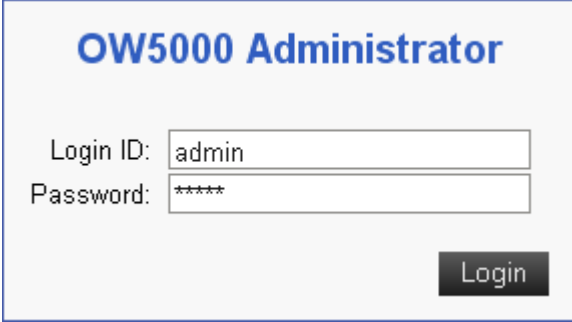

Configuration for Microsoft Exchange Server 2007

Step 1   On the Exchange 2007 Management Shell Console, execute the following command:

Get-MailboxDatabase -server <ExchangeServerName> | add-adpermission -user "<ExchangeAdminUser>" -accessRights GenericAll -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin, ms-Exch-Store-Visible -inheritanceType all

Step 2   Go to the IIS manager (under the default web site), then click on the application **ExchangeEventRegistration** and turn **OFF** the SSL settings.

Configuring Calendar Link

Follow the steps below to configure Calendar Link to support UC700 Clients.

Step 1   Launch OW5000 Administrator by selecting **Start** > **All Programs** > **NEC OW5000** > **Platform** > **OW5000 Administrator**. Figure 7-9 displays.

Figure 7-9 *OW5000 Administrator Login dialog*

Step 2   Enter the default login identification and password values. You will be required to change the password after login.

> **NOTE**
>
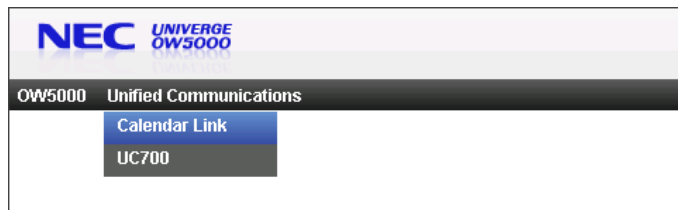> *The default Login ID is **admin** and the default Password is **admin**. It is necessary to change your password when prompted.*

Step 3   Click **Login**. Figure 7-10 displays.

Figure 7-10 *OW5000 Main Menu*

Step 4   Select **Calendar Link** from the **Unified Communications** menu. Figure 7-11 displays.

Figure 7-11 *Calendar Link Email Server Manager dialog*

Configuring EMail Server for Calendar Link

Step 1   Click **Add New Email Server Link**. Figure 7-12 displays.

Figure 7-12 *Calendar Link Email Server Manager dialog*

Step 2   To add an Exchange Email Server, use either of the options below:

—Enter the requested information in the required fields marked with an asterisk.

Exchange Server - IP address or server name of the Exchange Server

Exchange Admin - User Id with Administrative privileges

Exchange Admin Password - Password of the above mentioned user

Exchange Admin Email - Email address of the above mentioned user. This is optional.

Domain Controller - Domain Controller server used by the exchange server.

Active Directory User - User on Domain Controller who has privilege to query the Active Directory.

Active Directory User Password - Password of the above mentioned user.

> **NOTE**
>
> *If the **Exchange Admin** and **Active Directory User** belong to a different domain, the user name should be fully qualified to include the domain information.*

Error Messages

While trying to add a new email server, you may receive the following errors.

Error	Action
Server_Name_Duplicate	Change the name of the Exchange Server or edit the existing server with the same name.

Configuring the User Registration Status

Step 1   Click the **Registration Status** tab. Figure 7-13 displays.

Figure 7-13 *Calendar Link Registration Status dialog*

Step 2   Click the **Pencil** icon to edit the user registration for Calendar Link. Figure 7-14 displays.

Figure 7-14 *Add New User Registration dialog*

Calendar Link

| General Settings | Email Servers | Registration Status |

User: Administrator
*Primary Email: [   ]
*Email Server: [-Select- ▼]

[Apply] [Done] [Cancel]

> **Step 3**   Enter the **Primary Email** (SMTP) address.

> **Step 4**   Use the drop-down list to select the **Email Server** for the user.

NOTE   *The list of servers is populated by the servers listed on the Email Servers tab.*

NOTE   *Required fields are marked with an asterisk.*

> **Step 5**   Click **Done**. The **Status** column for the user displays Registered.

> **Step 6**   To edit or delete an **Email Server** or a Registered **User**, click the **Pencil** icon or the **Trashcan** icon.

Error Messages

While trying to register a user for Calendar Link, you may receive one of the following errors.

Error	Action
Person_ID_NOT_found_in_UserRole	Create a user role for person by selecting **OW5000** > **Directory** > **People**. Select person and go to the **Roles** tab and create user role.
Person_NOT_found_in_LDAP	Check the email address and the email server selected.
LDAP_Failure	Unable to connect to LDAP. Check connectivity to Domain Controller server of the email server in case of Exchange Server.
Exchange_Event_Sync_Registration_Failed	Exchange Registration Failed. Check if NEC Calendar link service is started on the exchange server.
Exchange_Server_NOT_reachable	Check if the Exchange Server is accessible. Check if NEC Calendar link service is started

Configuring Calendar Link when OW5000 Changes

This configuration change should be done in the following cases:

Case 1: When the server name of OW5000 changes.

Case 2: When an additional OW5000 server wants to connect to Calendar Link.

Case 3: When more than one OW5000 server is registered for Calendar Link and one OW5000 wants to remove registration.

Perform the following steps on Exchange Server for Exchange Calendar Link.

Step 1   Navigate to the folder **C:\Program Files\ComPlus Applications\{A0D3F58F-AB56-405F-B1E5-9851C1A73B06}**

Step 2   Open and edit the file **ExchangeEventSink.dll.config**

Step 3   Search for the setting/string **OpenWorxServer**, as shown below:

```
</setting>
<setting name="OpenWorXServer" serializeAs="String">
  <value>appslablucy;ufsow101</value>
</setting>
</NEC.OpenWorX.CalendarLink.ExchangeEventSink.Properties.Settings>
```

—**Case 1:** When the server name of OW5000 changes.
Do the following: Replace the existing server name with a new server name in the value tag.

—**Case 2:** When additional OW5000 registers for Calendarlink.
Do the following: Add a semicolon (;) followed by the new server name in the value tag.

—**Case 3:** When more than one OW5000 server is registered for Calendarlink and one OW5000 wants to remove registration.
Do the following: Remove that server name from the value tag.

Step 4   Restart the windows service: **NEC Calendar Link**.

Configuring Calendar Link when OW5000 is Upgraded

Exchange Calendar Link interacts with OW5000 using the Calendar Link Web Service. Calendar Link Web Service preserves backward compatibility; so Calendar link should work without any change when OW5000 is upgraded.

When upgrading Calendar Link on the Exchange Server, there is no need to re-register users on OW5000 for Calendar Link.

Configuring Calendar Link when OW5000 is Uninstalled

—**Case 1:** Exchange Server interacts with more than one OW5000 and one of the OW5000 is getting un-installed.

Follow the instructions, .

—**Case 2:** Exchange interacts with only one OW5000 and that OW5000 is getting uninstalled.

In this case uninstall Calendar Link from the Exchange Server using the following steps:

Step 1   Go to **Start** > **Control Panel** > **Program and Features**.

Step 2   Find **NEC UC700 Calendarlink** for Exchange Server.

Step 3   Right click and select **Uninstall**.

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

NEC NEC Corporation

UC for Enterprise (UCE) Desktop Client/Agent (UNIVERGE UC700) Installation Guide
NDA-30884, Revision 4.01